

ЧЕБЫШЕВСКИЙ СБОРНИК

Научно-теоретический журнал

Издается с 2001 года

Выходит 4 раза в год

Свидетельство о регистрации

СМИ: ПИ № ФС77-47855

ISSN 2226-8383

Том XXI

Выпуск 1 (73)

Тула

2020

Учредитель: ФГБОУ ВО
«ТГПУ им. Л. Н. Толстого»

Каталог «Пресса России»
Подписной индекс 10642

Адрес редакции: 300026,
г. Тула, пр. Ленина, 125

Тел: +79156812638,
8(4872)374051

E-mail: cheb@tspu.ru

URL:
<http://www.chebsbornik.ru>

В журнале публикуются оригинальные статьи по направлениям современной математики: теория чисел, алгебра и математическая логика, теория функций вещественного и комплексного переменного, функциональный анализ, дифференциальные уравнения, математическая физика, геометрия и топология, теория вероятностей и математическая статистика, численные методы, теория оптимизации и др. Также публикуются статьи о памятных датах и юбилеях.

Журнал включен в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученых степеней кандидата наук и доктора наук (перечень ВАК), индексируются и/или реферируются: Scopus, MathSciNet, Zentralblatt MATH, Russian Science Citation Index (RSCI), РЖ «Математика», «Mathematical Reviews», РИНЦ, Google Scholar Metrics.

Журнал выходит под эгидой Министерства науки и высшего образования Российской Федерации, Российской академии наук, Московского государственного университета им. М. В. Ломоносова, Математического института им. В. А. Стеклова РАН, Московского педагогического государственного университета, Тульского государственного университета.

Главный редактор

В. Н. Чубариков (Россия, г. Москва)

Ответственные секретари:

Н. Н. Добровольский (Россия, г. Тула)

И. Ю. Реброва (Россия, г. Тула)

Заместители главного редактора: Н. М. Добровольский (Россия, г. Тула), А. В. Михалёв (Россия, г. Москва), А. И. Нижников (Россия, г. Москва)

Редакционная коллегия:

В. А. Артамонов (Россия, г. Москва)
В. А. Быковский (Россия, г. Хабаровск)
С. В. Востоков (Россия, г. Санкт-Петербург)
А. Е. Гвоздев (Россия, г. Тула)
Д. В. Георгиевский (Россия, г. Москва)
С. А. Гриценко (Россия, г. Москва)
С. С. Демидов (Россия, г. Москва)
В. Г. Дурнев (Россия, г. Ярославль)
А. М. Зубков (Россия, г. Москва)
В. И. Иванов (Россия, г. Тула)
В. К. Карташов (Россия, г. Волгоград)
М. А. Королёв (Россия, г. Москва)
В. Н. Кузнецов (Россия, г. Саратов)
В. Н. Латышев (Россия, г. Москва)
Ю. В. Матиясевич (Россия, г. Санкт-Петербург)
С. П. Мищенко (Россия, г. Ульяновск)
Ю. В. Нестеренко (Россия, г. Москва)

В. А. Панин (Россия, г. Тула)
У. М. Пачев (Россия, г. Нальчик)
А. Л. Семёнов (Россия, г. Москва)
А. А. Фомин (Россия, г. Москва)
В. Г. Чирский (Россия, г. Москва)
И. Аллаков (Узбекистан, г. Термез)
А. Я. Белов (Израиль, г. Рамат Ган)
В. И. Берник (Беларусь, г. Минск)
П. О. Касьянов (Украина, г. Киев)
А. Лауринчикас (Литва, г. Вильнюс)
Лю Юнпин (Китай, г. Пекин)
М. Дж. Марданов (Азербайджан, г. Баку)
О. Р. Мусин (США, г. Браунсвилл)
З. Х. Рахмонов (Таджикистан, г. Душанбе)
Х. М. Салиба (Ливан)
А. Х. Табари (Таджикистан, г. Куляб)
Л. Фукшанский (США, г. Клермонт)
Д. Шяучюнас (Литва, г. Шяуляй)

От редакции

Данный выпуск Чебышевского сборника посвящен
80-летию выдающегося советского, российского
и белорусского математика, академика Российской
академии наук, академика Национальной академии
наук Белоруссии, доктора физико-математических
наук, профессора
Владимира Петровича Платонова



В. П. Платонов

Владимир Петрович Платонов

Владимир Петрович Платонов родился 1 декабря 1939 года в деревне Стайки Оршанского района Витебской области.

В 1961 году окончил Белорусский государственный университет. В 1963–1971 гг. — там же: доцент, профессор, заведующий кафедрой алгебры и топологии.

В 1971–1993 гг. — заведующий отделом алгебраической геометрии и топологии Института математики АН БССР, в 1977–1992 гг. — директор Института математики АН БССР. В 1987–1992 гг. — президент Академии наук Беларуси, в 1993–1996 гг. — главный научный сотрудник отдела алгебры и теории чисел Института математики АН Беларуси. С 1992–2004 гг. работал в университетах и научных центрах США, Канады и Германии: в университете Ватерлоо, в Мичиганском университете, в Институте математики общества Макса Планка, в Билефельдском университете и в Дюссельдорфском университете имени Генриха Гейне. С 2003 года возвращается в Белоруссию, затем в Россию — в РАН. В настоящее время является главным научным сотрудником Научно-исследовательского института системных исследований РАН и Математического института им. В. А. Стеклова РАН.

С 1968 года — член-корреспондент Академии Наук Беларуси, в 1971 года — академик Академии Наук Беларуси, с 1987 года академик АН СССР — член Отделения математики.

Специалист в области алгебры, алгебраической геометрии, алгебраической теории чисел; прикладной алгебры и криптографии.

Академик В. П. Платонов — выдающийся советский, белорусский и российский математик, всемирно известный специалист в области алгебры, алгебраической геометрии, алгебраической теории чисел; прикладной алгебры и криптографии.

Создал общий метод исследования линейных групп, базирующийся на алгебро-геометрических и теоретико-числовых идеях. Решил проблему сильной аппроксимации в алгебраических группах и проблему Кнезера — Титса. Разработал приведенную К-теорию и решил на этой основе проблему Таннака — Артина. Решил проблему рациональности спинорных многообразий и проблему Дьедонне о спинорных нормах. Исследовал локально-глобальный принцип, согласно которому строение групп, заданных над арифметическими полями, определяется строением их локализаций над соответствующими пополнениями. Доказал основную аппроксимационную теорему для линейных групп с конечным числом образующих. Построил теорию важнейших классов локально компактных топологических групп. Открыл новый локально-глобальный принцип для функциональных гиперэллиптических полей, определенных над полем алгебраических чисел, который позволил связать проблему вычисления фундаментальных единиц в гиперэллиптических полях с проблемой кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел и развить унифицированный метод для решения этих классических проблем.

Совместно с учениками решил проблему рациональности для групповых алгебраических многообразий над локальными и глобальными полями; построил теорию конечномерных гензелевых тел; решил проблему Гротендика о проконечных пополнениях групп и проблему жесткости для арифметических подгрупп алгебраических групп с радикалом; развил мультипликативную теорию конечномерных тел; решил проблему арифметичности для полициклических групп; развил новый подход к конгруэнц-проблеме, основанный на анализе комбинаторных свойств арифметических групп; развил теорию для нахождения фундаментальных единиц в гиперэллиптических полях и на ее основе построил и реализовал принципиально новые высокоэффективные алгоритмы их вычисления.

Эти глубокие результаты принесли В. П. Платонову широкую международную известность и признание, свидетельством которых явилось приглашение В. П. Платонова в качестве докладчика на международные конгрессы математиков в Ванкувере (1974 г.), Хельсинки (1978 г.) и на Европейский математический конгресс в Будапеште (1996 г.). Математическое

творчество В. П. Платонова многогранно и характеризуется глубиной, оригинальностью и самобытностью.

Автор более 190 научных работ.

Главный редактор журнала Доклады АН БССР (1987–1992). Член редколлегии журналов «Успехи математических наук» и «Доклады РАН».

Член Бюро Отделения математических наук РАН, член Национального комитета российских математиков. Член Президиума АН СССР (1989–1991).

В 1989–1991 гг. — депутат Верховного Совета СССР. В 1985–1990 гг. депутат Верховного Совета БССР. Председатель Комитета по Государственным премиям БССР (1988–1991).

Академик НАНБ с 1972 года. Иностранный член Индийской Национальной Академии Наук. Член Хенаньской академии наук.

Заслуженный деятель науки Республики Беларусь.

Награжден орденом Трудового Красного Знамени.

Лауреат Премии Ленинского комсомола — за работы по топологическим и линейным алгебраическим группам, лауреат Ленинской премии — за работы по арифметике алгебраических групп и приведенной К-теории.

Удостоен Премии Гумбольдта (Германия).

СОДЕРЖАНИЕ

Том 21 Выпуск 1

От редакции	3
Т. Аяно, В. М. Бухштабер. Аналитические и теоретико-числовые свойства двумерных сигма-функций	9
А. Я. Белов-Канель, А. М. Елишев, Ф. Разавиния, Ю. Джи-Тай, Венчао Жэнг. Некоммутативная теорема Бялыницкого — Бирули	51
В. В. Беньш-Кривец, А. Н. Адмиралова. О многообразиях представлений некоторых свободных произведений циклических групп с одним соотношением	62
Е. М. Вечтомов, Д. В. Чупраков. Конечные циклические полукольца с полурешеточным сло- жением, заданным двухпорожденным идеалом натуральных чисел	82
С. Б. Гашков, И. С. Сергеев. Умножение	101
В. А. Горелов. Об алгебраических тождествах между фундаментальными матрицами обобщённых гипергеометрических уравнений	135
Е. И. Деза, Б. Мханна. О специальных свойствах некоторых квазиметрик	145
Н. Н. Добровольский, И. Ю. Реброва, Н. М. Добровольский. Обратная задача для моноида с экспоненциальной последовательностью простых	165
В. Г. Дурнев, О. В. Зеткина, А. И. Зеткина. Об элементарных теориях алгебраически замкнутых групп	186
П. Л. Иванков. О линейных приближающих формах	200
Н. И. Калоша, И. А. Корлюкова, Е. В. Гусева. Интервалы малой длины, содержащие алгебраическое число заданной высоты	213
М. А. Королев. Суммы Клоостермана по простым числам и разрешимость одного сравнения с обратными вычетами — II	221
Н. В. Максименко. Пространство рядов Дирихле для многомерных решёток и алгебра рядов Дирихле решёток, повторяющихся умножением	233
И. А. Мартьянов. Константа Никольского для тригонометрических полиномов с периодическим весом Гегенбауэра	247
Ю. В. Матиясевич. Асимптотическая структура собственных чисел и собственных векторов некоторых треугольных ганкелевых матриц	259
В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников. Периодические элементы $\sqrt{f}$ в эллиптических полях с полем констант нулевой характеристики	273
В. И. Субботин. О полноте списка выпуклых RR -многогранников	297

Л. А. Толоконников, Т. Ш. Нгуен. Определение поля смещений в неоднородном покрытии упругой пластины при прохождении через нее плоской звуковой волны	310
Г. В. Федоров. О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков	322
В. Н. Чубариков. Об одной теореме о среднем значении кратных тригонометрических сумм	341
Ю. Н. Штейников. О размере множества произведения множеств рациональных чисел ..	357
КРАТКИЕ СООБЩЕНИЯ	
А. В. Бегунц, Д. В. Горяшин. О значениях последовательности Битти в арифметической прогрессии	364
С. В. Востоков, Р. П. Востокова, Е. В. Иконникова. Канонический базис Гензеля — Шафаревича для формальных модулей Хонды	368
Р. В. Почеревин. Обобщение определения среднего	374
И. А. Проскурнин. Минимальные морсификации функций двух вещественных переменных	381
ИСТОРИЯ МАТЕМАТИКИ И ПРИЛОЖЕНИЙ	
Ю. А. Басалов. О русской научной школе диофантовых приближений	388
ПАМЯТНЫЕ ДАТЫ	
В. Н. Чубариков, В. Г. Чирский, Е. И. Деза, Ю. Н. Баулина, Л. В. Котова, Е. В. Неискашова, В. С. Ванькова, Н. М. Добровольский, И. Ю. Реброва, А. Л. Рощеня. Василий Ильич Нечаев. К 100-летию юбилею	404
РЕДКОЛЛЕГИЯ	415
THE EDITORIAL BOARD	419
TABLE OF CONTENTS	423

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 515.178.2+517.58, 512.554.32+517.98 DOI 10.22405/2226-8383-2020-21-1-9-50

Аналитические и теоретико-числовые свойства
двумерных сигма-функций

Т. Аяно, В. М. Бухштабер

Аяно Таканори — Университет города Осака, Математический институт высших исследований (г. Осака, Япония).

e-mail: ayano@sci.osaka-cu.ac.jp

Бухштабер Виктор Матвеевич — член-корреспондент РАН, доктор физико-математических наук, профессор, Математический институт им. В. А. Стеклова Российской академии наук (г. Москва).

e-mail: buchstab@mi-ras.ru

Аннотация

Обзор посвящен классическим и современным задачам, связанным с целой функцией $\sigma(\mathbf{u}; \lambda)$, которая определяется семейством неособых алгебраических кривых рода 2, где $\mathbf{u} = (u_1, u_3)$, $\lambda = (\lambda_4, \lambda_6, \lambda_8, \lambda_{10})$. Эта функция является аналогом сигма-функции Вейерштрасса $\sigma(u; g_2, g_3)$ семейства эллиптических кривых. Логарифмические производные порядка 2 и выше функции $\sigma(\mathbf{u}; \lambda)$ порождают поле гиперэллиптических функций от $\mathbf{u} = (u_1, u_3)$ на якобианах кривых с фиксированным значением вектора параметров λ . Мы рассматриваем три ряда Гурвица $\sigma(\mathbf{u}; \lambda) = \sum_{m,n \geq 0} a_{m,n}(\lambda) \frac{u_1^m u_3^n}{m!n!}$, $\sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \xi_k(u_1; \lambda) \frac{u_3^k}{k!}$ и $\sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \mu_k(u_3; \lambda) \frac{u_1^k}{k!}$. Обзор посвящен теоретико-числовым свойствам функций $a_{m,n}(\lambda)$, $\xi_k(u_1; \lambda)$ и $\mu_k(u_3; \lambda)$. Он включает самые последние результаты, доказательства которых использует тот фундаментальный факт, что функция $\sigma(\mathbf{u}; \lambda)$ определяется системой четырех уравнений теплопроводности в неголономном репере шестимерного пространства.

Ключевые слова: абелевы функции, двумерные сигма-функции, целочисленность Гурвица, обобщенные числа Бернулли — Гурвица, уравнение теплопроводности в неголономном репере.

Библиография: 45 названий.

Для цитирования:

Т. Аяно, В. М. Бухштабер. Аналитические и теоретико-числовые свойства двумерных сигма-функций // Чебышевский сборник, 2020, т. 21, вып. 1, с. 9–50.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 515.178.2+517.58, 512.554.32+517.98 DOI 10.22405/2226-8383-2020-21-1-9-50

**Analytical and number-theoretical properties
of the two-dimensional sigma function**

T. Ayano, V. M. Buchstaber

Ayano Takanori — Osaka City University, Advanced Mathematical Institute (Osaka, Japan).*e-mail: ayano@sci.osaka-cu.ac.jp***Buchstaber Victor Matveevich** — correspondent member of RAS, doctor of physico-mathematical Sciences, Professor, Steklov Mathematical Institute of Russian Academy of Sciences (Moscow).*e-mail: buchstab@mi-ras.ru***Abstract**

This survey is devoted to the classical and modern problems related to the entire function $\sigma(\mathbf{u}; \lambda)$, defined by a family of nonsingular algebraic curves of genus 2, where $\mathbf{u} = (u_1, u_3)$ and $\lambda = (\lambda_4, \lambda_6, \lambda_8, \lambda_{10})$. It is an analogue of the Weierstrass sigma function $\sigma(u; g_2, g_3)$ of a family of elliptic curves. Logarithmic derivatives of order 2 and higher of the function $\sigma(\mathbf{u}; \lambda)$ generate fields of hyperelliptic functions of $\mathbf{u} = (u_1, u_3)$ on the Jacobians of curves with a fixed parameter vector λ . We consider three Hurwitz series $\sigma(\mathbf{u}; \lambda) = \sum_{m,n \geq 0} a_{m,n}(\lambda) \frac{u_1^m u_3^n}{m!n!}$, $\sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \xi_k(u_1; \lambda) \frac{u_3^k}{k!}$ and $\sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \mu_k(u_3; \lambda) \frac{u_1^k}{k!}$. The survey is devoted to the number-theoretic properties of the functions $a_{m,n}(\lambda)$, $\xi_k(u_1; \lambda)$ and $\mu_k(u_3; \lambda)$. It includes the latest results, which proofs use the fundamental fact that the function $\sigma(\mathbf{u}; \lambda)$ is determined by the system of four heat equations in a nonholonomic frame of six-dimensional space.

Keywords: Abelian functions, two-dimensional sigma functions, Hurwitz integrality, generalized Bernoulli–Hurwitz number, heat equation in a nonholonomic frame.

Bibliography: 45 titles.

For citation:

T. Ayano, V. M. Buchstaber, 2020, "Analytical and number-theoretical properties of the two-dimensional sigma function", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 9–50.

*Dedicated to the outstanding mathematician
Academician Vladimir Petrovich Platonov
in connection with his anniversary.*

1. Introduction

Deep results on the number-theoretic properties of fields of hyperelliptic functions were obtained in the papers of V. P. Platonov, where he gave answers to long-standing questions. The fields of meromorphic functions on the Jacobian of curves of genus 2 occupy one of the main places in these papers (see [40], [41] and [42]). Abelian functions, including meromorphic functions on the Jacobians of algebraic curves, were a central topic of the 19th century mathematics. In this review, we mainly discuss the results obtained due to a new direction in the study of fields of

Abelian functions. This direction arose in the mid-seventies of the last century in response to the discovery that Abelian functions provide a solution to a number of challenging problems of modern theoretical and mathematical physics. The elliptic sigma function, which was defined and investigated by Weierstrass, is important in many fields in mathematics and physics. This function is closely related to the theory of the elliptic curves. In [28] and [29], F. Klein posed the problem of the construction of multi-dimensional sigma functions associated with the hyperelliptic curves. He obtained important results in this direction. Many years later, F. Klein wrote a paper and a survey in which he acknowledged that the theory of his sigma functions is still far from complete (see [30] and [31]). The theory of the hyperelliptic sigma functions was developed by H. F. Baker in [5], [6], [7], and [8]. Recently, by a series of work of V. M. Buchstaber, V. Z. Enolskii, and D. V. Leykin, the theory of the hyperelliptic sigma functions was developed significantly and they were generalized to the large family of algebraic curves called (n, s) curves, which include the hyperelliptic curves as special cases (see [12], [13], [14], [15], [17]). After the publications of Buchstaber, Enolskii, and Leykin, many papers appeared on the theory and applications of multi-dimensional sigma functions. Our survey is devoted to the sigma functions of curves of genus 2. The focus of our attention is the number-theoretic aspects of the results on these functions. Throughout the present survey, we denote the sets of positive integers, integers, rational and complex numbers by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$, respectively.

Let V be a hyperelliptic curve of genus g defined by

$$y^2 = x^{2g+1} + \lambda_4 x^{2g-1} + \lambda_6 x^{2g-2} + \cdots + \lambda_{4g} x + \lambda_{4g+2}, \quad \lambda_i \in \mathbb{C}. \quad (1)$$

The sigma function $\sigma(\mathbf{u}; \lambda)$, where $\mathbf{u} = (u_1, u_3, \dots, u_{2g-1})$ and $\lambda = (\lambda_4, \dots, \lambda_{4g+2})$, associated with V , is an entire function in $\mathbf{u} \in \mathbb{C}^g$. It is shown that the coefficients of the power series expansion of $\sigma(\mathbf{u})$ around $\mathbf{u} = \mathbf{0}$ are polynomials of the coefficients $\lambda_4, \dots, \lambda_{4g+2}$ over the rationals ([14], [15], [17], [33]). Let R be an integral domain with characteristic 0, $u_1, u_3, \dots, u_{2g-1}$ be indeterminates, and

$$R\langle\langle u_1, u_3, \dots, u_{2g-1} \rangle\rangle = \left\{ \sum_{i_1, i_3, \dots, i_{2g-1} \geq 0} a_{i_1, i_3, \dots, i_{2g-1}} \frac{u_1^{i_1} u_3^{i_3} \cdots u_{2g-1}^{i_{2g-1}}}{i_1! i_3! \cdots i_{2g-1}!} \mid a_{i_1, i_3, \dots, i_{2g-1}} \in R \right\}.$$

If a power series belongs to $R\langle\langle u_1, u_3, \dots, u_{2g-1} \rangle\rangle$, then it is said to be *Hurwitz integral* over R . In [39], Y. Ônishi proved that the power series expansion of $\sigma(\mathbf{u})$ around $\mathbf{u} = \mathbf{0}$ is Hurwitz integral over the ring $\mathbb{Z}[\lambda_4, \dots, \lambda_{4g+2}]$ by using the expression of the sigma function in terms of the tau function of KP-hierarchy given in [34]. In [37], in the case of $g = 1$, the Hurwitz integrality of the sigma function is proved in a different way from [39] and relationships with number theory are discussed. In [21], in the case of $g = 1$, it is conjectured that the power series expansion of the sigma function is Hurwitz integral over $\mathbb{Z}[2\lambda_4, 24\lambda_6]$. The focus of our survey is on the above fundamental fact, i.e., the power series expansion of the sigma function around the origin is Hurwitz integral over $\mathbb{Z}[\lambda_4, \dots, \lambda_{4g+2}]$. In this survey, we will discuss in detail expansions of the sigma functions of curves of genus 1 and 2, including the Ônishi's proof for Hurwitz integrality (see Sections 2.2 and 2.3).

Weierstrass [45] showed that the elliptic sigma function $\sigma(u; \lambda_4, \lambda_6)$ satisfies the following system of equations

$$\begin{aligned} 4\lambda_4\sigma_{\lambda_4} + 6\lambda_6\sigma_{\lambda_6} - u\sigma_u + \sigma &= 0, \\ 6\lambda_6\sigma_{\lambda_4} - \frac{4}{3}\lambda_4^2\sigma_{\lambda_6} - \frac{1}{2}\sigma_{uu} + \frac{1}{6}\lambda_4 u^2\sigma &= 0. \end{aligned}$$

The second equation of this system is the heat equation or, equivalently, the Schrödinger equation of type $\ell_2\sigma = \frac{1}{2}H_2\sigma$, where $\ell_2 = 6\lambda_6\partial/\partial\lambda_4 - (4/3)\lambda_4^2\partial/\partial\lambda_6$ and $H_2 = \frac{\partial^2}{\partial u^2} - \frac{1}{3}\lambda_4 u^2$. Weierstrass gave

recurrence relations of the coefficients of series expansion of the elliptic sigma function. Buchstaber and Leykin succeeded in generalizing the theory of the heat equations to the sigma functions of higher genus curves ([18], [19], and [20]). In [24], the detailed proof of their theory is given. In [19] and [24], the recurrence relations of the coefficients of series expansion of the two-dimensional sigma function are given based on the heat equations. In [25], the theory of the heat equations is constructed for the elliptic curves defined by the most general Weierstrass equation. In [23], for $g = 1, 2$, it is shown that the holomorphic solution of the heat equations around $(\mathbf{u}_0, \mathbf{0}) \in \mathbb{C}^{3g}$ for some $\mathbf{u}_0 \in \mathbb{C}^g$ is the sigma function up to a multiplicative constant. We consider the case of $g = 2$. For $\lambda = (\lambda_4, \lambda_6, \lambda_8, \lambda_{10})$, we set

$$\sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \xi_k(u_1; \lambda) \frac{u_3^k}{k!}, \quad \sigma(\mathbf{u}; \lambda) = \sum_{k \geq 0} \mu_k(u_3; \lambda) \frac{u_1^k}{k!}.$$

In Section 3, we will derive the differential equations satisfied by ξ_k and μ_k from the heat equations. From these results, we will prove that two-dimensional sigma function is Hurwitz integral over $\mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}]$ (Corollary 2).

For $(x, y) \in V$, let

$$du_1 = -\frac{x}{2y} dx, \quad du_3 = -\frac{1}{2y} dx,$$

which are a basis of the vector space of holomorphic one forms on V . We have two ultra-elliptic integrals $\int_{\infty}^P du_1$ and $\int_{\infty}^P du_3$ obtained with the help of two holomorphic differentials du_1 and du_3 . We take a point $P_* \in V$ and an open neighborhood U_* of this point P_* such that U_* is homeomorphic to an open disk in $\mathbb{C}$. Let us fix a path γ_* on the curve V from ∞ to the point P_* . We consider the holomorphic mappings defined by the ultra-elliptic integrals

$$I_3 : U_* \rightarrow \mathbb{C}, \quad P = (x, y) \mapsto \int_{\infty}^P du_3,$$

$$I_1 : U_* \rightarrow \mathbb{C}, \quad P = (x, y) \mapsto \int_{\infty}^P du_1,$$

where as the path of integration we choose the composition of the fixed path γ_* from ∞ to the point P_* and some path in the neighborhood U_* from P_* to the point P . When we consider the map I_3 , we assume $P_* \neq \infty$. When we consider the map I_1 , we assume $P_* \neq (0, \pm\sqrt{\lambda_{10}})$. If U_* is sufficiently small, then the maps I_1 and I_3 are biholomorphisms. In [4], the inversion problems of the maps I_1 and I_3 are considered. In Section 4, we will summarize the results of [4]. Proposition 18 in the present survey gives the recurrence formula of the coefficients of series expansion of the solution of the inversion problem with respect to I_1 in the case of $P_* = \infty$. This result is not included in [4].

The classical Bernoulli numbers B_n are defined by the generating function

$$\frac{u}{e^u - 1} = \sum_{n=0}^{\infty} B_n \frac{u^n}{n!}. \quad (2)$$

Bernoulli numbers B_n are important in many areas of mathematics, including number theory and algebraic topology. Many beautiful properties for the Bernoulli numbers B_n are known. For example, the von Staudt-Clausen theorem states

$$B_{2n} + \sum_{(p-1)|2n} \frac{1}{p} \in \mathbb{Z},$$

where the summation is over all primes p such that $p - 1$ divides $2n$. Let $a \geq 1$ be an integer, p be a prime, and m, n be even positive integers such that $m, n \geq a + 1$, m and n are not divisible by $p - 1$, and $n \equiv m \pmod{(p - 1)p^{a-1}}$. Then the Kummer's congruence states

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p^a}.$$

Let us introduce the universal logarithmic series

$$\alpha(u) = u + \sum_{n \geq 1} \alpha_n \frac{u^{n+1}}{n+1} \quad (3)$$

over the grading ring $A = \mathbb{Z}[\alpha_1, \alpha_2, \dots]$, $\deg \alpha_n = -2n$, and the universal exponential series

$$\beta(t) = t + \sum_{n \geq 1} \beta_n \frac{t^{n+1}}{(n+1)!} \quad (4)$$

over the grading ring $B = \mathbb{Z}[\beta_1, \beta_2, \dots]$, $\deg \beta_n = -2n$. Set $\deg u = \deg t = 2$. Then $\alpha(u)$ and $\beta(t)$ are homogeneous series of degree 2. Imposing condition $\alpha(\beta(t)) = t$ that equivalent to condition $\beta(\alpha(u)) = u$, we obtain an isomorphism of rings preserving grading

$$\xi: \hat{A} = \mathbb{Z}[\hat{\alpha}_1, \hat{\alpha}_2, \dots] \longrightarrow \hat{B} = \mathbb{Z}[\hat{\beta}_1, \hat{\beta}_2, \dots],$$

where $\hat{\alpha}_n = \frac{\alpha_n}{n+1}$ and $\hat{\beta}_n = \frac{\beta_n}{(n+1)!}$. Thus, we obtain the polynomials

$$\hat{\beta}_n = \hat{\beta}_n(\hat{\alpha}_1, \dots, \hat{\alpha}_n) \in \hat{A}, \quad n = 1, 2, \dots,$$

which coefficients are integers satisfying the relations

$$\beta(\alpha(u) + \alpha(v)) \in \mathcal{A}[[u, v]],$$

where $\mathcal{A} = \mathbb{Z}[a_1, a_2, \dots] \subset \hat{A}$, and

$$\alpha_n \in \mathcal{A}, \quad \beta_n = (n+1)! \hat{\beta}_n \left(\frac{\alpha_1}{2}, \dots, \frac{\alpha_n}{n+1} \right) \in \mathcal{A}.$$

These relations play an important role in describing the coefficient ring of the universal formal group (see [32], [16]) and in the algebraic-topological applications of the formal group in the theory of complex cobordisms (see [36], [43]).

The polynomials $B_n = B_n(\hat{\alpha}_1, \dots, \hat{\alpha}_n) \in \hat{A}$ which generating series is given by the Hurwitz exponential series over the ring $\hat{A}$

$$\sum_{n \geq 0} B_n \frac{t^n}{n!} = \frac{t}{\beta(t)} \quad (5)$$

are called *universal Bernoulli numbers*.

The classic Bernoulli numbers are obtained by substituting $\alpha_n = (-1)^n$. For example,

$$B_1 = \hat{\alpha}_1, \quad B_2 = 2(\hat{\alpha}_2 - \hat{\alpha}_1^2), \quad B_3 = 3!(\hat{\alpha}_3 - 3\hat{\alpha}_1\hat{\alpha}_2 + 2\hat{\alpha}_1^3).$$

Substituting $\hat{\alpha}_1 = -\frac{1}{2}$, $\hat{\alpha}_2 = \frac{1}{3}$, $\hat{\alpha}_3 = -\frac{1}{4}$, we obtain numbers $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$.

Classical Bernoulli numbers entered into algebraic geometry and algebraic topology due to the fact that the generating series (2) defines the Hirzebruch genus, which associates to any smooth complex manifold an integer equal to the Todd genus of this manifold (see [26]). The generating series (5) of universal Bernoulli numbers defines the universal Todd genus, which associates to any

smooth complex manifold an integer polynomial (see details in [9]). In [22], F. Clarke generalized the von Staudt-Clausen theorem for the classical Bernoulli numbers to the universal Bernoulli numbers. The Kummer's congruence for the classical Bernoulli numbers was generalized to the universal Bernoulli numbers ([1], [2], [3], [38]).

For a hyperelliptic curve of genus g defined by equation (1), in a neighborhood of point (∞, ∞) , we can choose a local coordinate u such that the functions $x(u)$ and $y(u)$ can be expanded around $u = 0$ as

$$x(u) = \frac{1}{u^2} + \frac{c_{-1}}{u} + \sum_{n=2}^{\infty} \frac{C_n}{n} \frac{u^{n-2}}{(n-2)!},$$

$$y(u) = \frac{1}{u^{2g+1}} + \frac{d_{-2g}}{u^{2g}} + \cdots + \frac{d_{-1}}{u} + \sum_{n=2g+1}^{\infty} \frac{D_n}{n} \frac{u^{n-2g-1}}{(n-2g-1)!}.$$

Then C_n and D_n are called *generalized Bernoulli-Hurwitz numbers*. In [38], the von Staudt-Clausen theorem and the Kummer's congruence for the classical Bernoulli numbers are extended to the generalized Bernoulli-Hurwitz numbers in the case of the curves $y^2 = x^{2g+1} - 1$ and $y^2 = x^{2g+1} - x$. We will extend the methods of [38] to the curve $y^2 = x^5 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}$ and show some number-theoretical properties for the generalized Bernoulli-Hurwitz numbers associated with this curve (Theorem 11). These results will give the precise information on the series expansion of the solution of the inversion problem of the ultra-elliptic integrals.

2. Preliminaries

2.1. The sigma function

For a positive integer g , we set

$$\Delta = \{(\lambda_4, \lambda_6, \dots, \lambda_{4g+2}) \in \mathbb{C}^{2g} \mid f_g(x) \text{ has a multiple root}\},$$

where

$$f_g(x) = x^{2g+1} + \lambda_4 x^{2g-1} + \lambda_6 x^{2g-2} + \cdots + \lambda_{4g} x + \lambda_{4g+2},$$

and $\mathcal{B} = \mathbb{C}^{2g} \setminus \Delta$. We consider the non-singular hyperelliptic curve of genus g

$$V = \{(x, y) \in \mathbb{C}^2 \mid y^2 = f_g(x)\}, \quad (6)$$

where $(\lambda_4, \lambda_6, \dots, \lambda_{4g+2}) \in \mathcal{B}$. In this paragraph we recall the definition of the sigma-function for the curve V (see [15]) and give facts about it which will be used later on. For $(x, y) \in V$, let

$$du_{2i-1} = -\frac{x^{g-i}}{2y} dx, \quad 1 \leq i \leq g,$$

which are a basis of the vector space of holomorphic one forms on V , and $d\mathbf{u} = {}^t(du_1, du_3, \dots, du_{2g-1})$. Further, let

$$dr_{2i-1} = \frac{1}{2y} \sum_{k=g-i+1}^{g+i-1} (-1)^{g+i-k} (k+i-g) \lambda_{2g+2i-2k-2} x^k dx, \quad 1 \leq i \leq g, \quad (7)$$

which are meromorphic one forms on V with a pole only at ∞ . In (7) we set $\lambda_0 = 1$ and $\lambda_2 = 0$. For $g = 1$, we have

$$du_1 = -\frac{1}{2y} dx, \quad dr_1 = -\frac{x}{2y} dx,$$

for $g = 2$, we have

$$du_1 = -\frac{x}{2y}dx, \quad du_3 = -\frac{1}{2y}dx, \quad dr_1 = -\frac{x^2}{2y}dx, \quad dr_3 = \frac{-\lambda_4 x - 3x^3}{2y}dx.$$

Let $\{\alpha_i, \beta_i\}_{i=1}^g$ be a canonical basis in the one-dimensional homology group of the curve V . We define the matrices of periods by

$$2\omega_1 = \left(\int_{\alpha_j} du_i \right), \quad 2\omega_2 = \left(\int_{\beta_j} du_i \right), \quad -2\eta_1 = \left(\int_{\alpha_j} dr_i \right), \quad -2\eta_2 = \left(\int_{\beta_j} dr_i \right).$$

The matrix of normalized periods has the form $\tau = \omega_1^{-1}\omega_2$. Let $\delta = \tau\delta' + \delta''$, $\delta', \delta'' \in \mathbb{R}^g$, be the vectors of Riemann's constants with respect to the choice $(\{\alpha_i, \beta_i\}, \infty)$ and $\delta := {}^t(t\delta', t\delta'')$. Then we have $\delta' = {}^t(\frac{1}{2}, \dots, \frac{1}{2})$ and $\delta'' = {}^t(\frac{g}{2}, \frac{g-1}{2}, \dots, \frac{1}{2})$. If g is even, we define $A_0 = (2g-1, 2g-5, \dots, 7, 3)$ and c_0 by the sign of the permutation

$$c_0 = \text{sgn} \begin{pmatrix} 0 & 2 & \cdots & g-4 & g-2 & g-1 & g-3 & \cdots & 3 & 1 \\ g-1 & g-2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & 0 \end{pmatrix}.$$

If g is odd, we define $A_0 = (2g-1, 2g-5, \dots, 5, 1)$ and c_0 by the sign of the permutation

$$c_0 = \text{sgn} \begin{pmatrix} 0 & 2 & \cdots & g-3 & g-1 & g-2 & g-4 & \cdots & 3 & 1 \\ g-1 & g-2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & 0 \end{pmatrix}.$$

We consider the Riemann's theta-function with the characteristic δ , which is defined by

$$\theta[\delta](\mathbf{u}, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\{\pi\sqrt{-1} {}^t(n + \delta')\tau(n + \delta') + 2\pi\sqrt{-1} {}^t(n + \delta')(\mathbf{u} + \delta'')\},$$

where $\mathbf{u} = {}^t(u_1, u_3, \dots, u_{2g-1}) \in \mathbb{C}^g$. We set $\partial_{u_i} = \partial/\partial u_i$. For a non-empty subset $I = \{i_1, \dots, i_k\} \subset \{1, 3, \dots, 2g-1\}$, we set

$$\partial_I = \partial_{u_{i_1}} \cdots \partial_{u_{i_k}}.$$

It is known that $\partial_{A_0}\theta[\delta](\mathbf{0}, \tau) \neq 0$ ([35]). The sigma-function $\sigma(\mathbf{u})$ is defined by (cf. [15], [35])

$$\sigma(\mathbf{u}) = \exp\left(\frac{1}{2} {}^t\mathbf{u}\eta_1\omega_1^{-1}\mathbf{u}\right) \frac{\theta[\delta]((2\omega_1)^{-1}\mathbf{u}, \tau)}{c_0\partial_{A_0}\theta[\delta](\mathbf{0}, \tau)},$$

which is an entire function on $\mathbb{C}^g$. We set $\wp_{i,j} = -\partial_{u_i}\partial_{u_j} \log \sigma$, $\sigma_i = \partial_{u_i}\sigma$, and $\sigma_{i,j} = \partial_{u_i}\partial_{u_j}\sigma$. We define the period lattice $\Lambda = \{2\omega_1 m_1 + 2\omega_2 m_2 \mid m_1, m_2 \in \mathbb{Z}^g\}$ and set $W = \{\mathbf{u} \in \mathbb{C}^g \mid \sigma(\mathbf{u}) = 0\}$.

PROPOSITION 1. ([15] Theorem 1.1 and [33] p.193) *For $m_1, m_2 \in \mathbb{Z}^g$, let $\Omega = 2\omega_1 m_1 + 2\omega_2 m_2$, and let*

$$A = (-1)^{2({}^t\delta' m_1 - {}^t\delta'' m_2) + {}^t m_1 m_2} \exp({}^t(2\eta_1 m_1 + 2\eta_2 m_2)(\mathbf{u} + \omega_1 m_1 + \omega_2 m_2)).$$

Then

- (i) $\sigma(\mathbf{u} + \Omega) = A\sigma(\mathbf{u})$, where $\mathbf{u} \in \mathbb{C}^g$.
- (ii) $\sigma_i(\mathbf{u} + \Omega) = A\sigma_i(\mathbf{u})$, $i = 1, 3, \dots, 2g-1$, where $\mathbf{u} \in W$.

Proposition 1 (i) implies that $\mathbf{u} + \Omega \in W$ for any $\mathbf{u} \in W$ and $\Omega \in \Lambda$. The surface

$$(\sigma) := \{\mathbf{u} \in \mathbb{C}^g / \Lambda \mid \sigma(\mathbf{u}) = 0\}$$

is called the *sigma divisor*. We set $\deg u_{2k-1} = -(2k-1)$ and $\deg \lambda_{2i} = 2i$, where $1 \leq k \leq g$ and $2 \leq i \leq 2g+1$. A sequence of non-negative integers $\mu = (\mu_1, \mu_2, \dots, \mu_l)$ such that $\mu_1 \geq \mu_2 \geq \dots \geq \mu_l$ is called a *partition*. Let $S_{\mu_g}(\mathbf{u})$ be the Schur function associated with the partition $\mu_g = (g, g-1, \dots, 1)$ and set $|\mu_g| = g + (g-1) + \dots + 1$ (cf. [33] Section 4).

THEOREM 1. ([14] Theorem 6.3, [15] Theorem 7.7, [17], [33] Theorem 3, [35] Theorem 13) *The sigma function $\sigma(\mathbf{u})$ does not depend on the choice of $\{\alpha_i, \beta_i\}_{i=1}^g$ and has the series expansion of the form*

$$\sigma(\mathbf{u}) = S_{\mu_g}(\mathbf{u}) + \sum_{i_1+3i_3+\dots+(2g-1)i_{2g-1} > |\mu_g|} \alpha_{i_1, i_3, \dots, i_{2g-1}}^{(g)} u_1^{i_1} u_3^{i_3} \cdots u_{2g-1}^{i_{2g-1}}, \quad (8)$$

where the coefficient $\alpha_{i_1, i_3, \dots, i_{2g-1}}^{(g)}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \dots, \lambda_{4g+2}]$ of degree $i_1 + 3i_3 + \dots + (2g-1)i_{2g-1} - |\mu_g|$ if $\alpha_{i_1, i_3, \dots, i_{2g-1}}^{(g)} \neq 0$.

For $g = 1$, the sigma function $\sigma(u)$ is an entire odd function on $\mathbb{C}$ and it is given by the series

$$\sigma(u) = u + \sum_{i \geq 4} \alpha_i^{(1)} u^{i+1},$$

where the coefficient $\alpha_i^{(1)}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6]$ of degree i if $\alpha_i^{(1)} \neq 0$. For $g = 2$, the sigma function $\sigma(\mathbf{u}) = \sigma(u_1, u_3)$ is an entire odd function on $\mathbb{C}^2$ and it is given by the series

$$\sigma(u_1, u_3) = \frac{1}{3} u_1^3 - u_3 + \sum_{i+3j \geq 7} \alpha_{i,j}^{(2)} u_1^i u_3^j, \quad (9)$$

where the coefficient $\alpha_{i,j}^{(2)}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree $i + 3j - 3$ if $\alpha_{i,j}^{(2)} \neq 0$.

THEOREM 2. ([10, 12, 18, 19, 20, 24])

(i) For $g = 1$, the sigma function $\sigma(u; \lambda_4, \lambda_6)$ satisfies the following system of equations:

$$\begin{aligned} 4\lambda_4 \sigma_{\lambda_4} + 6\lambda_6 \sigma_{\lambda_6} - u \sigma_u + \sigma &= 0, \\ 6\lambda_6 \sigma_{\lambda_4} - \frac{4}{3} \lambda_4^2 \sigma_{\lambda_6} - \frac{1}{2} \sigma_{uu} + \frac{1}{6} \lambda_4 u^2 \sigma &= 0. \end{aligned}$$

(ii) For $g = 2$, the sigma function $\sigma(u_1, u_3; \lambda_4, \lambda_6, \lambda_8, \lambda_{10})$ satisfies the following system of equations:

$$Q_i \sigma = 0, \quad \text{where} \quad Q_i = \ell_i - H_i, \quad i = 0, 2, 4, 6,$$

$${}^t(\ell_0, \ell_2, \ell_4, \ell_6) = T {}^t(\partial_{\lambda_4}, \partial_{\lambda_6}, \partial_{\lambda_8}, \partial_{\lambda_{10}}),$$

$$T = \begin{pmatrix} 4\lambda_4 & 6\lambda_6 & 8\lambda_8 & 10\lambda_{10} \\ 6\lambda_6 & 8\lambda_8 - \frac{12}{5}\lambda_4^2 & 10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6 & -\frac{4}{5}\lambda_4\lambda_8 \\ 8\lambda_8 & 10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6 & 4\lambda_4\lambda_8 - \frac{12}{5}\lambda_6^2 & 6\lambda_4\lambda_{10} - \frac{6}{5}\lambda_6\lambda_8 \\ 10\lambda_{10} & -\frac{4}{5}\lambda_4\lambda_8 & 6\lambda_4\lambda_{10} - \frac{6}{5}\lambda_6\lambda_8 & 4\lambda_6\lambda_{10} - \frac{8}{5}\lambda_8^2 \end{pmatrix},$$

$$H_0 = u_1 \partial_{u_1} + 3u_3 \partial_{u_3} - 3,$$

$$H_2 = \frac{1}{2} \partial_{u_1}^2 - \frac{4}{5} \lambda_4 u_3 \partial_{u_1} + u_1 \partial_{u_3} - \frac{3}{10} \lambda_4 u_1^2 + \frac{1}{10} (15\lambda_8 - 4\lambda_4^2) u_3^2,$$

$$H_4 = \partial_{u_1} \partial_{u_3} - \frac{6}{5} \lambda_6 u_3 \partial_{u_1} + \lambda_4 u_3 \partial_{u_3} - \frac{1}{5} \lambda_6 u_1^2 + \lambda_8 u_1 u_3 + \frac{1}{10} (30\lambda_{10} - 6\lambda_4 \lambda_6) u_3^2 - \lambda_4,$$

$$H_6 = \frac{1}{2} \partial_{u_3}^2 - \frac{3}{5} \lambda_8 u_3 \partial_{u_1} - \frac{1}{10} \lambda_8 u_1^2 + 2\lambda_{10} u_1 u_3 - \frac{3}{10} \lambda_8 \lambda_4 u_3^2 - \frac{1}{2} \lambda_6.$$

2.2. Hurwitz integrality of the expansion of the elliptic sigma function

In [39], Hurwitz integrality of the expansion of the sigma functions is proved. In this subsection, we will explain the proof of [39] for $g = 1$.

In this subsection, we assume $g = 1$. For simplicity, we denote u_1 and du_1 by u and du , respectively. For an integral domain R with characteristic 0 and a variable u , let

$$R\langle\langle u \rangle\rangle = \left\{ \sum_{i=0}^{\infty} \alpha_i \frac{u^i}{i!} \mid \alpha_i \in R \right\}.$$

For $n < 0$ let $p_n(u) = 0$ and for $n \geq 0$ let

$$p_n(u) = \frac{u^n}{n!}.$$

For an arbitrary partition $\mu = (\mu_1, \mu_2, \dots, \mu_l)$, we define the Schur polynomial $s_\mu(u)$ by

$$s_\mu(u) = \det (p_{\mu_i - i + j}(u))_{1 \leq i, j \leq l}.$$

LEMMA 1. *We have $s_\mu(u) \in \mathbb{Z}\langle\langle u \rangle\rangle$.*

PROOF. For $i, j \geq 0$, we have

$$\frac{u^i}{i!} \frac{u^j}{j!} = \frac{(i+j)!}{i!j!} \frac{u^{i+j}}{(i+j)!} = \binom{i+j}{i} \frac{u^{i+j}}{(i+j)!}.$$

Since $\binom{i+j}{i} \in \mathbb{Z}$, we obtain the statement of the lemma. $\square$

Let

$$t = \frac{x}{y}, \quad s = \frac{1}{x}.$$

Then t is a local parameter of V around ∞ . We have

$$x = \frac{1}{s}, \quad y = \frac{1}{st}. \tag{10}$$

Denote by $\mathbb{Z}_{\geq r}$ the set of integers that are not less than r .

LEMMA 2. *We have the following expansion of s in terms of t around $t = 0$*

$$s = t^2 \left(1 + \sum_{i=4}^{\infty} \beta_i t^i \right),$$

where β_i is a homogeneous polynomial in $\mathbb{Z}[\lambda_4, \lambda_6]$ of degree i . In particular, we have

$$s = t^2 + \lambda_4 t^6 + \lambda_6 t^8 + \dots$$

PROOF. By substituting (10) into $y^2 = x^3 + \lambda_4 x + \lambda_6$, we have

$$s = t^2 + \lambda_4 s^2 t^2 + \lambda_6 s^3 t^2. \tag{11}$$

The expansion of s with respect to t around $t = 0$ takes the following form

$$s = t^2 \sum_{i=0}^{\infty} \beta_i t^i,$$

where $\beta_i \in \mathbb{C}$. By substituting the above expansion into (11), we have

$$\sum_{i=0}^{\infty} \beta_i t^i = 1 + \lambda_4 t^4 \left(\sum_{i=0}^{\infty} \beta_i t^i \right)^2 + \lambda_6 t^6 \left(\sum_{i=0}^{\infty} \beta_i t^i \right)^3.$$

By comparing the coefficients, we obtain $\beta_0 = 1, \beta_4 = \lambda_4, \beta_6 = \lambda_6$, and $\beta_n = 0$ for $n = 1, 2, 3, 5$. For $n \geq 6$, we have

$$\beta_n = \lambda_4 \sum_{(i_1, i_2) \in I_1} \beta_{i_1} \beta_{i_2} + \lambda_6 \sum_{(i_1, i_2, i_3) \in I_2} \beta_{i_1} \beta_{i_2} \beta_{i_3},$$

where $I_1 = \{(i_1, i_2) \in \mathbb{Z}_{\geq 0}^2 \mid i_1 + i_2 = n - 4\}$ and $I_2 = \{(i_1, i_2, i_3) \in \mathbb{Z}_{\geq 0}^3 \mid i_1 + i_2 + i_3 = n - 6\}$. Therefore we obtain the statement of the lemma. $\square$

From Lemma 2 and (10), we have the expansions

$$x = \frac{1}{t^2} \left(1 + \sum_{i=4}^{\infty} a_i t^i \right), \quad y = \frac{1}{t^3} \left(1 + \sum_{i=4}^{\infty} a_i t^i \right), \quad (12)$$

where a_i is a homogeneous polynomial in $\mathbb{Z}[\lambda_4, \lambda_6]$ of degree i . We enumerate the monomials $x^m y^n$, where m is a non-negative integer and $n = 0, 1$, according as the order of a pole at ∞ and denote them by φ_j , $j \geq 1$. In particular we have $\varphi_1 = 1$. We set $e_i = t^{i+1}$. We expand $t\varphi_j$ around ∞ with respect to t . Let

$$t\varphi_j = \sum_i \xi_{i,j} e_i,$$

where $\xi_{i,j} \in \mathbb{Z}[\lambda_4, \lambda_6]$. For a partition $\mu = (\mu_1, \mu_2, \dots)$, we define

$$\xi_\mu = \det(\xi_{m_i, j})_{i,j \in \mathbb{N}},$$

where $m_i = \mu_i - i$ and the infinite determinant is well defined. Then we have $\xi_\mu \in \mathbb{Z}[\lambda_4, \lambda_6]$. We define the tau function $\tau(u)$ by

$$\tau(u) = \sum_{\mu} \xi_{\mu} s_{\mu}(u),$$

where the sum is over all partitions. From Lemma 1, we obtain the following proposition.

PROPOSITION 2. *We have $\tau(u) \in \mathbb{Z}[\lambda_4, \lambda_6] \langle \langle u \rangle \rangle$.*

LEMMA 3. *The expansion of du around ∞ with respect to t takes the form*

$$du = \left(\sum_{j=1}^{\infty} b_j t^{j-1} \right) dt,$$

where $b_1 = 1$ and $b_2 = b_3 = b_4 = 0$.

PROOF. From (12), we have

$$du = -\frac{dx}{2y} = \frac{1 - \sum_{i=4}^{\infty} a_i \frac{i-2}{2} t^i}{1 + \sum_{i=4}^{\infty} a_i t^i} dt = (1 + O(t^4)) dt.$$

$\square$

We take the algebraic bilinear form

$$\omega(P, Q) = \frac{x_1 x_2 (x_1 + x_2) + \lambda_4 (x_1 + x_2) + 2y_1 y_2 + 2\lambda_6}{4y_1 y_2 (x_1 - x_2)^2} dx_1 dx_2, \quad (13)$$

where $P = (x_1, y_1), Q = (x_2, y_2) \in V$. We can expand $\omega(P, Q)$ around $\infty \times \infty$ as

$$\omega(P, Q) = \left(\frac{1}{(t_1 - t_2)^2} + \sum_{i, j \geq 1} q_{ij} t_1^{i-1} t_2^{j-1} \right) dt_1 dt_2, \quad (14)$$

where $q_{ij} \in \mathbb{C}$ and t_1, t_2 are copies of the local parameter t .

LEMMA 4. *We have $q_{11} = 0$.*

PROOF. From (13) and (14), we have

$$\begin{aligned} & \{x_1 x_2 (x_1 + x_2) + \lambda_4 (x_1 + x_2) + 2y_1 y_2 + 2\lambda_6\} dx_1 dx_2 \\ &= 4y_1 y_2 (x_1 - x_2)^2 \left(\frac{1}{(t_1 - t_2)^2} + \sum_{i, j \geq 1} q_{ij} t_1^{i-1} t_2^{j-1} \right) dt_1 dt_2. \end{aligned}$$

By substituting the expansions of x_1, x_2, y_1, y_2 into the above equation and multiplying the both sides of this equation by $t_1^7 t_2^7 (t_1 - t_2)^2$, we obtain

$$\begin{aligned} & (t_1 - t_2)^2 (-2 + 2a_4 t_1^4 + \dots) (-2 + 2a_4 t_2^4 + \dots) \\ & \times [f(t_1) f(t_2) \{t_2^2 f(t_1) + t_1^2 f(t_2)\} + \lambda_4 t_1^2 t_2^2 \{t_2^2 f(t_1) + t_1^2 f(t_2)\} + 2t_1 t_2 f(t_1) f(t_2) + 2\lambda_6 t_1^4 t_2^4] \\ &= 4f(t_1) f(t_2) \{t_2^2 f(t_1) - t_1^2 f(t_2)\}^2 \left\{ 1 + q_{11} (t_1 - t_2)^2 + \sum_{i+j \geq 3} \tilde{q}_{ij} t_1^i t_2^j \right\}, \end{aligned}$$

where $f(t)$ is defined by $x = t^{-2} f(t)$ and $\tilde{q}_{ij} \in \mathbb{C}$. By comparing the coefficient of t_2^6 in the above equation, we obtain $q_{11} = 0$. $\square$

We define c_i by the following relation

$$\sqrt{\frac{du}{dt}} = \exp \left(\sum_{i=1}^{\infty} \frac{c_i}{i} t^i \right).$$

LEMMA 5. *We have $c_1 = 0$.*

PROOF. From Lemma 3, we have the following expansion

$$\sqrt{\frac{du}{dt}} = 1 + O(t^4).$$

On the other hand, we have

$$\exp \left(\sum_{i=1}^{\infty} \frac{c_i}{i} t^i \right) = 1 + c_1 t + O(t^2).$$

Thus we have $c_1 = 0$. $\square$

THEOREM 3. ([34], Theorem 4) *We have*

$$\tau(u) = \exp \left(-c_1 u + \frac{1}{2} q_{11} u^2 \right) \sigma(b_1 u).$$

From Theorem 3, Lemma 3, Lemma 4, and Lemma 5, we have

$$\sigma(u) = \tau(u). \quad (15)$$

From Proposition 2 and (15), we obtain the following theorem.

THEOREM 4. ([39]) *We have*

$$\sigma(u) \in \mathbb{Z}[\lambda_4, \lambda_6] \langle \langle u \rangle \rangle.$$

2.3. Hurwitz integrality of the expansion of the two-dimensional sigma function

In this subsection, we will explain the proof of [39] for Hurwitz integrality of the expansion of the sigma function for $g = 2$.

In this subsection, we assume $g = 2$. For an integral domain R with characteristic 0 and variables u_1, u_3 , let

$$R\langle u_1, u_3 \rangle = \left\{ \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \alpha_{i,j} \frac{u_1^i u_3^j}{i!j!} \mid \alpha_{i,j} \in R \right\}.$$

For $n < 0$ let $p_n(u_1, u_3) = 0$ and for $n \geq 0$ let

$$p_n(u_1, u_3) = \sum \frac{u_1^i u_3^j}{i!j!},$$

where the summation is over all $(i, j) \in \mathbb{Z}_{\geq 0}^2$ satisfying $i + 3j = n$. For an arbitrary partition $\mu = (\mu_1, \mu_2, \dots, \mu_l)$, we define the Schur polynomial $s_\mu(u_1, u_3)$ by

$$s_\mu(u_1, u_3) = \det (p_{\mu_i - i + j}(u_1, u_3))_{1 \leq i, j \leq l}.$$

LEMMA 6. *We have $s_\mu(u_1, u_3) \in \mathbb{Z}\langle u_1, u_3 \rangle$.*

PROOF. For $i, j, k, \ell \geq 0$, we have

$$\frac{u_1^i u_3^j}{i!j!} \frac{u_1^k u_3^\ell}{k!\ell!} = \frac{(i+k)!(j+\ell)!}{i!j!k!\ell!} \frac{u_1^{i+k} u_3^{j+\ell}}{(i+k)!(j+\ell)!} = \binom{i+k}{i} \binom{j+\ell}{j} \frac{u_1^{i+k} u_3^{j+\ell}}{(i+k)!(j+\ell)!}.$$

Since $\binom{i+k}{i} \binom{j+\ell}{j} \in \mathbb{Z}$, we obtain the statement of the lemma. $\square$

Let

$$t = \frac{x^2}{y}, \quad s = \frac{1}{x}.$$

Then t is a local parameter of V around ∞ . We have

$$x = \frac{1}{s}, \quad y = \frac{1}{s^2 t}. \tag{16}$$

LEMMA 7. *We have the following expansion of s in terms of t around $t = 0$*

$$s = t^2 \left(1 + \sum_{i=4}^{\infty} \gamma_i t^i \right),$$

where γ_i is a homogeneous polynomial in $\mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree i . In particular, we have

$$s = t^2 + \lambda_4 t^6 + \lambda_6 t^8 + (2\lambda_4^2 + \lambda_8) t^{10} + (5\lambda_4 \lambda_6 + \lambda_{10}) t^{12} + \dots$$

PROOF. By substituting (16) into $y^2 = x^5 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}$, we have

$$s = t^2 + \lambda_4 s^2 t^2 + \lambda_6 s^3 t^2 + \lambda_8 s^4 t^2 + \lambda_{10} s^5 t^2. \tag{17}$$

The expansion of s with respect to t around $t = 0$ takes the following form

$$s = t^2 \sum_{i=0}^{\infty} \gamma_i t^i,$$

where $\gamma_i \in \mathbb{C}$. By substituting the above expansion into (17), we have

$$\sum_{i=0}^{\infty} \gamma_i t^i = 1 + \lambda_4 t^4 \left(\sum_{i=0}^{\infty} \gamma_i t^i \right)^2 + \lambda_6 t^6 \left(\sum_{i=0}^{\infty} \gamma_i t^i \right)^3 + \lambda_8 t^8 \left(\sum_{i=0}^{\infty} \gamma_i t^i \right)^4 + \lambda_{10} t^{10} \left(\sum_{i=0}^{\infty} \gamma_i t^i \right)^5.$$

By comparing the coefficients, we obtain $\gamma_0 = 1, \gamma_4 = \lambda_4, \gamma_6 = \lambda_6, \gamma_8 = 2\lambda_4^2 + \lambda_8, \gamma_{10} = 5\lambda_4\lambda_6 + \lambda_{10}$ and $\gamma_n = 0$ for $n = 1, 2, 3, 5, 7, 9$. For $n \geq 10$, we have

$$\begin{aligned} \gamma_n = & \lambda_4 \sum_{(i_1, i_2) \in I_1} \gamma_{i_1} \gamma_{i_2} + \lambda_6 \sum_{(i_1, i_2, i_3) \in I_2} \gamma_{i_1} \gamma_{i_2} \gamma_{i_3} + \lambda_8 \sum_{(i_1, i_2, i_3, i_4) \in I_3} \gamma_{i_1} \gamma_{i_2} \gamma_{i_3} \gamma_{i_4} \\ & + \lambda_{10} \sum_{(i_1, i_2, i_3, i_4, i_5) \in I_4} \gamma_{i_1} \gamma_{i_2} \gamma_{i_3} \gamma_{i_4} \gamma_{i_5}, \end{aligned}$$

where $I_1 = \{(i_1, i_2) \in \mathbb{Z}_{\geq 0}^2 \mid i_1 + i_2 = n - 4\}$, $I_2 = \{(i_1, i_2, i_3) \in \mathbb{Z}_{\geq 0}^3 \mid i_1 + i_2 + i_3 = n - 6\}$, $I_3 = \{(i_1, i_2, i_3, i_4) \in \mathbb{Z}_{\geq 0}^4 \mid i_1 + i_2 + i_3 + i_4 = n - 8\}$, and $I_4 = \{(i_1, i_2, i_3, i_4, i_5) \in \mathbb{Z}_{\geq 0}^5 \mid i_1 + i_2 + i_3 + i_4 + i_5 = n - 10\}$. Therefore we obtain the statement of the lemma. $\square$

From Lemma 7, we have the expansions

$$x = \frac{1}{t^2} \left(1 + \sum_{i=4}^{\infty} d_i^{(1)} t^i \right), \quad y = \frac{1}{t^5} \left(1 + \sum_{i=4}^{\infty} d_i^{(2)} t^i \right),$$

where $d_i^{(1)}, d_i^{(2)}$ are homogeneous polynomials in $\mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree i . We enumerate the monomials $x^m y^n$, where m is a non-negative integer and $n = 0, 1$, according as the order of a pole at ∞ and denote them by φ_j , $j \geq 1$. In particular we have $\varphi_1 = 1$. We set $e_i = t^{i+1}$. We expand $t^2 \varphi_j$ around ∞ with respect to t . Let

$$t^2 \varphi_j = \sum \xi_{i,j} e_i,$$

where $\xi_{i,j} \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$. For a partition $\mu = (\mu_1, \mu_2, \dots)$, we define

$$\xi_\mu = \det(\xi_{m_i, j})_{i,j \in \mathbb{N}},$$

where $m_i = \mu_i - i$ and the infinite determinant is well defined. Then we have $\xi_\mu \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$. We define the tau function $\tau(u_1, u_3)$ by

$$\tau(u_1, u_3) = \sum_{\mu} \xi_\mu s_\mu(u_1, u_3),$$

where the sum is over all partitions. From Lemma 6, we obtain the following proposition.

PROPOSITION 3. *We have $\tau(u_1, u_3) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \langle\langle u_1, u_3 \rangle\rangle$.*

The expansions of du_i around ∞ with respect to t take the following form

$$du_i = \sum_{j=1}^{\infty} b_{ij} t^{j-1} dt.$$

LEMMA 8. *We have $b_{11} = 1, b_{13} = 0, b_{31} = 0, b_{33} = 1$.*

PROOF. We have

$$du_1 = -\frac{x}{2y}dx = -\frac{t^{-2}(1 + \sum_{i=4}^{\infty} d_i^{(1)} t^i)}{2t^{-5}(1 + \sum_{i=4}^{\infty} d_i^{(2)} t^i)} \left(-2t^{-3} + \sum_{i=4}^{\infty} (i-2) d_i^{(1)} t^{i-3} \right) = (1 + O(t^4))dt.$$

Therefore we obtain $b_{11} = 1$ and $b_{13} = 0$. We have

$$du_3 = -\frac{dx}{2y} = -\frac{-2t^{-3} + \sum_{i=4}^{\infty} (i-2) d_i^{(1)} t^{i-3}}{2t^{-5}(1 + \sum_{i=4}^{\infty} d_i^{(2)} t^i)} = (t^2 + O(t^6))dt.$$

Therefore we obtain $b_{31} = 0$ and $b_{33} = 1$. $\square$

We define c_i by the following relation

$$\sqrt{\frac{du_3}{dt}} = t \exp \left(\sum_{i=1}^{\infty} \frac{c_i}{i} t^i \right).$$

LEMMA 9. We have $c_1 = c_2 = c_3 = 0$.

PROOF. We have the following expansion

$$\frac{du_3}{dt} = t^2(1 + O(t^4)).$$

Therefore we have the following expansion

$$\sqrt{\frac{du_3}{dt}} = t(1 + O(t^4)).$$

On the other hand, we have

$$\exp \left(\sum_{i=1}^{\infty} \frac{c_i}{i} t^i \right) = 1 + c_1 t + \left(\frac{c_2}{2} + \frac{c_1^2}{2} \right) t^2 + \left(\frac{c_3}{3} + \frac{c_1 c_2}{2} + \frac{c_1^3}{6} \right) t^3 + \dots$$

Thus we have $c_1 = c_2 = c_3 = 0$. $\square$

We take the algebraic bilinear form

$$\omega(P, Q) = \frac{x_1^2 x_2^2 (x_1 + x_2) + \lambda_4 x_1 x_2 (x_1 + x_2) + 2\lambda_6 x_1 x_2 + \lambda_8 (x_1 + x_2) + 2y_1 y_2 + 2\lambda_{10}}{4y_1 y_2 (x_1 - x_2)^2} dx_1 dx_2, \quad (18)$$

where $P = (x_1, y_1), Q = (x_2, y_2) \in V$ ([15], p.217). We can expand $\omega(P, Q)$ around $\infty \times \infty$ as

$$\omega(P, Q) = \left(\frac{1}{(t_1 - t_2)^2} + \sum_{i,j \geq 1} q_{ij} t_1^{i-1} t_2^{j-1} \right) dt_1 dt_2, \quad (19)$$

where $q_{ij} \in \mathbb{C}$ and t_1, t_2 are copies of the local parameter t .

LEMMA 10. We have $q_{11} = 0, q_{13} = q_{31} = \lambda_4, q_{51} = q_{15} = 2\lambda_6, q_{33} = 3\lambda_6$.

PROOF. We define $f(t)$ by $s = t^2 f(t)$. From Lemma 7, we have

$$f(t) = 1 + \lambda_4 t^4 + \lambda_6 t^6 + \dots$$

From (18) and (19), we obtain

$$AB - C = D \cdot (q_{11} + q_{31} t_1^2 + q_{13} t_2^2 + q_{51} t_1^4 + q_{15} t_2^4 + q_{33} t_1^2 t_2^2 + \dots),$$

where

$$\begin{aligned}
A &= t_1^2 f(t_1) + t_2^2 f(t_2) + \lambda_4 t_1^2 t_2^2 f(t_1) f(t_2) (t_1^2 f(t_1) + t_2^2 f(t_2)) + 2\lambda_6 t_1^4 t_2^4 f(t_1)^2 f(t_2)^2 \\
&\quad + \lambda_8 t_1^4 t_2^4 f(t_1)^2 f(t_2)^2 (t_1^2 f(t_1) + t_2^2 f(t_2)) + 2t_1 t_2 f(t_1) f(t_2) + 2\lambda_{10} t_1^6 t_2^6 f(t_1)^3 f(t_2)^3 \\
B &= (1 + 3\lambda_4 t_1^4 + 4\lambda_6 t_1^6 + \dots)(1 + 3\lambda_4 t_2^4 + 4\lambda_6 t_2^6 + \dots) \\
C &= f(t_1) f(t_2) (t_1 + t_2)^2 \{1 + \lambda_4 (t_1^4 + t_1^2 t_2^2 + t_2^4) + \lambda_6 (t_1^6 + t_1^4 t_2^2 + t_1^2 t_2^4 + t_2^6) + \dots\}^2 \\
D &= f(t_1) f(t_2) (t_1^2 - t_2^2)^2 \{1 + \lambda_4 (t_1^4 + t_1^2 t_2^2 + t_2^4) + \lambda_6 (t_1^6 + t_1^4 t_2^2 + t_1^2 t_2^4 + t_2^6) + \dots\}^2.
\end{aligned}$$

By comparing the coefficient of t_1^4 , we obtain $q_{11} = 0$. By comparing the coefficient of t_1^6 , we obtain $q_{31} = q_{13} = \lambda_4$. By comparing the coefficient of t_1^8 , we obtain $q_{51} = q_{15} = 2\lambda_6$. By comparing the coefficient of $t_1^6 t_2^2$, we obtain

$$q_{33} - 2q_{51} = -\lambda_6.$$

Therefore we obtain $q_{33} = 3\lambda_6$. $\square$

THEOREM 5. ([34], Theorem 4) We have

$$\tau(u_1, u_3) = \exp\left(-c_1 u_1 - c_3 u_3 + \frac{1}{2} q_{11} u_1^2 + \frac{1}{2} q_{33} u_3^2 + q_{13} u_1 u_3\right) \sigma(b_{11} u_1 + b_{13} u_3, b_{31} u_1 + b_{33} u_3).$$

From Theorem 5, Lemma 8, Lemma 9, and Lemma 10, we have

$$\sigma(u_1, u_3) = \exp\left(-3\lambda_6 \frac{u_3^2}{2} - \lambda_4 u_1 u_3\right) \tau(u_1, u_3). \quad (20)$$

LEMMA 11. For any non-negative integer n , we have $\varepsilon_n := \frac{(2n)!}{2^n n!} \in \mathbb{Z}$.

PROOF. We have $\varepsilon_1 = 1 \in \mathbb{Z}$. Assume $\varepsilon_n \in \mathbb{Z}$. Then we have

$$\varepsilon_{n+1} = \frac{(2n+2)!}{2^{n+1}(n+1)!} = \frac{(2n+2)(2n+1)}{2(n+1)} \varepsilon_n = (2n+1) \varepsilon_n \in \mathbb{Z}.$$

By mathematical induction, we obtain the statement. $\square$

LEMMA 12. We have

$$\exp\left(-3\lambda_6 \frac{u_3^2}{2} - \lambda_4 u_1 u_3\right) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \langle \langle u_1, u_3 \rangle \rangle.$$

PROOF. We have

$$\exp\left(-3\lambda_6 \frac{u_3^2}{2} - \lambda_4 u_1 u_3\right) = \sum_{n=0}^{\infty} \frac{1}{n!} \left(-3\lambda_6 \frac{u_3^2}{2} - \lambda_4 u_1 u_3\right)^n.$$

From Lemma 11, for any $k, \ell \in \mathbb{Z}_{\geq 0}$, we have

$$\begin{aligned}
&\frac{1}{(k+\ell)!} \binom{k+\ell}{k} \left(-3\lambda_6 \frac{u_3^2}{2}\right)^k (-\lambda_4 u_1 u_3)^\ell \\
&= (-3\lambda_6)^k (-\lambda_4)^\ell \frac{u_1^\ell}{\ell!} \frac{u_3^{2k+\ell}}{(2k+\ell)!} \frac{(2k+\ell)!}{2^k k!} \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \langle \langle u_1, u_3 \rangle \rangle.
\end{aligned}$$

Therefore we obtain the statement. $\square$

From Proposition 3, Lemma 12, and (20), we obtain the following theorem.

THEOREM 6. ([39]) We have

$$\sigma(u_1, u_3) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \langle \langle u_1, u_3 \rangle \rangle.$$

2.4. Universal Bernoulli numbers

In this subsection, we will describe the definition of the universal Bernoulli numbers and their properties according to [38].

Let $f_1, f_2, \dots$ be infinitely many indeterminates. We consider the power series

$$u = u(z) = z + \sum_{n=1}^{\infty} f_n \frac{z^{n+1}}{n+1}$$

and its formal inverse series

$$z = z(u) = u - f_1 \frac{u^2}{2!} + (3f_1^2 - 2f_2) \frac{u^3}{3!} + \dots,$$

namely, the series such that $u(z(u)) = u$. Then we define $\hat{B}_n \in \mathbb{Q}[f_1, f_2, \dots]$ by

$$\frac{u}{z(u)} = \sum_{n=0}^{\infty} \hat{B}_n \frac{u^n}{n!}$$

and call them the *universal Bernoulli numbers*. We have $\hat{B}_0 = 1$. If we set $\deg f_i = i$, then $\hat{B}_n$ is homogeneous of degree n if $\hat{B}_n \neq 0$. Let $\mathcal{S}$ be the set of finite sequences $U = (U_1, U_2, \dots)$ of non-negative integers. For $U = (U_1, U_2, \dots) \in \mathcal{S}$, we use the notations $U! = U_1! U_2! \dots$, $\Lambda^U = 2^{U_1} 3^{U_2} 4^{U_3} \dots$, $f^U = f_1^{U_1} f_2^{U_2} \dots$, $\gamma_U = \Lambda^U U!$, $w(U) = \sum_j j U_j$, and $d(U) = \sum_j U_j$.

PROPOSITION 4. ([38] Proposition 2.8) We have the expression

$$\frac{\hat{B}_n}{n} = \sum_{w(U)=n} \tau_U f^U,$$

where

$$\tau_U = (-1)^{d(U)-1} \frac{(w(U) + d(U) - 2)!}{\gamma_U}. \quad (21)$$

For a rational number α , we denote by $\lfloor \alpha \rfloor$ the largest integer which does not exceed α . If p is a prime and the p -part of given rational number r is p^e , then we write $e = \text{ord}_p r$. If τ is a polynomial (possibly in several variables) with rational coefficients, then we denote by $\text{ord}_p \tau$ the least number of $\text{ord}_p r$ for all the coefficients r of τ . For a prime number p and an integer a , let $a|_p = a/p^{\text{ord}_p a}$. For positive integers a, b and a prime number p , we have

$$\text{ord}_p(a+b)! - \text{ord}_p a! - \text{ord}_p b! = \text{ord}_p \frac{(a+b)!}{a!b!}.$$

Since $(a+b)!/(a!b!) \in \mathbb{Z}$, we have

$$\text{ord}_p(a+b)! \geq \text{ord}_p a! + \text{ord}_p b!. \quad (22)$$

For a positive integer a and a prime number p

$$\text{ord}_p(a!) = \sum_{\nu=1}^{\infty} \left\lfloor \frac{a}{p^\nu} \right\rfloor. \quad (23)$$

If positive integers a and b are relatively prime, we denote it by $a \perp b$.

LEMMA 13. ([38] Proposition 3.11) Let p be an odd prime and $U = (U_1, U_2, \dots)$ be an element of $\mathcal{S}$. If $p \geq 5$, we assume $U_1 = U_2 = U_{p-1} = U_{2p-1} = 0$ and $d(U) \neq 0$. If $p = 3$, we assume $U_1 = U_2 = U_5 = U_8 = 0$ and $d(U) \neq 0$. Then τ_U defined in (21) satisfies

$$\text{ord}_p(\tau_U) \geq \left\lfloor \frac{w(U) + d(U) - 2}{2p} \right\rfloor.$$

PROOF. For the sake to be complete and self-contained, we give a proof of this lemma. By using (22) and (23), we have

$$\begin{aligned} \text{ord}_p(\tau_U) &= \text{ord}_p(w(U) + d(U) - 2)! - \text{ord}_p(\gamma_U) \\ &= \text{ord}_p \left(\sum_{j \geq 1} jU_j + \sum_{j \geq 1} U_j - 2 \right)! - \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} kU_{\varepsilon p^k - 1} - \sum_{j \geq 1} \text{ord}_p(U_j!) \\ &\geq \text{ord}_p \left(\sum_{j \geq 1} jU_j - 2 \right)! - \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} kU_{\varepsilon p^k - 1} \\ &= \text{ord}_p \left(-2 + \sum_{p \nmid j+1} jU_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} \right)! - \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} kU_{\varepsilon p^k - 1} \\ &= \sum_{\nu=1}^{\infty} \left\lfloor \frac{1}{p^\nu} \left(-2 + \sum_{p \nmid j+1} jU_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} \right) \right\rfloor - \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} kU_{\varepsilon p^k - 1} \\ &\geq \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid j+1} jU_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} \right) \right\rfloor - \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} kU_{\varepsilon p^k - 1} \\ &= \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid j+1} jU_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} (\varepsilon p^k - kp - 1)U_{\varepsilon p^k - 1} \right) \right\rfloor \\ &= \left\lfloor \frac{1}{2p} \left(-4 + \sum_{p \nmid j+1} 2jU_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} 2(\varepsilon p^k - kp - 1)U_{\varepsilon p^k - 1} \right) \right\rfloor. \end{aligned}$$

By the assumption of the lemma, there exists a positive integer i such that $i \geq 3$ and $U_i \neq 0$. For $j \geq 3$, we have $2j - (j+1) \geq 2$. If $p \geq 5$, let $T_p = \{(1, 1), (2, 1)\}$. If $p = 3$, let $T_p = \{(1, 1), (2, 1), (1, 2)\}$. By the assumption of the lemma, we have $U_{\varepsilon p^k - 1} = 0$ for any $(\varepsilon, k) \in T_p$. For any integers $\varepsilon \geq 1$ and $k \geq 1$ such that $(\varepsilon, k) \notin T_p$ and $\varepsilon \perp p$, we can check

$$2(\varepsilon p^k - kp - 1) - \varepsilon p^k \geq 2.$$

Therefore we have

$$\text{ord}_p(\tau_U) \geq \left\lfloor \frac{1}{2p} \left(-2 + \sum_{p \nmid j+1} (j+1)U_j + \sum_{\varepsilon, k \geq 1, \varepsilon \perp p} \varepsilon p^k U_{\varepsilon p^k - 1} \right) \right\rfloor = \left\lfloor \frac{w(U) + d(U) - 2}{2p} \right\rfloor.$$

□

LEMMA 14. Let $U = (U_1, U_2, \dots)$ be an element of $\mathcal{S}$ such that $U_i = 0$ for any odd integer i , $U_2 = 0$, and $d(U) \neq 0$. Then we have

$$\text{ord}_2(\tau_U) \geq \left\lfloor \frac{w(U) + d(U) - 2}{4} \right\rfloor.$$

PROOF. We can prove this lemma in the same way as [38] Proposition 3.11. For the sake to be complete and self-contained, we give a proof of this lemma. By using (22), (23), and $\text{ord}_2(\Lambda^U) = 0$, we have

$$\begin{aligned} \text{ord}_2(\tau_U) &= \text{ord}_2(w(U) + d(U) - 2)! - \text{ord}_2(\gamma_U) = \text{ord}_2\left(\sum_{j \geq 4} jU_j + \sum_{j \geq 4} U_j - 2\right)! - \text{ord}_2(U!) \\ &\geq \text{ord}_2\left(\sum_{j \geq 4} jU_j - 2\right)! = \sum_{\nu=1}^{\infty} \left\lfloor \frac{\sum_{j \geq 4} jU_j - 2}{2^\nu} \right\rfloor \geq \left\lfloor \frac{\sum_{j \geq 4} jU_j - 2}{2} \right\rfloor \\ &= \left\lfloor \frac{\sum_{j \geq 4} 2jU_j - 4}{4} \right\rfloor. \end{aligned}$$

Since $j \geq 4$, we have $2j - (j + 1) \geq 3$. Therefore we have

$$\left\lfloor \frac{\sum_{j \geq 4} 2jU_j - 4}{4} \right\rfloor \geq \left\lfloor \frac{\sum_{j \geq 4} (j + 1)U_j - 2}{4} \right\rfloor = \left\lfloor \frac{w(U) + d(U) - 2}{4} \right\rfloor.$$

□

In [22], F. Clarke showed the following results, which are a generalization of the von Staudt-Clausen theorem for the classical Bernoulli numbers to the universal Bernoulli numbers, cf. the paper of Onishi [38]. These results were used in the proof of our Theorem 11 in the present survey.

THEOREM 7. (i) We have

$$\hat{B}_1 = \frac{1}{2}f_1, \quad \frac{\hat{B}_2}{2} = -\frac{1}{4}f_1^2 + \frac{1}{3}f_2,$$

(ii) If $n \equiv 0 \pmod{4}$, then we have

$$\frac{\hat{B}_n}{n} \equiv \sum_{n=a(p-1), p: \text{prime}} \frac{a|_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} f_{p-1}^a \pmod{\mathbb{Z}[f_1, f_2, \dots]}.$$

(iii) If $n \equiv 2 \pmod{4}$ and $n \neq 2$, then we have

$$\frac{\hat{B}_n}{n} \equiv \frac{f_1^{n-6} f_3^2}{2} - \frac{n f_1^n}{8} + \sum_{n=a(p-1), p: \text{odd prime}} \frac{a|_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} f_{p-1}^a \pmod{\mathbb{Z}[f_1, f_2, \dots]}.$$

(iv) If $n \equiv 1, 3 \pmod{4}$ and $n \neq 1$, then we have

$$\frac{\hat{B}_n}{n} \equiv \frac{f_1^n + f_1^{n-3} f_3}{2} \pmod{\mathbb{Z}[f_1, f_2, \dots]}.$$

In (ii) and (iii), $a|_p^{-1} \pmod{p^{1+\text{ord}_p a}}$ denotes an integer δ such that $(a|_p)\delta \equiv 1 \pmod{p^{1+\text{ord}_p a}}$.

3. Differential equations for the coefficients of the expansions of the two-dimensional sigma function

In this section, we assume $g = 2$.

3.1. The coefficients of u_3

Let $\lambda = (\lambda_4, \lambda_6, \lambda_8, \lambda_{10})$. We set

$$\sigma(u_1, u_3; \lambda) = \sum_{k \geq 0} \xi_k(u_1; \lambda) \frac{u_3^k}{k!}.$$

PROPOSITION 5. For $k \geq 0$, the functions $\xi_0, \xi_1, \dots$ satisfy the following hierarchy of systems

$$u_1 \xi'_k + 3(k-1)\xi_k = 4\lambda_4 \xi_{k,\lambda_4} + 6\lambda_6 \xi_{k,\lambda_6} + 8\lambda_8 \xi_{k,\lambda_8} + 10\lambda_{10} \xi_{k,\lambda_{10}}, \quad (24)$$

$$\begin{aligned} u_1 \xi_{k+1} = & -\frac{1}{2} \xi''_k + \frac{4k}{5} \lambda_4 \xi'_{k-1} + \frac{3}{10} \lambda_4 u_1^2 \xi_k - \frac{k(k-1)}{10} (15\lambda_8 - 4\lambda_4^2) \xi_{k-2} \\ & + 6\lambda_6 \xi_{k,\lambda_4} + (8\lambda_8 - \frac{12}{5} \lambda_4^2) \xi_{k,\lambda_6} + (10\lambda_{10} - \frac{8}{5} \lambda_4 \lambda_6) \xi_{k,\lambda_8} - \frac{4}{5} \lambda_4 \lambda_8 \xi_{k,\lambda_{10}}, \end{aligned} \quad (25)$$

$$\begin{aligned} \xi'_{k+1} = & \frac{6k}{5} \lambda_6 \xi'_{k-1} - k \lambda_4 \xi_k + \frac{\lambda_6}{5} u_1^2 \xi_k - k \lambda_8 u_1 \xi_{k-1} - \frac{k(k-1)}{10} (30\lambda_{10} - 6\lambda_4 \lambda_6) \xi_{k-2} + \lambda_4 \xi_k \\ & + 8\lambda_8 \xi_{k,\lambda_4} + (10\lambda_{10} - \frac{8}{5} \lambda_4 \lambda_6) \xi_{k,\lambda_6} + (4\lambda_4 \lambda_8 - \frac{12}{5} \lambda_6^2) \xi_{k,\lambda_8} + (6\lambda_4 \lambda_{10} - \frac{6}{5} \lambda_6 \lambda_8) \xi_{k,\lambda_{10}}, \end{aligned} \quad (26)$$

$$\begin{aligned} \xi_{k+2} = & \frac{6k}{5} \lambda_8 \xi'_{k-1} + \frac{\lambda_8}{5} u_1^2 \xi_k - 4k \lambda_{10} u_1 \xi_{k-1} + \frac{3k(k-1)}{5} \lambda_8 \lambda_4 \xi_{k-2} + \lambda_6 \xi_k \\ & + 20\lambda_{10} \xi_{k,\lambda_4} - \frac{8}{5} \lambda_4 \lambda_8 \xi_{k,\lambda_6} + (12\lambda_4 \lambda_{10} - \frac{12}{5} \lambda_6 \lambda_8) \xi_{k,\lambda_8} + (8\lambda_6 \lambda_{10} - \frac{16}{5} \lambda_8^2) \xi_{k,\lambda_{10}}, \end{aligned} \quad (27)$$

where the prime denotes the derivation with respect to u_1 and $\xi_{k,\lambda_{2j}}$ denotes the derivation of ξ_k with respect to λ_{2j} .

PROOF. We substitute the expressions

$$\begin{aligned} \sigma_1 &= \sum_{k \geq 0} \xi'_k(u_1) \frac{u_3^k}{k!}, \quad \sigma_3 = \sum_{k \geq 0} \xi_{k+1}(u_1) \frac{u_3^k}{k!}, \quad \sigma_{11} = \sum_{k \geq 0} \xi''_k(u_1) \frac{u_3^k}{k!}, \\ \sigma_{13} &= \sum_{k \geq 0} \xi'_{k+1}(u_1) \frac{u_3^k}{k!}, \quad \sigma_{33} = \sum_{k \geq 0} \xi_{k+2}(u_1) \frac{u_3^k}{k!}. \end{aligned}$$

into the equations $Q_i \sigma = 0$ for $i = 0, 2, 4, 6$ in Theorem 2 (ii) and compare the coefficients of $u_3^k/k!$. Then, from $Q_0 \sigma = 0, Q_2 \sigma = 0, Q_4 \sigma = 0, Q_6 \sigma = 0$, we obtain (24), (25), (26), (27), respectively. $\square$

LEMMA 15. The fact that ξ_k satisfies the differential equation (24) means that ξ_k is homogeneous in u_1 and λ_{2j} , $j = 2, \dots, 5$, with degree $3k - 3$.

PROOF. We set

$$\xi_k(u_1; \lambda) = \sum_{i_1, j_4, j_6, j_8, j_{10} \geq 0} a_{i_1, j_4, j_6, j_8, j_{10}}^{(k)} u_1^{i_1} \lambda_4^{j_4} \lambda_6^{j_6} \lambda_8^{j_8} \lambda_{10}^{j_{10}}, \quad a_{i_1, j_4, j_6, j_8, j_{10}}^{(k)} \in \mathbb{C}.$$

By substituting the above expression into (24) and comparing the coefficient of $u_1^{i_1} \lambda_4^{j_4} \lambda_6^{j_6} \lambda_8^{j_8} \lambda_{10}^{j_{10}}$, we have

$$a_{i_1, j_4, j_6, j_8, j_{10}}^{(k)} (i_1 + 3k - 3) = a_{i_1, j_4, j_6, j_8, j_{10}}^{(k)} (4j_4 + 6j_6 + 8j_8 + 10j_{10}).$$

If $a_{i_1, j_4, j_6, j_8, j_{10}}^{(k)} \neq 0$, we have $4j_4 + 6j_6 + 8j_8 + 10j_{10} - i_1 = 3k - 3$. $\square$

PROPOSITION 6. *The function ξ_0 satisfies the following differential equation*

$$\begin{aligned} & \frac{1}{2}\xi_0'' - \frac{1}{2}u_1\xi_0''' - \frac{7}{10}\lambda_4u_1^2\xi_0 - \frac{\lambda_6}{5}u_1^4\xi_0 + \frac{3}{10}\lambda_4u_1^3\xi_0' - 8\lambda_8u_1^2\xi_{0,\lambda_4} \\ & - (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)u_1^2\xi_{0,\lambda_6} - (4\lambda_4\lambda_8 - \frac{12}{5}\lambda_6^2)u_1^2\xi_{0,\lambda_8} - (6\lambda_4\lambda_{10} - \frac{6}{5}\lambda_6\lambda_8)u_1^2\xi_{0,\lambda_{10}} \\ & + 6\lambda_6u_1\xi_{0,\lambda_4}' + (8\lambda_8 - \frac{12}{5}\lambda_4^2)u_1\xi_{0,\lambda_6}' + (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)u_1\xi_{0,\lambda_8}' - \frac{4}{5}\lambda_4\lambda_8u_1\xi_{0,\lambda_{10}}' \\ & - 6\lambda_6\xi_{0,\lambda_4} - (8\lambda_8 - \frac{12}{5}\lambda_4^2)\xi_{0,\lambda_6} - (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)\xi_{0,\lambda_8} + \frac{4}{5}\lambda_4\lambda_8\xi_{0,\lambda_{10}} = 0. \end{aligned}$$

PROOF. From (25) with $k = 0$, we have

$$u_1\xi_1 = -\frac{1}{2}\xi_0'' + \frac{3}{10}\lambda_4u_1^2\xi_0 + 6\lambda_6\xi_{0,\lambda_4} + (8\lambda_8 - \frac{12}{5}\lambda_4^2)\xi_{0,\lambda_6} + (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)\xi_{0,\lambda_8} - \frac{4}{5}\lambda_4\lambda_8\xi_{0,\lambda_{10}}. \quad (28)$$

From (26) with $k = 0$, ξ_1' can be expressed in terms of ξ_0 and its derivatives. We take the derivative with respect to u_1 of (28) and substitute into it the expression for ξ_1' . As a result, we obtain

$$\begin{aligned} \xi_1 &= -\frac{1}{2}\xi_0''' - \frac{2}{5}\lambda_4u_1\xi_0 - \frac{\lambda_6}{5}u_1^3\xi_0 + \frac{3}{10}\lambda_4u_1^2\xi_0' - 8\lambda_8u_1\xi_{0,\lambda_4} - (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)u_1\xi_{0,\lambda_6} \\ & - (4\lambda_4\lambda_8 - \frac{12}{5}\lambda_6^2)u_1\xi_{0,\lambda_8} - (6\lambda_4\lambda_{10} - \frac{6}{5}\lambda_6\lambda_8)u_1\xi_{0,\lambda_{10}} + 6\lambda_6\xi_{0,\lambda_4}' + (8\lambda_8 - \frac{12}{5}\lambda_4^2)\xi_{0,\lambda_6}' \\ & + (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)\xi_{0,\lambda_8}' - \frac{4}{5}\lambda_4\lambda_8\xi_{0,\lambda_{10}}'. \end{aligned}$$

We substitute the above equation into (28) and finally obtain the statement of the proposition. $\square$

We set

$$\xi_0 = \sum_{\ell \geq 0} p_\ell(\lambda) \frac{u_1^\ell}{\ell!}. \quad (29)$$

LEMMA 16. *If ℓ is even, then $p_\ell = 0$. We have $p_1 = 0$ and $p_3 \in \mathbb{C}$.*

PROOF. From Lemma 15 and (24) with $k = 0$, we obtain the statement of the lemma. $\square$

PROPOSITION 7. *For $\ell \geq 2$, the following recurrence relation holds :*

$$\begin{aligned} p_{\ell+2} &= \frac{\lambda_4\ell(3\ell-13)}{5}p_{\ell-2} - \frac{2\lambda_6}{5}\ell(\ell-2)(\ell-3)p_{\ell-4} - 16\lambda_8\ell p_{\ell-2,\lambda_4} \\ & - (20\lambda_{10} - \frac{16}{5}\lambda_4\lambda_6)\ell p_{\ell-2,\lambda_6} - (8\lambda_4\lambda_8 - \frac{24}{5}\lambda_6^2)\ell p_{\ell-2,\lambda_8} - (12\lambda_4\lambda_{10} - \frac{12}{5}\lambda_6\lambda_8)\ell p_{\ell-2,\lambda_{10}} \\ & + 12\lambda_6p_{\ell,\lambda_4} + (16\lambda_8 - \frac{24}{5}\lambda_4^2)p_{\ell,\lambda_6} + (20\lambda_{10} - \frac{16}{5}\lambda_4\lambda_6)p_{\ell,\lambda_8} - \frac{8}{5}\lambda_4\lambda_8p_{\ell,\lambda_{10}}, \end{aligned}$$

where $p_{i,\lambda_{2j}}$ denotes the derivative of p_i with respect to λ_{2j} .

PROOF. By substituting (29) into the differential equation in Proposition 6 and comparing the coefficients of $u_1^\ell/\ell!$, we obtain the statement of the proposition. $\square$

COROLLARY 1. *The sigma function $\sigma(u_1, u_3; \lambda)$ is uniquely determined by the differential equations $Q_i\sigma = 0$, $i = 0, 2, 4$, up to a multiplicative constant.*

PROOF. From Lemma 16 and Proposition 7, we find that all the coefficients p_ℓ are determined from p_3 . Note that Lemma 16 and Proposition 7 follow from (24), (25), and (26). By (25), all the functions ξ_k are determined from ξ_0 . As mentioned in the proof of Proposition 5, (24), (25), (26) follow from $Q_0\sigma = 0, Q_2\sigma = 0, Q_4\sigma = 0$. Therefore we obtain the statement of this corollary. $\square$

REMARK 1. *It is known that the sigma function $\sigma(u_1, u_3; \lambda)$ is uniquely determined by the differential equations $Q_i \sigma = 0$, $i = 0, 2, 4, 6$, up to a multiplicative constant ([18], [19], [24]). In [11], the following expression is proved :*

$$10Q_6 = 5[Q_2, Q_4] - 8\lambda_6 Q_0 + 8\lambda_4 Q_2,$$

where $[Q_2, Q_4]$ is the commutator of Q_2 and Q_4 . From this result, in [11], it is shown that the sigma function $\sigma(u_1, u_3; \lambda)$ is uniquely determined by the differential equations $Q_i \sigma = 0$, $i = 0, 2, 4$, up to a multiplicative constant.

COROLLARY 2. *We have*

$$\sigma(u_1, u_3) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1, u_3 \rangle \rangle.$$

PROOF. From Lemma 16 and (9), we have $p_0 = p_1 = p_2 = 0$ and $p_3 = 2$. From Proposition 7, we can show $p_\ell \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}]$ for any ℓ by mathematical induction. Therefore we have $\xi_0 \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1 \rangle \rangle$. From (26) with $k = 0$, we can show $\xi'_1 \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1 \rangle \rangle$. Since $\xi_1 = -1 + O(u_1)$, we have $\xi_1 \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1 \rangle \rangle$. From (27), we can show $\xi_k \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1 \rangle \rangle$ for any k by mathematical induction. Therefore we have

$$\sigma(u_1, u_3) \in \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, 2\lambda_{10}] \langle \langle u_1, u_3 \rangle \rangle.$$

From Theorem 6, we obtain the statement of the corollary. $\square$

3.2. Expansions of ξ_k

In this subsection we will calculate the expansions of ξ_k . From (9), we have $p_3 = 2$. The initial terms of ξ_i , $i = 0, 1, 2, 3, 4$, are as follows.

$$\begin{aligned} \xi_0 &= 2 \frac{u_1^3}{3!} + 2^2 \lambda_4 \frac{u_1^7}{7!} - 2^6 \lambda_6 \frac{u_1^9}{9!} + 2^3 (51 \lambda_4^2 - 200 \lambda_8) \frac{u_1^{11}}{11!} + 2^7 (67 \lambda_4 \lambda_6 - 140 \lambda_{10}) \frac{u_1^{13}}{13!} + \dots, \\ \xi_1 &= -1 + 2 \lambda_4 \frac{u_1^4}{4!} + 2^3 \lambda_6 \frac{u_1^6}{6!} + 2^2 (\lambda_4^2 + 8 \lambda_8) \frac{u_1^8}{8!} + 2^5 (3 \lambda_4 \lambda_6 - 20 \lambda_{10}) \frac{u_1^{10}}{10!} \\ &\quad + 2^3 (304 \lambda_6^2 + 51 \lambda_4^3 - 184 \lambda_4 \lambda_8) \frac{u_1^{12}}{12!} + 2^5 (1256 \lambda_6 \lambda_8 + 237 \lambda_4^2 \lambda_6 - 1240 \lambda_4 \lambda_{10}) \frac{u_1^{14}}{14!} + \dots, \\ \xi_2 &= 2 \lambda_6 \frac{u_1^3}{3!} + 2^3 \lambda_8 \frac{u_1^5}{5!} + 2^2 (20 \lambda_{10} + \lambda_4 \lambda_6) \frac{u_1^7}{7!} + 2^5 (5 \lambda_4 \lambda_8 - 2 \lambda_6^2) \frac{u_1^9}{9!} + 2^3 (51 \lambda_4^2 \lambda_6 + 104 \lambda_6 \lambda_8 \\ &\quad - 360 \lambda_4 \lambda_{10}) \frac{u_1^{11}}{11!} + 2^5 (232 \lambda_8^2 - 31 \lambda_4^2 \lambda_8 + 268 \lambda_4 \lambda_6^2 + 320 \lambda_6 \lambda_{10}) \frac{u_1^{13}}{13!} + \dots, \\ \xi_3 &= -\lambda_6 + 2 \lambda_8 \frac{u_1^2}{2!} + 2 (\lambda_4 \lambda_6 + 4 \lambda_{10}) \frac{u_1^4}{4!} + 2^2 (\lambda_4 \lambda_8 + 2 \lambda_6^2) \frac{u_1^6}{6!} + 2^2 (\lambda_4^2 \lambda_6 + 104 \lambda_4 \lambda_{10} - 8 \lambda_6 \lambda_8) \frac{u_1^8}{8!} \\ &\quad + 2^3 (88 \lambda_8^2 + 51 \lambda_4^2 \lambda_8 + 12 \lambda_4 \lambda_6^2 - 160 \lambda_6 \lambda_{10}) \frac{u_1^{10}}{10!} \\ &\quad + (7104 \lambda_4 \lambda_6 \lambda_8 + 8960 \lambda_8 \lambda_{10} + 2432 \lambda_6^3 + 408 \lambda_4^3 \lambda_6 - 12768 \lambda_4^2 \lambda_{10}) \frac{u_1^{12}}{12!} + \dots, \\ \xi_4 &= 2^3 \lambda_{10} \frac{u_1}{1!} + 2 (\lambda_6^2 + 2 \lambda_4 \lambda_8) \frac{u_1^3}{3!} + 2^4 (\lambda_6 \lambda_8 + \lambda_4 \lambda_{10}) \frac{u_1^5}{5!} \\ &\quad + 2^2 (2 \lambda_4^2 \lambda_8 + \lambda_4 \lambda_6^2 + 88 \lambda_6 \lambda_{10} - 28 \lambda_8^2) \frac{u_1^7}{7!} + 2^5 (6 \lambda_4 \lambda_6 \lambda_8 + 16 \lambda_8 \lambda_{10} - 2 \lambda_6^3 + 51 \lambda_4^2 \lambda_{10}) \frac{u_1^9}{9!} \\ &\quad + 2^3 (744 \lambda_4 \lambda_8^2 + 408 \lambda_6^2 \lambda_8 + 102 \lambda_4^3 \lambda_8 + 51 \lambda_4^2 \lambda_6^2 - 1008 \lambda_4 \lambda_6 \lambda_{10} - 160 \lambda_{10}^2) \frac{u_1^{11}}{11!} \\ &\quad + 2^6 (960 \lambda_6 \lambda_8^2 + 237 \lambda_4^2 \lambda_6 \lambda_8 + 1072 \lambda_4 \lambda_8 \lambda_{10} + 134 \lambda_4 \lambda_6^3 + 168 \lambda_6^2 \lambda_{10} - 849 \lambda_4^3 \lambda_{10}) \frac{u_1^{13}}{13!} + \dots \end{aligned}$$

3.3. The coefficients of u_1

We set

$$\sigma(u_1, u_3; \lambda) = \sum_{k \geq 0} \mu_k(u_3; \lambda) \frac{u_1^k}{k!}. \quad (30)$$

PROPOSITION 8. *For $k \geq 0$, the functions $\mu_0, \mu_1, \dots$ satisfy the following hierarchy of systems*

$$(k-3)\mu_k + 3u_3\mu'_k = 4\lambda_4\mu_{k,\lambda_4} + 6\lambda_6\mu_{k,\lambda_6} + 8\lambda_8\mu_{k,\lambda_8} + 10\lambda_{10}\mu_{k,\lambda_{10}}, \quad (31)$$

$$\begin{aligned} \mu_{k+2} = & \frac{8}{5}\lambda_4u_3\mu_{k+1} - 2k\mu'_{k-1} + \frac{3k(k-1)}{5}\lambda_4\mu_{k-2} - \frac{15\lambda_8 - 4\lambda_4^2}{5}u_3^2\mu_k \\ & + 12\lambda_6\mu_{k,\lambda_4} + (16\lambda_8 - \frac{24}{5}\lambda_4^2)\mu_{k,\lambda_6} + (20\lambda_{10} - \frac{16}{5}\lambda_4\lambda_6)\mu_{k,\lambda_8} - \frac{8}{5}\lambda_4\lambda_8\mu_{k,\lambda_{10}}, \end{aligned} \quad (32)$$

$$\begin{aligned} \mu'_{k+1} - \frac{6}{5}\lambda_6u_3\mu_{k+1} = & -\lambda_4u_3\mu'_k + \frac{k(k-1)}{5}\lambda_6\mu_{k-2} - k\lambda_8u_3\mu_{k-1} - (3\lambda_{10} - \frac{3}{5}\lambda_4\lambda_6)u_3^2\mu_k \\ & + \lambda_4\mu_k + 8\lambda_8\mu_{k,\lambda_4} + (10\lambda_{10} - \frac{8}{5}\lambda_4\lambda_6)\mu_{k,\lambda_6} + (4\lambda_4\lambda_8 - \frac{12}{5}\lambda_6^2)\mu_{k,\lambda_8} \\ & + (6\lambda_4\lambda_{10} - \frac{6}{5}\lambda_6\lambda_8)\mu_{k,\lambda_{10}}, \end{aligned} \quad (33)$$

$$\begin{aligned} \lambda_8u_3\mu_{k+1} = & \frac{5}{6}\mu''_k - \frac{k(k-1)}{6}\lambda_8\mu_{k-2} + \frac{10}{3}k\lambda_{10}u_3\mu_{k-1} - \frac{\lambda_4\lambda_8}{2}u_3^2\mu_k - \frac{5}{6}\lambda_6\mu_k \\ & - \frac{50}{3}\lambda_{10}\mu_{k,\lambda_4} + \frac{4}{3}\lambda_4\lambda_8\mu_{k,\lambda_6} - (10\lambda_4\lambda_{10} - 2\lambda_6\lambda_8)\mu_{k,\lambda_8} - (\frac{20}{3}\lambda_6\lambda_{10} - \frac{8}{3}\lambda_8^2)\mu_{k,\lambda_{10}}, \end{aligned} \quad (34)$$

where the prime denotes the derivation with respect to u_3 and $\mu_{k,\lambda_{2j}}$ denotes the derivation of μ_k with respect to λ_{2j} .

PROOF. We substitute the expression (30) into the equations $Q_i\sigma = 0$ for $i = 0, 2, 4, 6$ in Theorem 2 (ii) and compare the coefficients of $u_1^k/k!$. Then, from $Q_0\sigma = 0$, $Q_2\sigma = 0$, $Q_4\sigma = 0$, $Q_6\sigma = 0$, we obtain (31), (32), (33), (34), respectively. $\square$

LEMMA 17. *The fact that μ_k satisfies the differential equation (31) means that μ_k is homogeneous in u_3 and λ_{2j} , $j = 2, \dots, 5$, with degree $k-3$.*

PROOF. In the same way as Lemma 15, we obtain the statement of the lemma. $\square$

PROPOSITION 9. *The function μ_0 satisfies the following differential equation*

$$\begin{aligned} \mu''_0 + \frac{9}{5}\lambda_4\lambda_8u_3^2\mu_0 - \lambda_6\mu_0 - \frac{6}{5}\lambda_6^2u_3^2\mu_0 - \frac{18}{5}\lambda_8\lambda_{10}u_3^4\mu_0 - u_3\mu_0''' + \frac{6}{5}\lambda_6u_3^2\mu_0'' - \frac{3}{5}\lambda_4\lambda_8u_3^3\mu_0' \\ + \lambda_6u_3\mu_0' - 20\lambda_{10}\mu_{0,\lambda_4} + \frac{8}{5}\lambda_4\lambda_8\mu_{0,\lambda_6} + \left(\frac{12}{5}\lambda_6\lambda_8 - 12\lambda_4\lambda_{10}\right)\mu_{0,\lambda_8} + \left(\frac{16}{5}\lambda_8^2 - 8\lambda_6\lambda_{10}\right)\mu_{0,\lambda_{10}} \\ + 20\lambda_{10}u_3\mu_{0,\lambda_4}' - \frac{8}{5}\lambda_4\lambda_8u_3\mu_{0,\lambda_6}' + \left(12\lambda_4\lambda_{10} - \frac{12}{5}\lambda_6\lambda_8\right)u_3\mu_{0,\lambda_8}' + \left(8\lambda_6\lambda_{10} - \frac{16}{5}\lambda_8^2\right)u_3\mu_{0,\lambda_{10}}' \\ + \left(\frac{48}{5}\lambda_8^2 - 24\lambda_6\lambda_{10}\right)u_3^2\mu_{0,\lambda_4} + 12\lambda_8\lambda_{10}u_3^2\mu_{0,\lambda_6} + \left(\frac{24}{5}\lambda_4\lambda_8^2 - \frac{72}{5}\lambda_4\lambda_6\lambda_{10}\right)u_3^2\mu_{0,\lambda_8} \\ + \left(\frac{36}{5}\lambda_4\lambda_8\lambda_{10} - \frac{48}{5}\lambda_6^2\lambda_{10} + \frac{12}{5}\lambda_6\lambda_8^2\right)u_3^2\mu_{0,\lambda_{10}} = 0 \end{aligned}$$

PROOF. By substituting (34) for $k = 0$ into (33) for $k = 0$, we obtain the statement of the proposition. $\square$

We set

$$\mu_0 = \sum_{\ell \geq 0} q_\ell(\lambda) \frac{u_3^\ell}{\ell!}. \quad (35)$$

LEMMA 18. *If ℓ is even, then $q_\ell = 0$. We have $q_1 \in \mathbb{C}$ and $q_3 = \lambda_6 q_1$.*

PROOF. From Lemma 17 and (31), we obtain $q_\ell = 0$ for any non-negative even integer ℓ and $q_1 \in \mathbb{C}$. Further, we find that the coefficient of u_3^0 in μ_1 is equal to 0. By comparing the coefficient of u_3 in the equation (34) for $k = 0$, we obtain $q_3 = \lambda_6 q_1$. $\square$

PROPOSITION 10. *For $\ell \geq 2$, the following recurrence relation holds :*

$$\begin{aligned} q_{\ell+2} = & \left(\frac{6}{5}\ell + 1\right)\lambda_6 q_\ell + \ell\left(3 - \frac{3}{5}\ell\right)\lambda_4 \lambda_8 q_{\ell-2} - \frac{6}{5}\lambda_6^2 \ell q_{\ell-2} - \frac{18\ell(\ell-2)(\ell-3)}{5}\lambda_8 \lambda_{10} q_{\ell-4} \\ & + 20\lambda_{10} q_{\ell, \lambda_4} - \frac{8}{5}\lambda_4 \lambda_8 q_{\ell, \lambda_6} + (12\lambda_4 \lambda_{10} - \frac{12}{5}\lambda_6 \lambda_8) q_{\ell, \lambda_8} + (8\lambda_6 \lambda_{10} - \frac{16}{5}\lambda_8^2) q_{\ell, \lambda_{10}} \\ & + \left(\frac{48}{5}\lambda_8^2 - 24\lambda_6 \lambda_{10}\right) \ell q_{\ell-2, \lambda_4} + 12\lambda_8 \lambda_{10} \ell q_{\ell-2, \lambda_6} + \left(\frac{24}{5}\lambda_4 \lambda_8^2 - \frac{72}{5}\lambda_4 \lambda_6 \lambda_{10}\right) \ell q_{\ell-2, \lambda_8} \\ & + \left(\frac{36}{5}\lambda_4 \lambda_8 \lambda_{10} - \frac{48}{5}\lambda_6^2 \lambda_{10} + \frac{12}{5}\lambda_6 \lambda_8^2\right) \ell q_{\ell-2, \lambda_{10}}, \end{aligned}$$

where $q_{i, \lambda_{2j}}$ denotes the derivative of q_i with respect to λ_{2j} .

PROOF. By substituting (35) into the differential equation in Proposition 9 and comparing the coefficients of $u_3^\ell/\ell!$, we obtain the statement of the proposition. $\square$

COROLLARY 3. *Let $\lambda_8 \neq 0$. Then the sigma function $\sigma(u_1, u_3; \lambda)$ is uniquely determined by the differential equations $Q_i \sigma = 0$, $i = 0, 4, 6$, up to a multiplicative constant.*

PROOF. From Lemma 18 and Proposition 10, we find that all the coefficients q_ℓ are determined from q_1 . Note that Lemma 18 and Proposition 10 follow from (31), (33), and (34). By (34), all the functions μ_k are determined from μ_0 . As mentioned in the proof of Proposition 8, (31), (33), (34) follow from $Q_0 \sigma = 0$, $Q_4 \sigma = 0$, $Q_6 \sigma = 0$. Therefore we obtain the statement of this corollary. $\square$

REMARK 2. *In [11], the following expression is proved :*

$$6\lambda_8 Q_2 = 5[Q_4, Q_6] + 10\lambda_{10} Q_0 + 6\lambda_6 Q_4 - 10\lambda_4 Q_6.$$

From this result, the statement of Corollary 3 can be also proved.

3.4. Expansions of μ_k

In this subsection we will calculate the expansions of μ_k . From (9), we have $q_1 = -1$. The initial terms of μ_i , $i = 0, 1, 2, 3$, are as follows.

$$\begin{aligned} \mu_0 &= -u_3 - \lambda_6 \frac{u_3^3}{3!} - (\lambda_6^2 + 2\lambda_4 \lambda_8) \frac{u_3^5}{5!} + (8\lambda_8 \lambda_{10} - 6\lambda_4 \lambda_6 \lambda_8 - \lambda_6^3 - 24\lambda_4^2 \lambda_{10}) \frac{u_3^7}{7!} + \cdots, \\ \mu_1 &= 8\lambda_{10} \frac{u_3^4}{4!} + (88\lambda_6 \lambda_{10} - 16\lambda_8^2) \frac{u_3^6}{6!} + (816\lambda_6^2 \lambda_{10} - 192\lambda_6 \lambda_8^2 - 160\lambda_4 \lambda_8 \lambda_{10}) \frac{u_3^8}{8!} + \cdots, \\ \mu_2 &= 2\lambda_8 \frac{u_3^3}{3!} + (24\lambda_4 \lambda_{10} + 4\lambda_6 \lambda_8) \frac{u_3^5}{5!} + (160\lambda_{10}^2 + 264\lambda_4 \lambda_6 \lambda_{10} + 6\lambda_6^2 \lambda_8 - 36\lambda_4 \lambda_8^2) \frac{u_3^7}{7!} + \cdots, \\ \mu_3 &= 2 + 2\lambda_6 \frac{u_3^2}{2!} + (2\lambda_6^2 + 4\lambda_4 \lambda_8) \frac{u_3^4}{4!} + (12\lambda_4 \lambda_6 \lambda_8 + 32\lambda_8 \lambda_{10} + 2\lambda_6^3 + 48\lambda_4^2 \lambda_{10}) \frac{u_3^6}{6!} + \cdots. \end{aligned}$$

4. The ultra-elliptic integrals

In [4], the inversion problem of the ultra-elliptic integrals is considered. In this section, we will summarize the main results in [4]. Proposition 18 is not described in [4].

In this section, we assume $g = 2$. Let us take a point $P_* \in V$ and an open neighborhood U_* of this point that is homeomorphic to an open disk in $\mathbb{C}$. We fix a path γ_* on the curve V from ∞ to P_* . Let us consider the holomorphic mappings

$$I_1 : U_* \rightarrow \mathbb{C}, \quad P = (x, y) \mapsto \int_{\infty}^P du_1,$$

$$I_3 : U_* \rightarrow \mathbb{C}, \quad P = (x, y) \mapsto \int_{\infty}^P du_3,$$

where as the path of integration we choose the composition of the path γ_* from ∞ to the point P_* and any path in the neighborhood U_* from P_* to the point P . We consider the meromorphic function on $\mathbb{C}^2$

$$f = -\frac{\sigma_3}{\sigma_1}.$$

We assume $P_* \neq \infty$. If we take the open neighborhood U_* sufficiently small, then I_3 is injective. Let $\varphi(u)$ be the implicit function defined by $\sigma(\varphi(u), u) = 0$ around $(I_1(P_*), I_3(P_*))$. We define the function $F(u) = f(\varphi(u), u)$.

PROPOSITION 11. ([4]) *Set $u = I_3(P)$, where $P = (x, y) \in U_*$. Then $x = F(u)$ and $y = -F'(u)/2$, where F' is the derivative of F with respect to u .*

THEOREM 8. ([4]) *The function $F(u)$ satisfies the following ordinary differential equations:*

$$(F'/2)^2 = F^5 + \lambda_4 F^3 + \lambda_6 F^2 + \lambda_8 F + \lambda_{10}, \quad (36)$$

$$F'' = 10F^4 + 6\lambda_4 F^2 + 4\lambda_6 F + 2\lambda_8. \quad (37)$$

From Proposition 11 and Theorem 8, one can obtain the series expansion of $F(u)$. Since the function $F(u)$ is holomorphic in a neighborhood of $u^* = I_3(P_*)$, the expansion in the neighborhood of this point has the form

$$F(u) = \sum_{n=0}^{\infty} \tilde{p}_{3n+2} (u - u^*)^n, \quad \tilde{p}_{3n+2} \in \mathbb{C}. \quad (38)$$

PROPOSITION 12. ([4]) *Set $P_* = (x_*, y_*)$. Then in the expansion (38) we have $\tilde{p}_2 = x_*$ and $\tilde{p}_5 = -2y_*$.*

We set $\deg \tilde{p}_2 = 2$ and $\deg \tilde{p}_5 = 5$.

PROPOSITION 13. ([4]) *The coefficients $\tilde{p}_{3n+2}$ in the expansion (38) are determined from the following recurrence relations:*

- $\tilde{p}_8 = 5\tilde{p}_2^4 + 3\lambda_4 \tilde{p}_2^2 + 2\lambda_6 \tilde{p}_2 + \lambda_8,$
- $(n+2)(n+1)\tilde{p}_{3n+8} = 10 \sum_{(n_1, n_2, n_3, n_4) \in S_1} \tilde{p}_{3n_1+2} \tilde{p}_{3n_2+2} \tilde{p}_{3n_3+2} \tilde{p}_{3n_4+2} +$
 $+ 6\lambda_4 \sum_{(n_1, n_2) \in S_2} \tilde{p}_{3n_1+2} \tilde{p}_{3n_2+2} + 4\lambda_6 \tilde{p}_{3n+2}, \quad n \geq 1, \text{ where}$

$$S_1 = \{(n_1, n_2, n_3, n_4) \in \mathbb{Z}_{\geq 0}^4 \mid n_1 + n_2 + n_3 + n_4 = n\}, S_2 = \{(n_1, n_2) \in \mathbb{Z}_{\geq 0}^2 \mid n_1 + n_2 = n\},$$

and the coefficient $\tilde{p}_{3n+2}$ is a homogeneous polynomial in $\mathbb{Q}[\tilde{p}_2, \tilde{p}_5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree $3n+2$, if $\tilde{p}_{3n+2} \neq 0$.

We assume $P_* \neq (0, \pm\sqrt{\lambda_{10}})$. If we take the open neighborhood U_* sufficiently small, then I_1 is injective. Let $\eta(u)$ be the implicit function defined by $\sigma(u, \eta(u)) = 0$ around $(I_1(P_*), I_3(P_*))$. Let us define the function $G(u) = f(u, \eta(u))$.

PROPOSITION 14. ([4]) For $P = (x, y) \in U_*$ let $u = I_1(P)$. Then we have $x = G(u)$ and $y = -G(u)G'(u)/2$, where G' is the derivative of G with respect to u .

THEOREM 9. ([4]) The function $G(u)$ satisfies the following ordinary differential equations:

$$(GG'/2)^2 = G^5 + \lambda_4 G^3 + \lambda_6 G^2 + \lambda_8 G + \lambda_{10}, \quad (39)$$

$$G^4(G''' - 12GG') - 4\lambda_8 GG' - 12\lambda_{10}G' = 0. \quad (40)$$

Let us assume that $P_* \neq (0, \pm\sqrt{\lambda_{10}})$ and $P_* \neq \infty$. Using Proposition 14 and Theorem 9, one can obtain the series expansion of the function $G(u)$. Since the function $G(u)$ is holomorphic in the neighborhood of the point $u^* = I_1(P_*)$, this expansion in the neighborhood of this point has the form

$$G(u) = \sum_{n=0}^{\infty} \tilde{q}_{n+2}(u - u^*)^n, \quad \tilde{q}_{n+2} \in \mathbb{C}. \quad (41)$$

PROPOSITION 15. ([4]) Let $P_* = (x_*, y_*)$. Then we have $\tilde{q}_2 = x_*$ and $\tilde{q}_3 = -2y_*/x_*$.

Let us set $\deg \tilde{q}_2 = 2$ and $\deg \tilde{q}_3 = 3$.

PROPOSITION 16. ([4]) The coefficients $\tilde{q}_{n+2}$ are determined from the following recurrence relations:

$$\begin{aligned} & \bullet \tilde{q}_4 = \tilde{q}_2^{-3}(3\tilde{q}_2^5 + \lambda_4\tilde{q}_2^3 - \lambda_8\tilde{q}_2 - 2\lambda_{10}), \\ & \bullet \tilde{q}_2^3(n+2)(n+1)\tilde{q}_{n+4} = - \sum_{k=0}^{n-1} \left\{ (k+2)(k+1)\tilde{q}_{k+4} \sum_{(n_1, n_2, n_3) \in T_1^{(k)}} \tilde{q}_{n_1+2} \tilde{q}_{n_2+2} \tilde{q}_{n_3+2} \right\} + \\ & + 6 \sum_{(n_1, n_2, n_3, n_4, n_5) \in T_2} \tilde{q}_{n_1+2} \tilde{q}_{n_2+2} \tilde{q}_{n_3+2} \tilde{q}_{n_4+2} \tilde{q}_{n_5+2} + \\ & + 2\lambda_4 \sum_{(n_1, n_2, n_3) \in T_3} \tilde{q}_{n_1+2} \tilde{q}_{n_2+2} \tilde{q}_{n_3+2} - 2\lambda_8 \tilde{q}_{n+2}, \quad n \geq 1, \text{ where} \end{aligned}$$

$T_1^{(k)} = \{(n_1, n_2, n_3) \in \mathbb{Z}_{\geq 0}^3 \mid n_1 + n_2 + n_3 = n - k\}$, $T_2 = \{(n_1, n_2, n_3, n_4, n_5) \in \mathbb{Z}_{\geq 0}^5 \mid n_1 + n_2 + n_3 + n_4 + n_5 = n\}$, $T_3 = \{(n_1, n_2, n_3) \in \mathbb{Z}_{\geq 0}^3 \mid n_1 + n_2 + n_3 = n\}$, and the coefficient $\tilde{q}_{n+2}$ is a homogeneous polynomial in $\mathbb{Q}[\tilde{q}_2, \tilde{q}_3, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree $n+2$ if $\tilde{q}_{n+2} \neq 0$.

Let us take $P_* = \infty$ and the path γ_* defined by the function $R : [0, 1] \rightarrow V$ such that $R(r) = \infty$ for any point $r \in [0, 1]$. Then we have $(I_1(P_*), I_3(P_*)) = (0, 0)$.

PROPOSITION 17. ([4]) In a neighborhood of the point $u = 0$, the function $G(u)$ is given by a series

$$G(u) = \frac{1}{u^2} - \frac{\lambda_4}{5}u^2 - \frac{\lambda_6}{7}u^4 + \left(\frac{\lambda_4^2}{75} - \frac{\lambda_8}{9}\right)u^6 + \left(\frac{3}{385}\lambda_4\lambda_6 - \frac{\lambda_{10}}{11}\right)u^8 + \sum_{n \geq 10} \tau_{n+2}u^n,$$

where the coefficient τ_{n+2} is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree $n + 2$ if $\tau_{n+2} \neq 0$.

PROPOSITION 18. The coefficients τ_n for $n \geq 12$ are determined from the following recurrence formula :

$$\begin{aligned} (n+1)\tau_n &= \sum_{(n_1, n_2, n_3, n_4) \in T_1} \frac{n_3-2}{2} \frac{n_4-2}{2} \tau_{n_1} \tau_{n_2} \tau_{n_3} \tau_{n_4} \\ &- \sum_{(n_1, n_2, n_3, n_4, n_5) \in T_2} \tau_{n_1} \tau_{n_2} \tau_{n_3} \tau_{n_4} \tau_{n_5} - \lambda_4 \sum_{(n_1, n_2, n_3) \in T_3} \tau_{n_1} \tau_{n_2} \tau_{n_3} \\ &- \lambda_6 \sum_{(n_1, n_2) \in T_4} \tau_{n_1} \tau_{n_2} - \lambda_8 \tau_{n-8}, \end{aligned}$$

where $T_1 = \{(n_1, n_2, n_3, n_4) \in \mathbb{Z}_{\geq 0}^4 \mid n_1 + \dots + n_4 = n, 0 \leq n_1, \dots, n_4 < n\}$, $T_2 = \{(n_1, n_2, n_3, n_4, n_5) \in \mathbb{Z}_{\geq 0}^5 \mid n_1 + \dots + n_5 = n, 0 \leq n_1, \dots, n_5 < n\}$, $T_3 = \{(n_1, n_2, n_3) \in \mathbb{Z}_{\geq 0}^3 \mid n_1 + n_2 + n_3 = n - 4\}$, and $T_4 = \{(n_1, n_2) \in \mathbb{Z}_{\geq 0}^2 \mid n_1 + n_2 = n - 6\}$.

PROOF. Let

$$G(u) = \frac{1}{u^2} + \sum_{n=0}^{\infty} \tau_{n+2}u^n. \quad (42)$$

Then we have

$$\begin{aligned} -\frac{G'(u)}{2} &= \frac{1}{u^3} - \sum_{n=0}^{\infty} \frac{n+1}{2} \tau_{n+3}u^n, \\ u^2 G(u) &= \sum_{n=0}^{\infty} \tau_n u^n, \quad u^3 \frac{G'(u)}{2} = \sum_{n=0}^{\infty} \frac{n-2}{2} \tau_n u^n, \end{aligned}$$

where $\tau_0 = 1$ and $\tau_1 = 0$. By substituting (42) into (39) and multiplying the both sides by u^{10} , we obtain

$$\begin{aligned} \left(\sum_{n=0}^{\infty} \tau_n u^n\right)^2 \left(\sum_{n=0}^{\infty} \frac{n-2}{2} \tau_n u^n\right)^2 &= \left(\sum_{n=0}^{\infty} \tau_n u^n\right)^5 + \lambda_4 u^4 \left(\sum_{n=0}^{\infty} \tau_n u^n\right)^3 \\ &+ \lambda_6 u^6 \left(\sum_{n=0}^{\infty} \tau_n u^n\right)^2 + \lambda_8 u^8 \sum_{n=0}^{\infty} \tau_n u^n + \lambda_{10} u^{10}. \end{aligned}$$

By comparing the coefficient of u^n for $n \geq 12$, we obtain the statement of the proposition. $\square$

PROPOSITION 19. ([4]) There exists the formula

$$G(u) = \wp(u) + g(u),$$

where $g(u)$ is a holomorphic function that in a neighborhood of the point $u = 0$ is given by a series

$$g(u) = -\frac{\lambda_8}{9}u^6 - \frac{\lambda_{10}}{11}u^8 + \sum_{n \geq 10} \tilde{\tau}_{n+2}u^n.$$

Here the coefficient $\tilde{\tau}_{n+2}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree $n+2$ if $\tilde{\tau}_{n+2} \neq 0$.

Denote by $G_d(u)$ the formal Laurent series obtained from $G(u)$ by substitution $\lambda_8 = \lambda_{10} = 0$ in the series expansion of this function in a neighborhood of the point $u = 0$.

COROLLARY 4. ([4]) *We have $G_d(u) = \wp(u)$.*

5. Number-theoretical properties of the generalized Bernoulli–Hurwitz numbers for the curve of genus 2

In this section, we assume $g = 2$. Let V be a hyperelliptic curve of genus 2 defined by

$$y^2 = x^5 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}. \quad (43)$$

We take an open neighborhood U_* of ∞ such that U_* is homeomorphic to an open disk in $\mathbb{C}$. We consider the map

$$I_1 : U_* \rightarrow \mathbb{C}, \quad P = (x, y) \mapsto \int_{\infty}^P -\frac{x}{2y} dx,$$

where as the path of integration we take any path in U_* from ∞ to P . For $P = (x, y) \in U_*$, let $u = I_1(P)$. If U_* is sufficiently small, then the map I_1 is biholomorphism. Therefore, we can regard x and y as functions of u . From Proposition 14, we have $x(u) = G(u)$ and $y(u) = -G(u)G'(u)/2$. From Proposition 17, the function $x(u)$ can be expanded around $u = 0$ as

$$x(u) = \frac{1}{u^2} + \sum_{n=4}^{\infty} \frac{C_n}{n} \frac{u^{n-2}}{(n-2)!}, \quad (44)$$

where the coefficient C_n is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $C_n \neq 0$.

LEMMA 19. *We have*

$$y(u) = -\frac{1}{4}(x(u)^2)',$$

where $(x(u)^2)'$ denotes the derivative of $x(u)^2$ with respect to u .

PROOF. From Proposition 14, we obtain the statement of the lemma. $\square$

From (44) and Lemma 19, we find that $y(u)$ can be expanded around $u = 0$ as

$$y(u) = \frac{1}{u^5} + \sum_{n=6}^{\infty} \frac{D_n}{n} \frac{u^{n-5}}{(n-5)!}, \quad (45)$$

where the coefficient D_n is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $D_n \neq 0$. Then C_n and D_n are called *generalized Bernoulli–Hurwitz numbers*. In particular, we find that $C_n = D_n = 0$ for any odd integer n . In [38], the hyperelliptic curve of genus 2 defined by $y^2 = x^5 - 1$ is considered and the following formulae are proved.

THEOREM 10. ([38]) *For the curve $y^2 = x^5 - 1$, we have*

$$\begin{aligned} \frac{C_{10n}}{10n} &\equiv - \sum_{p: \text{prime}, p \equiv 1 \pmod{10}, 10n=a(p-1)} \frac{a|_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a \pmod{\mathbb{Z}}, \\ \frac{D_{10n}}{10n} &\equiv - \sum_{p: \text{prime}, p \equiv 1 \pmod{10}, 10n=a(p-1)} \frac{(4!a)|_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a \pmod{\mathbb{Z}}, \end{aligned}$$

where $A_p = (-1)^{(p-1)/10} \cdot \begin{pmatrix} (p-1)/2 \\ (p-1)/10 \end{pmatrix}$.

In this section, we will generalize the method of [38] to the curve V defined by (43) and derive some number-theoretical properties of the generalized Bernoulli-Hurwitz numbers for the curve V .

PROPOSITION 20. *It is possible to take a local parameter z of V around ∞ such that*

$$x = \frac{1}{z^2}, \quad y = \frac{1}{z^5} \left(1 + \sum_{n=4}^{\infty} a_n z^n \right),$$

where a_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $a_n \neq 0$.

PROOF. It is possible to take a local parameter z_1 such that

$$x = \frac{1}{z_1^2}.$$

The expansion of y around ∞ with respect to z_1 takes the following form

$$y = \frac{\alpha}{z_1^5} (1 + O(z_1)), \quad \alpha \in \mathbb{C}.$$

By substituting the above expansions into (43), multiplying the both sides by z_1^{10} , and comparing the coefficient of z_1^0 , we obtain

$$\alpha^2 = 1.$$

If $\alpha = 1$, then we set $z = z_1$. If $\alpha = -1$, then we set $z = -z_1$. Then we have

$$x = \frac{1}{z^2}, \quad y = \frac{1}{z^5} \left(1 + \sum_{n=1}^{\infty} a_n z^n \right),$$

where $a_n \in \mathbb{C}$. By substituting the above expressions into (43), we obtain

$$\left(1 + \sum_{n=1}^{\infty} a_n z^n \right)^2 = 1 + \lambda_4 z^4 + \lambda_6 z^6 + \lambda_8 z^8 + \lambda_{10} z^{10}.$$

From the above equation, we can find that a_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $a_n \neq 0$ recursively. $\square$

We can regard $u(z)$ as a function defined around $z = 0$.

PROPOSITION 21. *The function $u(z)$ is expanded around $z = 0$ as*

$$u(z) = z + \sum_{n=1}^{\infty} f_n \frac{z^{n+1}}{n+1}, \tag{46}$$

where $f_1 = f_2 = f_3 = 0$ and f_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $f_n \neq 0$.

PROOF. From Proposition 20, we have

$$u = \int_0^z -\frac{z^{-2} \cdot (-2)z^{-3}}{2z^{-5}(1 + \sum_{n=4}^{\infty} a_n z^n)} dz = \int_0^z \left(1 + \sum_{n=4}^{\infty} a_n z^n \right)^{-1} dz.$$

From Proposition 20, we obtain the statement of the proposition. $\square$

For positive integers n and k such that $n \geq k$, we use the notation

$$(n)_k = n(n-1) \cdots (n-k+1).$$

We consider the inverse mapping $z(u)$ of $u(z)$. The expansions of z^{-k} , where $k = 1, 2, 3, 4$, have the following forms :

$$\frac{1}{z^k} = \frac{1}{u^k} + \sum_{n=4}^{\infty} \frac{C_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!}, \quad k = 1, 2, 3, 4, \quad (47)$$

where $C_n^{(k)}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $C_n^{(k)} \neq 0$.

From Theorem 7, we obtain

$$\frac{C_n^{(1)}}{n} = \sum_{n=a(p-1), p \geq 5 : \text{prime}} \frac{z_1(p, n)}{p^{1+\text{ord}_p a}} f_{p-1}^a + \tilde{f}_n, \quad (48)$$

where $z_1(p, n) \in \mathbb{Z}$ and $\tilde{f}_n \in \mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$.

LEMMA 20. For $k = 1, 2, 3$, we have

$$k \sum_{n=4}^{\infty} \frac{C_n^{(k+1)}}{(n)_{k+1}} \frac{u^{n-k}}{(n-k)!} + \sum_{n=4}^{\infty} \frac{C_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!} = k \sum_{n=4}^{\infty} f_n \frac{z^{n-k}}{n-k}.$$

PROOF. For $k = 1, 2, 3$, we have

$$\int_0^u \left(\frac{1}{z^{k+1}} - \frac{1}{u^{k+1}} \right) du = \sum_{n=4}^{\infty} \frac{C_n^{(k+1)}}{(n)_{k+1}} \frac{u^{n-k}}{(n-k)!}.$$

By differentiating the both sides of (46) with respect to u , we obtain

$$1 = \frac{dz}{du} + \sum_{n=4}^{\infty} f_n z^n \frac{dz}{du}.$$

By dividing the both sides of the above equation by z^{k+1} , we have

$$\frac{1}{z^{k+1}} = \frac{1}{z^{k+1}} \frac{dz}{du} + \sum_{n=4}^{\infty} f_n z^{n-k-1} \frac{dz}{du}.$$

Therefore we have

$$\int_0^u \left(\frac{1}{z^{k+1}} - \frac{1}{u^{k+1}} \right) du = -\frac{1}{k} \frac{1}{z^k} + \sum_{n=4}^{\infty} f_n \frac{z^{n-k}}{n-k} + \frac{1}{k} \frac{1}{u^k} = -\frac{1}{k} \sum_{n=4}^{\infty} \frac{C_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!} + \sum_{n=4}^{\infty} f_n \frac{z^{n-k}}{n-k}.$$

Thus we have

$$k \sum_{n=4}^{\infty} \frac{C_n^{(k+1)}}{(n)_{k+1}} \frac{u^{n-k}}{(n-k)!} + \sum_{n=4}^{\infty} \frac{C_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!} = k \sum_{n=4}^{\infty} f_n \frac{z^{n-k}}{n-k}.$$

□

LEMMA 21. ([27], [38]) Let R_1 and R_2 be two integral domains with characteristic 0 satisfying $R_1 \subset R_2$. We consider a formal power series of z

$$h(z) = \sum_{n=0}^{\infty} \alpha_n \frac{z^n}{n!}, \quad \alpha_n \in R_2.$$

If $\alpha_0, \dots, \alpha_{n-1}$ belong to R_1 , and there is a polynomial F of n variables over R_1 such that

$$h^{(n)}(z) = F(h(z), h'(z), \dots, h^{(n-1)}(z)),$$

where $h^{(n)}(z)$ is the n -th derivative of $h(z)$ with respect to z , then we have $h(z) \in R_1\langle\langle z \rangle\rangle$.

LEMMA 22. ([27], [38]) Let R be an integral domain with characteristic 0 and

$$h(z) = z + O(z^2) \in R\langle\langle z \rangle\rangle.$$

Then for any positive integer m ,

$$\frac{h(z)^m}{m!}$$

also belongs to $R\langle\langle z \rangle\rangle$.

LEMMA 23. ([27], [38], [44]) Let R be an integral domain with characteristic 0 and

$$w(z) = z + O(z^2) \in R\langle\langle z \rangle\rangle.$$

Then, the formal inverse series $z(w) = w + O(w^2)$ belongs to $R\langle\langle w \rangle\rangle$.

We set $\deg u = -1$.

PROPOSITION 22. We have $z(u) = u + O(u^2) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]\langle\langle u \rangle\rangle$ and $z(u)$ is homogeneous of degree -1 with respect to $u, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}$.

PROOF. We have $x(u) = z(u)^{-2}$. Therefore we have $x'(u) = -2z(u)^{-3}z'(u)$. From Lemma 19, we obtain $y(u) = z(u)^{-5}z'(u)$. From (43), we obtain

$$(z')^2 = 1 + \lambda_4 z^4 + \lambda_6 z^6 + \lambda_8 z^8 + \lambda_{10} z^{10}.$$

By differentiating the both sides of the above equation with respect to u and dividing by $2z'$, we obtain

$$z'' = 2\lambda_4 z^3 + 3\lambda_6 z^5 + 4\lambda_8 z^7 + 5\lambda_{10} z^9. \quad (49)$$

We define the polynomial $F(Z_1, Z_2)$ over $\mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ by

$$F(Z_1, Z_2) = 2\lambda_4 Z_1^3 + 3\lambda_6 Z_1^5 + 4\lambda_8 Z_1^7 + 5\lambda_{10} Z_1^9.$$

From (49), we have $z'' = F(z, z')$. Since the function $z(u)$ is expanded around $u = 0$ as

$$z(u) = u + O(u^2),$$

we have $z(0) = 0$ and $z'(0) = 1$. From Lemma 21, we have $z(u) \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]\langle\langle u \rangle\rangle$. $\square$

LEMMA 24. For $n \geq 4$, we have the following relations.

$$\begin{aligned}
 (i) \quad & \frac{C_n^{(2)}}{(n)_2} + \frac{C_n^{(1)}}{n} \in \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (ii) \quad & 2 \frac{C_n^{(3)}}{(n)_3} + \frac{C_n^{(2)}}{(n)_2} \in \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (iii) \quad & 3 \frac{C_n^{(4)}}{(n)_4} + \frac{C_n^{(3)}}{(n)_3} \in 3 \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (iv) \quad & \frac{C_n^{(1)}}{n} + 6 \frac{C_n^{(4)}}{(n)_4} \in \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]
 \end{aligned}$$

PROOF. In Lemma 20, we set $k = 1$. Then we have

$$\sum_{n=4}^{\infty} \frac{C_n^{(2)}}{(n)_2} \frac{u^{n-1}}{(n-1)!} + \sum_{n=4}^{\infty} \frac{C_n^{(1)}}{n} \frac{u^{n-1}}{(n-1)!} = \sum_{n=4}^{\infty} f_n(n-2)! \frac{z^{n-1}}{(n-1)!}. \quad (50)$$

From Lemma 22 and Proposition 22, we have

$$\frac{z^{n-1}}{(n-1)!} \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}][\langle u \rangle].$$

By comparing the coefficient of $\frac{u^{n-1}}{(n-1)!}$ in (50) and using $f_n \in \mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$, we obtain

$$\frac{C_n^{(2)}}{(n)_2} + \frac{C_n^{(1)}}{n} \in \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}].$$

In Lemma 20, we set $k = 2$. Then we have

$$2 \sum_{n=4}^{\infty} \frac{C_n^{(3)}}{(n)_3} \frac{u^{n-2}}{(n-2)!} + \sum_{n=4}^{\infty} \frac{C_n^{(2)}}{(n)_2} \frac{u^{n-2}}{(n-2)!} = 2 \sum_{n=4}^{\infty} f_n(n-3)! \frac{z^{n-2}}{(n-2)!}. \quad (51)$$

By comparing the coefficient of $\frac{u^{n-2}}{(n-2)!}$ in (51) and using $f_n \in \mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$, we obtain

$$2 \frac{C_n^{(3)}}{(n)_3} + \frac{C_n^{(2)}}{(n)_2} \in \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}].$$

In Lemma 20, we set $k = 3$. Then we have

$$3 \sum_{n=4}^{\infty} \frac{C_n^{(4)}}{(n)_4} \frac{u^{n-3}}{(n-3)!} + \sum_{n=4}^{\infty} \frac{C_n^{(3)}}{(n)_3} \frac{u^{n-3}}{(n-3)!} = 3 \sum_{n=4}^{\infty} f_n(n-4)! \frac{z^{n-3}}{(n-3)!}. \quad (52)$$

By comparing the coefficient of $\frac{u^{n-3}}{(n-3)!}$ in (52) and using $f_n \in \mathbb{Z}[\frac{1}{2}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$, we obtain

$$3 \frac{C_n^{(4)}}{(n)_4} + \frac{C_n^{(3)}}{(n)_3} \in 3 \mathbb{Z}[1/2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}].$$

From (i), (ii), and (iii), we obtain (iv). $\square$

LEMMA 25. *It is possible to take a local parameter s of V around ∞ such that*

$$x = \frac{1}{s^2}(1 + \sum_{n=1}^{\infty} \alpha_n s^n), \quad y = \frac{1}{s^5},$$

where α_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $\alpha_n \neq 0$.

PROOF. It is possible to take a local parameter s_1 of V around ∞ such that

$$y = \frac{1}{s_1^5}.$$

The expansion of x around ∞ with respect to s_1 takes the following form

$$x = \frac{\alpha}{s_1^2}(1 + O(s_1)), \quad \alpha \in \mathbb{C}.$$

By substituting the above expansions into (43), multiplying the both sides by s_1^{10} , and comparing the coefficient of s_1^0 , we obtain

$$1 = \alpha^5.$$

There exists $\beta \in \mathbb{C}$ such that $\beta^5 = 1$ and $\beta^2 = \alpha$. Let $s = \beta^{-1}s_1$. Then we have

$$x = \frac{1}{s^2}(1 + \sum_{n=1}^{\infty} \alpha_n s^n), \quad y = \frac{1}{s^5},$$

where $\alpha_n \in \mathbb{C}$. By substituting the above expressions into (43) and multiplying the both sides by s^{10} , we obtain

$$1 = (1 + \sum_{n=1}^{\infty} \alpha_n s^n)^5 + \lambda_4 s^4 (1 + \sum_{n=1}^{\infty} \alpha_n s^n)^3 + \lambda_6 s^6 (1 + \sum_{n=1}^{\infty} \alpha_n s^n)^2 + \lambda_8 s^8 (1 + \sum_{n=1}^{\infty} \alpha_n s^n) + \lambda_{10} s^{10}.$$

From the above equation, we can find that α_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $\alpha_n \neq 0$ recursively. $\square$

We can regard $u(s)$ as a function defined around $s = 0$.

LEMMA 26. *The function $u(s)$ is expanded around $s = 0$ as*

$$u(s) = s + \sum_{n=1}^{\infty} g_n \frac{s^{n+1}}{n+1}, \tag{53}$$

where $g_1 = g_2 = g_3 = g_4 = 0$ and g_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $g_n \neq 0$.

PROOF. We have

$$x(s) = s^{-2} + \sum_{n=4}^{\infty} \alpha_n s^{n-2}, \quad x'(s) = -2s^{-3} + \sum_{n=4}^{\infty} (n-2) \alpha_n s^{n-3}.$$

Since $\alpha_n \in \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ is homogeneous of degree n if $\alpha_n \neq 0$, we have $\alpha_n = 0$ if n is odd. Therefore, all the coefficients of the expansion of $x'(s)$ are included in $2 \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$. We have

$$u(s) = \int_0^s -\frac{(s^{-2} + \sum_{n=4}^{\infty} \alpha_n s^{n-2})(-2s^{-3} + \sum_{n=4}^{\infty} (n-2) \alpha_n s^{n-3})}{2s^{-5}} ds$$

$$= \int_0^s s^5 (s^{-2} + \sum_{n=4}^{\infty} \alpha_n s^{n-2}) (s^{-3} - \sum_{n=4}^{\infty} \frac{n-2}{2} \alpha_n s^{n-3}) ds = s + \sum_{n=1}^{\infty} g_n \frac{s^{n+1}}{n+1}, \quad (54)$$

where $g_1 = g_2 = g_3 = 0$ and g_n is a homogeneous polynomial in $\mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $g_n \neq 0$. We find that the coefficient of s^{-1} in

$$(s^{-2} + \sum_{n=4}^{\infty} \alpha_n s^{n-2}) (s^{-3} - \sum_{n=4}^{\infty} \frac{n-2}{2} \alpha_n s^{n-3})$$

is equal to 0. From (54), we have $g_4 = 0$. $\square$

We consider the inverse mapping $s(u)$ of $u(s)$.

PROPOSITION 23. *We have $s(u) \in \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}][\langle u \rangle]$ and $s(u)$ is homogeneous of degree -1 with respect to $u, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}$.*

PROOF. From Lemma 26, we have $u(s) = s + O(s^2) \in \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}][\langle s \rangle]$. Therefore, from Lemma 23, we have $s(u) = u + O(u^2) \in \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}][\langle u \rangle]$. From Lemma 26, we can find that $s(u)$ is homogeneous of degree -1 with respect to $u, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}$. $\square$

Therefore the expansions of s^{-k} , where $k = 1, 2, 3, 4, 5$, have the following forms :

$$\frac{1}{s^k} = \frac{1}{u^k} + \sum_{n=6}^{\infty} \frac{D_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!}, \quad k = 1, 2, 3, 4, 5,$$

where $D_n^{(k)}$ is a homogeneous polynomial in $\mathbb{Q}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$ of degree n if $D_n^{(k)} \neq 0$. From Theorem 7, we obtain

$$\frac{D_n^{(1)}}{n} = \sum_{n=a(p-1), p \geq 7 : \text{prime}} \frac{z_2(p, n)}{p^{1+ord_{pa}}} g_{p-1}^a + \tilde{g}_n, \quad (55)$$

where $z_2(p, n) \in \mathbb{Z}$ and $\tilde{g}_n \in \mathbb{Z}[\frac{1}{5}, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]$.

LEMMA 27. *For any integer $n \geq 6$, we have*

$$ord_2 \left(\frac{D_n^{(1)}}{n} \right) \geq \left\lfloor \frac{n-1}{4} \right\rfloor.$$

PROOF. From Proposition 4, we have

$$\frac{D_n^{(1)}}{n} = \sum_{w(U)=n} \tau_U g^U.$$

Note that $g_2 = 0$ and $g_i = 0$ for any odd integer i . Therefore, from Lemma 14, we obtain the statement of the lemma. $\square$

LEMMA 28. *For $k = 1, 2, 3, 4$, we have*

$$k \sum_{n=6}^{\infty} \frac{D_n^{(k+1)}}{(n)_{k+1}} \frac{u^{n-k}}{(n-k)!} + \sum_{n=6}^{\infty} \frac{D_n^{(k)}}{(n)_k} \frac{u^{n-k}}{(n-k)!} = k \sum_{n=6}^{\infty} g_n \frac{s^{n-k}}{n-k}.$$

PROOF. We can prove this lemma in the same way as Lemma 20. $\square$

LEMMA 29. *For $n \geq 6$, we have the following relations.*

$$\begin{aligned}
 (i) \quad & \frac{D_n^{(2)}}{(n)_2} + \frac{D_n^{(1)}}{n} \in 2^3 \cdot 3 \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (ii) \quad & 2 \frac{D_n^{(3)}}{(n)_3} + \frac{D_n^{(2)}}{(n)_2} \in 2^2 \cdot 3 \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (iii) \quad & 3 \frac{D_n^{(4)}}{(n)_4} + \frac{D_n^{(3)}}{(n)_3} \in 2 \cdot 3 \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (iv) \quad & 4 \frac{D_n^{(5)}}{(n)_5} + \frac{D_n^{(4)}}{(n)_4} \in 2^2 \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \\
 (v) \quad & \frac{D_n^{(1)}}{n} - 24 \frac{D_n^{(5)}}{(n)_5} \in 2^2 \cdot 3 \mathbb{Z}[1/5, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}]
 \end{aligned}$$

PROOF. We can prove this lemma in the same way as Lemma 24. $\square$

LEMMA 30. *The function $x(u)$ satisfies the following differential equation*

$$x'' = 6x^2 + 2\lambda_4 - 2\lambda_8 x^{-2} - 4\lambda_{10} x^{-3}.$$

PROOF. From $y(u) = -x(u)x'(u)/2$ and (43), we have

$$\left(-\frac{xx'}{2}\right)^2 = x^5 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}.$$

By multiplying the above equation by x^{-2} and differentiating this equation with respect to u , we obtain the statement of the lemma. $\square$

LEMMA 31. *The first terms of C_n/n and D_n/n are as follows :*

$$\begin{aligned}
 \frac{C_4}{4} &= -\frac{2}{5}\lambda_4, \quad \frac{C_6}{6} = -\frac{2^3 \cdot 3}{7}\lambda_6, \quad \frac{C_8}{8} = \frac{2^4 \cdot 3}{5}\lambda_4^2 - 2^4 \cdot 5\lambda_8, \\
 \frac{C_{10}}{10} &= \frac{2^7 \cdot 3^3}{11}\lambda_4\lambda_6 - \frac{2^7 \cdot 3^2 \cdot 5 \cdot 7}{11}\lambda_{10}, \\
 \frac{D_6}{6} &= \frac{1}{7}\lambda_6, \quad \frac{D_8}{8} = \frac{2^2}{3}\lambda_8 - \frac{2}{5}\lambda_4^2, \quad \frac{D_{10}}{10} = \frac{2^3 \cdot 3^2 \cdot 5}{11}\lambda_{10} - \frac{2^4 \cdot 3^2}{11}\lambda_4\lambda_6.
 \end{aligned}$$

PROOF. From Proposition 17 and Lemma 19, we obtain the statement of the lemma. $\square$

THEOREM 11. (i) *For any $n \geq 4$, we have*

$$\text{ord}_2 \left(\frac{C_n}{n} \right) \geq 1, \quad \text{ord}_3 \left(\frac{C_n}{n} \right) \geq 0.$$

(ii) *For any $n \geq 6$, we have*

$$\text{ord}_2 \left(\frac{D_n}{n} \right) \geq -1, \quad \text{ord}_3 \left(\frac{D_n}{n} \right) \geq -1.$$

Let $p \geq 5$ be a prime.

(iii) *If $p-1 \nmid n$, then we have*

$$\text{ord}_p \left(\frac{C_n}{n} \right) \geq 0, \quad \text{ord}_p \left(\frac{D_n}{n} \right) \geq 0.$$

(iv) If $p - 1 \mid n$, then we have

$$\text{ord}_p \left(\frac{C_n}{n} \right) \geq -1 - \text{ord}_p a, \quad \text{ord}_p \left(\frac{D_n}{n} \right) \geq -1 - \text{ord}_p a.$$

where $n = a(p - 1)$.

PROOF. For $n \geq 4$, we have

$$\frac{C_n}{n} = \frac{C_n^{(2)}}{(n)_2}.$$

From (48) and Lemma 24 (i), we obtain

$$\text{ord}_3 \left(\frac{C_n}{n} \right) \geq 0.$$

From (48) and Lemma 24 (i), we find that if $p \geq 5$ and $p - 1 \nmid n$, then we have

$$\text{ord}_p \left(\frac{C_n}{n} \right) \geq 0,$$

if $p \geq 5$ and $p - 1 \mid n$, then we have

$$\text{ord}_p \left(\frac{C_n}{n} \right) \geq -1 - \text{ord}_p a,$$

where $n = a(p - 1)$. From $x^2 = 1/z^4$ and Lemma 19, for $n \geq 6$, we have

$$\frac{D_n}{n} = -\frac{1}{4} \frac{C_n^{(4)}}{(n)_4}. \quad (56)$$

From Lemma 24 (iv), (48), and (56), we obtain if $p \geq 5$ and $p - 1 \nmid n$,

$$\text{ord}_p \left(\frac{D_n}{n} \right) \geq 0,$$

if $p \geq 5$ and $p - 1 \mid n$,

$$\text{ord}_p \left(\frac{D_n}{n} \right) \geq -1 - \text{ord}_p a,$$

where $n = a(p - 1)$. Since $y = 1/s^5$, we have

$$\frac{D_n}{n} = \frac{D_n^{(5)}}{(n)_5}. \quad (57)$$

From Lemma 29 (v), (55), and (57), we obtain

$$\text{ord}_3 \left(\frac{D_n}{n} \right) \geq -1.$$

From Lemma 27, we have

$$\text{ord}_2 \left(\frac{D_n^{(1)}}{n} \right) \geq 2, \quad \text{for } n \geq 10.$$

Therefore, from Lemma 29 (v), (57), and Lemma 31, we have

$$\text{ord}_2 \left(\frac{D_n}{n} \right) \geq -1, \quad \text{for } n \geq 6.$$

From (56), we have

$$\text{ord}_2 \left(\frac{C_n^{(4)}}{(n)_4} \right) \geq 1, \quad \text{for } n \geq 6.$$

From the above equation, $x^{-1} = z^2 \in \mathbb{Z}[\lambda_4, \lambda_6, \lambda_8, \lambda_{10}] \langle \langle u \rangle \rangle$, Lemma 30, and Lemma 31, we obtain

$$\text{ord}_2 \left(\frac{C_n}{n} \right) \geq 1, \quad \text{for } n \geq 4.$$

□

REMARK 3. *Theorem 11* gives the precise information on the series expansion of the solution of the inversion problem of the ultra-elliptic integrals given in Proposition 17.

We assume $\lambda_4 = \lambda_6 = \lambda_8 = 0$ and consider the curve defined by $y^2 = x^5 + \lambda_{10}$.

LEMMA 32. *For any integer $m \geq 1$, we have*

$$\text{ord}_3 \left(\frac{C_{10m}^{(1)}}{10m} \right) \geq \left\lfloor \frac{10m-1}{6} \right\rfloor, \quad \text{ord}_5 \left(\frac{C_{10m}^{(1)}}{10m} \right) \geq \left\lfloor \frac{10m-1}{10} \right\rfloor, \quad \text{ord}_7 \left(\frac{C_{10m}^{(1)}}{10m} \right) \geq \left\lfloor \frac{10m-1}{14} \right\rfloor.$$

PROOF. From Proposition 4 and Lemma 13, we obtain the statement of the lemma. □

LEMMA 33. ([38]) *For $m \geq 1$, we have the following relations.*

$$\begin{aligned} (i) \quad & \frac{C_{10m}^{(2)}}{(10m)_2} + \frac{C_{10m}^{(1)}}{10m} \in 3^2 \cdot 5 \cdot 7 \mathbb{Z}[1/2, \lambda_{10}] \\ (ii) \quad & 2 \frac{C_{10m}^{(3)}}{(10m)_3} + \frac{C_{10m}^{(2)}}{(10m)_2} \in 3^2 \cdot 5 \cdot 7 \mathbb{Z}[1/2, \lambda_{10}] \\ (iii) \quad & 3 \frac{C_{10m}^{(4)}}{(10m)_4} + \frac{C_{10m}^{(3)}}{(10m)_3} \in 3^3 \cdot 5 \mathbb{Z}[1/2, \lambda_{10}] \\ (iv) \quad & 6 \frac{C_{10m}^{(4)}}{(10m)_4} + \frac{C_{10m}^{(1)}}{10m} \in 3^2 \cdot 5 \mathbb{Z}[1/2, \lambda_{10}] \end{aligned}$$

PROOF. Since $\lambda_4 = \lambda_6 = \lambda_8 = 0$, we have $f_n = 0$ for $1 \leq n \leq 9$ in (46). We can prove this lemma in the same way as Lemma 24. □

LEMMA 34. ([38]) *For $m \geq 1$, we have the following relations.*

$$\begin{aligned} (i) \quad & \frac{D_{10m}^{(2)}}{(10m)_2} + \frac{D_{10m}^{(1)}}{10m} \in 2^7 \cdot 3^2 \cdot 7 \mathbb{Z}[1/5, \lambda_{10}] \\ (ii) \quad & 2 \frac{D_{10m}^{(3)}}{(10m)_3} + \frac{D_{10m}^{(2)}}{(10m)_2} \in 2^5 \cdot 3^2 \cdot 7 \mathbb{Z}[1/5, \lambda_{10}] \\ (iii) \quad & 3 \frac{D_{10m}^{(4)}}{(10m)_4} + \frac{D_{10m}^{(3)}}{(10m)_3} \in 2^4 \cdot 3^3 \mathbb{Z}[1/5, \lambda_{10}] \\ (iv) \quad & 4 \frac{D_{10m}^{(5)}}{(10m)_5} + \frac{D_{10m}^{(4)}}{(10m)_4} \in 2^5 \cdot 3 \mathbb{Z}[1/5, \lambda_{10}] \\ (v) \quad & -24 \frac{D_{10m}^{(5)}}{(10m)_5} + \frac{D_{10m}^{(1)}}{10m} \in 2^5 \cdot 3^2 \mathbb{Z}[1/5, \lambda_{10}] \end{aligned}$$

PROOF. Since $\lambda_4 = \lambda_6 = \lambda_8 = 0$, we have $g_n = 0$ for $1 \leq n \leq 9$ in (53). We can prove this lemma in the same way as Lemma 24. $\square$

For the curve $y^2 = x^5 + \lambda_{10}$, we obtain the following theorem.

THEOREM 12. *For $m \geq 1$, we have*

$$\text{ord}_2 \left(\frac{C_{10m}}{10m} \right) \geq 2, \quad \text{ord}_3 \left(\frac{C_{10m}}{10m} \right) \geq 2, \quad \text{ord}_5 \left(\frac{C_{10m}}{10m} \right) \geq 1, \quad \text{ord}_7 \left(\frac{C_{10m}}{10m} \right) \geq 1.$$

$$\text{ord}_2 \left(\frac{D_{10m}}{10m} \right) \geq 2, \quad \text{ord}_3 \left(\frac{D_{10m}}{10m} \right) \geq 1, \quad \text{ord}_5 \left(\frac{D_{10m}}{10m} \right) \geq 1, \quad \text{ord}_7 \left(\frac{D_{10m}}{10m} \right) \geq 0.$$

PROOF. From Lemma 32, Lemma 33 (i), and Lemma 31, for $m \geq 1$, we have

$$\text{ord}_3 \left(\frac{C_{10m}}{10m} \right) \geq 2, \quad \text{ord}_5 \left(\frac{C_{10m}}{10m} \right) \geq 1, \quad \text{ord}_7 \left(\frac{C_{10m}}{10m} \right) \geq 1.$$

From Lemma 33 (iv), for $m \geq 1$, we have

$$\text{ord}_3 \left(\frac{C_{10m}^{(4)}}{(10m)_4} \right) \geq 1, \quad \text{ord}_5 \left(\frac{C_{10m}^{(4)}}{(10m)_4} \right) \geq 1, \quad \text{ord}_7 \left(\frac{C_{10m}^{(4)}}{(10m)_4} \right) \geq 0.$$

From (56), we have

$$\text{ord}_3 \left(\frac{D_{10m}}{10m} \right) \geq 1, \quad \text{ord}_5 \left(\frac{D_{10m}}{10m} \right) \geq 1, \quad \text{ord}_7 \left(\frac{D_{10m}}{10m} \right) \geq 0.$$

From Lemma 27, for $m \geq 3$, we have

$$\text{ord}_2 \left(\frac{D_{10m}^{(1)}}{10m} \right) \geq 7.$$

From Lemma 34 (v), Lemma 31, and $D_{20}/20 = -2^{13} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 13 \cdot \lambda_{10}^2/11$, for $m \geq 1$, we have

$$\text{ord}_2 \left(\frac{D_{10m}}{10m} \right) \geq 2.$$

From (56), we have

$$\text{ord}_2 \left(\frac{C_{10m}^{(4)}}{(10m)_4} \right) \geq 4.$$

From Lemma 30, we have

$$\text{ord}_2 \left(\frac{C_{10m}}{10m} \right) \geq 2.$$

$\square$

Acknowledgements. This work was (partly) supported by Osaka City University Advanced Mathematical Institute (MEXT Joint Usage/Research Center on Mathematics and Theoretical Physics).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. A. Adelberg. Universal Higher Order Bernoulli Numbers and Kummer and Related Congruences // J. Number Theory, Vol. 84, Issue 1, 2000, 119–135.
2. A. Adelberg. Kummer Congruences For Universal Bernoulli Numbers And Related Congruences For Poly-Bernoulli Numbers // Int. Math. J., Vol. 1, No. 1, 2002, 53–63.
3. A. Adelberg. Universal Kummer congruences mod prime powers // J. Number Theory, Vol. 109, Issue 2, 2004, 362–378.
4. T. Ayano, V. M. Buchstaber, Ultraelliptic integrals and two-dimensional sigma function. // Funct. Anal. Appl., 53:3, 2019, 157–173.
5. H. F. Baker. On the hyperelliptic sigma functions // Amer. J. Math., Vol. 20, No. 4, 1898, 301–384.
6. H. F. Baker. On a system of differential equations leading to periodic functions // Acta Math., Vol. 27, 1903, 135–156.
7. H. F. Baker. An introduction to the theory of multiply periodic functions // Cambridge University Press, Cambridge, 1907, available at <http://name.umd.umich.edu/ACR0014.0001.001>.
8. H. F. Baker. Abelian functions. Abel's theorem and the allied theory of theta functions // Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1995.
9. V. M. Buchstaber. The Chern-Dold Character in Cobordisms, I // Math.USSR Sbornik, 12:4, 1970, 573–594.
10. V. M. Buchstaber, Polynomial dynamical systems and the Korteweg-de Vries equation. // Proc. Steklov Inst. Math., 294, 2016, 176–200, arXiv:1605.04061.
11. V. M. Buchstaber, E. Yu. Bunkova, Lie algebras of heat operators in nonholonomic frame. // arXiv:1911.08266v2 [math-ph] 28 Nov 2019.
12. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin. Hyperelliptic Kleinian functions and applications // Solitons, Geometry and Topology: On the Crossroad, V. M. Buchstaber, S. P. Novikov Editors, AMS Trans., 179:2, 1997, 1–33.
13. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin. Kleinian functions, hyperelliptic Jacobians and applications // Reviews in Mathematics and Math. Physics, I. M. Krichever, S. P. Novikov Editors, v. 10, part 2, Gordon and Breach, London, 1997, 3–120.
14. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin. Rational analogues of Abelian functions // Functional Anal. Appl., 33:2, 1999, 83–94.
15. V. M. Buchstaber, V. Z. Enolskii, D. V. Leykin. Multi-dimensional sigma functions // arXiv:1208.0990[math-ph] (v1), 5 Aug 2012.
16. V. M. Buchstaber, A. V. Ustinov, Coefficient rings of formal group laws. // Sb. Math., 206:11, 2015, 1524–1563.
17. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin, Multi-variable sigma-functions: old and new results. // arXiv:1810.11079 v1 [nlin.SI], 25 Oct 2018.

18. V. M. Buchstaber, D. V. Leykin. Heat Equations in a Nonholonomic Frame // *Funct. Anal. Appl.*, 38:2, 2004, 88–101.
19. V. M. Buchstaber, D. V. Leykin. Addition laws on Jacobian varieties of plane algebraic curves // *Nonlinear dynamics, Proceedings of the Steklov Math. Inst.*, 251:4, 2005, 49–120.
20. V. M. Buchstaber, D. V. Leykin. Solution of the problem of differentiation of Abelian functions over parameters for families of (n, s) -curves // *Funct. Anal. Appl.*, 42:4, 2008, 268–278.
21. E. Yu. Bunkova. Weierstrass Sigma Function Coefficients Divisibility Hypothesis // *arXiv:1701.00848*, 2017.
22. F. Clarke. The universal von Staudt theorems // *Transactions of the American Mathematical Society*, Vol. 315, No. 2, 1989, 591–603.
23. A. V. Domrin. Uniqueness theorem for the two-dimensional sigma function // *Funct. Anal. Appl.*, Vol. 54, Issue 1, 2020.
24. J. C. Eilbeck, J. Gibbons, Y. Ônishi, S. Yasuda. Theory of Heat Equations for Sigma Functions // *arXiv:1711.08395*, 2018.
25. J. C. Eilbeck, Y. Ônishi. Recursion relations on the power series expansion of the universal Weierstrass sigma function // *RIMS Kôkyûroku Bessatsu*, 2019.
26. F. Hirzebruch. *Topological methods in algebraic geometry* // Springer-Verlag, 1966.
27. A. Hurwitz. Ueber die Entwicklungscoefficienten der lemniscatischen Functionen // *Math. Ann.*, Vol. 51, 1898, 196–226.
28. F. Klein. Ueber hyperelliptische Sigmafunctionen // *Math. Ann.*, Vol. 27, Issue 3, 1886, 431–464.
29. F. Klein. Ueber hyperelliptische Sigmafunctionen // *Math. Ann.*, Vol. 32, Issue 3, 1888, 351–380.
30. F. Klein. Vorbemerkungen zu den Arbeiten über hyperelliptische und Abelsche Funktionen // *Gesammelte Mathematische Abhandlungen*, Vol. 3, Teubner, Berlin, 1923, s. 317–322.
31. F. Klein. Über hyperelliptische Sigmafunctionen // *Gesammelte Mathematische Abhandlungen*, Vol. 3, Teubner, Berlin, 1923, 323–387.
32. M. Lazard. Sur les groupes de Lie formels a un parametre. // *Bull. Soc. Math. France*, 83, 1955, 251–274.
33. A. Nakayashiki. On algebraic expressions of sigma functions for (n, s) curves // *Asian J. Math.*, Vol. 14, No. 2, 2010, 175–212, *arXiv:0803.2083*.
34. A. Nakayashiki. Sigma function as a tau function // *Int. Math. Res. Not.*, Vol. 2010, No. 3, 2009, 373–394, *arXiv:0904.0846*.
35. A. Nakayashiki. Tau Function Approach to Theta Functions // *Int. Math. Res. Not.*, Vol. 2016, Issue 17, 2016, 5202–5248.
36. S. P. Novikov. The methods of algebraic topology from the viewpoint of cobordism theory. // *Math. USSR-Izv.*, 1:4, 1967, 827–913.
37. Y. Ônishi. Universal elliptic functions // (in Japanese), available at <http://www2.meijo-u.ac.jp/~yonishi/#publications>

38. Y. Ônishi. Generalized Bernoulli-Hurwitz numbers and the universal Bernoulli numbers // Russian Mathematical Surveys, Vol. 66, No. 5, 2011, 871–932.
39. Y. Ônishi. Arithmetical Power Series Expansion of the Sigma Function for a Plane Curve // Proceedings of the Edinburgh Mathematical Society, Vol. 61, Issue 4, 2018, 995–1022.
40. B. P. Platonov, M. M. Petrunin. On the torsion problem in Jacobians of curves of genus 2 over the rational number field // Dokl. Math., 86:2, 2012, 642–643.
41. V. P. Platonov. Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field // Russian Math. Surveys, 69:1, 2014, 1–34.
42. V. P. Platonov, G. V. Fedorov. An Infinite Family of Curves of Genus 2 over the Field of Rational Numbers Whose Jacobian Varieties Contain Rational Points of Order 28 // Dokl. Math., 98:2, 2018, 468–471.
43. D. Quillen. On the formal group laws of unoriented and complex cobordism theory. // Bull. Amer. Math. Soc., 75:6, 1969, 1293–1298.
44. J. H. Silverman. The Arithmetic of Elliptic Curves // Graduate Texts in Mathematics, Springer, 1986.
45. K. Weierstrass. Zur theorie der elliptischen functionen // Mathematische Werke, Bd.2: 245–255, 1894.

REFERENCES

1. A. Adelberg, *Universal Higher Order Bernoulli Numbers and Kummer and Related Congruences*, J. Number Theory, Vol. 84, Issue 1, (2000), 119–135.
2. A. Adelberg, *Kummer Congruences For Universal Bernoulli Numbers And Related Congruences For Poly-Bernoulli Numbers*, Int. Math. J., Vol. 1, No. 1, (2002), 53–63.
3. A. Adelberg, *Universal Kummer congruences mod prime powers*, J. Number Theory, Vol. 109, Issue 2, (2004), 362–378.
4. T. Ayano, V. M. Buchstaber, *Ultraelliptic integrals and two-dimensional sigma function.*, Funct. Anal. Appl., 53:3 (2019), 157–173.
5. H. F. Baker, *On the hyperelliptic sigma functions*, Amer. J. Math., Vol. 20, No. 4, (1898), 301–384.
6. H. F. Baker, *On a system of differential equations leading to periodic functions*, Acta Math., Vol. 27, (1903), 135–156.
7. H. F. Baker, *An introduction to the theory of multiply periodic functions*, Cambridge University Press, Cambridge, (1907), available at <http://name.umd1.umich.edu/ACR0014.0001.001>.
8. H. F. Baker, *Abelian functions. Abel's theorem and the allied theory of theta functions*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, (1995).
9. V. M. Buchstaber, *The Chern-Dold Character in Cobordisms, I*, Math. USSR Sbornik, 12:4 (1970), 573–594.

10. V. M. Buchstaber, *Polynomial dynamical systems and the Korteweg-de Vries equation.*, Proc. Steklov Inst. Math., 294, 2016, 176–200, arXiv:1605.04061.
11. V. M. Buchstaber, E. Yu. Bunkova, *Lie algebras of heat operators in nonholonomic frame.*, arXiv:1911.08266v2 [math-ph] 28 Nov 2019.
12. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin, *Hyperelliptic Kleinian functions and applications*, Solitons, Geometry and Topology: On the Crossroad, V. M. Buchstaber, S. P. Novikov Editors, AMS Trans., 179:2, 1997, 1–33.
13. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin, *Kleinian functions, hyperelliptic Jacobians and applications*, Reviews in Mathematics and Math. Physics, I. M. Krichever, S. P. Novikov Editors, v. 10, part 2, Gordon and Breach, London, 1997, 3–120.
14. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin, *Rational analogues of Abelian functions*, Functional Anal. Appl., 33:2, 1999, 83–94.
15. V. M. Buchstaber, V. Z. Enolskii, D. V. Leykin, *Multi-dimensional sigma functions*, arXiv:1208.0990[math-ph] (v1), 5 Aug 2012.
16. V. M. Buchstaber, A. V. Ustinov, *Coefficient rings of formal group laws.*, Sb. Math., 206:11, 2015, 1524–1563.
17. V. M. Buchstaber, V. Z. Enolskii, D. V. Leikin, *Multi-variable sigma-functions: old and new results.*, arXiv:1810.11079 v1 [nlin.SI], 25 Oct 2018.
18. V. M. Buchstaber, D. V. Leykin, *Heat Equations in a Nonholonomic Frame*, Funct. Anal. Appl., 38:2, 2004, 88–101.
19. V. M. Buchstaber, D. V. Leykin, *Addition laws on Jacobian varieties of plane algebraic curves*, Nonlinear dynamics, Proceedings of the Steklov Math. Inst., 251:4, 2005, 49–120.
20. V. M. Buchstaber, D. V. Leykin, *Solution of the problem of differentiation of Abelian functions over parameters for families of (n, s) -curves*, Funct. Anal. Appl., 42:4, 2008, 268–278.
21. E. Yu. Bunkova, *Weierstrass Sigma Function Coefficients Divisibility Hypothesis*, arXiv:1701.00848, (2017).
22. F. Clarke, *The universal von Staudt theorems*, Transactions of the American Mathematical Society, Vol. 315, No. 2, (1989), 591–603.
23. A. V. Domrin, *Uniqueness theorem for the two-dimensional sigma function*, Funct. Anal. Appl., Vol. 54, Issue 1, (2020).
24. J. C. Eilbeck, J. Gibbons, Y. Ônishi, S. Yasuda, *Theory of Heat Equations for Sigma Functions*, arXiv:1711.08395, (2018).
25. J. C. Eilbeck, Y. Ônishi, *Recursion relations on the power series expansion of the universal Weierstrass sigma function*, RIMS Kôkyûroku Bessatsu, (2019).
26. F. Hirzebruch, *Topological methods in algebraic geometry*, Springer-Verlag, 1966.
27. A. Hurwitz, *Ueber die Entwicklungskoeffizienten der lemniscatischen Functionen*, Math. Ann., Vol. 51, (1898), 196–226.
28. F. Klein, *Ueber hyperelliptische Sigmafunctionen*, Math. Ann., Vol. 27, Issue 3, (1886), 431–464.

29. F. Klein, *Ueber hyperelliptische Sigmafunctionen*, Math. Ann., Vol. 32, Issue 3, (1888), 351–380.
30. F. Klein, *Vorbemerkungen zu den Arbeiten über hyperelliptische und Abelsche Funktionen*, Gesammelte Mathematische Abhandlungen, Vol. 3, Teubner, Berlin, (1923), s. 317–322.
31. F. Klein, *Über hyperelliptische Sigmafunctionen*, Gesammelte Mathematische Abhandlungen, Vol. 3, Teubner, Berlin, (1923), 323–387.
32. M. Lazard, *Sur les groupes de Lie formels a un parametre.*, Bull. Soc. Math. France, 83, 1955, 251–274.
33. A. Nakayashiki, *On algebraic expressions of sigma functions for (n, s) curves*, Asian J. Math., Vol. 14, No. 2, (2010), 175–212, arXiv:0803.2083.
34. A. Nakayashiki, *Sigma function as a tau function*, Int. Math. Res. Not., Vol. 2010, No. 3, (2009), 373–394, arXiv:0904.0846.
35. A. Nakayashiki, *Tau Function Approach to Theta Functions*, Int. Math. Res. Not., Vol. 2016, Issue 17, (2016), 5202–5248.
36. S. P. Novikov, *The methods of algebraic topology from the viewpoint of cobordism theory.*, Math. USSR-Izv., 1:4 (1967), 827–913.
37. Y. Ônishi, *Universal elliptic functions*, (in Japanese), available at <http://www2.meijo-u.ac.jp/~yonishi/#publications>
38. Y. Ônishi, *Generalized Bernoulli-Hurwitz numbers and the universal Bernoulli numbers*, Russian Mathematical Surveys, Vol. 66, No. 5, (2011), 871–932.
39. Y. Ônishi, *Arithmetical Power Series Expansion of the Sigma Function for a Plane Curve*, Proceedings of the Edinburgh Mathematical Society, Vol. 61, Issue 4, (2018), 995–1022.
40. B. P. Platonov, M. M. Petrunin, *On the torsion problem in Jacobians of curves of genus 2 over the rational number field*, Dokl. Math., 86:2 (2012), 642–643.
41. V. P. Platonov, *Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field*, Russian Math. Surveys, 69:1 (2014), 1–34.
42. V. P. Platonov, G. V. Fedorov, *An Infinite Family of Curves of Genus 2 over the Field of Rational Numbers Whose Jacobian Varieties Contain Rational Points of Order 28*, Dokl. Math., 98:2 (2018), 468–471.
43. D. Quillen, *On the formal group laws of unoriented and complex cobordism theory.*, Bull. Amer. Math. Soc., 75:6, 1969, 1293–1298.
44. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, (1986).
45. K. Weierstrass, *Zur theorie der elliptischen functionen*, Mathmatische Werke, Bd.2: 245–255, (1894).

Получено 11.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512.7

DOI 10.22405/2226-8383-2020-21-1-51-61

Некоммутативная теорема Бялыницкого — Бирули¹

А. Я. Белов-Канель, А. М. Елишев, Ф. Разавиния, Ю. Джи-Тай, Венчао Жэнг

Белов-Канель Алексей Яковлевич — доктор физико-математических наук, профессор, Колледж математики и статистики, Шэньчжэньский университет (г. Шэньчжэнь).

e-mail: kanel@mcsm.ru

Елишев Андрей Михайлович — кандидат физико-математических наук, ассистент кафедры дискретной математики и лаборатории продвинутой комбинаторики и сетевых приложений, Московский физико-технический институт (Национальный исследовательский университет) (г. Москва).

e-mail: elishev@phystech.edu

Разавиния Фаррох — факультет математики, Университет Порту, Московский физико-технический институт (Национальный исследовательский университет) (г. Порту).

e-mail: f.razavinia@phystech.edu

Ю. Джи-Тай — Ph.D., профессор, Колледж математики и статистики, Шэньчжэньский университет (г. Шэньчжэнь).

e-mail: jietaiyu@szu.edu.cn

Венчао Жэнг — факультет математики, Университет Бар-Илан (г. Рамат-Ган).

e-mail: whzecomjm@gmail.com

Аннотация

Изучение действий алгебраических групп на алгебраических многообразиях и их координатных алгебрах является важной областью исследований в алгебраической геометрии и теории колец. Эта область связана с теорией полиномиальных отображений, ручных и диких автоморфизмов, проблемой якобиана, теорией бесконечномерных многообразий по Шафаревичу, проблемой сокращения (вместе с другими подобными вопросами), теорией локально нильпотентных дифференцирований. Одной из центральных задач теории действий алгебраических групп является проблема линеаризации, изученная в работе Т. Камбаяши и П. Расселла, утверждающая, что всякое действие тора на аффинном пространстве линейно в некоторой системе координат. Гипотеза о линеаризации была основана на хорошо известной классической теореме А. Бялыницкого — Бирули, которая гласит, что всякое эффективное регулярное действие тора максимальной размерности на аффинном пространстве над алгебраически замкнутым полем допускает линеаризацию.

Несмотря на то что гипотеза о линеаризации оказалась отрицательной в ее общем виде — контрпримеры в положительной характеристике были построены Т. Асанума — теорема Бялыницкого — Бирули остается важным результатом теории благодаря ее связи с теорией полиномиальных автоморфизмов. Недавние продвижения в последней мотивировали поиск различных некоммутативных разновидностей теоремы Бялыницкого — Бирули. В данной статье мы приведем доказательство теоремы о линеаризации эффективного действия максимального тора автоморфизмами свободной ассоциативной алгебры, являющейся таким образом свободным аналогом теоремы Бялыницкого — Бирули.

Ключевые слова: действия тора, задача линеаризации, полиномиальные автоморфизмы.

Библиография: 16 названий.

¹Исследование выполнено за счет гранта Российского научного фонда (проект 17-11-01377).

Для цитирования:

А. Я. Белов-Канель, А. М. Елишев, Ф. Разавиния, Ю. Джи-Тай, Венчао Жэнг Некоммутативная теорема Бялыницкого — Бирули // Чебышевский сборник, 2020, т. 21, вып. 1, с. 51–61.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512.7

DOI 10.22405/2226-8383-2020-21-1-51-61

Noncommutative Białynicki–Birula Theorem

A. Ya. Belov-Kanel, A. M. Elishev, F. Razavinia, Yu Jie-Tai, Wenchao Zhang

Belov-Kanel Alexei Yakovlevich — College of Mathematics and Statistics, Shenzhen University (Shenzhen).

e-mail: kanel@mccme.ru

Elishev Andrey Mikhailovich — Department of Discrete Mathematics, Moscow Institute of Physics and Technology (Moscow).

e-mail: elishev@phystech.edu

Razavinia Farrokh — Department of Mathematics, University of Porto, Praça de Gomes Teixeira (Porto).

e-mail: f.razavinia@phystech.edu

Yu Jie-Tai — College of Mathematics and Statistics, Shenzhen University (Shenzhen).

e-mail: jietaiyu@szu.edu.cn

Wenchao Zhang — Mathematics Department, Bar-Ilan University (Ramat-Gan).

e-mail: whzecomjm@gmail.com

Abstract

The study of algebraic group actions on varieties and coordinate algebras is a major area of research in algebraic geometry and ring theory. The subject has its connections with the theory of polynomial mappings, tame and wild automorphisms, the Jacobian conjecture of O.-H. Keller, infinite-dimensional varieties according to Shafarevich, the cancellation problem (together with various cancellation-type problems), the theory of locally nilpotent derivations, among other topics. One of the central problems in the theory of algebraic group actions has been the linearization problem, formulated and studied in the work of T. Kambayashi and P. Russell, which states that any algebraic torus action on an affine space is always linear with respect to some coordinate system. The linearization conjecture was inspired by the classical and well known result of A. Białynicki–Birula, which states that every effective regular torus action of maximal dimension on the affine space over algebraically closed field is linearizable.

Although the linearization conjecture has turned out negative in its full generality, according to, among other results, the positive-characteristic counterexamples of T. Asanuma, the Białynicki–Birula has remained an important milestone of the theory thanks to its connection to the theory of polynomial automorphisms. Recent progress in the latter area has stimulated the search for various noncommutative analogues of the Białynicki–Birula theorem. In this paper, we give the proof of the linearization theorem for effective maximal torus actions by automorphisms of the free associative algebra, which is the free analogue of the Białynicki–Birula theorem.

Keywords: torus actions, linearization problem, polynomial automorphisms.

Bibliography: 16 titles.

For citation:

A. Ya. Belov-Kanel, A. M. Elishev, F. Razavinia, Yu Jie-Tai, Wenchao Zhang, 2020, "Noncommutative Białynicki–Birula Theorem", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 51–61.

1. Introduction

In this paper we consider algebraic torus actions on the affine space, according to Białynicki-Birula, and formulate certain noncommutative generalizations.

We begin by recalling a few basic definitions. Let $\mathbb{K}$ be an algebraically closed field.

DEFINITION 1. *An algebraic group is a variety G equipped with the structure of a group, such that the multiplication map $m : G \times G \rightarrow G : (g_1, g_2) \mapsto g_1 g_2$ and the inverse map $\iota : G \rightarrow G : g \mapsto g^{-1}$ are morphisms of varieties.*

DEFINITION 2. *A G -variety is a variety equipped with an action of the algebraic group G ,*

$$\alpha : G \times X \rightarrow X : (g, x) \mapsto g \cdot x,$$

which is also a morphism of varieties. We then say that α is an algebraic G -action.

Let $\mathbb{K}$ be our ground field, which is assumed to be algebraically closed. Let $Z = \{z_1, z_2, \dots\} = \{z_i : i \in I\}$ be a finite or a countable set of variables (where $I = \{1, 2, \dots\}$ is an index set), and let Z^* denote the free semigroup generated by Z , $Z^+ = Z^* \setminus \{1\}$. Moreover let $F_I(\mathbb{K}) = \mathbb{K}\langle Z \rangle$ be the free associative $\mathbb{K}$ -algebra and $\hat{F}_I(\mathbb{K}) = \mathbb{K}\langle\langle Z \rangle\rangle$ be the algebra of formal power series in free variables.

Denote by $\mathcal{W} = \langle Z \rangle$ the free monoid of words over the alphabet Z (with 1 as the empty word) such that $|\mathcal{W}| \geq 1$, for $|\mathcal{W}|$ the length of the word $\mathcal{W} \in Z^+$.

For an alphabet Z , the free associative $\mathbb{K}$ -algebra on Z is

$$\mathbb{K}\langle Z \rangle := \bigoplus_{\mathcal{W} \in Z^*} \mathbb{K}\mathcal{W},$$

where the multiplication is $\mathbb{K}$ -bilinear extension of the concatenation on words, Z^* denotes the free monoid on Z , and $\mathbb{K}\mathcal{W}$ denotes the free $\mathbb{K}$ -module on one element, the word $\mathcal{W}$. Any element of $\mathbb{K}\langle Z \rangle$ can thus be written uniquely in the form

$$\sum_{k=0}^{\infty} \sum_{i_1, \dots, i_k \in I} a_{i_1, i_2, \dots, i_k} z_{i_1} z_{i_2} \dots z_{i_k},$$

where the coefficients $a_{i_1, i_2, \dots, i_k}$ are elements of the field $\mathbb{K}$ and all but finitely many of these elements are zero.

In our context, the alphabet Z is the same as the set of algebra generators, therefore the terms "monomial" and "word" will be used interchangeably.

In the sequel, we employ a (slightly ambiguous) short-hand notation for a free algebra monomial. For an element z , its powers are defined as usual. Any monomial $z_{i_1} z_{i_2} \dots z_{i_k}$ can then be written in a reduced form with subwords $zz \dots z$ replaced by powers.

We then write

$$z^I = z_{j_1}^{i_1} z_{j_2}^{i_2} \dots z_{j_k}^{i_k}$$

where by I we mean an assignment of i_k to j_k in the word z^I . Sometimes we refer to I as a multi-index, although the term is not entirely accurate. If I is such a multi-index, its absolute value $|I|$ is defined as the sum $i_1 + \dots + i_k$.

For a field $\mathbb{K}$, let $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ denote the multiplicative group of its non-zero elements viewed as an algebraic $\mathbb{K}$ -group.

DEFINITION 3. *An n -dimensional algebraic $\mathbb{K}$ -torus is a group*

$$\mathbb{T}_n \simeq (\mathbb{K}^\times)^n$$

(with obvious multiplication).

Denote by $\mathbb{A}^n$ the affine space of dimension n over $\mathbb{K}$.

DEFINITION 4. A (left) torus action is a morphism

$$\sigma : \mathbb{T}_n \times \mathbb{A}^n \rightarrow \mathbb{A}^n.$$

that fulfills the usual axioms (identity and compatibility):

$$\sigma(1, x) = x, \quad \sigma(t_1, \sigma(t_2, x)) = \sigma(t_1 t_2, x).$$

The action σ is effective if for every $t \neq 1$ there is an element $x \in \mathbb{A}^n$ such that $\sigma(t, x) \neq x$.

In [3], Białynicki-Birula proved the following two theorems.

THEOREM 1. Any regular action of $\mathbb{T}_n$ on $\mathbb{A}^n$ has a fixed point.

THEOREM 2. Any effective and regular action of $\mathbb{T}_n$ on $\mathbb{A}^n$ is a representation in some coordinate system.

The term "regular" is to be understood here as in the algebro-geometric context of regular function (Białynicki-Birula also considered birational actions). The last theorem says that any effective regular maximal torus action on the affine space is conjugate to a linear action, or, as it is sometimes called, *linearizable*.

An algebraic group action on $\mathbb{A}^n$ is the same as an action by automorphisms on the algebra

$$\mathbb{K}[x_1, \dots, x_n]$$

of global sections of the structure sheaf. In other words, it is a homomorphism

$$\sigma : \mathbb{T}_n \rightarrow \text{Aut } \mathbb{K}[x_1, \dots, x_n].$$

An action is effective iff $\text{Ker } \sigma = \{1\}$.

The polynomial algebra is a quotient of the free associative algebra

$$F_n = \mathbb{K}\langle z_1, \dots, z_n \rangle$$

by the commutator ideal I (it is the two-sided ideal generated by all elements of the form $fg - gf$). From the standpoint of Noncommutative geometry, the algebra $\Gamma(X, \mathcal{O}_X)$ of global sections (along with the category of f.g. projective modules) contains all the relevant topological data of X , and various non-commutative algebras (PI-algebras) may be thought of as global function algebras over "noncommutative spaces". Therefore, noncommutative analogue of the Białynicki-Birula theorem is a subject of legitimate interest.

In this short note we establish the free algebra version of the Białynicki-Birula theorem. The latter is formulated as follows.

THEOREM 3 (Main Theorem). Suppose given a regular action σ of the algebraic n -torus $\mathbb{T}_n$ on the free algebra F_n . If σ is effective, then it is linearizable.

The linearization problem, as it has become known since Kambayashi, asks whether all (effective, regular) actions of a given type of algebraic groups on the affine space of given dimension are conjugate to representations. According to Theorem 3, the linearization problem extends to the noncommutative category. Several known results concerning the (commutative) linearization problem are summarized below.

1. Any effective regular torus action on $\mathbb{A}^2$ is linearizable (Gutwirth [8]).
2. Any effective regular torus action on $\mathbb{A}^n$ has a fixed point (Białynicki-Birula [3]).
3. Any effective regular action of $\mathbb{T}_{n-1}$ on $\mathbb{A}^n$ is linearizable (Białynicki-Birula [4]).
4. Any (effective, regular) one-dimensional torus action (i.e., action of $\mathbb{K}^\times$) on $\mathbb{A}^3$ is linearizable (Koras and Russell [14]).
5. If the ground field is not algebraically closed, then a torus action on $\mathbb{A}^n$ need not be linearizable. In [1], Asanuma proved that over any field $\mathbb{K}$, if there exists a non-rectifiable closed embedding from $\mathbb{A}^m$ into $\mathbb{A}^n$, then there exist non-linearizable effective actions of $(\mathbb{K}^\times)^r$ on $\mathbb{A}^{1+n+m}$ for $1 \leq r \leq 1+m$.
6. When $\mathbb{K}$ is infinite and has positive characteristic, there are examples of non-linearizable torus actions on $\mathbb{A}^n$ (Asanuma [1]).

REMARK 1. *A closed embedding $\iota : \mathbb{A}^m \rightarrow \mathbb{A}^n$ is said to be rectifiable if it is conjugate to a linear embedding by an automorphism of $\mathbb{A}^n$.*

As can be inferred from the review above, the context of the linearization problem is rather broad, even in the case of torus actions. The regulating parameters are the dimensions of the torus and the affine space. This situation is due to the fact that the general form of the linearization conjecture (i.e., the conjecture that states that any effective regular torus action on any affine space is linearizable) has a negative answer.

Transition to the noncommutative geometry presents the inquirer with an even broader context: one now may vary the dimensions as well as impose restrictions on the action in the form of preservation of the PI-identities. Caution is well advised. Some of the results are generalized in a straightforward manner — the main theorem of this paper being the typical example, others require more subtlety and effort (cf. 2 and the discussion at the end of the note). Of some note to us, given our ongoing work in deformation quantization (see, for instance, [12]) is the following instance of the linearization problem, which we formulate as a conjecture.

CONJECTURE 1. *For $n \geq 1$, let P_n denote the commutative Poisson algebra, i.e. the polynomial algebra*

$$\mathbb{K}[z_1, \dots, z_{2n}]$$

equipped with the Poisson bracket defined by

$$\{z_i, z_j\} = \delta_{i,n+j} - \delta_{i+n,j}.$$

Then any effective regular action of $\mathbb{T}_n$ by automorphisms of P_n is linearizable.

It is interesting to note that the context of Conjecture 1 admits a vague analogy in the real transcendental category (with P_n replaced by an appropriate algebra of smooth functions, cf. for instance the work of Zung [16]). Although the instances of the linearization problem we consider in this note, as well as the original theorem of Białynicki-Birula, are essentially of complex algebraic nature, it may be worthwhile to search for analytic analogues of the real transcendental linearization (however whether this will give a feasible approach to Conjecture 1 is unclear, the hurdles being significant and fairly obvious).

Acknowledgments

We are grateful to I. V. Arzhantsev, V. L. Dolnikov, R.N. Karasev, V. O. Manturov, A. M. Raigorodskii, G. B. Shabat and N. A. Vavilov for stimulating discussions.

The main result of this note was conceived in the prior work [13] of A. K.-B., J.-T. Y. and A. E.. Theorem 3 is due to A. E. and A. K.-B.; Lemma 1 and the review of known results for the linearization problem is due to F. R., J.-T. Y. and W. Z..

F. R. is also responsible for the investigation of possible transcendental analogies.

A. E. and A. K.-B. are supported by the Russian Science Foundation grant No. 17-11-01377.

F. R. is supported by the FCT (Foundation for Science and Technology of Portugal) scholarship with reference number PD/BD/142959/2018.

2. Proof of the Main Theorem

The proof proceeds along the lines of the original commutative case proof of Białynicki-Birula.

If σ is the effective action of Theorem 3, then for each $t \in \mathbb{T}_n$ the automorphism

$$\sigma(t) : F_n \rightarrow F_n$$

is given by the n -tuple of images of the generators $z_1, \dots, z_n$ of the free algebra:

$$(f_1(t, z_1, \dots, z_n), \dots, f_n(t, z_1, \dots, z_n)).$$

Each of the $f_1, \dots, f_n$ is a polynomial in the free variables.

LEMMA 1. *There is a translation of the free generators*

$$(z_1, \dots, z_n) \rightarrow (z_1 - c_1, \dots, z_n - c_n), \quad (c_i \in \mathbb{K})$$

such that (for all $t \in \mathbb{T}_n$) the polynomials $f_i(t, z_1 - c_1, \dots, z_n - c_n)$ have zero free part.

PROOF. This is a direct corollary of Theorem 1. Indeed, any action σ on the free algebra induces, by taking the canonical projection with respect to the commutator ideal I , an action $\bar{\sigma}$ on the commutative algebra $\mathbb{K}[x_1, \dots, x_n]$. If σ is regular, then so is $\bar{\sigma}$. By Theorem 1, $\bar{\sigma}$ (or rather, its geometric counterpart) has a fixed point, therefore the images of commutative generators x_i under $\bar{\sigma}(t)$ (for every t) will be polynomials with trivial degree-zero part. Consequently, the same will hold for σ . $\square$

We may then suppose, without loss of generality, that the polynomials f_i have the form

$$f_i(t, z_1, \dots, z_n) = \sum_{j=1}^n a_{ij}(t)z_j + \sum_{j,l=1}^n a_{ijl}(t)z_jz_l + \sum_{k=3}^N \sum_{|J|=k} a_{i,J}(t)z^J$$

where by z^J we denote, as in the introduction, a particular monomial

$$z_{i_1}^{k_1} z_{i_2}^{k_2} \dots$$

(a word in the alphabet $\{z_1, \dots, z_n\}$ in the reduced notation; J is the multi-index in the sense described above); also, N is the degree of the automorphism (which is finite) and $a_{ij}, a_{ijl}, \dots$ are polynomials in $t_1, \dots, t_n$.

As σ_t is an automorphism, the matrix $[a_{ij}]$ that determines the linear part is non-singular. Therefore, without loss of generality we may assume it to be diagonal (just as in the commutative case [3]) of the form

$$\text{diag}(t_1^{m_{11}} \dots t_n^{m_{1n}}, \dots, t_1^{m_{n1}} \dots t_n^{m_{nn}}).$$

Now, just as in [3], we have the following

LEMMA 2. *The power matrix $[m_{ij}]$ is non-singular.*

PROOF. Consider a linear action τ defined by

$$\tau(t) : (z_1, \dots, z_n) \mapsto (t_1^{m_{11}} \dots t_n^{m_{1n}} z_1, \dots, t_1^{m_{n1}} \dots t_n^{m_{nn}} z_n), \quad (t_1, \dots, t_n) \in \mathbb{T}_n.$$

If $T_1 \subset T_n$ is any one-dimensional torus, the restriction of τ to $\mathbb{T}_1$ is non-trivial. Indeed, were it to happen that for some $\mathbb{T}_1$,

$$\tau(t)z = z, \quad t \in \mathbb{T}_1, \quad (z = (z_1, \dots, z_n))$$

then our initial action σ , whose linear part is represented by τ , would be identity modulo terms of degree > 1 :

$$\sigma(t)(z_i) = z_i + \sum_{j,l} a_{ijl}(t) z_j z_l + \dots$$

Now, equality $\sigma(t^2)(z) = \sigma(t)(\sigma(t)(z))$ implies

$$\begin{aligned} \sigma(t)(\sigma(t)(z_i)) &= \sigma(t) \left(z_i + \sum_{j,l} a_{ijl}(t) z_j z_l + \dots \right) \\ &= z_i + \sum_{j,l} a_{ijl}(t) z_j z_l + \sum_{j,l} a_{ijl}(t) (z_j + \sum_{k,m} a_{jkm}(t) z_k z_m + \dots) \\ &\quad (z_l + \sum_{k',m'} a_{lk'm'}(t) z_{k'} z_{m'} + \dots) + \dots \\ &= z_i + \sum_{j,l} a_{ijl}(t^2) z_j z_l + \dots \end{aligned}$$

which means that

$$2a_{ijl}(t) = a_{ijl}(t^2)$$

and therefore $a_{ijl}(t) = 0$. The coefficients of the higher-degree terms are processed by induction (on the total degree of the monomial). Thus

$$\sigma(t)(z) = z, \quad t \in \mathbb{T}_1$$

which is a contradiction since σ is effective. Finally, if $[m_{ij}]$ were singular, then one would easily find a one-dimensional torus such that the restriction of τ were trivial. $\square$

Consider the action

$$\varphi(t) = \tau(t^{-1}) \circ \sigma(t).$$

The images under $\varphi(t)$ are

$$(g_1(z, t), \dots, g_n(z, t)), \quad (t = (t_1, \dots, t_n))$$

with

$$g_i(z, t) = \sum g_{i,m_1 \dots m_n}(z) t_1^{m_1} \dots t_n^{m_n}, \quad m_1, \dots, m_n \in \mathbb{Z}.$$

Define $G_i(z) = g_{i,0 \dots 0}(z)$ and consider the map $\beta : F_n \rightarrow F_n$,

$$\beta : (z_1, \dots, z_n) \mapsto (G_1(z), \dots, G_n(z)).$$

LEMMA 3. $\beta \in \text{Aut } F_n$ and

$$\beta = \tau(t^{-1}) \circ \beta \circ \sigma(t).$$

PROOF. This lemma mirrors the final part in the proof in [3]. The conjugation is straightforward, since for every $s, t \in \mathbb{T}_n$ one has

$$\varphi(st) = \tau(t^{-1}s^{-1}) \circ \sigma(st) = \tau(t^{-1}) \circ \tau(s^{-1}) \circ \sigma(s) \circ \sigma(t) = \tau(t^{-1}) \circ \varphi(s) \circ \sigma(t).$$

Denote by $\hat{F}_n$ the power series completion of the free algebra F_n , and let $\hat{\sigma}$, $\hat{\tau}$ and $\hat{\beta}$ denote the endomorphisms of the power series algebra induced by corresponding morphisms of F_n . The endomorphisms $\hat{\sigma}$, $\hat{\tau}$, $\hat{\beta}$ come from (polynomial) automorphisms and therefore are invertible.

Let

$$\hat{\beta}^{-1}(z_i) \equiv B_i(z) = \sum_J b_{i,J} z^J$$

(just as before, z^J is the monomial with multi-index J). Then

$$\hat{\beta} \circ \hat{\tau}(t) \circ \hat{\beta}^{-1}(z_i) = B_i(t_1^{m_{11}} \dots t_n^{m_{1n}} G_1(z), \dots, t_1^{m_{n1}} \dots t_n^{m_{nn}} G_n(z)).$$

Now, from the conjugation property we must have

$$\hat{\beta} = \hat{\sigma}(t^{-1}) \circ \hat{\beta} \circ \hat{\tau}(t),$$

therefore $\hat{\sigma}(t) = \hat{\beta} \circ \hat{\tau}(t) \circ \hat{\beta}^{-1}$ and

$$\hat{\sigma}(t)(z_i) = \sum_J b_{i,J} (t_1^{m_{11}} \dots t_n^{m_{1n}})^{j_1} \dots (t_1^{m_{n1}} \dots t_n^{m_{nn}})^{j_n} G(z)^J;$$

here the notation $G(z)^J$ stands for a word in $G_i(z)$ with multi-index J , while the exponents $j_1, \dots, j_n$ count how many times a given index appears in J (or, equivalently, how many times a given generator z_i appears in the word z^J).

Therefore, the coefficient of $\hat{\sigma}(t)(z_i)$ at z^J has the form

$$b_{i,J} (t_1^{m_{11}} \dots t_n^{m_{1n}})^{j_1} \dots (t_1^{m_{n1}} \dots t_n^{m_{nn}})^{j_n} + S$$

with S a finite sum of monomials of the form

$$c_L (t_1^{m_{11}} \dots t_n^{m_{1n}})^{l_1} \dots (t_1^{m_{n1}} \dots t_n^{m_{nn}})^{l_n}$$

with $(j_1, \dots, j_n) \neq (l_1, \dots, l_n)$. Since the power matrix $[m_{ij}]$ is non-singular, if $b_{i,J} \neq 0$, we can find a $t \in \mathbb{T}_n$ such that the coefficient is not zero. Since σ is an algebraic action, the degree

$$\sup_t \deg(\hat{\sigma})$$

is a finite integer N . With the previous statement, this implies that

$$b_{i,J} = 0, \text{ whenever } |J| > N.$$

Therefore, $B_i(z)$ are polynomials in the free variables. What remains is to notice that

$$z_i = B_i(G_1(z), \dots, G_n(z)).$$

Thus β is an automorphism. $\square$

From Lemma 3 it follows that

$$\tau(t) = \beta^{-1} \circ \sigma(t) \circ \beta$$

which is the linearization of σ . Theorem 3 is proved.

3. Discussion

The noncommutative torus action linearization theorem that we have proved has several useful applications. In the work [13] (cf. also [7]), it is used to investigate the properties of the group $\text{Aut } F_n$ of automorphisms of the free algebra. As a corollary of Theorem 3, one gets

COROLLARY 1. *Let θ denote the standard action of $\mathbb{T}_n$ on $K[x_1, \dots, x_n]$ — i.e., the action*

$$\theta_t : (x_1, \dots, x_n) \mapsto (t_1 x_1, \dots, t_n x_n).$$

Let $\tilde{\theta}$ denote its lifting to an action on the free associative algebra F_n . Then $\tilde{\theta}$ is also given by the standard torus action.

This statement plays a part, along with a number of results concerning the induced formal power series topology on $\text{Aut } F_n$, in the establishment of the following proposition (cf. [13]).

PROPOSITION 1. *When $n \geq 3$, any Ind-scheme automorphism φ of $\text{Aut}(K\langle x_1, \dots, x_n \rangle)$ is inner.*

One could try and generalize the free algebra version of the Białynicki-Birula's theorem to other noncommutative situations. Another way of generalization lies in changing the dimension of the torus. In a complete analogy with further work of Białynicki-Birula [4], we expect the following to hold.

CONJECTURE 2. *Any effective action of $\mathbb{T}_{n-1}$ on F_n is linearizable.*

On the other hand, there is little reason to expect this statement to hold with further lowering of the torus dimension. In fact, even in the commutative case the conjecture that any effective toric action is linearizable, in spite of considerable effort (see [9]), proved negative (counterexamples in positive characteristic due to Asanuma, [1]).

Another direction would be to replace $\mathbb{T}$ by an arbitrary reductive algebraic group, however the commutative case also does not hold even in characteristic zero (cf. [15]).

It is also a problem of legitimate interest to obtain the proof of Conjecture 1 — i.e. to resolve the linearization problem of the regular action of the n -dimensional torus on the group $\text{Sympl}(k^{2n})$ of polynomial symplectomorphisms of the $2n$ -dimensional affine space (k is a field of characteristic zero). One could hope to utilize the latter result in order to obtain a description of the space of Ind-scheme automorphisms of $\text{Sympl}(k^{2n})$ along the lines of [13]. This space plays a prominent role in the study of quantization of symplectomorphisms, initiated by Kanel-Belov and Kontsevich [2], where the characteristic zero isomorphism between the group of automorphisms of the n -th Poisson and Weyl algebras has been posed as the main conjecture (Kontsevich conjecture). Recently, the first, the second and the fourth named authors have proposed a proof of this conjecture [10, 11].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. T. Asanuma. Non-linearizable k^* -actions in affine space // Invent. Math. 1999, Vol. 138. P. 281-306.
2. A. Belov-Kanel and M. Kontsevich. Automorphisms of the Weyl algebra // Lett. Math. Phys. 2005, Vol. 74, No.2. P. 181-199.
3. A. Białynicki-Birula. Remarks on the action of an algebraic torus on k^n // Bull. Acad. Polon. Sci., Ser. Sci. Math. Astro. Phys. 1966, Vol. 14. P. 177-181.

4. A. Białynicki-Birula. Remarks on the action of an algebraic torus on k^n . II // Bull. Acad. Polon. Sci. Ser. Sci. Math. Astro. Phys. 1967, Vol. 15. P. 123-125.
5. A. Białynicki-Birula. Some theorems on actions of algebraic groups // Ann. Math. Second Series 1973, Vol. 98, No. 3, P. 480-497.
6. M. Brion. Introduction to actions of algebraic groups // Les cours du CIRM 2010, Vol. 1. No. 1. P. 1-22.
7. A. Elishev. Automorphisms of polynomial algebras, quantization and Kontsevich conjecture // PhD Thesis (in Russian), 2019.
8. A. Gutwirth. The action of an algebraic torus on the affine plane // Trans. Amer. Math. Soc. 1962, Vol. 105, No.3. P. 407-414.
9. T. Kambayashi and P. Russell. On linearizing algebraic torus actions // J. Pure and Applied Algebra 1982, Vol. 23, Iss. 3. P. 243-250.
10. A. Kanel-Belov, A. Elishev, and J.-T. Yu. Augmented polynomial symplectomorphisms and quantization // arXiv:1812.02859, 2018.
11. A. Kanel-Belov, A. Elishev, and J.-T. Yu. Independence of the B-KK isomorphism of infinite prime // arXiv:1512.06533, 2015.
12. A. Kanel-Belov, S. Grigoriev, A. Elishev, J.-T. Yu and W. Zhang. Lifting of Polynomial Symplectomorphisms and Deformation Quantization // Commun. in Algebra 2018, Vol. 46, P. 3926-3938.
13. A. Kanel-Belov, J.-T. Yu, A. Elishev. On the Augmentation Topology on Automorphism Groups of Affine Spaces and Algebras // Int. J. Alg. Comp. 2018, Vol. 28, No. 08. P. 1449-1485.
14. M. Koras and P. Russell. C^* -actions on C^3 : The smooth locus of the quotient is not of hyperbolic type // J. Alg. Geom. 1999, Vol. 8, No. 4. P. 603-694.
15. G. Schwarz. Exotic algebraic group actions // C. R. Acad. Sci. Paris 1989, Ser. I Vol. 309. P. 89-94.
16. N. T. Zung. Torus actions and integrable systems // arXiv math/0407455 (2004).

REFERENCES

1. Asanuma, T. 1999, "Non-linearizable k^* -actions in affine space", *Invent. Math.*, vol. 138, pp. 281-306.
2. Belov-Kanel, A. & Kontsevich, M. 2005, "Automorphisms of the Weyl algebra", *Lett. Math. Phys.*, vol. 74, no. 2, pp. 181-199.
3. Białynicki-Birula, A. 1966, "Remarks on the action of an algebraic torus on k^n ", *Bull. Acad. Polon. Sci., Ser. Sci. Math. Astro. Phys.*, vol. 14, pp. 177-181.
4. Białynicki-Birula, A. 1967, "Remarks on the action of an algebraic torus on k^n , II", *Bull. Acad. Polon. Sci., Ser. Sci. Math. Astro. Phys.*, vol. 15, pp. 123-125.
5. Białynicki-Birula, A. 1973, "Some theorems on actions of algebraic groups", *Ann. Math. Second Series*, vol. 98, no. 3, pp. 480-497.

6. Brion, M. 2010, “Introduction to actions of algebraic groups“, *Les cours du CIRM*, vol. 1, no. 1, pp. 1-22.
7. Elishev, A. 2019, “Automorphisms of polynomial algebras, quantization and Kontsevich conjecture“, PhD thesis (in Russian).
8. Gutwirth, A. 1962, “The action of an algebraic torus on the affine plane“, *Trans. Amer. Math. Soc.*, vol. 105, no. 3, pp. 407-414.
9. Kambayashi, T. & Russell, P. 1982, “On linearizing algebraic torus actions“, *J. Pure and Applied Algebra*, vol. 23, iss. 3, pp. 243-250.
10. Kanel-Belov, A., Elishev, A. & Yu, J.-T. 2018, “Augmented polynomial symplectomorphisms and quantization“, *arXiv*: 1812.02859.
11. Kanel-Belov, A., Elishev, A. & Yu, J.-T. 2015, “Independence of the B-KK isomorphism of infinite prime“, *arXiv*: 1512.06533.
12. Kanel-Belov, A., Grigoriev, S., Elishev, A., Yu, J.-T. & Zhang, W. 2018, “Lifting of Polynomial Symplectomorphisms and Deformation Quantization“, *Commun. in Algebra*, vol. 46, pp. 3926-3938.
13. Kanel-Belov, A., Yu, J.-T. & Elishev, A. 2018, “On the Augmentation Topology on Automorphism Groups of Affine Spaces and Algebras“, *Int. J. Alg. Comp.*, vol. 28, no. 08, pp. 1449-1485.
14. Koras, M. & Russell, P. 1999, “ C^* -actions on C^3 : The smooth locus of the quotient is not of hyperbolic type“, *J. Alg. Geom.*, vol. 8, no. 4, pp. 603-694.
15. Schwarz, G. 1989, “Exotic algebraic group actions“, *C. R. Acad. Sci. Paris Ser. I*, vol. 309, pp. 89-94.
16. Zung, N., T. 2004, “Torus actions and integrable systems“, *arXiv*, math/0407455.

Получено 17.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512.547

DOI 10.22405/2226-8383-2020-21-1-62-81

О многообразиях представлений некоторых свободных произведений циклических групп с одним соотношением

В. В. Беньаш-Кривец, А. Н. Адмиралова

Беньаш-Кривец Валерий Вацлавович — доктор физико-математических наук, профессор, заведующий кафедрой высшей алгебры и защиты информации, Белорусский государственный университет (г. Минск).

e-mail: benyash@tut.by

Адмиралова Александра Николаевна — инженер-программист, ООО «СОФТКЛУБ» (г. Минск).

e-mail: al.admiralova@gmail.com

Аннотация

В работе исследуются многообразия представлений двух классов конечно порожденных групп. Первый класс состоит из групп с копредставлением

$$G = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g \mid a_1^{m_1} = \dots = a_s^{m_s} = x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k) = 1 \rangle,$$

где $g \geq 3$, $m_i \geq 2$ для $i = 1, \dots, s$ и $W(a_1, \dots, a_s, b_1, \dots, b_k)$ — элемент в нормальной форме в свободном произведении циклических групп $H = \langle a_1 \mid a_1^{m_1} \rangle * \dots * \langle a_s \mid a_s^{m_s} \rangle * \langle b_1 \rangle * \dots * \langle b_k \rangle$.

Второй класс состоит из групп с копредставлением

$$G(p, q) = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g, t \mid a_1^{m_1} = \dots = a_s^{m_s} = 1, tU^p t^{-1} = U^q \rangle,$$

где p и q — целые числа, такие, что $p > |q| \geq 1$, $(p, q) = 1$, $m_i \geq 2$ для $i = 1, \dots, s$, $g \geq 3$, $U = x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k)$ и $W(a_1, \dots, a_s, b_1, \dots, b_k)$ — элемент, определенный выше.

Найдены неприводимые компоненты многообразий представлений $R_n(G)$ и $R_n(G(p, q))$, вычислены их размерности и доказано, что каждая неприводимая компонента является рациональным многообразием.

Ключевые слова: копредставление группы, многообразие представлений, размерность многообразия, рациональное многообразие.

Библиография: 20 названий.

Для цитирования:

В. В. Беньаш-Кривец, А. Н. Адмиралова. О многообразиях представлений некоторых свободных произведений циклических групп с одним соотношением // Чебышевский сборник, 2020, т. 21, вып. 1, с. 62–81.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512.547

DOI 10.22405/2226-8383-2020-21-1-62-81

On representation varieties of some one-relator products of cyclic groups

V. V. Beniash-Kryvets, A. N. Admiralova

Beniash-Kryvets Valery Vatslavovich — doctor of physical and mathematical Sciences, Professor, head of the Department of higher algebra and information security, Belarusian State University (Minsk).

e-mail: benyash@tut.by

Admiralova Alexandra Nikolaevna — software engineer, Limited Liability Company “SoftClub” (Minsk).

e-mail: al.admiralova@gmail.com

Abstract

In the paper representation varieties of two classes of finitely generated groups are investigated. The first class consists of groups with the presentation

$$G = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g \mid a_1^{m_1} = \dots = a_s^{m_s} = x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k) = 1 \rangle,$$

where $g \geq 3$, $m_i \geq 2$ for $i = 1, \dots, s$ and $W(a_1, \dots, a_s, b_1, \dots, b_k)$ is an element in normal form in the free product of cyclic groups

$$H = \langle a_1 \mid a_1^{m_1} \rangle * \dots * \langle a_s \mid a_s^{m_s} \rangle * \langle b_1 \rangle * \dots * \langle b_k \rangle.$$

The second class consists of groups with the presentation

$$G(p, q) = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g, t \mid a_1^{m_1} = \dots = a_s^{m_s} = 1, tU^p t^{-1} = U^q \rangle,$$

where p and q are integer numbers such that $p > |q| \geq 1$, $(p, q) = 1$, $m_i \geq 2$ for $i = 1, \dots, s$, $g \geq 3$, $U = x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k)$ and $W(a_1, \dots, a_s, b_1, \dots, b_k)$ is an above defined element.

Irreducible components of representation varieties $R_n(G)$ and $R_n(G(p, q))$ are found, their dimensions are calculated and it is proved, that every irreducible component is a rational variety.

Keywords: a group presentation; a representation variety; a dimension of a variety; a rational variety.

Bibliography: 20 titles.

For citation:

V. V. Beniash-Kryvets, A. N. Admiralova, 2020, "On representation varieties of some one-relator products of cyclic groups", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 62–81.

1. Введение

Пусть $G = \langle g_1, \dots, g_m \rangle$ — конечно порожденная группа, $H \subset GL_n(K)$ — связная линейная алгебраическая группа, определенная над полем K , которое всюду далее предполагается алгебраически замкнутым и имеющим нулевую характеристику. Тогда любое линейное представление $\rho : G \rightarrow H$ однозначно определяется набором элементов $\rho(g_1), \dots, \rho(g_m)$. Эти элементы удовлетворяют всем определяющим соотношениям группы G , и, таким образом, имеет место вложение $\rho \mapsto (\rho(g_1), \dots, \rho(g_m))$ множества $\text{Hom}(G, H)$ в H^m . Образ множества $\text{Hom}(G, H)$ относительно этого вложения является аффинным K -многообразием $R_n(G, H) \subset H^m$, и это многообразие называют многообразием представлений группы G в алгебраическую группу H . В случае $H = GL_n(K)$ мы будем обозначать многообразие $R_n(G, GL_n(K))$ через $R_n(G)$ и называть многообразием n -мерных представлений группы G .

Детально изучены многообразия $R_n(G)$ для конечных групп G . В этом случае каждое представление является вполне приводимым и с точностью до эквивалентности существует лишь конечное число представлений, каждое из которых однозначно определяется своим характером. Поэтому каждая неприводимая компонента многообразия $R_n(G)$ является орбитой некоторого вполне приводимого представления группы G и эти компоненты не пересекаются между собой. Для бесконечных нильпотентных групп большая часть известных результатов была собрана А. Любоцким и Э. Магидом в работе [1]. В ней были описаны многообразия характеров для бесконечных нильпотентных групп G . В статье [2] З. Рудник обобщил эти результаты на разрешимые группы. Кольцо характеров Фрике исследовалось в работе [3].

Однако в общем случае о структуре многообразий $R_n(G)$ известно немного. Такие описания получены только для некоторых классов групп. В статьях [4] и [5] описаны многообразия представлений фундаментальных групп компактных ориентируемых и неориентируемых поверхностей.

В работе [6] описаны многообразия представлений групп, имеющих копредставление вида:

$$\Gamma_g = \langle x_1, \dots, x_s, y_1, \dots, y_g \mid x_1^{m_1} = \dots = x_s^{m_s} = x_1 \dots x_s y_1^2 \dots y_g^2 = 1 \rangle,$$

где $m_i \geq 2$ для $i = 1, \dots, s$. В статье [7] описаны все неприводимые компоненты многообразий представлений F -групп и их обобщений, т.е. групп, имеющих копредставление вида:

$$\Gamma_g = \langle (x_1, \dots, x_s, t_1, \dots, t_k, y_1, \dots, y_g, z_1, \dots, z_g) \mid x_1^{m_1} = \dots = x_s^{m_s} = W(x_1, \dots, x_s, t_1, \dots, t_k)[y_1, z_1], \dots, [y_g, z_g] = 1 \rangle,$$

где $m_i = 0$ или $m_i \geq 2$ для $i = 1, \dots, s$, а $W(x_1, \dots, x_s, t_1, \dots, t_k)$ — элемент в нормальной форме (возможно, равный единице) в свободном произведении циклических групп $H = \langle x_1 \mid x_1^{m_1} \rangle * \dots * \langle x_s \mid x_s^{m_s} \rangle * \langle t_1 \rangle * \dots * \langle t_k \rangle$.

В работе [8] исследовано многообразие представлений группы $SL_2(\mathbb{Z})$. В статье [9] были описаны многообразия представлений $R_n(BS(p, q))$ групп Баумслэга-Солитера $BS(p, q)$, т.е. групп, имеющих копредставление вида

$$BS(p, q) = \langle a, b \mid ba^p b^{-1} = a^q \rangle$$

для взаимно простых показателей p и q , таких, что $|p| > q > 1$. В [10] исследования групп Баумслэга-Солитера были продолжены, и результаты [9] были расширены на случай не взаимно простых p и q .

В работе [11] получено описание всех подгрупп конечного индекса групп Баумслэга-Солитера. Установлено, что все подгруппы индекса m в группе $BS(p, q)$ изоморфны группе H_m , имеющей копредставление

$$H_m = \langle a_1, \dots, a_m, b \mid a_i^p = a_{i+1}^q, i = 1, \dots, m-1, ba^p b^{-1} = a_1^q \rangle.$$

В работе [12] найдены все неприводимые представления групп H_m над полем $\mathbb{C}$. Используя эти результаты, в [13] получено описание многообразий представлений $R_n(H_m)$ подгрупп конечного индекса групп Баумслага-Солитера.

В [14] были описаны структура и свойства многообразий представлений групп, имеющих копредставление

$$H = \langle x_1, y_1, \dots, x_g, y_g, t \mid t([x_1, y_1] \dots [x_g, y_g])^p t^{-1} = ([x_1, y_1] \dots [x_g, y_g])^q \rangle,$$

где $g \geq 2$, $p > |q| \geq 1$, p и q взаимно просты.

В настоящей статье мы будем рассматривать 2 класса групп. Первый класс — это группы с копредставлением

$$G = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g \mid a_1^{m_1} = \dots = a_s^{m_s} = 1, x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k) = 1 \rangle, \quad (1)$$

где $g \geq 3$, $m_i \geq 2$ для $i = 1, \dots, s$ и $W(a_1, \dots, a_s, b_1, \dots, b_k)$ — элемент в нормальной форме (возможно, равный единице) в свободном произведении циклических групп

$$H = \langle a_1 \mid a_1^{m_1} \rangle * \dots * \langle a_s \mid a_s^{m_s} \rangle * \langle b_1 \rangle * \dots * \langle b_k \rangle.$$

Отметим, что при этом числа s и k допускаются равными нулю, и в случае $s = 0, k = 0$ такая группа G совпадает с фундаментальной группой компактной неориентируемой поверхности. Многообразия представлений таких групп рассмотрены в [5].

Второй класс — это группы с копредставлением

$$G(p, q) = \langle a_1, \dots, a_s, b_1, \dots, b_k, x_1, \dots, x_g, y_1, \dots, y_g, t \mid a_1^{m_1} = \dots = a_s^{m_s} = 1, tU^p t^{-1} = U^q \rangle, \quad (2)$$

где p и q — целые числа, такие, что $p > |q| \geq 1$, $g \geq 3$, $m_i \geq 2$ для $i = 1, \dots, s$, $U = x_1^2 \dots x_g^2 W(a_1, \dots, a_s, b_1, \dots, b_k)$ и элемент $W(a_1, \dots, a_s, b_1, \dots, b_k)$ удовлетворяет условиям, описанным выше. Отметим, что если $s = 0, k = 0$, то класс таких групп $G(p, q)$ совпадает с рассмотренным в [15]. Заметим также, что группа $G(p, q)$ является HNN-расширением свободного произведения циклических групп $\langle a_1 \mid a_1^{m_1} \rangle * \dots * \langle a_s \mid a_s^{m_s} \rangle * \langle b_1 \rangle * \dots * \langle b_k \rangle * \langle x_1 \rangle * \dots * \langle x_g \rangle$ с проходной буквой t и связанными бесконечными циклическими подгруппами $\langle U^p \rangle$ и $\langle U^q \rangle$. Группы G и $G(p, q)$ можно также рассматривать как свободное произведение циклических групп с одним соотношением. Такие группы изучались в монографии [16].

2. Многообразия представлений групп с копредставлением (1)

Следующее предложение дает описание многообразия представлений конечной циклической группы. В дальнейшем через E_n будем обозначать единичную матрицу порядка n .

Предложение 1. Пусть $C_l = \langle a \mid a^l = 1 \rangle$ — циклическая группа порядка l , γ — первообразный корень из единицы степени l . Для произвольного разбиения $\alpha = (k_1, \dots, k_l)$ числа n на l неотрицательных частей (т.е. $n = k_1 + \dots + k_l$, $k_i \geq 0$) положим

$$V_\alpha = \{ XZ_\alpha X^{-1} \mid X \in GL_n(K) \},$$

где $Z_\alpha = \text{diag}(\gamma E_{k_1}, \gamma^2 E_{k_2}, \dots, \gamma^l E_{k_l})$ (если $k_i = 0$, то блок $\gamma^i E_{k_i}$ в матрице V_α отсутствует). Тогда V_α является неприводимой компонентой многообразия представлений $R_n(C_l)$ размерности $n^2 - \sum_{i=1}^l k_i^2$ и V_α — рациональное многообразие. При этом $V_\alpha \cap V_\beta = \emptyset$ при $\alpha \neq \beta$ и $R_n(C_l) = \cup V_\alpha$, где объединение берется по всем возможным разбиениям α . Общее число неприводимых компонент $R_n(C_l)$ равно числу сочетаний C_{n+l-1}^{l-1} .

Доказательство. V_α является неприводимым замкнутым множеством, поскольку класс сопряженности полупростого элемента в $GL_n(K)$ неприводим и замкнут в топологии Зарисского

(см., например, [17]). Очевидно, что $Y_\alpha^l = E_n$, $V_\alpha \cap V_\beta = \emptyset$ при $\alpha \neq \beta$ и $\cup_\alpha V_\alpha = R_n(C_l)$, где объединение берется по всем разбиениям n на l частей. Таким образом, множества V_α составляют полный набор неприводимых компонент $R_n(C_l)$. Размерность V_α равна коразмерности централизатора Z_α в $GL_n(K)$, т. е. $\dim V_\alpha = n^2 - \sum_{i=1}^l k_i^2$. Покажем, что V_α — рациональное многообразие. Пусть T — множество блочных матриц вида (T_{ij}) , где $T_{ii} = E_{k_i}$, и пусть $\varphi : T \rightarrow V_\alpha$ — морфизм, задаваемый формулой $\varphi(t) = tZ_\alpha t^{-1}$. Ясно, что $\dim T = \dim V_\alpha$, и непосредственное вычисление показывает, что φ — инъективный (и, следовательно, доминантный) морфизм. Значит, φ — бирациональный изоморфизм (см. [18, предложение 3.17]). Очевидно, что T — рациональное многообразие, поэтому и V_α рационально. Наконец, общее число неприводимых компонент $R_n(C_l)$ совпадает с числом решений в целых неотрицательных числах уравнения $x_1 + \dots + x_l = n$. В [19, глава 1] показано, что это число равно C_{n+l-1}^{l-1} . $\square$

Введем следующие обозначения. Пусть T — группа, определенная в (1). Для каждого i , $1 \leq i \leq s$, обозначим через n_i сумму всех показателей, с которыми элемент b_i входит в слово $W(a_1, \dots, a_s, b_1, \dots, b_k)$ (если b_i не входит в $W(a_1, \dots, a_s, b_1, \dots, b_k)$, то полагаем $n_i = 0$). Пусть d — наибольший общий делитель чисел $2, n_1, \dots, n_s$. Таким образом, $d = 2$, если все n_i четны, и $d = 1$ в противном случае. Далее, положим ε_i , $1 \leq i \leq s$, — первообразный корень из 1 степени m_i . Для каждого i , $1 \leq i \leq s$, выберем разбиение $\alpha_i = (k_{i,1}, \dots, k_{i,m_i})$ числа n на m_i неотрицательных слагаемых. Пусть

$$V_{(\alpha_1, \dots, \alpha_s)} = V_{\alpha_1} \times \dots \times V_{\alpha_s} \times GL_n(K)^k$$

и для фиксированной матрицы $A \in GL_n(K)$ рассмотрим следующее многообразие:

$$T(\alpha_1, \dots, \alpha_s, A) = \{(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g) \in V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^g \mid \\ X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k) = A\}.$$

Нам также необходим морфизм

$$f_W : GL_n(K)^{s+k} \rightarrow GL_n(K), \quad f_W(A_1, \dots, A_s, B_1, \dots, B_k) = W(A_1, \dots, A_s, B_1, \dots, B_k). \quad (3)$$

Справедлива следующая теорема.

ТЕОРЕМА 1. 1. *Предположим, что выполнено одно из условий: 1) пара (n, g) отлична от $(2, 3)$; 2) $(n, g) = (2, 3)$ и A — не скалярная матрица; 3) $n = 2$, $g = 3$, $A = \alpha E_2$ и $f_W(V_{(\alpha_1, \dots, \alpha_s)})$ содержит более одной точки. Тогда многообразие $T(\alpha_1, \dots, \alpha_s, A)$ состоит из d неприводимых компонент, каждая из которых является рациональным многообразием.*

2. *Если $n = 2$, $g = 3$, $A = \alpha E_2$ и $f_W(V_{(\alpha_1, \dots, \alpha_s)})$ состоит из одной точки, то $T(\alpha_1, \dots, \alpha_s, A)$ состоит из 3 неприводимых компонент, каждая из которых является рациональным многообразием.*

Размерность любой неприводимой компоненты U многообразия $T(\alpha_1, \dots, \alpha_s, A)$ равна

$$\dim U = (g + k + s - 1)n^2 - \sum_{i=1}^s \sum_{j=1}^{m_i} (k_{i,j}^2). \quad (4)$$

Легко видеть, что

$$R_n(G) = \cup T(\alpha_1, \dots, \alpha_s, E_n),$$

где объединение берется по всем наборам разбиений $(\alpha_1, \dots, \alpha_s)$, где α_i — разбиение n на m_i неотрицательных частей. Из теоремы 1 получаем описание многообразий представлений $R_n(G)$ группы G , заданной копредставлением (1).

ТЕОРЕМА 2. 1. Если пара (n, g) отлична от $(2, 3)$, то многообразие $T(\alpha_1, \dots, \alpha_s, E_n)$ состоит из d неприводимых компонент многообразия $R_n(G)$, каждая из которых является рациональным многообразием. Общее число неприводимых компонент $R_n(G)$ равно $d \prod_{i=1}^s C_{n+m_i-1}^{m_i-1}$.

2. Если $n = 2$, $g = 3$ и образ $f_W(V_{(\alpha_1, \dots, \alpha_s)})$ содержит более одной точки, то многообразие $T(\alpha_1, \dots, \alpha_s, E_2)$ состоит из d неприводимых компонент многообразия $R_n(G)$, каждая из которых является рациональным многообразием.

2. Если $n = 2$, $g = 3$ и образ $f_W(V_{(\alpha_1, \dots, \alpha_s)})$ состоит из одной точки, то $T(\alpha_1, \dots, \alpha_s, E_2)$ состоит из 3 неприводимых компонент многообразия $R_2(G)$, каждая из которых является рациональным многообразием.

В случае $n = 2$, $g = 3$ многообразие $R_n(G)$ состоит из $(3-d)f + d \prod_{i=1}^s C_{n+m_i-1}^{m_i-1}$ компонент, где f — число таких наборов разбиений $(\alpha_1, \dots, \alpha_s)$, что $f_W(V_{(\alpha_1, \dots, \alpha_s)})$ состоит из одной точки.

Размерности неприводимых компонент описываются формулой (4).

Для доказательства теоремы 1 нам необходим ряд лемм. Следующая лемма может быть доказана дословным повторением рассуждений из [5].

ЛЕММА 1. Пусть $A \in GL_n(K)$. Положим

$$V_g(A) = \{(y_1, \dots, y_g) \in GL_n(K)^g \mid y_1^2 \dots y_g^2 = A\}.$$

Пусть $g \geq 3$. Справедливы следующие утверждения.

1) Если $(n, g) \neq (2, 3)$, либо $(n, g) = (2, 3)$ и A не является скалярной матрицей, то $V_g(A)$ состоит из двух непересекающихся рациональных компонент размерности $(g-1)n^2$.

2) Если $n = 2$, $g = 3$, $A = \beta E_2$, то $V_3(A)$ состоит из трех рациональных компонент размерности 8.

ЛЕММА 2. Если U — неприводимая компонента многообразия $T(\alpha_1, \dots, \alpha_s, A)$, то

$$\dim U = (g-1)n^2 + \dim V_{(\alpha_1, \dots, \alpha_s)}.$$

ДОКАЗАТЕЛЬСТВО. Так как $T(\alpha_1, \dots, \alpha_s, A)$ является подмногообразием в

$$V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^g,$$

задаваемым n^2 уравнениями, то

$$\dim U \geq \dim V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^g - n^2 = (g-1)n^2 + \dim V_{(\alpha_1, \dots, \alpha_s)}. \quad (5)$$

Чтобы доказать противоположное неравенство, рассмотрим морфизм

$$\begin{aligned} \pi : T(\alpha_1, \dots, \alpha_s, A) &\rightarrow V_{(\alpha_1, \dots, \alpha_s)}, \\ \pi(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) &= (A_1, \dots, A_s, B_1, \dots, B_k). \end{aligned} \quad (6)$$

Пусть π' — ограничение π на U . Для произвольной точки $(A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$ слой

$$\begin{aligned} \pi'^{-1}(A_1, \dots, A_s, B_1, \dots, B_k) &= \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \mid \\ &C_1, \dots, C_g \in GL_n(K), C_1^2 \dots C_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k) = A\}, \end{aligned}$$

можно отождествить с подмногообразием в $V_g(D)$, где $D = AW(A_1, \dots, A_s, B_1, \dots, B_k)^{-1}$. Поэтому по лемме 1 все слои морфизма π' имеют размерность не более чем $(g-1)n^2$. Тогда по теореме о размерности слоев морфизма,

$$\dim U \leq \dim V_{(\alpha_1, \dots, \alpha_s)} + (g-1)n^2. \quad (7)$$

Из неравенств (5), (7) следует требуемое равенство. $\square$

ЛЕММА 3. Для любой неприводимой компоненты U многообразия $T(\alpha_1, \dots, \alpha_s, A)$ ограничение π' морфизма π на U является доминантным морфизмом $U \rightarrow V_{(\alpha_1, \dots, \alpha_s)}$. При этом все слои морфизма π' имеют размерность $(g-1)n^2$.

ДОКАЗАТЕЛЬСТВО. В самом деле, предположим, что $\dim \overline{\pi(U)} < \dim V_{(\alpha_1, \dots, \alpha_s)}$. Для точки $v = (A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$ слой $\pi^{-1}(v)$ можно отождествить с подмногообразием в $V_g(D)$, где $D = AW(A_1, \dots, A_s, B_1, \dots, B_k)^{-1}$. Поэтому по лемме 1 все слои морфизма π' имеют размерность не более чем $(g-1)n^2$. Тогда по теореме о размерности слоев морфизма,

$$\dim U < \dim V_{(\alpha_1, \dots, \alpha_s)} + (g-1)n^2. \quad (8)$$

Получили противоречие, доказывающее доминантность π' . Для того, чтобы в (8) было равенство, также необходимо, чтобы все слои π' имели размерность $(g-1)n^2$. Лемма 3 доказана. $\square$

ЛЕММА 4. Для любой неприводимой компоненты V многообразия $T(\alpha_1, \dots, \alpha_s, A)$ справедливы утверждения:

1) множество

$$U = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \in V \mid C_1, \dots, C_g \text{ — регулярные элементы}\} \text{ —}$$

непустое открытое по Зарисскому подмножество в V ;

2) если пара (n, g) отлична от $(2, 3)$, то множество

$$U' = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \in V \mid C_1^2, \dots, C_g^2 \text{ — регулярные полупростые элементы}\} \text{ —}$$

непустое открытое по Зарисскому подмножество в V ;

Лемма доказывается аналогично доказательству предложений 1.1 и 1.3 в [5].

ЛЕММА 5. Если пара (n, g) отлична от $(2, 3)$, то многообразие $T(\alpha_1, \dots, \alpha_s, A)$ имеет не более двух неприводимых компонент.

ДОКАЗАТЕЛЬСТВО. Допустим противное, пусть $T(\alpha_1, \dots, \alpha_s, A)$ имеет l компонент W_i , где $l > 2$. Обозначим через W'_i открытое подмножество в W_i , получающееся удалением из W_i всех пересечений $W_i \cap W_j$, $j \neq i$. Тогда $W'_i \cap W'_j = \emptyset$ при $i \neq j$. Поскольку все множества $\pi(W'_i)$ плотны в $V_{(\alpha_1, \dots, \alpha_s)}$, то $\cap_i \pi(W'_i) \neq \emptyset$. Пусть $x \in \cap_i \pi(W'_i)$. В силу леммы 1, слой $\pi^{-1}(x)$ состоит из двух неприводимых непересекающихся компонент T_1 и T_2 . Тогда $T_1 \subset W_i$, $T_2 \subset W_j$ для некоторых индексов i, j . При этом $T_1 \cap W'_i \neq \emptyset$, $T_2 \cap W'_j \neq \emptyset$. Но поскольку мы допустили, что $l \geq 3$ и по построению $x \in \cap_i \pi(W'_i)$, то для любого k , отличного от i, j , мы должны иметь $\pi^{-1}(x) \cap W'_k \neq \emptyset$. Следовательно, либо $T_1 \cap W'_k \neq \emptyset$, либо $T_2 \cap W'_k \neq \emptyset$. В первом случае $T_1 \cap W'_k$ и $T_1 \cap W'_i$ — два плотных подмножества в T_1 . Следовательно, $W'_i \cap W'_k \neq \emptyset$ — противоречие. Аналогично получаем противоречие и во втором случае. Лемма 5 доказана. $\square$

ЛЕММА 6. Если пара (n, g) отлична от $(2, 3)$ и $d = 2$, то многообразие $T(\alpha_1, \dots, \alpha_s, A)$ состоит из двух непересекающихся неприводимых компонент.

ДОКАЗАТЕЛЬСТВО. Пусть

$$U = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \in V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^g \mid \det(C_1^2 \dots C_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k)) = \det A\}. \quad (9)$$

Так как $d = 2$, т.е. все n_i четны, то уравнение, задающее U , можно записать в виде

$$(\det C_1 \dots \det C_g (\det B_1)^{\frac{n_1}{2}} \dots (\det B_k)^{\frac{n_k}{2}})^2 = b,$$

где $b \in K$ — константа, определяемая равенством

$$b = \det A (\det A_1)^{-p_1} \dots (\det A_s)^{-p_s}.$$

Здесь p_i — сумма показателей, с которыми A_i входит в слово W . Элемент b является константой, поскольку каждая матрица A_i сопряжена с фиксированной матрицей Z_{α_i} , определенной в предложении 1, и, следовательно, $\det A_i$ не зависит от выбора матрицы $A_i \in V_{\alpha_i}$. Пусть $b_1 \in K$ такой элемент, что $b_1^2 = b$. Тогда многообразие U является объединением двух замкнутых непересекающихся подмножеств U_1 и U_2 , задаваемых уравнениями

$$U_1 = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \in U \mid \det(C_1 \dots C_g) (\det B_1)^{\frac{n_1}{2}} \dots (\det B_k)^{\frac{n_k}{2}} = b_1,$$

$$U_2 = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) \in U \mid \det(C_1 \dots C_g) (\det B_1)^{\frac{n_1}{2}} \dots (\det B_k)^{\frac{n_k}{2}} = -b_1.$$

Следовательно, $T(\alpha_1, \dots, \alpha_s, A)$ является объединением двух непустых непересекающихся замкнутых подмножеств $T_1 = T(\alpha_1, \dots, \alpha_s, A) \cap U_1$ и $T_2 = T(\alpha_1, \dots, \alpha_s, A) \cap U_2$. Значит, $T(\alpha_1, \dots, \alpha_s, A)$ имеет не менее двух неприводимых компонент. Учитывая лемму 5, получаем, что $T(\alpha_1, \dots, \alpha_s, A)$ имеет ровно две неприводимые компоненты. $\square$

ЛЕММА 7. *Если пара (n, g) отлична от $(2, 3)$ и $d = 1$, то многообразие $T(\alpha_1, \dots, \alpha_s, A)$ неприводимо.*

ДОКАЗАТЕЛЬСТВО. Покажем, что в этом случае многообразие U , определенное в (9), неприводимо. Уравнение, задающее U , можно записать в виде

$$(\det C_1)^2 \dots (\det C_g)^2 (\det B_1)^{n_1} \dots (\det B_k)^{n_k} = b, \quad (10)$$

где b определено в доказательстве леммы 6. По условию леммы существует нечетное n_i . Пусть для определенности $n_1 = 2k + 1$. Сделаем замену переменных

$$C_1 = \bar{C}_1 \bar{B}_1^{-k}, \quad C_i = \bar{C}_i, \quad 2 \leq i \leq s, \quad B_j = \bar{B}_j, \quad 1 \leq j \leq k.$$

Тогда уравнение (10) можно переписать в виде

$$\det \bar{B}_1 ((\det \bar{C}_1)^2 \dots (\det \bar{C}_g)^2 (\det \bar{B}_2)^{n_2} \dots (\det \bar{B}_k)^{n_k}) - b = 0.$$

Нетрудно убедиться, что многочлен в левой части неприводим, поскольку $\det \bar{B}_1$ входит в него в первой степени.

Многообразие $T(\alpha_1, \dots, \alpha_s, A)$ содержится в U . Дальнейшее доказательство с незначительными модификациями повторяет доказательство теоремы из § 3 в [5]. Для произвольной неприводимой компоненты $V \subset T(\alpha_1, \dots, \alpha_s, A)$ строится коммутативная диаграмма вида

$$\begin{array}{ccc} V & \xrightarrow{\psi} & W \\ \delta \searrow & & \swarrow \varphi \\ & V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^{g-1} & \end{array}$$

где W — некоторое неприводимое многообразие размерности $(g-1)n^2$, φ, ψ — регулярные морфизмы, а δ — проекция, задаваемая формулой

$$\delta(A_1, \dots, A_s, B_1, \dots, B_k, C_1, \dots, C_g) = (C_2, \dots, C_g).$$

Доказывается, что морфизмы δ, φ, ψ являются доминантными и

$$[K(W) : \delta^*(K(V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^{g-1}))] = 2^n.$$

Отсюда и из коммутативности диаграммы непосредственно следует, что листность морфизма δ на некотором открытом множестве не меньше, чем 2^n . С другой стороны, легко убедиться, что слой $\tilde{\delta}^{-1}(z)$ для аналогичной проекции

$$\tilde{\pi} : T(\alpha_1, \dots, \alpha_s, A) \rightarrow V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^{g-1},$$

где $z \in V_{(\alpha_1, \dots, \alpha_s)} \times GL_n(K)^{g-1}$ — точка "общего" положения, состоит в точности из 2^n элементов. Это означает, что V обязано совпадать с $T(\alpha_1, \dots, \alpha_s, A)$, т.е. $T(\alpha_1, \dots, \alpha_s, A)$ — неприводимое многообразие. $\square$

ЛЕММА 8. Пусть $n = 2$, $g = 3$.

1. Если $\text{Im } f_W$ состоит из одной точки B , то B — скалярная матрица.

2. Если $\text{Im } f_W$ содержит более одной точки, то $\text{Im } f_W$ содержит нескаларную матрицу.

ДОКАЗАТЕЛЬСТВО. 1. Отметим, что если $(A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$, то для любой матрицы $C \in GL_2(K)$

$$(CA_1C^{-1}, \dots, CA_sC^{-1}, CB_1C^{-1}, \dots, CB_kC^{-1}) \in V_{(\alpha_1, \dots, \alpha_s)}.$$

Поэтому

$$\begin{aligned} W(CA_1C^{-1}, \dots, CA_sC^{-1}, CB_1C^{-1}, \dots, CB_kC^{-1}) &= \\ &= CW(A_1, \dots, A_s, B_1, \dots, B_k)C^{-1} = CBC^{-1} = B. \end{aligned}$$

Значит, матрица B перестановочна со всеми матрицами из $GL_2(K)$ и поэтому B — скалярная матрица.

2. Вначале предположим, что существует $n_i \neq 0$. Положим

$$B_i = \text{diag}(d_1, d_2), \quad B_j = E_2 \text{ при } j \neq i, \quad A_r = Z_{\alpha_r},$$

где диагональные матрицы Z_{α_r} определены в предложении 1. Тогда

$$W(A_1, \dots, A_s, B_1, \dots, B_k) = \begin{pmatrix} d_1^{n_i} b_1 & 0 \\ 0 & d_2^{n_i} b_2 \end{pmatrix}$$

для некоторых констант b_1, b_2 и поэтому $W(A_1, \dots, A_s, B_1, \dots, B_k)$ не скалярная матрица при подходящем выборе d_1, d_2 .

Пусть теперь все $n_i = 0$. Тогда для любой точки $(A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$

$$\det W(A_1, \dots, A_s, B_1, \dots, B_k) = b$$

для некоторой константы b . Допустим, что $\text{Im } f_W \subset \{\gamma E_2 \mid \gamma \in K^*\} = L$. Поскольку $\dim \overline{\text{Im } f_W} \geq 1$, то $\text{Im } f_W$ плотное подмножество в L , поэтому функция $\det$ не может быть константой на $\text{Im } f_W$. $\square$

ЛЕММА 9. Пусть $n = 2$, $g = 3$.

1. Пусть $\text{Im } f_W$ состоит из одной точки. Тогда если A — скалярная матрица, то $T(\alpha_1, \dots, \alpha_s, A)$ состоит из 3 неприводимых компонент, а если A — не скалярная матрица, то $T(\alpha_1, \dots, \alpha_s, A)$ состоит из 2 неприводимых компонент.

2. Пусть $\text{Im } f_W$ — не точка. Тогда $T(\alpha_1, \dots, \alpha_s, A)$ состоит из d неприводимых компонент.

Во всех случаях каждая неприводимая компонента является рациональным многообразием размерности $8 + \dim V_{(\alpha_1, \dots, \alpha_s)}$.

ДОКАЗАТЕЛЬСТВО. 1. По лемме 8 $W(A_1, \dots, A_s, B_1, \dots, B_k) = \gamma E_2$ для некоторой константы $\gamma \in K^*$ и для всех точек $(A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$. Поэтому многообразие $T(\alpha_1, \dots, \alpha_s, A)$ задается уравнением

$$C_1^2 C_2^2 C_3^2 = \gamma^{-1} A.$$

Следовательно,

$$T(\alpha_1, \dots, \alpha_s, A) = V_3(\gamma^{-1}A) \times V_{(\alpha_1, \dots, \alpha_s)}$$

и утверждение пункта 1 следует из леммы 1.

2. Покажем вначале, что $T(\alpha_1, \dots, \alpha_s, A)$ имеет не более двух неприводимых компонент. Пусть $L = \overline{\text{Im } f_W}$, $M = \{\gamma A \mid \gamma \in K^*\}$.

Проверим, что $L \not\subset M$. По лемме 8 $\text{Im } f_W$ содержит нескаллярную матрицу D . Если A — скалярная матрица, то очевидно, что $L \not\subset M$. Пусть A — нескаллярная матрица и допустим, что $L \subset M$. Тогда $D = \gamma A$, $\gamma \in K^*$. Поскольку $CDC^{-1} \in L$ для любой матрицы $C \in GL_2(K)$, то $CDC^{-1} = \gamma_C A$, $\gamma_C \in K^*$. Следовательно, $\gamma CAC^{-1} = \gamma_C A$ и это равенство выполняется для всех матриц $C \in GL_2(K)$, что невозможно для нескаллярной матрицы A .

Таким образом, $U = L \setminus M$ — открытое по Зарисскому подмножество в L . Кроме того, существует открытое подмножество $U_1 \subset L$ такое, что $U_1 \subset \text{Im } f_W$. Пусть $U_2 = U_1 \cap U$. Для любой точки $z \in U_2$ по лемме 1 слой $\pi^{-1}(z)$ состоит из двух непересекающихся неприводимых компонент. Рассуждая как при доказательстве леммы 5, получаем, что $T(\alpha_1, \dots, \alpha_s, A)$ имеет не более двух неприводимых компонент.

Пусть теперь $d = 2$. Как и при доказательстве леммы 6, получаем, что $T(\alpha_1, \dots, \alpha_s, A)$ является объединением двух замкнутых непересекающихся подмножеств. Следовательно, эти подмножества являются неприводимыми компонентами $T(\alpha_1, \dots, \alpha_s, A)$.

Пусть $d = 1$. Как и при доказательстве леммы 7, можно показать, что существует только одна неприводимая компонента S многообразия $T(\alpha_1, \dots, \alpha_s, A)$ такая, что открытое подмножество

$$U = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, C_2, C_3) \in S \mid C_1^2, C_2^2, C_3^2 \text{ — регулярные полупростые}\}$$

непусто. Таким образом, объединение S_1 оставшихся компонент должно совпадать с замыканием множества

$$U_1 = \{(A_1, \dots, A_s, B_1, \dots, B_k, C_1, C_2, C_3) \in T(\alpha_1, \dots, \alpha_s, A) \mid C_1^2, C_2^2, C_3^2 \text{ — нерегулярны}\}$$

Мы знаем также по лемме 4, что на любой неприводимой компоненте многообразия $T(\alpha_1, \dots, \alpha_s, A)$ найдется точка $(A_1, \dots, A_s, B_1, \dots, B_k, C_1, C_2, C_3)$ с регулярными C_1, C_2, C_3 . Но условие X — регулярная, а X^2 — нерегулярная матрица эквивалентно тому, что X сопряжена диагональной матрице вида $\text{diag}(a, -a)$; в частности, в этом случае X^2 — скалярная матрица. Поэтому S_1 обязано совпадать с замыканием множества

$$U_2 = \{(A_1, \dots, A_s, B_1, \dots, B_k, X \text{diag}(a, -a)X^{-1}, Y \text{diag}(b, -b)Y^{-1}, Z \text{diag}(c, -c)Z^{-1}) \mid \\ a, b, c \in K^*, X, Y, Z \in GL_2(K)\} \cap T(\alpha_1, \dots, \alpha_s, A).$$

Пусть V — неприводимая компонента $T(\alpha_1, \dots, \alpha_s, A)$, содержащаяся в S_1 . По лемме 3 проекция $\pi' : V \rightarrow V_{(\alpha_1, \dots, \alpha_s)}$ доминантна. Пусть U_3 — открытое подмножество, содержащееся в $V \cap U_2$ и U_4 — открытое подмножество $V_{(\alpha_1, \dots, \alpha_s)}$, содержащееся в $\pi'(U_3)$. Тогда для любой точки $(A_1, \dots, A_s, B_1, \dots, B_k) \in U_4$ справедливо

$$W(A_1, \dots, A_s, B_1, \dots, B_k) = tA$$

для некоторой константы $t \in K^*$. Обозначим $P = \{tA \mid t \in K^*\}$. Тогда $f_W(U_4) \subset P$. Поскольку $\overline{U_4} = V_{(\alpha_1, \dots, \alpha_s)}$, то $f_W(V_{(\alpha_1, \dots, \alpha_s)}) = \overline{f_W(U_4)} \subset P$ в силу того, что P замкнуто в $GL_2(K)$.

Если A — скалярная матрица, то получаем противоречие с леммой 8. Если же A — не скалярная матрица, то для любой точки $(A_1, \dots, A_s, B_1, \dots, B_k) \in V_{(\alpha_1, \dots, \alpha_s)}$ и для любой матрицы

$C \in GL_2(K)$ имеем

$$\begin{aligned} W(A_1, \dots, A_s, B_1, \dots, B_k) &= tA, \\ W(CA_1C^{-1}, \dots, CA_sC^{-1}, CB_1C^{-1}, \dots, CB_kC^{-1}) &= t_1A = \\ &= CW(A_1, \dots, A_s, B_1, \dots, B_k)C^{-1} = tCAC^{-1} \end{aligned}$$

для некоторых $t, t_1 \in K^*$. Таким образом, для любой матрицы C найдется $t_1 \in K^*$ такой, что $t_1A = tCAC^{-1}$. Нетрудно видеть, что для нескаларной матрицы A это не так. Полученное противоречие и доказывает, что многообразие $T(\alpha_1, \dots, \alpha_s, A)$ неприводимо. $\square$

ЛЕММА 10. *Каждая неприводимая компонента многообразия $T(\alpha_1, \dots, \alpha_s, A)$ является рациональным многообразием.*

Доказательство рациональности неприводимых компонент многообразия $T(\alpha_1, \dots, \alpha_s, A)$ полностью аналогично доказательству рациональности неприводимых компонент многообразия представлений фундаментальной группы компактной неориентируемой поверхности в [5].

Леммы 1–10 в совокупности дают доказательство теоремы 1, а теорема 2 является непосредственным следствием теоремы 1.

3. Многообразие представлений групп с копредставлением (2)

Введем некоторые необходимые обозначения. Через f обозначим наибольший общий делитель p и q , через $\Omega(p, q)$ — множество матриц $A \in GL_n(K)$, таких, что A^p и A^q сопряжены. Для матрицы $A \in GL_n(K)$ обозначим через $Z(A)$ ее централизатор. Пусть $A \in \Omega(p, q)$, T_0 — некоторая фиксированная матрица, для которой справедливо равенство:

$$T_0A^pT_0^{-1} = A^q \quad (11)$$

Отметим, что в силу леммы 2.3 из [9], следующие централизаторы совпадают:

$$Z(A^f) = Z(A^p) = Z(A^q) \quad (12)$$

Для матрицы $A \in GL_n(K)$ обозначим через $V_g(A)$ следующее многообразие:

$$V_g(A) = \bigcup_{(\alpha_1, \dots, \alpha_s)} T(\alpha_1, \dots, \alpha_s, E_n),$$

где объединение берется по всем наборам разбиений $(\alpha_1, \dots, \alpha_s)$, а α_i — разбиение n на m_i неотрицательных частей. Пусть d_A число неприводимых компонент многообразия $V_g(A)$, формулу для вычисления d_A можно получить из теоремы 1, а сами неприводимые компоненты будем обозначать $L_i(A)$, $1 \leq i \leq d_A$. Для каждой пары матриц A, T_0 и числа i , $1 \leq i \leq d_A$, рассмотрим морфизм

$$\begin{aligned} f_{A,i,T_0} : L_i(A) \times Z(A^f) \times GL_n(K) &\rightarrow GL_n(K)^{s+k+g+1}, \\ (A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z, T) &\mapsto T(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T_0z)T^{-1} \end{aligned} \quad (13)$$

Докажем следующие утверждения о свойствах морфизма f_{A,i,T_0} .

ЛЕММА 11. *Образ морфизма $\text{Im } f_{A,i,T_0}$ содержится в многообразии $R_n(G(p, q))$.*

ДОКАЗАТЕЛЬСТВО. Для произвольного набора

$$T(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T_0z)T^{-1} \in \text{Im } f_{A,i,T_0}$$

имеем:

$$\begin{aligned} & T(T_0 z)T^{-1}((TX_1 T^{-1})^2 \dots (TX_g T^{-1})^2 W(TA_1 T^{-1}, \dots, TA_s T^{-1}, \\ & \quad TB_1 T^{-1}, \dots, TB_k T^{-1}))^p T(T_0 z)^{-1} T^{-1} = \\ & = TT_0 z(X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k))^p z^{-1} T_0^{-1} T^{-1} = TT_0 z A^p z^{-1} T_0^{-1} T^{-1} \end{aligned} \quad (14)$$

Так как $z \in Z(A^f)$, то в силу (12) правая часть (14) преобразуется к виду

$$TT_0 A^p T_0^{-1} T^{-1} = TA^q T^{-1}.$$

С другой стороны, мы имеем равенство

$$\begin{aligned} & ((TX_1 T^{-1})^2 \dots (TX_g T^{-1})^2 W(TA_1 T^{-1}, \dots, TA_s T^{-1}, TB_1 T^{-1}, \dots, TB_k T^{-1}))^q = \\ & = T(X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k))^q T^{-1} = TA^q T^{-1} \end{aligned}$$

Это означает, что точка $T(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T_0 z)T^{-1}$ принадлежит многообразию $R_n(G(p, q))$, что и завершает доказательство леммы 11. $\square$

ЛЕММА 12. *Образ морфизма $\text{Im } f_{A,i,T_0}$ не зависит от выбора матрицы T_0 .*

ДОКАЗАТЕЛЬСТВО. Пусть $T_1, T_1 \neq T_0$, — другая матрица, для которой также справедливо равенство $T_1 A^p T_1^{-1} = A^q$, и f_{A,i,T_0}, f_{A,i,T_1} — соответствующие морфизмы. Тогда с учётом (11) имеем $T_1^{-1} T_0 A^p T_0^{-1} T_1 = A^p$, откуда следует, что $T_1^{-1} T_0 \in Z(A^p)$. Следовательно, для любого элемента централизатора $z_0 \in Z(A^f)$ в силу равенств (12) имеем $z_1 = T_1^{-1} T_0 z_0 \in Z(A^f)$ и $T_0 z_0 = T_1 z_1$. Следовательно, для любого упорядоченного набора $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T) \in L_i(A) \times GL_n(K)$ справедливо равенство

$$\begin{aligned} & f_{A,i,T_0}(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z_0, T) = \\ & = f_{A,i,T_1}(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z_1, T), \end{aligned}$$

что и требовалось доказать. $\square$

Таким образом, ввиду независимости образа $\text{Im } f_{A,i,T_0}$ от выбора матрицы t_0 далее для образов морфизмов f_{A,i,T_0} мы будем пользоваться обозначением $\text{Im } f_{A,i}$. Замыкание образа $\text{Im } f_{A,i}$ в топологии Зарисского будем обозначать $W_i(A)$. Справедлива следующая теорема.

ТЕОРЕМА 3. 1. *Многообразие $W_i(A)$ является неприводимой компонентной $R_n(G(p, q))$, и этими компонентами исчерпываются все неприводимые компоненты $R_n(G(p, q))$.*

2. *Размерность компоненты $W_i(A)$ равна $\dim V_g(A) + \dim Z(A^f) - \dim Z(A)$.*

3. *Число неприводимых компонент многообразия $R_n(G(p, q))$ равно $\sum_{A \in X} d_A$, где X — множество представителей всех классов сопряженности в $\Omega(p, q)$.*

Для доказательства теоремы 3 нам необходим ряд лемм.

ЛЕММА 13. *Многообразие $R_n(G(p, q))$ является объединением всех своих замкнутых неприводимых подмножеств вида $W_i(A)$.*

ДОКАЗАТЕЛЬСТВО. Многообразие $W_i(A)$ неприводимо как замыкание образа неприводимого многообразия относительно регулярного морфизма. Покажем, что многообразия $W_i(A)$ покрывают $R_n(G(p, q))$. Рассмотрим произвольную точку

$$(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, t) \in R_n(G(p, q)).$$

Пусть $\tilde{A} = X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k)$. Нетрудно видеть, что $\tilde{A} \in \Omega(p, q)$, и найдется неприводимая компонента $L_k(\tilde{A})$, такая, что $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g) \in L_k(\tilde{A})$. Легко проверить, что в таком случае точка $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, t)$ является образом упорядоченного набора $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, E, E) \in L_k(\tilde{A}) \times Z(\tilde{A}^d) \times GL_n(K)$ относительно морфизма $f_{\tilde{A},k,t}$. $\square$

ЛЕММА 14. Если $A, B \in \Omega(p, q)$ — подобные матрицы, то при подходящей нумерации компонент $W_i(A) = W_i(B)$, $1 \leq i \leq d_A$.

ДОКАЗАТЕЛЬСТВО. Пусть $B = SAS^{-1}$. Тогда для всякой матрицы T_0 , такой, что $T_0 A^p T_0^{-1} = A^q$, справедливо равенство $(ST_0 S^{-1})B^p (ST_0 S^{-1})^{-1} = B^q$. Отображение

$$f : V_g(A) \rightarrow V_g(B),$$

$$f(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g) = S(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g)S^{-1},$$

очевидно, является бирегулярным изоморфизмом. Положим $L_i(B) = f(L_i(A))$. Рассмотрим произвольную точку $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z, T) \in L_i(A) \times Z(A^f) \times GL_n(K)$. Тогда, так как $Z(A^f) = S^{-1}Z(B^f)S$, то

$$(S^{-1}A_1 S, \dots, S^{-1}A_s S, S^{-1}B_1 S, \dots, S^{-1}B_k S, S^{-1}X_1 S, \dots, S^{-1}X_g S, S^{-1}z S, TS) \in$$

$$\in L_i(B) \times Z(B^d) \times GL_n(K)$$

и

$$f_{A,i,T_0}(x_1, \dots, x_g, z, T) = f_{B,i,S^{-1}T_0 S}(S^{-1}x_1 S, \dots, S^{-1}x_g S, S^{-1}z S, TS).$$

Значит, $\text{Im } f_{A,i} \subset \text{Im } f_{B,i}$. Аналогично доказывается противоположное включение. Таким образом, $\text{Im } f_{A,i} = \text{Im } f_{B,i}$ и, переходя к замыканиям, получаем, что $W_i(A) = W_i(B)$. $\square$

ЛЕММА 15. Если матрицы $A, B \in \Omega(p, q)$ не подобны, то многообразия $W_i(A)$ и $W_j(B)$ не содержатся друг в друге.

ДОКАЗАТЕЛЬСТВО. Для доказательства нам понадобится описание многообразий представлений групп Баумслэга-Солитера $R_n(BS(p, q))$, полученное в [10]. Пусть $A \in \Omega(p, q)$ — фиксированная матрица, $A_1 = A^f$, где $f = (p, q)$ — наибольший общий делитель p и q , и $T_0 \in GL_n(K)$ такая матрица, что $T_0 A_1^{p_1} T_0^{-1} = A_1^{q_1}$, где $p_1 = \frac{p}{f}$, $q_1 = \frac{q}{f}$. Рассмотрим отображение

$$g_A : Z(A_1) \times GL_n(K) \rightarrow GL_n(K) \times GL_n(K), (Z, X) \mapsto (XAX^{-1}, XT_0 ZX^{-1}).$$

Обозначим через $H(A)$ замыкание в топологии Зарисского образа $\text{Im } g_A$. В [10] доказано, что многообразия $H(A)$ являются в точности неприводимыми компонентами $R_n(BS(p, q))$, и если матрицы A и B не подобны, то многообразия $H(A)$ и $H(B)$ не содержатся друг в друге.

Рассмотрим теперь следующий морфизм:

$$\alpha : R_n(G(p, q)) \rightarrow R_n(BS(p, q)), \alpha(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, t) =$$

$$= (x_1^2 \dots x_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k), t).$$

Поскольку для произвольной точки $z = (A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, t) \in \text{Im } f_{A,i}$ справедливо $\alpha(z) \in H(A)$ и $\text{Im } f_{A,i}$ плотно в $W_i(A)$, то $\alpha(W_i(A)) \subset H(A)$, $1 \leq i \leq d_A$. Покажем теперь, что $\alpha(W_i(A))$ плотно в $H(A)$. Рассмотрим произвольную точку

$$y = g_A(Z, X) = X(A, T_0 Z)X^{-1} \in \text{Im } g_A.$$

Тогда для любой точки $(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g) \in L_i(A)$ имеем

$$\alpha \circ f_{A,i,T_0}(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, Z, X) =$$

$$= X(x_1^2, \dots, x_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k), T_0 Z)X^{-1} = X(A, T_0 Z)X^{-1} = y.$$

Значит, $\alpha(W_i(A)) \supset \text{Im } g_A$, следовательно, $\alpha(W_i(A))$ является плотным подмножеством в $H(A)$.

Допустим теперь, что матрицы $A, B \in \Omega(p, q)$ не подобны, но имеет место включение $W_i(A) \supset W_j(B)$. Тогда $\alpha(W_i(A)) \supset \alpha(W_j(B))$ и мы имеем

$$H(A) = \overline{\alpha(W_i(A))} \supset \overline{\alpha(W_j(B))} = H(B).$$

Приходим к противоречию. Следовательно, многообразия $W_i(A)$ и $W_j(B)$ не содержатся друг в друге. $\square$

ЛЕММА 16. *Размерность многообразия $W_i(A)$ равна $\dim L_i(A) + n^2 + \dim Z(A^f) - \dim Z(A)$, где размерность $\dim L_i(A)$ вычислена в теореме 1.*

ДОКАЗАТЕЛЬСТВО. Для вычисления размерности $W_i(A)$ воспользуемся теоремой о размерности слоев морфизма. Вычислим размерность слоев морфизма f_{A,i,T_0} . Пусть

$$w_0 = f_{A,i,T_0}(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z_0, T_0).$$

Вычислим $\dim f_{A,i,T_0}^{-1}(w_0)$. Пусть

$$u = (C_1, \dots, C_s, D_1, \dots, D_k, Y_1, \dots, Y_g, z, T)$$

и пусть $f_{A,i,T_0}(u) = w_0$. Тогда справедливо равенство

$$\begin{aligned} T_0(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T_0 z_0) T_0^{-1} = \\ = T(C_1, \dots, C_s, D_1, \dots, D_k, Y_1, \dots, Y_g, T_0 z) T^{-1}. \end{aligned} \quad (15)$$

В результате получаем следующую систему уравнений:

$$\begin{aligned} C_i &= T^{-1} T_0 A_i T_0^{-1} T, 1 \leq i \leq s, \\ D_i &= T^{-1} T_0 B_i T_0^{-1} T, 1 \leq i \leq k, \\ Y_i &= T^{-1} T_0 X_i T_0^{-1} T, 1 \leq i \leq g. \end{aligned} \quad (16)$$

Поскольку для точек

$$(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g), (C_1, \dots, C_s, D_1, \dots, D_k, Y_1, \dots, Y_g) \in L_i(A)$$

справедливо равенство

$$X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k) = Y_1^2 \dots Y_g^2 W(C_1, \dots, C_s, D_1, \dots, D_k) = A, \quad (17)$$

то из равенств (16)–(17) получаем $A = T_0^{-1} T A T^{-1} T_0$. Следовательно, $T_0^{-1} T \in Z(A)$, откуда

$$T = T_0 Z_1, \quad (18)$$

где $Z_1 \in Z(A)$. Тогда

$$\begin{aligned} C_i &= Z_1^{-1} A_i Z_1, 1 \leq i \leq s, \\ D_i &= Z_1^{-1} B_i Z_1, 1 \leq i \leq k, \\ Y_i &= Z_1^{-1} X_i Z_1, 1 \leq i \leq g, \end{aligned} \quad (19)$$

и из равенств (15) и (18) получаем $T_0 z_0 = Z_1 T_0 z Z_1^{-1}$, а значит,

$$z = t_o^{-1} Z_1^{-1} T_0 z_0 Z_1. \quad (20)$$

Проверим, что элемент z , определяемый формулой (20), принадлежит $Z(A^f)$. Поскольку $Z(A^f) = Z(A^p) = Z(A^q)$ в силу (12), то следующее вычисление показывает, что $z \in Z(A^f)$:

$$\begin{aligned} zA^pz^{-1} &= (t_o^{-1}Z_1^{-1}T_0z_0Z_1)A^p(Z_1^{-1}z_0^{-1}T_0^{-1}Z_1T_0) = \\ &= t_o^{-1}Z_1^{-1}T_0A^pT_0^{-1}Z_1T_0 = t_o^{-1}Z_1^{-1}A^qZ_1T_0 = t_o^{-1}A^qT_0 = A^p. \end{aligned}$$

Из равенств (18)–(20) следует, что слой $f_{A,i,T_0}^{-1}(w_0)$ изоморфен $Z(A)$. Следовательно, все слои морфизма f_{A,i,T_0} имеют одинаковую размерность, равную $\dim Z(A)$. Поэтому размерность многообразия $W_i(A)$ равна

$$\begin{aligned} \dim W_i(A) &= (\dim L_i(A) + \dim Z(A^f) + \dim GL_n(K)) - \dim Z(A) = \\ &= \dim L_i(A) + n^2 + \dim Z(A^f) - \dim Z(A). \end{aligned}$$

□

ЛЕММА 17. $W_i(A) \neq W_j(A)$ при $i \neq j$.

ДОКАЗАТЕЛЬСТВО. Пусть

$$W_i(A) = \overline{f_{A,i}(L_i(A))}, \quad W_j(A) = \overline{f_{A,j}(L_j(A))},$$

где $L_i(A) \subset T(\alpha_1, \dots, \alpha_s, A)$, $L_i(A) \subset T(\beta_1, \dots, \beta_s, A)$. Допустим, что $W_i(A) = W_j(A)$ при $i \neq j$. Покажем вначале, что тогда $(\alpha_1, \dots, \alpha_s) = (\beta_1, \dots, \beta_s)$. Предположим противное и рассмотрим морфизм

$$\gamma : W_i(A) \rightarrow GL_n(K)^s, \quad \gamma(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z) = (A_1, \dots, A_s).$$

Тогда легко видеть, что $\gamma(W_i(A)) \subset V_{(\alpha_1, \dots, \alpha_s)}$, а $\gamma(W_j(A)) \subset V_{(\beta_1, \dots, \beta_s)}$.

Но $V_{(\alpha_1, \dots, \alpha_s)} \cap V_{(\beta_1, \dots, \beta_s)} = \emptyset$ — противоречие.

Таким образом, $L_i(A), L_j(A) \subset T(\alpha_1, \dots, \alpha_s, A)$. Если многообразие $T(\alpha_1, \dots, \alpha_s, A)$ состоит из одной неприводимой компоненты, то $i = j$ — противоречие. Если многообразие $T(\alpha_1, \dots, \alpha_s, A)$ состоит из двух неприводимых компонент, то $L_i(A), L_j(A)$ являются этими компонентами. По теореме 1 все показатели n_i , с которыми B_i входит в слово $W(A_1, \dots, A_s, B_1, \dots, B_k)$, четны. Рассмотрим регулярную функцию

$$\begin{aligned} \delta : W_i(A) &\rightarrow K, \\ (A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z) &\mapsto \det X_1 \dots \det X_g (\det B_1)^{\frac{n_1}{2}} \dots (\det B_k)^{\frac{n_k}{2}}. \end{aligned} \quad (21)$$

Как и при доказательстве леммы 6 видим, что функция δ принимает значения b на $W_i(A)$ и $-b$ на $W_j(A)$ для некоторой константы b , что невозможно в случае равенства $W_i(A) = W_j(A)$.

Пусть теперь $(g, n) = (3, 2)$, матрица A скалярна и $\text{Im } f_W$ состоит из одной точки. В этом случае многообразие $T(\alpha_1, \dots, \alpha_s, A)$ по теореме 1 состоит из трех неприводимых компонент $L_1(A)$, $L_2(A)$, и $L_3(A)$ равной размерности. Тогда по лемме 16 размерности многообразий $W_1(A), W_2(A), W_3(A)$ равны между собой. Как и выше, регулярная функция δ , определенная в (21), принимает значение b и $-b$ соответственно на многообразиях $W_1(A)$ и $W_2(A)$, поэтому $W_1(A) \cap W_2(A) = \emptyset$.

Остается доказать, что $W_3(A)$ не совпадает ни с $W_1(A)$, ни с $W_2(A)$. Допустим, что $W_1(A) = W_3(A)$. Рассмотрим регулярную функцию

$$\delta_1 : W_1(A) \rightarrow K, \quad (A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, z) \mapsto \text{tr } X_1.$$

Из доказательства теоремы 1 следует, что функция δ_1 тождественно равна нулю на $W_3(A)$, но не обращается тождественно в 0 на $W_1(A)$, что противоречит равенству $W_1(A) = W_3(A)$. □

Доказательство теоремы 3 следует из лемм 13-17.

ТЕОРЕМА 4. *Каждая неприводимая компонента $W_i(A)$ многообразия $R_n(G(p, q))$ является рациональным многообразием.*

ДОКАЗАТЕЛЬСТВО. Введем необходимые обозначения. $(m \times n)$ -матрицу X будем называть правильной верхней треугольной, если она имеет вид

$$\begin{pmatrix} 0 & \dots & 0 & a_1 & a_2 & \dots & a_m \\ \vdots & \dots & \dots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 0 & a_1 & a_2 \\ 0 & \dots & \dots & \dots & \dots & 0 & a_1 \end{pmatrix} \text{ если } m \leq n, \text{ и } \begin{pmatrix} a_1 & a_2 & \dots & \dots & a_n \\ 0 & a_1 & a_2 & \dots & a_{n-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & a_1 & a_2 \\ 0 & 0 & 0 & \dots & a_1 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \text{ если } m \geq n.$$

Без ограничения общности можно считать, что A имеет жорданову нормальную форму $A = \text{diag}(A_1, \dots, A_s)$, где $A_i = \text{diag}(J_{m_{i,1}}(\alpha_i), \dots, J_{m_{i,s_i}}(\alpha_i))$ — $(n_i \times n_i)$ -матрица, являющаяся прямой суммой всех клеток Жордана $J_{m_{i,j}}(\alpha_i)$ из A с собственным значением α_i . Тогда централизатор $Z(A)$ состоит из невырожденных матриц вида

$$C = \text{diag}(C_1, \dots, C_s), \text{ где } C_i = \begin{pmatrix} X_{11} & \dots & X_{1,s_1} \\ \vdots & \ddots & \vdots \\ X_{s_i,1} & \dots & X_{s_i,s_i} \end{pmatrix} \quad (22)$$

и X_{rt} — произвольная правильная верхняя треугольная $(m_{i,r} \times m_{i,t})$ -матрица (см. [20, гл. 3]). Рассмотрим множество $T(A)$ матриц вида $Y = (Y_{ij}) \in GL_n(K)$, где Y_{ij} при $i \neq j$ — произвольная $(n_i \times n_j)$ -матрица, а Y_{ii} имеет следующий вид:

$$Y_{ii} = \begin{pmatrix} Z_{11}^{(i)} & \dots & Z_{1,s_i}^{(i)} \\ \vdots & \ddots & \vdots \\ Z_{s_i,1}^{(i)} & \dots & Z_{s_i,s_i}^{(i)} \end{pmatrix} -$$

блочная матрица, блоки которой описываются следующим образом. Матрица $Z_{rr}^{(i)}$ размера $m_{ir} \times m_{ir}$ имеет вид

$$Z_{rr}^{(i)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ u_{21} & u_{22} & \dots & u_{2,m_{ir}} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m_{ir},1} & u_{m_{ir},2} & \dots & u_{m_{ir},m_{ir}} \end{pmatrix}.$$

Если же $r \neq k$, то $Z_{rk}^{(i)}$ — матрица размера $m_{ir} \times m_{ik}$ следующего вида: если $m_{ir} \leq m_{ik}$, то

$$Z_{rk}^{(i)} = \begin{pmatrix} w_{11} & \dots & w_{1,m_{ik}-m_{ir}} & 0 & \dots & 0 \\ w_{21} & \dots & \dots & \dots & \dots & w_{2,m_{ik}} \\ \vdots & \dots & \dots & \dots & \dots & \vdots \\ w_{m_{ir},1} & \dots & \dots & \dots & \dots & w_{m_{ir},m_{ik}} \end{pmatrix},$$

если же $m_{ir} \geq m_{ik}$, то

$$Z_{rk}^{(i)} = \begin{pmatrix} 0 & \dots & 0 \\ w_{21} & \dots & w_{2,m_{ik}} \\ \vdots & \ddots & \vdots \\ w_{m_{ir},1} & \dots & w_{m_{ir},m_{ik}} \end{pmatrix}$$

Нетрудно видеть, что $\dim T(A) = n^2 - \dim Z(A)$. Обозначим через h_{A,i,T_0} ограничение морфизма f_{A,i,T_0} на $L_i(A) \times Z(A^f) \times T(A)$. Несложное вычисление показывает, что h_{A,i,T_0} — инъективный морфизм. Действительно, если

$$\begin{aligned} h_{A,i,T_0}(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, Z_1, T_1) = \\ h_{A,i,T_0}(A'_1, \dots, A'_s, B'_1, \dots, B'_k, X'_1, \dots, X'_g, Z_2, T_2), \end{aligned}$$

то

$$\begin{aligned} T_1(A_1, \dots, A_s, B_1, \dots, B_k, X_1, \dots, X_g, T_0 Z_1) T_1^{-1} = \\ T_2(A'_1, \dots, A'_s, B'_1, \dots, B'_k, X'_1, \dots, X'_g, T_0 Z_2) T_2^{-1}. \end{aligned} \quad (23)$$

Значит,

$$\begin{aligned} T_1 A_i T_1^{-1} &= T_2 A'_i T_2^{-1}, \quad 1 \leq i \leq s, \\ T_1 B_j T_1^{-1} &= T_2 B'_j T_2^{-1}, \quad 1 \leq j \leq k, \\ T_1 X_r T_1^{-1} &= T_2 X'_r T_2^{-1}, \quad 1 \leq r \leq g, \end{aligned}$$

откуда

$$T_1 X_1^2 \dots X_g^2 W(A_1, \dots, A_s, B_1, \dots, B_k) T_1^{-1} = T_2 X_1'^2 \dots X_g'^2 W(A'_1, \dots, A'_s, B'_1, \dots, B'_k) T_2^{-1}.$$

Следовательно, $T_1 A T_1^{-1} = T_2 A T_2^{-1}$, поэтому $T_2 = T_1 B$ для некоторой матрицы $B \in Z(A)$. Учитывая вид (22) матриц из централизатора $Z(A)$ и вид матриц из $T(A)$, мы получаем, что $B = E$ и, следовательно, $T_1 = T_2$. Тогда равенство (23) влечет $A'_i = A_i$, $B'_j = B_j$, $X'_r = X_r$ для всех индексов i, j, r и $Z_1 = Z_2$, что и доказывает инъективность h_{A,i,T_0} .

Так как $\dim L_i(A) \times Z(A^f) \times T(A) = \dim W_i(A)$, то морфизм h_{A,i,T_0} доминантен. Следовательно, h_{A,i,T_0} — бирациональный изоморфизм (см. [18]), и $W_i(A)$ бирационально изоморфно многообразию $L_i(A) \times Z(A^f) \times T(A)$. По теореме 1 $L_i(A)$ рационально и, очевидно, $Z(A^f)$ и $T(A)$ также рациональны. Следовательно, $W_i(A)$ — рациональное многообразие. Теорема 4 доказана. $\square$

4. Заключение

В статье исследованы многообразия представлений двух классов конечно порожденных групп, которые являются свободными произведениями циклических групп с одним соотношением. Получено описание неприводимых компонент этих многообразий, найдены размерности этих компонент и доказана их рациональность.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Lubotzky A., Magid A. Varieties of representations of finitely generated groups // Memoirs AMS. 1985. Vol. 58, № 336. P. 1-116.
2. Rudnick Z. Representation varieties of solvable groups // J. Pure Appl. Algebra. 1987. Vol. 45. P. 261-272.
3. Беньш-Кривец В. В., Платонов В. П. Кольца характеров представлений конечно порожденных групп // Труды МИАН СССР им. В. А. Стеклова. 1990. Т. 183. С. 169–178.

4. Benyash-Krivetz V.V., Rapinchuk A.S., Chernousov V.I. Representation varieties of the fundamental groups of compact orientable surfaces // Israel J. Math. 1996. Vol. 93. P. 29-71.
5. Беньаш-Кривец В.В., Черноусов В.И. Многообразия представлений фундаментальных групп компактных неориентируемых поверхностей // Матем. сборник. 1997. Т. 188, № 7. С. 47-92.
6. Беньаш-Кривец В. В. Многообразия представлений неевклидовых кристаллографических групп // Докл. НАН Беларуси. 2000. Т. 44, № 4. С. 37-40.
7. Беньаш-Кривец В.В. Многообразия представлений F -групп и их обобщений // Докл. НАН Беларуси. 2001. Т. 45, № 1. С. 9-12.
8. Беньаш-Кривец В.В. Многообразия представлений группы $SL_2(\mathbb{Z})$ // Известия НАН Беларуси. 2001. № 1. С. 8-11.
9. Беньаш-Кривец В.В., Говорушко И.О. Многообразия представлений и характеров групп Баумслага-Солитера // Алгебра, геометрия и теория чисел. Сборник статей. К 75-летию со дня рождения академика Владимира Петровича Платонова. Труды МИАН. 2016. Т. 292. С. 26-42.
10. Беньаш-Кривец В.В., Говорушко И.О. Многообразия представлений групп Баумслага-Солитера в случае не взаимно простых показателей // Весці НАН Беларусі. Сер. фіз.-мат. навук. 2016, № 1. С. 52-56.
11. Дудкин Ф.А. Подгруппы конечного индекса в группах Баумслага-Солитера // Алгебра и логика. 2010. Т. 49, № 3. С. 331-345.
12. Дудкин Ф.А. Неприводимые представления подгрупп конечного индекса групп Баумслага-Солитера // Сиб. матем. журнал. 2013. Т. 54, № 6.
13. Беньаш-Кривец В.В., Говорушко И.О. Многообразия представлений подгрупп конечного индекса групп Баумслага-Солитера // Труды Института математики НАН Беларуси. 2015. Т. 23, № 2. С. 1273-1279.
14. Адмиралова А.Н., Беньаш-Кривец В.В. О многообразиях представлений и характеров одного класса групп с одним соотношением // Вестник БГУ, сер. 1. 2016. № 3. С. 166-172.
15. Адмиралова А.Н., Беньаш-Кривец В.В. О многообразиях представлений некоторых HNN расширений свободных групп // Журнал Белорусского государственного университета. Математика. Информатика. 2018. № 2. С. 10-16.
16. Fine B., Rosenberger G. Algebraic generalizations of discrete groups. A path to combinatorial group theory through one-relator products. New York, Basel: Marcel Dekker, 1999.
17. Спрингер Т.А., Штейнберг Р. Классы сопряженных элементов // Семинар по алгебраическим группам. М.: Мир, 1973. С. 162-262.
18. Мамфорд Д. Алгебраическая геометрия. (I). Комплексные проективные многообразия. М.: Мир, 1979.
19. Холл М. Комбинаторика. М.: Мир, 1970.
20. Гантмахер Ф.Р. Теория матриц. М.: Наука, 1967.

REFERENCES

1. Lubotzky A. & Magid A. 1985, "Varieties of representations of finitely generated groups", *Memoirs AMS.*, vol. 58, no 336, pp. 1-116.
2. Rudnick Z. 1987, "Representation varieties of solvable groups", *J. Pure Appl. Algebra*, vol. 45, pp. 261-272.
3. Benyash-Krivets V. V. & Platonov V. P. 1991, "Character rings of representations of finitely generated groups", *Proc. of the Steklov Institute of Math.*, no. 4, pp. 203-213.
4. Benyash-Krivetz V. V. & Rapinchuk A. S. & Chernousov V. I. 1996, "Representation varieties of the fundamental groups of compact orientable surfaces" *Israel J. Math.*, vol. 93, pp. 29-71.
5. Benyash-Krivetz V. V. & Chernousov V. I. 1997, "Representation varieties of the fundamental groups of compact non-orientable surfaces", *Sbornik: Mathematics*, vol. 188, no. 7, pp. 997-1039.
6. Benyash-Krivetz V. V. 2000, "Representation varieties of non-Euclidean crystallographic groups", *Doklady of the National Academy of Sciences of Belarus*, vol. 44, no. 4, pp. 37-40.
7. Benyash-Krivetz V. V. 2001, "Representation varieties of F -groups and their generalizations", *Doklady of the National Academy of Sciences of Belarus*, vol. 45, no. 1, pp. 9-12.
8. Benyash-Krivetz V. V. 2001, "Representation varieties of the group $SL_2(\mathbb{Z})$ ", *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*, no. 1, pp. 8-11.
9. Benyash-Krivets V. V. & Govorushko I. O. 2016, "Representation and character varieties of the Baumslag–Solitar groups", *Proc. of the Steklov Institute of Math.*, vol. 92, pp. 20-36.
10. Benyash-Krivets V. V. & Govorushko I. O. 2016, "Representation varieties of the Baumslag–Solitar groups in the case of not coprime exponents", *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series*, no. 1, pp. 52-56.
11. Dudkin F. A. 2010, "Subgroups of finite index in Baumslag–Solitar groups", *Algebra and Logic*, vol. 49, no. 3, pp. 221-232.
12. Dudkin F. A., 2013, "Irreducible representations of subgroups of finite index in Baumslag–Solitar groups", *Siberian Math. J.*, vol. 54, no. 6, pp. 1013-1017.
13. Benyash-Krivets V. V. & Govorushko I. O. 2015. "Representation varieties of finite index subgroups of the Baumslag–Solitar groups", *Trudy Inst. Math.*, vol. 23, no. 2, pp. 24–28.
14. Admiralova A. N. & Benyash-Krivets V. V. 2016. "On representation varieties and characters of one class of groups with one relation", *Vestn. Belarus. Gos. Univ. Ser. 1, Fiz. Mat. Inform.*, no. 3, pp. 166–172.
15. Admiralova A. N. & Benyash-Krivets V. V. 2018, "On representation varieties of some HNN-extensions of free groups", *Journal of the Belarusian State University. Mathematics and Informatics*, no. 2, pp. 10–16. (Russian)
16. Fine B., Rosenberger G. 1999, "Algebraic generalizations of discrete groups. A path to combinatorial group theory through one-relator products", New York, Basel: Marcel Dekker.
17. Springer T. A. 1970, "Conjugacy classes", *Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics*, Springer-Verlag Berlin Heidelberg, vol. 131.

-
18. Mumford D. 1976, "Algebraic Geometry, Vol. 1: Complex Projective Varieties", Springer, Berlin.
 19. Hall M. "Combinatorial Theory", John Wiley & Sons Inc, 1975.
 20. Gantmacher F.R. "The Theory of Matrices", Nauka, Moscow, 1967; AMS Chelsea Publ., Providence, RI, 1998.

Получено 5.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512.55

DOI 10.22405/2226-8383-2020-21-1-82-100

Конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом натуральных чисел¹

Е. М. Вечтомов, Д. В. Чупраков

Вечтомов Евгений Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой фундаментальной математики, Вятский государственный университет (г. Киров).

e-mail: vecht@mail.ru

Чупраков Дмитрий Вячеславович — кандидат физико-математических наук, доцент кафедры фундаментальной математики, Вятский государственный университет (г. Киров).

e-mail: chupdiv@yandex.ru

Аннотация

В работе исследуются конечные циклические полукольца с полурешеточным сложением, определенные как конечные циклические мультипликативные моноиды $\langle S, \cdot \rangle$ с введенной на них операцией сложения $(+)$, так, что алгебраическая структура $\langle S, + \rangle$ является верхней полурешеткой и выполняются законы дистрибутивности умножения относительно сложения.

Описано строение конечных циклических полуколец с полурешеточной аддитивной операцией, заданной двухпорожденным идеалом полукольца целых неотрицательных чисел.

Результатом работы является теорема о строении циклических полуколец с полурешеточной аддитивной операцией, заданной двухпорожденным идеалом полукольца целых неотрицательных чисел. Полученный результат, в частности, позволяет установить количество циклических полуколец, соответствующих каждому двухпорожденному идеалу полукольца целых неотрицательных чисел.

В работе используется аппарат идеалов полукольца целых неотрицательных чисел. Получены некоторые свойства идеалов полукольца целых неотрицательных чисел, определяющих структуру конечных циклических полуколец.

Работа дополняет исследования Е. М. Вечтомова и И. В. Орловой, где строение конечных циклических полуколец с идемпотентным некоммутативным сложением описано через конечные циклические полуполя и конечные циклические полукольца с полурешеточным сложением.

Ключевые слова: конечное циклическое полукольцо, полурешеточное сложение, полукольцо целых неотрицательных чисел, идеал.

Библиография: 27 названий.

Для цитирования:

Е. М. Вечтомов, Д. В. Чупраков. Конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом натуральных чисел // Чебышевский сборник, 2020, т. 21, вып. 1, с. 82–100.

¹Работа выполнена при финансовой поддержке государственного задания Минобрнауки РФ «Полукольца и их связи», проект № 1.5879.2017/8.9.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512.55

DOI 10.22405/2226-8383-2020-21-1-82-100

Finite cyclic semirings with semilattice additive operation defined by two-generated ideal of natural numbers

E. M. Vechtomov, D. V. Chuprakov

E. M. Vechtomov — Doctor of Physical and Mathematical Sciences, Professor, Head of Department fundamental mathematics, Vyatka State University (Kirov).

e-mail: vecht@mail.ru

D. V. Chuprakov — Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Fundamental Mathematics, Vyatka State University (Kirov).

e-mail: chupdiv@yandex.ru

Abstract

The article deals with finite cyclic semirings with a semilattice addition which are defined as finite cyclic multiplicative monoids $\langle S, \cdot \rangle$ with an operation of addition $(+)$ such that the algebraic structure $\langle S, + \rangle$ is an upper semilattice and laws of distributivity of multiplication over addition are satisfied.

The structure of finite cyclic semirings with a semilattice additive operation defined by a two-generated semiring of nonnegative integers is described.

The result of the work is a theorem about a structure of cyclic semirings with the semilattice additive operation defined by a two-generated ideal of non-negative numbers. This fact, in particular, allows to calculate the number of cyclic semirings corresponding to each two-generated ideal of non-negative integers.

The method of ideals of a semiring of nonnegative integers is used in the article. Some properties of ideals of semirings of nonnegative integers determining the structure of finite cyclic semirings are obtained.

This work complements the research of E. M. Vechtomova and I. V. Orlova where the structure of finite cyclic semirings with idempotent noncommutative addition is described in terms of cyclic semifields and finite cyclic semirings with semilattice addition.

Keywords: finite cyclic semiring, semilattice addition, semiring of non-negative integers, ideal.

Bibliography: 27 titles.

For citation:

E. M. Vechtomov, D. V. Chuprakov, 2020, "Finite cyclic semirings with semilattice additive operation defined by two-generated ideal of natural numbers", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 82–100.

1. Введение. Основные понятия

Работа посвящена исследованию конечных мультипликативно циклических полуколец с *полурешеточным* (т. е. идемпотентным коммутативным) сложением.

Полукольцом [27] называется алгебраическая структура $\langle S, +, \cdot \rangle$, представляющая собой непустое множество S с заданными на нем двумя ассоциативными бинарными операциями сложения $(+)$ и умножения $(\cdot)$, такими, что умножение дистрибутивно относительно сложения

с обеих сторон: $x(y+z) = xy+xz$, $(x+y)z = xz+yz$. При этом $\langle S, + \rangle$ — аддитивная полугруппа полукольца S , а $\langle S, \cdot \rangle$ — его мультипликативная полугруппа.

Полукольцо может обладать выделенными элементами: нулем 0 — нейтральным по сложению ($x+0=0+x=x$) и поглощающим по умножению ($x \cdot 0 = 0 \cdot x = 0$) и единицей 1 — нейтральным элементом по умножению ($x \cdot 1 = 1 \cdot x = x$). Полукольцо, мультипликативная полугруппа которого является абелевой группой, называется *полуполем*.

В любом полукольце S с полурешеточным сложением естественным образом вводится разностный порядок:

$$a \leq b \iff \exists c \in S \ a + c = b, \quad \text{для всех } a, b \in S. \quad (1)$$

При этом $a + b = \sup\{a, b\}$.

Полукольцо S называется (*мультипликативно*) *циклическим* с образующим α , в обозначениях $S = (\alpha)$, если его мультипликативная полугруппа $\langle S, \cdot \rangle$ является циклической полугруппой $\{\alpha, \alpha^2, \dots, \alpha^n\}$, элемент α — образующий этой полугруппы. При этом, если циклическое полукольцо S содержит единицу 1 , то $1 = \alpha^0$.

Циклическая структура играет важную роль в современной математике. Хорошо известно строение циклических групп, их значение в теории групп [12]. Полностью описаны циклические (моногонные) полугруппы [14]. Класс неоднородных циклических колец в точности совпадает с классом конечных полей [13]. Также известна структура полуколец с циклическим сложением [18]. Обзор основных результатов теории циклических полуколец приведен в работе [6]. Циклические и идемпотентные алгебраические структуры находят приложения в теории кодирования и криптологии [24, 25, 26], в частности теория конечных полей положена в основу названных дисциплин [15].

Напомним, что циклической полугруппой $\langle S, \cdot \rangle$ называется множество S с заданной на нем ассоциативной операцией умножения ($\cdot$), имеющей образующий элемент α , натуральные степени которого α^k , $k \in \mathbb{N}$, исчерпывают множество S . Любая конечная циклическая полугруппа S с образующим α однозначно характеризуется парой натуральных чисел $k, l \in \mathbb{N}$ такими, что $S = \{\alpha, \alpha^2, \dots, \alpha^n, \dots, \alpha^{n+l-1}\}$ и $\alpha^{n+l} = \alpha^n$ [14]. Множество $\{\alpha, \alpha^2, \dots, \alpha^{n-1}\}$ называют хвостом, а множество $\{\alpha^n, \dots, \alpha^{n+l-1}\}$ — циклом полугруппы S . При наличии единицы n -элементная циклическая полугруппа имеет вид $T = \{1, \alpha, \dots, \alpha^{n-1}, \dots, \alpha^{n+l-2}\}$, где $\alpha^{n+l-1} = \alpha^{n-1}$.

Конечные циклические полугруппы без хвоста ($k = 1$) и только они являются конечными группами. При $l = 1$, в свою очередь, будем иметь n -элементную циклическую полугруппу $S = \{\alpha, \alpha^2, \dots, \alpha^n\}$ с поглощающим элементом α^n .

Далее будем рассматривать только конечные циклические полугруппы, не являющиеся группами, иными словами $n \geq 2$.

Задавая на мультипликативных полугруппах S и T всевозможные полукольцевые операции сложения, мы получим все конечные циклические полукольца, отличные от полуполей. Биекция $a^m \leftrightarrow a^{m-1}$, $m \in \{1, \dots, n+l-1\}$, между ними позволяет переносить операцию сложения с S на T , и обратно [10]. Таким образом, между классом всех циклических полуколец без единицы и классом всех циклических полуколец с единицей существует естественное взаимно однозначное соответствие.

Отметим, что мультипликативная полугруппа любого конечного циклического полукольца с коммутативным сложением имеет одноэлементный цикл $\{\alpha^n\}$ (см. [2]), иными словами, выполняется свойство $\alpha^n = \alpha^{n+1}$. Таким образом, α^n является поглощающим элементом как по сложению, так и по умножению.

Задача исследования циклических полуколец с коммутативным сложением поставлена Е. М. Вечтомовым в 2000 году [5, задача 8]. В этой работе описаны бесконечные циклические полукольца с коммутативным сложением [5, теорема 4].

Систематическое изучение конечных циклических полуколец ведется с 2010 года [22]. Подробный обзор результатов исследований циклических полуколец приведен в статье [6]. Мы отметим только основные вехи изучения конечных циклических полуколец с идемпотентным сложением.

Начиная с доклада [2], Е. М. Вечтомовым и И. В. Орловой исследуются циклические полукольца с некоммутативным сложением [7, 8, 9, 16]. В частности, изучение конечных циклических полуколец с идемпотентным некоммутативным сложением сведено к конечным циклическим полуполям и конечным циклическим полукольцам с полурешеточным сложением [7].

Начало исследований конечных циклических полуколец с полурешеточным сложением положено А. С. Бестужевым в работе [1]. В этой работе установлено, что свойства операции сложения в конечном циклическом полукольце с полурешеточным сложением определяются элементами, непосредственно большими 1, и в терминах полурешеток описаны идемпотентные конечные циклические полукольца, представимые полурешетками ширины $m \leq 3$.

Дальнейшее исследование ведется Е. М. Вечтомовым, Д. В. Чупраковым и А. В. Ведерниковой [4, 21, 23]. В статье [4] задача описания конечных циклических полуколец с полурешеточным сложением сведена к исследованию свойств идеалов полукольца целых неотрицательных чисел. В докладе [23] изложен алгоритм построения конечных циклических полуколец с полурешеточным сложением по числу элементов и базису идеала показателей элементов верхнего конуса единицы полукольца. В работе [21] описаны конечные циклические полукольца с полурешеточным сложением, заданные идеалом полукольца целых неотрицательных чисел с двумя взаимно простыми образующими. Наконец, основные результаты данной работы анонсированы в докладах [11, 20].

Ниже в работе мы будем рассматривать циклические полукольца $S = \{1, \alpha, \alpha^2, \dots, \alpha^n\}$ с полурешеточным сложением.

2. Представление конечных мультипликативных циклических полуколец с полурешеточным сложением

Через $\mathbb{N}_0$ обозначим полукольцо целых неотрицательных чисел с арифметическими операциями сложения и умножения. Рассмотрим отрезок первых $n + 1$ целых неотрицательных чисел $\{0, 1, \dots, n\}$ и введем на нем аддитивную (+) и мультипликативную ($\cdot$) операции, заданные для всех $x, y \in \{0, 1, \dots, n\}$ формулами

$$x + y = \min_{x, y, n \in \mathbb{N}_0} \{x + y, n\}, \quad x \cdot y = \min_{x, y, n \in \mathbb{N}_0} \{xy, n\}.$$

Построенная алгебра $\mathbb{N}_n = \langle \{0, 1, \dots, n\}, +, \cdot \rangle$ является полукольцом.

Пусть $S = \{1, \alpha, \dots, \alpha^n\}$ — $(n + 1)$ -элементное циклическое полукольцо с единицей и полурешеточным сложением. На полукольце $\mathbb{N}_n$ зададим порядок $\preceq$ правилом

$$x \preceq y \iff \alpha^x \leq \alpha^y \tag{2}$$

для всевозможных $x, y \in \mathbb{N}_n$.

Порядок $\preceq$ будем называть *порядком, индуцированным конечным циклическим полукольцом S* , а упорядоченное полукольцо $\langle \mathbb{N}_n, \preceq \rangle$ — *полукольцом показателей S* .

Отображение $\alpha^i \rightarrow i$ устанавливает порядковый изоморфизм

$$\langle S, \leq \rangle \cong \langle \mathbb{N}_n, \preceq \rangle \tag{3}$$

между полукольцом S с разностным порядком, заданным правилом (1), и полукольцом $\mathbb{N}_n$ с порядком $\preceq$.

Естественный линейный порядок на множестве $\mathbb{N}_n$ обозначим через $\leq$.

Вводя на верхней полурешетке $\langle \mathbb{N}_n, \preceq \rangle$ аддитивную операцию $\vee_{\preceq}$ правилом

$$b \vee_{\preceq} c = \sup\{b, c\}, \quad b, c \in \mathbb{N}_n,$$

получаем полукольцо

$$\check{\mathbb{N}}_n = \langle \mathbb{N}_n, \vee_{\preceq}, + \rangle,$$

изоморфное полукольцу S .

Таким образом, $(n+1)$ -элементное циклическое полукольцо S с полурешеточным сложением однозначно определяется своей аддитивной полугруппой $\langle S, + \rangle$.

На полукольце $\check{\mathbb{N}}_n$ имеет место аналог сократимости [4, лемма 1]. Если $x + d = y + d < n$ для некоторого $d \in \mathbb{N}_n$, то $x = y$.

Определим в $\check{\mathbb{N}}_n$ разность $y - x$ как наименьший элемент d , относительно естественного порядка $\leq$ такой, что $x + d = y$. Тогда для любых $x, y \in \check{\mathbb{N}}$, если $n - y = n - x$, то $x = y$.

Значит, в силу дистрибутивности в конечном циклическом полукольце S операция полурешеточного сложения однозначно задается суммами единицы со всеми его элементами $\alpha^{p_k} = 1 + \alpha^k, k \in \{0, 1, \dots, n\}$. Иными словами, каждое $(n+1)$ -элементное циклическое полукольцо S с полурешеточным сложением однозначно задается $(n+1)$ -элементным кортежем:

$$(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}, \text{ где } 1 + \alpha^i = \alpha^{p_i}. \quad (4)$$

Операции $\vee_{\preceq}$ и $+$ на полукольце $\check{\mathbb{N}}_n$ связаны следующим соотношением:

$$b \vee_{\preceq} c = \min\{b, c\} + p_{|b-c|}.$$

Обозначим через I множество всех компонент кортежа (4) конечного полукольца S :

$$I = \{p_i : i \in \{0, 1, \dots, n\}\}. \quad (5)$$

Множество I обладает следующими свойствами:

1. Множество $I \subseteq \mathbb{N}_n$ является верхним конусом нуля $0 \in \mathbb{N}_n$ относительно порядка $\preceq$.
2. Множество I является множеством показателей элементов S , выдерживающих прибавление единицы:

$$I = \{k \in \{0, 1, \dots, n\} : k = p_k\}.$$

3. Множество I является идеалом полукольца $\mathbb{N}_n$ [4, Теорема 2].

ЛЕММА 1. Для любых элементов a и b полукольца $\mathbb{N}_n$ с отношением $\preceq$, индуцированным полукольцом S , справедливо свойство:

$$a \preceq b \iff b = a + j, \text{ для некоторого } j \in I, \quad (6)$$

где I — множество элементов кортежа (4), задающего полукольцо S .

ДОКАЗАТЕЛЬСТВО. Для любых двух элементов a и b полукольца $\mathbb{N}_n$, отношение $a \preceq b$ по определению (2) равносильно отношению $\alpha^a \leq \alpha^b$ в S , что, в свою очередь, по (1) равносильно $\alpha^b = \alpha^a + \alpha^c = \alpha^a(1 + \alpha^c) = \alpha^{a+p_c}$. Иными словами, $b = a + j$ для $j = p_c \in I$.

Обратно, пусть $b = a + j$ и $j \in I$. По свойству 2 справедливо равенство $j = p_j$ и, следовательно, $\alpha^b = \alpha^a(1 + \alpha^j) = \alpha^a + \alpha^{(a+j)} = \alpha^a + \alpha^b$, что равносильно $a \preceq b$. Лемма доказана.

Обозначим через I_k множество показателей элементов верхнего конуса $\{\alpha^k\}^\Delta$ конечного циклического полукольца S . В силу леммы 1 выполняется равенство $I_k = I + k$.

Так как полукольцо S является верхней полурешеткой, то и для каждого индекса $k \in \{0, 1, 2, \dots, n\}$ справедливо равенство

$$p_k = \min(I \cap I_k). \quad (7)$$

Отсюда вытекает справедливость следующих утверждений, характеризующих взаимосвязь порядков:

СЛЕДСТВИЕ 1 ([21, лемма 3]). *Для любых элементов $k, l \in \mathbb{N}_n$ и порядка $\preceq$, индуцированного конечным циклическим полукольцом S , из справедливости неравенства $k \preceq l$ следует $k \leq l$, а если $k \leq l$, то либо $k \preceq l$, либо k и l несравнимы.*

СЛЕДСТВИЕ 2 ([4, предложение 2]). *Для каждого элемента p_k кортежа (4), задающего некоторое конечное циклическое полукольцо с полурешеточным сложением, справедливо неравенство $p_k \geq k$.*

Идеал I полукольца $\mathbb{N}_n$ конечен и, значит, порожден конечным базисом $G = \{g_1, \dots, g_l\}$, то есть каждый элемент $b \in I$ представим в виде линейной комбинации $b = \sum_{i=1}^l k_i g_i$, где $k_1, \dots, k_l \in \mathbb{N}_n$ и никакой элемент множества G нельзя представить в виде комбинации остальных элементов G с коэффициентами из $\mathbb{N}_n$. Ясно, что поглощающий элемент n полукольца $\mathbb{N}_n$ может быть базисным только в случае, когда $I = \{0, n\}$.

Так как построение базиса идеала I сводится к последовательному выбору наименьшего элемента $i_j \in I$, не представимого в виде комбинации $i_1, \dots, i_{j-1}$, то базис идеала I определен однозначно.

Идеал I , порожденный базисом $G = \{g_1, \dots, g_l\}$, будем обозначать $I = \langle g_1, g_2, \dots, g_l \rangle$.

Заметим, что имеют место следующие предложения:

ПРЕДЛОЖЕНИЕ 1 ([21, предложение 3]). *Каждое упорядоченное множество $\langle I_k, \preceq \rangle$ относительно порядка $\preceq$, индуцированного конечным циклическим полукольцом S с полурешеточным сложением по правилу (2), является решеткой с наименьшим элементом k и наибольшим — n . Атомами решетки $\langle I_k, \preceq \rangle$ являются в точности элементы вида $k + g_i$ для всевозможных базисных элементов g_i идеала I .*

ПРЕДЛОЖЕНИЕ 2 ([4, теорема 3]). *Кортеж (4), определяющий полурешеточную операцию сложения $(n+1)$ -элементного циклического полукольца S , однозначно восстанавливается по множеству G базисных элементов идеала его компонентов.*

Идеал полукольца целых неотрицательных чисел $J = \langle g_1, g_2, \dots, g_l \rangle$ с базисом $G = (g_1, g_2, \dots, g_l)$ будем называть идеалом, ассоциированным с полукольцом S . Полукольцо S , в свою очередь, назовем ассоциированным с идеалом J .

Ясно, что для каждого $(n+1)$ -элементного циклического полукольца S , ассоциированного с идеалом натуральных чисел J , множество элементов $I = \{p_i : i \in \{0, 1, \dots, n\}\}$ кортежа (4) выражается через идеал J следующим образом:

$$I = \{\min\{j, n\} : j \in J\} \cup \{n\} \quad (8)$$

3. Общие свойства конечных циклических полуколец с полурешеточным сложением

ЛЕММА 2 ([21, лемма 2]). *Если элемент $p_j \neq n$ идеала $I \subseteq \mathbb{N}_n$ с базисом $G = \{g_1, \dots, g_l\}$ представлен в виде*

$$p_j = \sum_{i=1}^l c_i g_i = k + \sum_{i=1}^l d_i g_i, \quad c_i, d_i \in \mathbb{N}_n,$$

то $\min\{c_i, d_i\} = 0$ для каждого $i \in \{1, 2, \dots, l\}$.

ТЕОРЕМА 1 (критерий существования конечного циклического полукольца с полурешеточным сложением [21, теорема 1]). Пусть I — идеал полукольца $\mathbb{N}_n$, порожденный базисом $G = \{g_1, g_2, \dots, g_l\}$, и на полукольце $\mathbb{N}_n$ определен порядок $\preccurlyeq$ свойством:

$$b \preccurlyeq c \iff c = b + j, \text{ для некоторого } j \in I.$$

Тогда следующие условия равносильны:

1) существует единственное $(n+1)$ -элементное циклическое полукольцо S с образующим α и полурешеточным сложением, заданным кортежем:

$$(p_0, p_1, \dots, p_n), \quad 1 + \alpha^i = \alpha^{p_i}, \quad p_i \in I,$$

причем, каждый элемент идеала I входит в кортеж;

2) идеал I является решеткой относительно порядка $\preccurlyeq$;

3) для каждого элемента k полукольца $\mathbb{N}_n$ найдется элемент $p_k \in I$ такой, что $I \cap I_k = I_{p_k}$;

4) для каждого элемента $k < \min G$ полукольца $\mathbb{N}_n$ найдется элемент $p_k \in I$ такой, что $I \cap I_k = I_{p_k}$.

ЛЕММА 3. Пусть $(n+1)$ -элементное циклическое полукольцо S с полурешеточной аддитивной операцией, заданной кортежем

$$(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}$$

ассоциировано с идеалом полукольца целых неотрицательных чисел $J = \langle g_1, g_2, \dots, g_l \rangle$, где наибольший общий делитель базисных элементов $g_1, g_2, \dots, g_l$ равен d . Тогда для каждого $k \in \{0, 1, 2, \dots, n\}$ элемент p_k делится на d в полукольце $\mathbb{N}_n$. При этом, если k не делится на d , то $p_k = n$.

Действительно, $n \in \mathbb{N}_n$ делится на d как поглощающий элемент, а если $p_k \neq n$, то p_k лежит в идеале J , все элементы которого кратны d . Теперь, если k не делится на d , то все элементы $J_k = J + k$ не кратны d , значит, $J \cap J_k = \emptyset$ и, следовательно, $I \cap I_k = \{n\}$, откуда $p_k = n$.

ПРЕДЛОЖЕНИЕ 3. Пусть S — $(n+1)$ -элементное циклическое полукольцо с полурешеточной аддитивной операцией, заданной кортежем

$$(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}.$$

Тогда кортеж

$$(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, dn\}^{dn+1},$$

где $q_k = dn$ для всех индексов $k \in \{0, 1, \dots, dn\}$, не кратных d , и $q_{dt} = dp_t$ для всех $t \in \{0, 1, \dots, n\}$, определяет $(dn+1)$ -элементное циклическое полукольцо.

ДОКАЗАТЕЛЬСТВО. Пусть полукольцо S задано кортежем $(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}$ и I — множество элементов этого кортежа. Рассмотрим множество $S' = \{0, 1, \dots, n\}$ и кортеж $(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, dn\}^{dn+1}$. Согласно теореме 1, этот кортеж определяет $(dn+1)$ -элементное полукольцо, если справедливы условия $I' \cap I'_k = I'_{q_k}$, где $I' = \{q_0, q_1, \dots, q_{dn}\}$, $I'_k = I' + k$ для каждого $k \in \{0, 1, \dots, dn\}$. Ясно, что $I' = dI$.

Для каждого $k \in \{0, 1, \dots, dn\}$, не кратного d , множество I'_k не содержит элементов кратных d , отличных от dn — показателя поглощающего элемента. Значит, $I \cap I'_k = I'_{q_k} = \{dn\}$.

Рассмотрим теперь $k = dt$, где $t \in \{0, 1, \dots, n\}$. Имеем

$$\begin{aligned} I'_k &= I' + dt = dI + dt = d(I + t) = dI_t, \\ I' \cap I'_k &= d(I \cap I_t) = dI_{p_t} = I_{q_{dt}} = I_{q_k}. \end{aligned}$$

Таким образом, по теореме 1, кортеж $(q_0, q_1, \dots, q_{dn}) \in \{0, 1, \dots, dn\}^{dn+1}$ определяет $(dn+1)$ -элементное циклическое полукольцо. Предложение доказано.

ПРЕДЛОЖЕНИЕ 4. Пусть существует $(N + 1)$ -элементное циклическое полукольцо, ассоциированное с идеалом J полукольца целых неотрицательных чисел, порожденным базисом G . Тогда для каждого n , удовлетворяющего неравенству $M < n \leq N$, где $M = \min G$, найдется единственное $(n + 1)$ -элементное циклическое полукольцо S , ассоциированное с идеалом J полукольца целых неотрицательных чисел.

ДОКАЗАТЕЛЬСТВО. Рассмотрим конечное циклическое полукольцо S с полурешеточным сложением, заданным $(N + 1)$ -элементным кортежем $(p_0, p_1, \dots, p_N) \in \{0, 1, \dots, N\}^{N+1}$. Множество I элементов этого кортежа является идеалом.

Для каждого n , удовлетворяющего неравенству $M < n \leq N$, рассмотрим кортеж

$$(q_0, p_1, \dots, q_n) \in \{0, 1, \dots, n\}^{n+1}, \quad q_k = \min\{p_k, n\} \in \{0, 1, \dots, n\}$$

и идеал

$$I' = \{q_k : k \in \{0, 1, \dots, n\}\}.$$

По теореме 1 достаточно показать, что для каждого $k \in \{0, 1, \dots, n\}$ справедливо равенство $I'_{p_k} = I' \cap I'_k$.

С учетом неравенства $p_i \geq i$ для каждого $i \in \{0, 1, \dots, N\}$ имеем

$$\begin{aligned} I' &= \{\min\{p_i, n\} : i \in \{0, 1, \dots, N\}\} = \{\min\{p_i, n\} : p_i \in I\}; \\ I'_k &= I' + k = \{\min\{p_i, n\} + k : p_i \in I\} = \{\min\{p_i + k, n\} : p_i \in I\} = \{\min\{p_i, n\} : p_i \in I_k\}; \\ I' \cap I'_k &= \{\min\{p_i, n\} : p_i \in I \cap I_k\} = \{\min\{p_i, n\} : p_i \in I_{p_k}\} = I'_{p_k}. \end{aligned}$$

Предложение доказано.

Из равносильности 1) $\iff$ 4) теоремы 1, равенства (8) и предложения 4 вытекает следующее утверждение.

СЛЕДСТВИЕ 3. Для каждого идеала J полукольца целых неотрицательных чисел, заданного неодноэлементным базисом $G = \{g_1, g_2, \dots, g_l\}$, и каждого числа n , удовлетворяющего двойному неравенству

$$\max G < n \leq \min \bigcup_{j=1}^{\min G-1} ((J \cap J_j) \setminus J_{p_j}),$$

существует единственное $(n + 1)$ -элементное циклическое полукольцо с полурешеточным сложением, ассоциированное с идеалом J , причем других полуколец с полурешеточным сложением, ассоциированных с идеалом J , нет.

ЗАМЕЧАНИЕ 1. Отметим, что для любого неодноэлементного главного идеала $J = (m)$, полукольца целых неотрицательных чисел каждому числу $n \geq m$ соответствует единственное $(n + 1)$ -элементное циклическое полукольцо с полурешеточным сложением, заданным кортежем $(p_0, p_1, \dots, p_n)$, где $p_k = k$, если k кратно m , и $p_k = n - m$ в противном случае.

ПРЕДЛОЖЕНИЕ 5. Пусть J' — идеал полукольца натуральных чисел и полукольцо S , ассоциировано с идеалом $J = dJ' = \{dj : j \in J'\}$ полукольца целых неотрицательных чисел, тогда S содержит подполукольцо, изоморфное полукольцу S' , ассоциированному с идеалом J' .

ДОКАЗАТЕЛЬСТВО. Пусть J' — идеал полукольца натуральных чисел, $J = dJ'$ и циклическое полукольцо S , ассоциированное с идеалом J , задано кортежем $(p_0, p_1, \dots, p_n) \in \{0, 1, \dots, n\}^{n+1}$. Обозначим через α образующий элемент S .

Рассмотрим натуральное число m , удовлетворяющее условию

$$(m - 1)d < n \leq md,$$

и $(m+1)$ -элементное циклическое полукольцо S' , ассоциированное с идеалом J' , имеющее образующий элемент $\beta \in S'$.

Пусть S' задано кортежем $(q_0, q_1, \dots, q_m) \in \{0, 1, \dots, m\}^{m+1}$. По предложениям 3 и 4 имеет место свойство $p_{dt} = dq_t$ для всех $t < m$.

Рассмотрим отображение $\varphi: S' \rightarrow S$, заданное правилом $\varphi(b^i) = \alpha^{di}$ для всех $i < m$ и $\varphi(\beta^m) = \alpha^n$.

Тогда для произвольных $i, j \leq m$ справедливы равенства

$$\begin{aligned}\varphi(\beta^i \beta^j) &= \varphi(\beta^{\min\{i+j, m\}}) = \alpha^{\min\{d(i+j), n\}} = \alpha^{di} \alpha^{dj} = \varphi(\beta^i) \varphi(\beta^j); \\ \varphi(\beta^i + \beta^m) &= \varphi(\beta^m) = \alpha^n = \alpha^{di} + \alpha^m = \varphi(\beta^i) + \varphi(\beta^m).\end{aligned}$$

Для всех $i \leq j < m$, $i+j < m$ имеем

$$\begin{aligned}\varphi(\beta^i + \beta^j) &= \varphi(\beta^i(1 + \beta^{j-i})) = \varphi(\beta^i \beta^{q_{j-i}}) = \alpha^{di} \alpha^{dq_{j-i}} = \alpha^{di} \alpha^{p_{dj-di}} = \\ &= \alpha^{di}(1 + \alpha^{dj-di}) = \alpha^{di} + \alpha^{dj} = \varphi(\beta^i) + \varphi(\beta^j).\end{aligned}$$

Наконец, для всех $i \leq j < m$, $i+j \geq m$ имеем $di + dj \geq dm \geq n$ и

$$\begin{aligned}\varphi(\beta^i + \beta^j) &= \varphi(\beta^m) = \alpha^n = \alpha^{di} + \alpha^{dj} = \varphi(\beta^i) + \varphi(\beta^j) = \\ &= \alpha^{di}(1 + \alpha^{dj-di}) = \alpha^{di} + \alpha^{dj} = \varphi(\beta^i) + \varphi(\beta^j)\end{aligned}$$

Итак, $\varphi: S' \rightarrow S$ — полукольцевой гомоморфизм и, следовательно, осуществляет требуемое вложение. Предложение доказано.

Следующие диаграммы Хассе (рис. 1) иллюстрируют применение предложения 5.

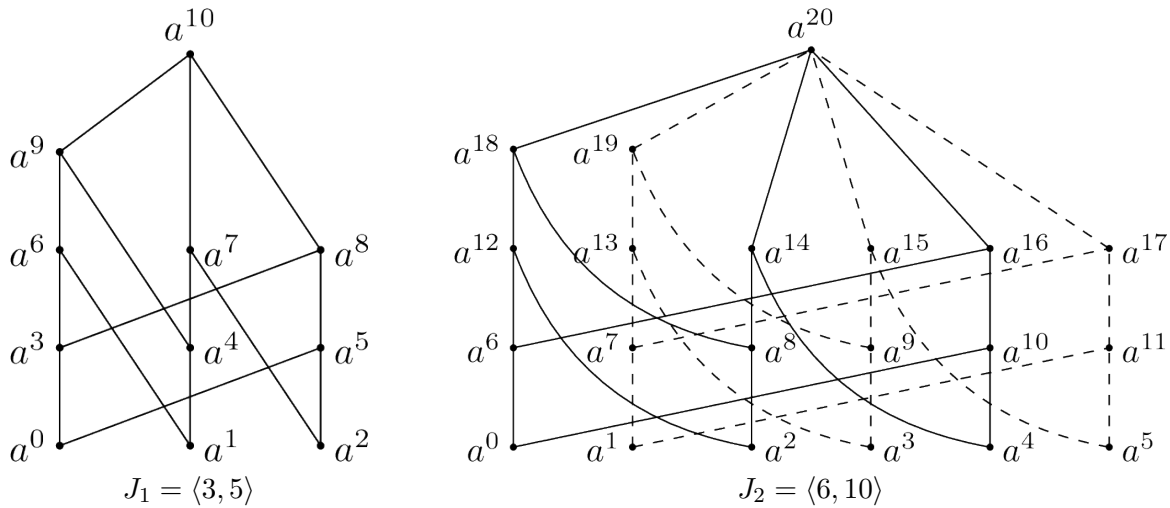


Рис. 1: Диаграммы Хассе полуколец с полурешеточным сложением

В полукольце с операцией сложения, заданной идеалом $J_2 = \langle 6, 10 \rangle$, выделено подполукольцо, изоморфное полукольцу с операцией сложения, заданной идеалом $J_1 = \langle 3, 5 \rangle$.

Заметим также, что для построения циклических полуколец с полурешеточным сложением полезно следующее свойство базисных элементов идеала полукольца целых неотрицательных чисел, ассоциированного с полукольцом S :

ПРЕДЛОЖЕНИЕ 6 ([21]). Пусть $G = \{g_1, \dots, g_k\}$ — базис идеала полукольца целых неотрицательных чисел, ассоциированного с полукольцом S с полурешеточным сложением. Тогда все попарные разности элементов множества G различны.

ДОКАЗАТЕЛЬСТВО. Допустим, что нашлись элементы $g_{i_1}, g_{i_2}, g_{i_3}, g_{i_4} \in G$ и целое неотрицательное число Δ такие, что $g_{i_1} + \Delta = g_{i_2}$, $g_{i_3} + \Delta = g_{i_4}$.

1) Если $g_{i_2} \leq g_{i_3}$, то найдется неотрицательное целое число l , что $g_{i_3} = g_{i_2} + l$.

В полукольце S $\alpha^{g_{i_1}} = \alpha^{g_{i_1}} + \alpha^0$, следовательно $\alpha^{g_{i_3}} = \alpha^{g_{i_1} + l + \Delta} = \alpha^{g_{i_1} + l + \Delta} + \alpha^{l + \Delta}$. Иными словами, $\alpha^{g_{i_3}} > \alpha^{l + \Delta}$. В то же время $\alpha^{g_{i_3}} > \alpha^0$. Значит, $\alpha^{g_{i_3}} \geq \alpha^{p(l + \Delta)}$. Аналогично $\alpha^{g_{i_4}} \geq \alpha^{p(l + \Delta)}$. Так как $\alpha^{g_{i_3}}$ и $\alpha^{g_{i_4}}$ несравнимы, то $\alpha^{g_{i_3}} > \alpha^{p(l + \Delta)}$ и $\alpha^{g_{i_4}} > \alpha^{p(l + \Delta)}$, что противоречит атомарности элементов $\alpha^{g_{i_3}}$ и $\alpha^{g_{i_4}}$.

2) Если $g_{i_2} \geq g_{i_3}$, то существует неотрицательное целое число l , такое, что $g_{i_2} = g_{i_3} + l$. При этом $g_{i_2} = g_{i_1} + \Delta$. Если $g_{i_1} < g_{i_3}$, то $g_{i_3} = g_{i_1} + \Delta'$ и $g_{i_4} = g_{i_2} + \Delta'$, где $\Delta' + l = \Delta$. Дальнейшие рассуждения аналогичны случаю 1.

Результаты параграфа 3 позволяют свести вопрос описания структуры конечных циклических полуколец с полурешеточным сложением к задаче определения наибольшего числа элементов полукольца, ассоциированного с идеалом полукольца целых неотрицательных чисел, базисные элементы которого взаимно просты в совокупности.

4. Строение конечных циклических полуколец с полурешеточным сложением, заданным двухпорожженным идеалом полукольца целых неотрицательных чисел

В начале параграфа (леммы 4, 5, предложение 7) установим свойства идеалов полукольца целых неотрицательных чисел, полезные для исследования конечных циклических полуколец с полурешеточным сложением.

ЛЕММА 4. Для произвольных взаимно простых натуральных чисел g_1 и g_2 , и каждого натурального числа $k \leq \min\{g_1, g_2\}$ существует единственная пара целых чисел v_1 и v_2 таких, что

$$k = v_1 g_1 + v_2 g_2, \quad |v_1| \leq \frac{g_2}{2}, \quad |v_2| \leq \frac{g_1}{2}, \quad (9)$$

причем, хотя бы одно из неравенств строгое.

ДОКАЗАТЕЛЬСТВО. Пусть $\text{НОД}(g_1, g_2) = 1$. Для них найдется единственная пара (см. [17, предложение 61]) целых чисел u_1 и u_2 , что

$$1 = u_1 g_1 + u_2 g_2, \quad |u_1| \leq \frac{g_2}{2}, \quad |u_2| \leq \frac{g_1}{2}. \quad (10)$$

Пусть $u_1 > 0$ и $u_2 < 0$. Если это не так, то изменим нумерацию чисел g_1 и g_2 и соответствующих коэффициентов u_1, u_2 .

Возьмем произвольное натуральное число $k < \min\{g_1, g_2\}$, рассмотрим $k = ku_1 g_1 + ku_2 g_2$ и представим $ku_1 = q_1 g_2 + r_1$ и $-ku_2 = q_2 g_1 + r_2$. Ясно, что $r_1 \neq 0$ и $r_2 \neq 0$. Имеем

$$k = (q_1 - q_2)g_1 g_2 + r_1 g_1 - r_2 g_2.$$

Так как $k < \min\{g_1, g_2\}$, то $k + r_2 g_2 - r_1 g_1 < (r_2 + 1)g_2 - r_1 g_1 < g_1 g_2$. Следовательно, $q_1 - q_2 = 0$. Иными словами, нашлись коэффициенты $r_1 < g_2$, $r_2 < g_1$, что

$$k = r_1 g_1 - r_2 g_2.$$

Покажем, что либо $r_1 \leq \frac{g_2}{2}$ и $r_2 \leq \frac{g_1}{2}$, либо $r_1 \geq \frac{g_2}{2}$ и $r_2 \geq \frac{g_1}{2}$.

Действительно, если $r_1 > \frac{g_2}{2}$, $r_2 < \frac{g_1}{2}$, то $2r_1 = g_2 + t_1$, $2r_2 = g_1 - t_2$ для некоторых натуральных t_1 и t_2 . Значит,

$$2k = 2r_1 g_1 - 2r_2 g_2 = g_1 g_2 + g_1 t_1 - g_1 g_2 + g_2 t_2 = g_1 t_1 + g_2 t_2 > g_1 + g_2.$$

Однако, $2k = 2\min\{g_1, g_2\} < g_1 + g_2$.

Аналогично, если $r_1 < \frac{g_2}{2}$, $r_2 > \frac{g_1}{2}$, то для некоторых натуральных чисел t_1, t_2 имеем $2r_1 = g_2 - t_1$, $2r_2 = g_1 + t_2$,

$$2k = g_1g_2 - g_1t_1 - g_1g_2 - g_2t_2 = -(g_1t_1 + g_2t_2) < 0,$$

что невозможно.

Итак, если $r_1 \leq \frac{g_2}{2}$, $r_2 \leq \frac{g_1}{2}$, то $v_1 = r_1$ и $v_2 = -r_2$. Если же $r_1 \geq \frac{g_2}{2}$, $r_2 \geq \frac{g_1}{2}$, то $v_1 = g_1 - r_2$ и $v_2 = r_1 - g_2$. При этом хотя бы одно из неравенств (9) строгое, так как $k \neq 0$.

Докажем единственность коэффициентов v_1 и v_2 . Ясно, что если $k = v'_1g_1 + v'_2g_2$ для $v'_1 \neq v_1$, $v'_2 \neq v_2$, то $(v'_1 - v_1)g_1 + (v'_2 - v_2)g_2 = 0$ и $v'_1 = v_1 + q_1g_2$, $v'_2 = v_2 + q_2g_1$ для некоторых целых ненулевых q_1, q_2 . Следовательно, $|v'_1| \geq \frac{g_2}{2}$ и $|v'_2| \geq \frac{g_1}{2}$, причем хотя бы одно из неравенств строгое. Лемма доказана.

Непосредственно из леммы 4 вытекает

СЛЕДСТВИЕ 4. Для произвольных натуральных чисел g_1 и g_2 , таких, что $d = (g_1, g_2) \neq \min\{g_1, g_2\}$, и каждого натурального числа $k \leq \min\{g_1, g_2\}$, кратного d , существует единственная пара целых чисел v_1 и v_2 таких, что

$$k = v_1g_1 + v_2g_2, \quad |v_1| \leq \frac{g_2}{2d}, \quad |v_2| \leq \frac{g_1}{2d}, \quad (11)$$

причем хотя бы одно из неравенств строгое.

В линейном представлении (11) числа $k \leq \min\{g_1, g_2\}$ положительное слагаемое обозначим символом k_{g_1, g_2}^+ , а отрицательное — k_{g_1, g_2}^- .

ЛЕММА 5. Для произвольных взаимно простых натуральных чисел g_1, g_2 , и каждого представления натурального числа $k \leq \min\{g_1, g_2\}$ в виде сумм

$$k = \alpha_1g_1 - \alpha_2g_2 = \beta_2g_2 - \beta_1g_1, \quad \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$$

справедливы неравенства

$$\alpha_1g_1 \geq k_{g_1, g_2}^+, \quad \alpha_2g_2 \geq -k_{g_1, g_2}^-, \quad \beta_2g_2 \geq k_{g_1, g_2}^+, \quad \beta_1g_1 \geq -k_{g_1, g_2}^-.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим взаимно простые натуральные числа g_1 и g_2 и число $k \leq \min\{g_1, g_2\}$. По лемме 4 найдутся целые числа v_1, v_2 , что $k = v_1g_1 + v_2g_2$, $|v_1| \leq \frac{g_2}{2}$, $|v_2| \leq \frac{g_1}{2}$, причем хотя бы одно из неравенств строгое. Не умаляя общности будем считать, что

$$k_{g_1, g_2}^+ = v_1g_1, \quad k_{g_1, g_2}^- = v_2g_2.$$

Предположим, что нашлась пара натуральных чисел α_1 и α_2 , для которых $k = \alpha_1g_1 - \alpha_2g_2$ и $0 < \alpha_1g_1 < k_{g_1, g_2}^+$. Тогда $\alpha_1g_1 - \alpha_2g_2 = v_1g_1 - |v_2|g_2 = k$. Так как $\alpha_1g_1 < v_1g_1$ и числа g_1 и g_2 взаимно просты, то $v_1 - \alpha_1 = \delta g_2$, для некоторого $\delta \in \mathbb{N}$.

Однако, в этом случае,

$$\alpha_1g_1 = v_1g_1 - \delta g_2g_1 \leq \frac{g_1g_2}{2} - \delta g_1g_2 = g_1g_2 \left(\frac{1}{2} - \delta \right) < 0.$$

Получаем противоречие предположению.

Пусть натуральные числа α_1 и α_2 таковы, что $k = \alpha_1g_1 - \alpha_2g_2$ и $0 < \alpha_2g_1 < -k_{g_1, g_2}^-$. Тогда $0 < \alpha_2g_1 + k_{g_1, g_2}^- < 0$ и $0 < \alpha_1g_1 = (\alpha_2g_2 + k_{g_1, g_2}^-) + v_1g_1 < v_1g_1$. Что невозможно по доказанному выше.

Рассмотрим теперь произвольные натуральные числа β_1 и β_2 , для которых выполняется условие $k = \beta_2 g_2 - \beta_1 g_1$. Имеем $\beta_2 g_2 - \beta_1 g_1 = v_1 g_1 - |v_2| g_2 = k$. В силу взаимной простоты чисел g_1 и g_2 имеет место равенство $\beta_2 + |v_2| = \delta g_1$ для некоторого натурального числа δ .

$$\beta_2 g_2 = \delta g_1 g_2 - |v_2| g_2 \geq \delta g_1 g_2 - \frac{g_1 g_2}{2} = g_1 g_2 \left(\delta - \frac{1}{2} \right) > \frac{g_1 g_2}{2} \geq |v_1| g_1 = k_{g_1, g_2}^+.$$

Итак, установлено неравенство $\beta_2 g_2 \geq k_{g_1, g_2}^+$.

Справедливость неравенства $\beta_1 g_1 \geq -k_{g_1, g_2}^-$ проверяется аналогично неравенству $\alpha_2 g_2 \geq -k_{g_1, g_2}^-$. Лемма доказана.

ПРЕДЛОЖЕНИЕ 7. Для каждого двухпорожденного идеала целых неотрицательных чисел $J = \langle g_1, g_2 \rangle$, $\text{НОД}(g_1, g_2) = 1$, справедливы следующие утверждения:

- 1) наименьшим элементом множества $J \cap J_k$ является число k_{g_1, g_2}^+ ;
- 2) наименьшим элементом множества $J \cap J_k$, не лежащим во множестве $J_{k_{g_1, g_2}^+}$, является число $g_1 g_2 + k_{g_1, g_2}^-$.

ДОКАЗАТЕЛЬСТВО. Первое утверждение непосредственно следует из лемм 4 и 5.

Докажем второе утверждение. Пусть g_1, g_2 взаимно простые базисные элементы двухпорожденного идеала J . По лемме 4 для каждого $k \leq \min\{g_1, g_2\}$ найдется единственная пара целых чисел v_1 и v_2 , удовлетворяющих условию (9). Причем хотя бы одно из неравенств $|v_1| \leq \frac{g_2}{2}$ или $|v_2| \leq \frac{g_1}{2}$ строгое.

Будем считать, что $v_1 > 0$, $v_2 < 0$. Тогда

$$k_{g_1, g_2}^+ = v_1 g_1, \quad k_{g_1, g_2}^- = v_2 g_2.$$

Обозначим

$$u_1 = (g_2 - v_1) > 0, \quad u_2 = (g_1 + v_2) > 0.$$

Ясно, что

$$k = u_2 g_2 - u_1 g_1, \quad \frac{g_2}{2} \leq u_1 < g_2, \quad \frac{g_1}{2} \leq u_2 < g_1. \quad (12)$$

Рассмотрим элемент $z \in J \cap J_k$, заданный равенством

$$z = u_2 g_2 = k + u_1 g_1. \quad (13)$$

Заметим, что $k_{g_1, g_2}^+ \leq \frac{g_1 g_2}{2} \leq z$, причем хотя бы одно из двух неравенств строгое.

Нам нужно доказать, что $z = \min((J \cap J_k) \setminus J_{k_{g_1, g_2}^+})$.

Сначала установим, что $z \notin J_{k_{g_1, g_2}^+}$. Действительно, предположим, что $z \in J_{k_{g_1, g_2}^+}$, тогда найдутся целые неотрицательные числа c_1, c_2 :

$$z = c_1 g_1 + c_2 g_2 + k_{g_1, g_2}^+.$$

Подставляя в данное равенство линейные представления чисел k_{g_1, g_2}^+ и z в базисе G , получаем:

$$u_2 g_2 = (c_1 + v_1) g_1 + c_2 g_2.$$

Значит, $u_2 > c_2$ и $(u_2 - c_2) g_2 = (c_1 + v_1) g_1$. В силу взаимной простоты чисел g_1 и g_2 разность $u_2 - c_2$ делится на g_1 . Откуда $u_2 - c_2 \geq g_1$, однако, $0 < u_2 - c_2 < u_2 < g_1$. Полученное противоречие доказывает, что $z \in (J \cap J_k) \setminus J_{k_{g_1, g_2}^+}$.

Покажем, что z — наименьший элемент множества $(J \cap J_k) \setminus J_{k_{g_1, g_2}^+}$.

Действительно, пусть $z^* \in (J \cap J_k) \setminus J_{k_{g_1, g_2}^+}$ и $z^* < z$. Ясно, что

$$k_{g_1, g_2}^+ < z^* < z.$$

Так как $z^* \in J \cap J_k$, то $z^* < z$. Найдутся целые неотрицательные числа d_1, d_2 , для которых выполняется равенство $z^* = d_1 g_1 + d_2 g_2$.

Используя равенства (13), получаем

$$g_1 v_1 < d_1 g_1 + d_2 g_2 < u_2 g_2.$$

Заметим, что $d_2 < u_2$ и $d_1 < v_1$. Так как, если $d_2 \geq u_2$, то $z^* = d_1 g_1 + (d_2 - u_2) g_2 + z \in J_{k_{g_1, g_2}^+}$, что невозможно в силу выбора z^* . Противоречие также получается, если допустить, что $d_1 \geq u_1$. В этом случае $z^* = (d_1 - v_1) g_1 + d_2 g_2 + z_0 \in J_{z_0}$.

Так как $z^* \in J_k$, то найдутся целые неотрицательные числа e_1 и e_2 такие, что $z^* = e_1 g_1 + e_2 g_2 + k$.

Пусть $l_1 = \min\{d_1, e_1\}$, $l_2 = \min\{d_2, e_2\}$. Рассмотрим элемент

$$z' = (d_1 - l_1) g_1 + (d_2 - l_2) g_2 = (e_1 - l_1) g_1 + (e_2 - l_2) g_2 + 1 \in J \cap J_1.$$

Ясно, что $z^* = z' + l_1 g_1 + l_2 g_2$. Иными словами, $z' \leq z^*$.

По лемме 2 либо $d_1 - l_1 = 0$, либо $e_1 - l_1 = 0$.

Пусть $d_1 - l_1 = 0$. Обозначим $y_1 = e_1 - l_1 \neq 0$ и $y_2 = d_2 - l_2 \neq 0$. Значит, по лемме 2 $(e_2 - l_2) g_2 = 0$ и $z' = y_2 g_2 = y_1 g_1 + k$.

Имеем, $y_2 g_2 - y_1 g_1 = k$, $y_2 < g_1$ и $y_1 < g_2$.

Из доказательства леммы 4 следует, что возможно два случая:

а) $y_2 \leq \frac{g_1}{2}$ и $y_1 \leq \frac{g_2}{2}$, причем равенства не достигаются одновременно.

б) $\frac{g_1}{2} \leq y_2 < g_1$ и $\frac{g_2}{2} \leq y_1 < g_2$, причем хотя бы одно из неравенств строгое.

В случае а) $z' = z_0$ в силу (13) и леммы 4. При этом, $z^* = z_0 + l_1 g_1 + l_2 g_2 \in J_{k_{g_1, g_2}^+}$, что противоречит доказанному выше.

В случае б) $z' = z$, $z^* \geq z$ и, в силу произвольности выбора элемента $z^* \in (J \cap J_k) \setminus J_{z_0}$, число z — наименьший элемент множества $(J \cap J_k) \setminus J_{z_0}$.

Ситуация $(e_1 - l_1) = 0$ аналогична рассмотренной. Предложение доказано.

Непосредственно из предложения 7 вытекает

ПРЕДЛОЖЕНИЕ 8. Пусть I идеал показателей элементов верхнего конуса $\{\alpha^0\}^\Delta$ конечного циклического полукольца S с полурешеточным сложением, заданный условием (5) и $G = \{g_1, g_2\}$ — его базис, причем $\text{НОД}(g_1, g_2) = 1$. Тогда для каждого элемента $k < \min\{g_1, g_2\}$ полукольца $\mathbb{N}_n$ элемент $p_k = k_{g_1, g_2}^+$.

Сформулируем центральный результат работы.

ТЕОРЕМА 2 (о строении конечного циклического полукольца с полурешеточным сложением, заданным двухпорожденным идеалом). Пусть натуральные числа g_1, g_2 таковы, что $d = (g_1, g_2)$ и $d < g_1 < g_2$. Каждому натуральному числу n , удовлетворяющему неравенствам

$$g_2 < n \leq \frac{g_1 g_2}{d} + \min\{k_{g_1, g_2}^- : k = dt < g_1, t \in \mathbb{N}\}, \quad (14)$$

$$k = k_{g_1, g_2}^+ + k_{g_1, g_2}^-, \quad -\frac{g_1 g_2}{2d} \leq k_{g_1, g_2}^- < 0 < k_{g_1, g_2}^+ \leq \frac{g_1 g_2}{2d}, \quad k_{g_1, g_2}^+, k_{g_1, g_2}^- \in \mathbb{N},$$

соответствует единственное $(n+1)$ -элементное циклическое полукольцо $S = \{1, \alpha, \dots, \alpha^n\}$ с полурешеточным сложением, заданным двухпорожденным идеалом $\langle g_1, g_2 \rangle$. Операция сложения на S определяется свойством $\alpha^{p_i} = 1 + \alpha^i$, где

$$p_i = \begin{cases} k_{g_1, g_2}^+, & k \text{ делится на } d, \\ n, & k \text{ не делится на } d, \end{cases} \quad i \in \{0, 1, \dots, n\}.$$

При этом построенными полукольцами с точностью до изоморфизма исчерпываются все конечные циклические полукольца с полурешеточным сложением, заданным двухпорожденным идеалом $\langle g_1, g_2 \rangle$ полукольца $\mathbb{N}_0$.

ДОКАЗАТЕЛЬСТВО. Пусть $J = \langle g_1, g_2 \rangle$ — двухпорожденный идеал целых неотрицательных чисел и $d = (g_1, g_2)$ — наибольший общий делитель базисных элементов. Будем считать, что $g_1 < g_2$. В силу того, что базис идеала J содержит два элемента, их наибольший общий делитель не совпадает ни с одним из них. Следовательно, $g_1 \geq 2$.

Сначала рассмотрим случай взаимно простых базисных элементов g_1 и g_2 .

По лемме 4 каждое число $k \leq g_1$ может быть единственным образом представлено в виде линейной комбинации $k = k_{g_1, g_2}^+ + k_{g_1, g_2}^-$. Рассмотрим идеалы

$$J \subset \mathbb{N}_0, \quad I = (J \cup \{n\}) \cap \{0, 1, \dots, n\} \subset \mathbb{N}_n$$

и множества

$$J_k = J + k \subset \mathbb{N}_0, \quad I_k = (J_k \cup \{n\}) \cap \{0, 1, \dots, n\} \subset \mathbb{N}_n.$$

По предложению 7 для каждого числа n , удовлетворяющего условию (14), и каждого натурального $k \leq g_1$ справедливо неравенство $\min((J \cap J_k) \setminus J_{k_{g_1, g_2}^+}) \geq n$. Следовательно, выполняется равенство $I_{k_{g_1, g_2}^+} = I \cap I_k$. По теореме 1 существует единственное $(n+1)$ -элементное полукольцо S с множеством показателей элементов верхнего конуса $\{\alpha^0\}^\Delta$.

Пусть теперь $d = (g_1, g_2) \neq 1$. Обозначим $g'_1 = \frac{g_1}{d}$, $g'_2 = \frac{g_2}{d}$ и рассмотрим идеал $J' = \langle g'_1, g'_2 \rangle$, где $g'_1 < g'_2$, $(g'_1, g'_2) = 1$.

Найдется $N' + 1$ -элементное полукольцо S' , ассоциированное с идеалом J' , где $N' = g'_1 g'_2 + \min\{k_{g'_1 g'_2}^- : k \in \mathbb{N}, k < g'_1\}$ — максимально возможный показатель поглощающего элемента полукольца S' .

Так как полукольцо S' однозначно задается кортежем

$$(p_0, p_1, \dots, p_{N'}) \in \{0, 1, \dots, N'\}^{N'+1},$$

то в силу предложения 3 существует $(dN' + 1)$ -элементное циклическое полукольцо S с полурешеточной операцией сложения, определенной кортежем $(q_0, q_1, \dots, q_{dN'}) \in \{0, 1, \dots, dN'\}^{dN'+1}$, где $q_k = dN'$ для всех индексов $k \in \{0, 1, \dots, dN'\}$, некратных d , и $q_{dt} = dp_t$ для всех $t \in \{0, 1, \dots, N'\}$, причем S' вкладывается в S по предложению 5. Ясно, что полукольцо S ассоциировано с идеалом $J = \langle g_1, g_2 \rangle$.

По предложению 4 для каждого n , удовлетворяющего неравенству $dM < n \leq dN$, существует единственное полукольцо, ассоциированное с идеалом J .

Наконец, по следствию 3 других циклических полуколец с полурешеточным сложением, заданным идеалом J , нет. Теорема доказана.

5. Число конечных циклических полуколец с полурешеточным сложением и небольшим числом элементов

Опираясь на теоремы 1, 2, предложения 3, 5, 6, следствие 3 и замечание 1 в системе компьютерной алгебры SageMath нами была составлена программа, подсчитывающая число полуколец и формирующая кортежи (4) для каждого полукольца. С помощью неё найдены, с точностью до изоморфизма, все циклические полукольца с полурешеточным сложением, заданные идеалами полукольца $\mathbb{N}_0$ с базисом G мощности l и содержащие не более 31 элемента. Их число приведено в табл. 1.

Отметим, что все полукольца, найденные программно, обладают свойством, которое мы сформулируем в качестве гипотезы:

Гипотеза. Число элементов конечного циклического полукольца с полурешеточным сложением, заданным идеалом $\langle g_1, g_2, \dots, g_m \rangle$, где $g_1 < g_2 < \dots < g_m$ и $m > 2$, не превосходит максимального числа элементов полукольца, ассоциированного с идеалом $\langle g_1, g_2 \rangle$.

Таблица 1: Число циклических полуколец с полурешеточным сложением

$ G = l$	Порядок полукольца														
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	0	0	1	1	4	5	10	11	17	21	30	32	43	51
3	0	0	0	0	0	0	0	2	2	6	6	17	17	32	39
4	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Число полуко- лец	1	2	3	5	6	10	12	20	22	33	38	59	62	91	107

$ G = l$	Порядок полукольца														
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	62	67	82	91	108	116	132	148	169	175	197	217	239	255	282
3	62	69	105	115	169	182	241	275	369	379	482	540	662	726	890
4	10	10	26	26	60	63	116	122	214	222	355	395	565	614	879
5	0	0	0	0	0	0	0	0	4	4	22	22	68	68	156
Число полуко- лец	150	163	231	251	357	382	511	568	780	805	1082	1201	1562	1692	2237

Данное предположение продиктовано его справедливостью для рассмотренных полуколец малых порядков и тем фактом, что добавление нового элемента к базису идеала J полукольца целых неотрицательных чисел не увеличивает отличные от n значения элементов кортежа (4), задающего полукольцо S , ассоциированное с идеалом J , где n — степень поглощающего элемента полукольца S .

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бестужев А. С. Конечные идемпотентные циклические полукольца // Математический вестник педвузов и университетов Волго-Вятского региона. 2011. Вып. 13. С. 71–78.
2. Бестужев А. С. Вечтомов Е. М. Циклические полукольца с коммутативным сложением // Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика. 2015. Вып. 20. С. 8–39.
3. Бестужев А. С., Вечтомов Е. М., Лубягина И. В. Полукольца с циклическим умножением // Международная конференция «Алгебра и математическая логика», посвященная 100-летию В. В. Морозова. Казань: КФУ, 2011. С. 51–52.
4. Ведерникова А. В., Чупраков Д. В. О представлении конечных идемпотентных циклических полуколец кортежами целых чисел // Математический вестник педвузов и университетов Волго-Вятского региона. 2017. Вып. 19. С. 70–76.
5. Вечтомов Е. М. Введение в полукольца. Киров: ВГПУ, 2000. 44 с.
6. Вечтомов Е. М. Мультипликативно циклические полукольца // Технологии продуктивного обучения математике: традиции и новации. Арзамас: Арзамасский филиал ННГУ, 2016. С. 130–140.
7. Вечтомов Е. М., Лубягина (Орлова) И. В. Циклические полукольца с идемпотентным некоммутативным сложением // Фундаментальная и прикладная математика. 2012. Т. 17. Вып. 1. С. 33–52.

8. Вечтомов Е. М., Орлова И. В. Циклические полукольца с неидемпотентным некоммутативным сложением // *Фундаментальная и прикладная математика*, 2015, Т. 20, № 6, С. 17–41.
9. Вечтомов Е. М., Орлова И. В. Идеалы и конгруэнции циклических полуколец // *Вестник Сыктывкарского университета. Сер.1: Математика. Механика. Информатика*. 2017. Вып. 1(22). С. 29–40.
10. Вечтомов Е. М., Орлова И. В. Конечные циклические полукольца без единицы // *Алгебра и теория алгоритмов [Электронный ресурс]: Всероссийская конференция, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета: сборник материалов. — Иваново: Иван. гос. ун-т, 2018. С. 113–115. Режим доступа: <http://math.ivanovo.ac.ru/math-ivsu-100/materials.html>*
11. Вечтомов Е. М., Орлова И. В., Чупраков Д. В. К теории мультипликативно циклических полуколец // *XV Международная конференция «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения», посвященная столетию со дня рождения профессора Николая Михайловича Коробова 29 мая 2018 г. Тула: ТГПУ им. Л. Н. Толстого, 2018 С. 136–138.*
12. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. 3-е изд., перераб. и доп. М.: Наука, 1982. 288 с.
13. Клиффорд А., Престон Г. Алгебраическая теория полугрупп. В 2-х т. Т. 1. М.: Мир, 1972. 286 с.
14. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Т. 1. М.: Мир, 1988. 430 с.
15. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Т. 2. М.: Мир, 1988. 822 с.
16. Лубягина И. В. О циклических полукольцах с некоммутативным сложением // *Труды Математического центра им. Н. И. Лобачевского. Казань: Издательство Казанского математического общества, 2010. Т. 40. С. 212–215.*
17. Ноден П., Китте К. Алгебраическая алгоритмика с упражнениями и решениями. М.: Мир, 1999. 720 с.
18. Перевощикова Т. Н. О конечных полукольцах // *Вестник ВятГГУ*. 2003. № 8. С. 135–137.
19. Чермных В. В., Николаева О. В. Об идеалах полукольца натуральных чисел // *Математический вестник педвузов и университетов Волго-Вятского региона*. 2009. Вып. 11. С. 118–121.
20. Чупраков Д. В. Конечные циклические полукольца с коммутативным идемпотентным сложением, ассоциированные с двухпорожденными идеалами полукольца натуральных чисел // *Математическое моделирование и информационные технологии : сборник статей Международной научной конференции (10–11 ноября 2017 г., г. Сыктывкар)*. Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2017. с. 148–152.
21. Чупраков Д. В., Ведерникова А. В. О структуре конечных циклических полуколец с идемпотентным коммутативным сложением // *Вестник Сыктывкарского университета. Серия 1: Математика. Механика. Информатика*. 2017. № 2 (23). С. 92–109.

22. Bestugev A. S., Vechtomov E. M. Multiplicatively cyclic semirings // XIII Международная научная конференция им. Академика М. Кравчука. Киев: Национальный технический университет Украины, 2010. С. 39.
23. Chuprakov D. V. Algorithm for constructing finite idempotent cyclic semirings with commutative addition // Proceedings of the 4th Conference of Mathematical Society of Moldova CMSM4'2017, June 28-July 2, 2017, Chisinau, Republic of Moldova. p. 59–62.
24. Durcheva M. I., Trendafilov I. D. Public key cryptosystem based on max-semirings // AIP Conference Proceedings. AIP, 2012. T. 1497. №. 1. P. 357–364.
25. He M., Fan P. A multi-level secret sharing scheme based on semigroup structures // Journal of Software. 2002 V. 13, №. 2 P. 168–175
26. Kumar G., Saini H. Novel Noncommutative Cryptography Scheme Using Extra Special Group // Security and communication networks. 2017. V. 2017.
27. Vandiver H. S. Note on a simple type of algebra in which cancellation law of addition does not hold // Bull. Amer. Math. Soc. 1934. V. 40. № 12. P. 914–920.

REFERENCES

1. Bestuzhev A. S. 2011, “Konechnye idempotentnye ciklicheskie polukolca“, *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 13, pp. 71–78.
2. Bestuzhev A. S. & Vechtomov E. M. 2015, “Cyclic semirings with commutative addition“ *Vestnik Syktyukarskogo universiteta. Seriya 1: Matematika. Mekhanika. Informatika*, no. 20, pp. 8–39.
3. Bestuzhev A. S., Vechtomov E. M. & Lubyagina I. V. 2011, “Polukolca s ciklicheskim umnozheniem“, *Mezhdunarodnaya konferenciya “Algebra i matematicheskaya logika“, posvyashchennaya 100-letiyu V. V. Morozova*, KFU, Kazan, pp. 51–52.
4. Vedernikova A. V. & Chuprakov D. V. 2017, “O predstavlenii konechnyh idempotentnyh ciklicheskih polukolec kortezhami celyh chisel“ *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 19. pp. 70–76.
5. Vechtomov E. M. 2000, “Vvedenie v polukolca“, VGPU, Kirov, 44 p.
6. Vechtomov E. M. 2016, “Multiplicativity idempotent semirings“ *Tekhnologii produktivnogo obucheniya matematike: tradicii i novacii*. Arzamasskij filial NNGU, Arzamas: . pp. 130–140.
7. Vechtomov, E.M. & Orlova, I.V. 2011, “Cyclic semirings with idempotent noncommutative addition“ *Fundamentalnaya i Prikladnaya Matematika*, vol. 17, no. 1, pp. 33–52.
8. Vechtomov, E.M. & Orlova, I.V. 2015, “Cyclic Semirings with Nonidempotent Noncommutative Addition“ *Fundamentalnaya i Prikladnaya Matematika*, vol. 20, no. 6, pp.17–41,
doi: <https://doi.org/10.1007/s10958-018-3922-x>
9. Vechtomov E. M., & Orlova I. V. 2017, “Idealy i kongruencii ciklicheskih polukolec“, *Vestnik Syktyukarskogo universiteta. Seriya 1: Matematika. Mekhanika. Informatika*, no. 1(22). pp. 29–40.

10. Vechtomov E.M. & Orlova I.V. 2018, “Konechnye ciklicheskie polukolca bez edinicy“ *Algebra i teoriya algoritmov: Vserossiyskaya konferenciya, posvyashchennaya 100-letiyu fakul'teta matematiki i komp'yuternykh nauk Ivanovskogo gosudarstvennogo universiteta: sbornik materialov*. — Ivanovo state university, Ivanovo, pp. 113–115. <http://math.ivanovo.ac.ru/math-ivsu-100/materials.html>
11. Vechtomov E.M., Orlova I.V. & Chuprakov D.V. 2018, “K teorii mul'tiplikativno ciklicheskih polukolec“ *XV Mezhdunarodnaya konferenciya «Algebra, teoriya chisel i diskretnaya geometriya: sovremennye problemy i prilozheniya», posvyashchennaya stoletiyu so dnya rozhdeniya profesora Nikolaya Mihajlovicha Korobova 29 may 2018*, TGPU im. L.N. Tolstogo, Tula, pp. 136–138.
12. Kargapolov M.I. & Merzlyakov Y.I. 1982, “Osnovy teorii grupp“. Nauka, Moscow, 288 p.
13. Klifford A. & Preston G. 1972, “Algebraicheskaya teoriya polugrupp“, vol. 1, Mir, Moscow, 286 p.
14. Lidl R., & Niderrajter G. 1988, “Konechnye polya“, vol. v. Mir, Moscow, 430 p.
15. Lidl R., & Niderrajter G. 1988, “Konechnye polya“, vol. 2. Mir, Moscow, 822 p.
16. Lubyagina I.V. 2010, “O ciklicheskih polukolcah s nekommutativnym slozheniem“ *Trudy Matematicheskogo centra im. N.I. Lobachevskogo*, Izdatel'stvo Kazanskogo matematicheskogo obshchestva, Kazan, vol. 40. pp. 212–215.
17. Noden P. & Kitte K. 1999, “Algebraicheskaya algoritmika s uprazhneniyami i resheniyami“, Mir, Moscow, 720 p.
18. Perevoshchikova T.N. 2003, “O konechnykh polukolcah“, no. 8, *Vestnik VyatGGU*, pp. 135–137.
19. Chermnykh V.V. & Nikolaeva O.V. 2009, “Ob idealah polukol'tsa naturalnih chisel“ *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona*, no. 11. pp. 118–121.
20. Chuprakov D.V. 2017, “Konechnye ciklicheskie polukolca s kommutativnym idempotentnym slozheniem, associirovannye s dvuxporozhdennymi idealami polukol'ca naturalnykh chisel“ *Mathematical modeling and information technologies (10–11 november 2017, Syktyvkar)*. Publisher Pitirim Sorokin Syktyvkar State University, Syktyvkar, pp. 148–152.
21. Chuprakov D.V. & Vedernikova A.V. 2017, “About structure of finite cyclic semirings with idempotent commutative addition“ *Vestnik Syktyvskarskogo universiteta. Seria 1: Matematika. Mekhanika. Informatika.*, no. 2 (23), pp. 92–109.
22. Bestugev A.S. & Vechtomov E.M. 2010, “Multiplicatively cyclic semirings“ *XIII Myhaylo Kravchuk's conference*, Kiev, p. 39.
23. Chuprakov D.V. 2017, “Algorithm for constructing finite idempotent cyclic semirings with commutative addition“ *Proceedings of the 4th Conference of Mathematical Society of Moldova CMSM4'2017, June 28–July 2*, Chisinau, Republic of Moldova, pp. 59–62.
24. Durcheva M.I. & 2012, “Trendafilov I.D. Public key cryptosystem based on max-semirings“, *AIP Conference Proceedings*. vol. 1497. no. 1. pp. 357–364.
25. He M. & Fan P. 2002, “A multi-level secret sharing scheme based on semigroup structures“ *Journal of Software*, vol. 13, no. 2 pp. 168–175.

26. Kumar G. & Saini H. 2017, “Novel Noncommutative Cryptography Scheme Using Extra Special Group“, *Security and communication networks*, vol. 2017.
27. Vandiver H. S. 1934, “Note on a simple type of algebra in which cancellation law of addition does not hold“, *Bull. Amer. Math. Soc.*, vol. 40. no. 12. pp. 914–920.

Получено 24.11.2018 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 519.7

DOI 10.22405/2226-8383-2020-21-1-101-134

Умножение¹

С. Б. Гашков, И. С. Сергеев

Гашков Сергей Борисович — доктор физико-математических наук, профессор, Московский государственный университет им. М. В. Ломоносова (г. Москва).

e-mail: sbgashkov@gmail.com

Сергеев Игорь Сергеевич — кандидат физико-математических наук; начальник лаборатории, Научно-исследовательский институт «Квант» (г. Москва).

e-mail: issereg@gmail.com

Аннотация

В работе предпринимается обзор современного состояния теории быстрых алгоритмов умножения чисел и многочленов. Рассматривается процесс эволюции методов умножения от первых блочных алгоритмов Карацубы и Тоома 1960-х гг. к методам 1970-х гг., опирающимся на дискретное преобразование Фурье (ДПФ), и далее к новейшим методам, разработанным в 2007–2019 гг. Современные методы умножения сочетают использование специальных алгебраических структур, переход к приближенным вычислениям, особые формы преобразований Фурье: многомерное ДПФ, аддитивный аналог ДПФ. Эти и другие существенные для быстрых методов умножения концепции подробно рассматриваются в настоящем обзоре. Отдельно предусмотрено введение в теорию ДПФ с извлечением необходимых для изложения материала фактов. В заключительной части обзора приводятся краткие сведения о результатах в области параллельных алгоритмов умножения, аккуратных оценок сложности базовых методов умножения, алгоритмов умножения в реальном времени, мультипликативной сложности умножения многочленов над конечными полями. Отмечены модели вычислений, в которых умножение имеет линейную или квадратичную сложность.

Ключевые слова: быстрые вычисления, умножение, сложность, дискретное преобразование Фурье, аддитивное ДПФ.

Библиография: 89 названий.

Для цитирования:

С. Б. Гашков, И. С. Сергеев. Умножение // Чебышевский сборник, 2020, т. 21, вып. 1, с. 101–134.

¹Исследование выполнено при поддержке гранта РФФИ (проект 19-01-00294а).

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 519.7

DOI 10.22405/2226-8383-2020-21-1-101-134

Multiplication

S. B. Gashkov, I. S. Sergeev

Gashkov Sergey Borisovich — doctor of science, professor, Lomonosov Moscow State University (Moscow).

e-mail: sbgashkov@gmail.com

Sergeev Igor Sergeevich — candidate of science; head of laboratory, Federal State Unitary Enterprise "Scientific and Research Institute "Kvant"(Moscow).

e-mail: isserg@gmail.com

Abstract

The paper provides a survey of the modern state of the theory of fast multiplication of numbers and polynomials. We consider the development of multiplication methods from the initial block algorithms of 1960s due to Karatsuba and Toom to the methods of 1970s based on the Discrete Fourier transform (DFT) and further to the novel methods invented in 2007–2009. Modern multiplication methods combine exploiting of special algebraic structures, the use of approximate computations, special forms of Fourier transforms, namely, multidimensional DFT, additive analogue of DFT. These and other concepts essential for the fast multiplication algorithms are thoroughly discussed in the present survey. In particular, we provide an introduction to the theory of DFT with derivation of facts necessary for the exposition. The final part of the survey contains a brief discussion of results on parallel multiplication algorithms, accurate complexity bounds of the basic methods, online multiplication algorithms, multiplicative complexity of the multiplication of polynomials over finite fields. We mention computational models where multiplication has either linear, or quadratic complexity.

Keywords: fast computations, multiplication, complexity, discrete Fourier transform, additive DFT.

Bibliography: 89 titles.

For citation:

S. B. Gashkov, I. S. Sergeev, 2020, "Multiplication", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 101–134.

1. Введение

Интерес к приемам быстрых вычислений возникал еще у математиков древности: достаточно вспомнить алгоритм Евклида для наибольшего общего делителя. Но только в начале 20-го века появилась математическая теория, позволяющая строго формулировать и давать точные ответы на вопросы типа «как быстро работает данный алгоритм?» или «какой алгоритм быстрее?». Центральное понятие этой теории — *сложность*.

Теория сложности, которую можно отнести к математической логике, дискретной математике или математической кибернетике, возникла в работах американского инженера-теоретика К. Шеннона в 1930-40-е гг.

Технологическая революция середины 20-го века, которая привела к рождению современной электроники, спровоцировала стремительное развитие сопутствующих научных дисциплин: информатики, кибернетики, вычислительных методов, теории алгоритмов и сложности.

Помимо Шеннона, значительный вклад в создание математического аппарата этих теорий внес А. Н. Колмогоров (см., например, [13]). Он же активно поддерживал работы по новым направлениям в СССР и за рубежом.

Быстрые алгоритмы для отдельных арифметических операций стали появляться, не дожидаясь ни окончательного оформления теории, ни появления мощных вычислительных средств. Несколько примеров. В 1938 г. Д. Лехмер построил ускоренную версию алгоритма НОД Евклида, что интересно, специально ориентированную для применения в вычислительных машинах. Метод Лехмера лежит в основе современных быстрых алгоритмов НОД. Год спустя А. Брауэр опубликовал оптимальный по числу умножений метод возведения в натуральную степень — он примерно вдвое быстрее тривиального бинарного метода.

В 1950-е годы инженеры и математики уже активно разрабатывали эффективные конструкции схем или программ для быстрой реализации арифметики. Из теоретических результатов можно отметить полученное в конце 1950-х гг. учениками А. Г. Витушкина (который, в свою очередь, был учеником Колмогорова) В. Я. Паном и Э. Г. Белагой окончательное решение задачи о сложности вычисления значения заданного многочлена в точке. Чуть раньше в США этой задачей занимался Т. Моцкин. В частности, ими были построены быстрые алгоритмы вычисления многочлена, использующие примерно в 2 раза меньше умножений коэффициентов, чем в схеме Горнера.

Однако именно с появлением быстрого метода умножения чисел А. А. Карацубы в 1960 г. (а вернее, с его опубликованием в 1962 г.) связывается становление нового научного направления — теории быстрых вычислений. Экстраординарное влияние, которое оказал результат Карацубы на развитие теории, объясняется совокупным действием нескольких обстоятельств. С одной стороны, результат оказался сенсационным (многие считали, что школьный метод умножения оптимален). С другой стороны, метод Карацубы демонстрирует эффективность общего приема сведения большой задачи к задачам меньшего размера, который затем успешно применялся для построения быстрых алгоритмов многих других арифметических операций. В-третьих, умножение является фундаментальной операцией — строительным блоком для многих других операций арифметики, которые, как следствие, автоматически ускоряются за счет ускорения алгоритма умножения.

В результате, как объективные факторы (фундаментальность операции умножения), так и субъективные (эффект, произведенный методом Карацубы) привели к тому, что задача исследования сложности умножения стала центральной для теории быстрых вычислений.

К моменту появления первых быстрых алгоритмов умножения (Карацубы и Тоома) в начале 1960-х гг. аппарат теории сложности вполне сформировался, и центральный вопрос о сложности реализации произвольной булевой функции был решен в асимптотическом смысле для нескольких основных вычислительных моделей О. Б. Лупановым.

Можно увидеть сходство сюжетов развития быстрых методов вычисления булевых функций и быстрых методов умножения. Первую нетривиальную оценку сложности вычисления функции дает метод каскадов Шеннона. При помощи формулы

$$f(x_1, x_2, \dots, x_n) = f(1, x_2, \dots, x_n) \cdot x_1 \vee f(0, x_2, \dots, x_n) \cdot \overline{x_1}$$

он сводит исходную задачу к двум подобным задачам меньшего размера — реализации подфункций ($\bar{x}$ — отрицание переменной x). Аналогично, метод Карацубы сводит исходное умножение к трем умножениям меньшего размера, только используемая в нем формула менее очевидна. Асимптотически оптимальный метод Лупанова нетривиально развивает идею метода каскадов и состоит в сведении к вычислению функции в локальных областях. Принцип, лежащий в основе метода, получил название принципа локального кодирования. В задаче умножения этому принципу соответствует идея интерполяции. На интерполяции основаны все быстрые методы умножения, начиная с метода Тоома.

Эту оценку можно также вывести рекурсивным способом. Разобьем $2n$ -разрядные числа A и B на блоки по n разрядов: $A = A_1 2^n + A_0$, $B = B_1 2^n + B_0$. Теперь умножение исходных чисел выполняется при помощи четырех умножений «половинок» и нескольких сложений по формуле

$$AB = A_1 B_1 2^{2n} + (A_0 B_1 + A_1 B_0) 2^n + A_0 B_0. \quad (1)$$

Размышляя над поставленной А. Н. Колмогоровым задачей о сложности умножения, в 1960 г. А. А. Карацуба (в то время аспирант МГУ) обнаружил более экономную, чем (1), формулу

$$AB = A_1 B_1 2^{2n} + (A_1 B_1 + A_0 B_0 - (A_0 - A_1)(B_0 - B_1)) 2^n + A_0 B_0, \quad (2)$$

которая требует только трех умножений n -разрядных чисел и нескольких сложений-вычитаний. Для сложности метода $K(n)$ получается рекуррентное соотношение:

$$K(2n) \leq 3K(n) + O(n),$$

которое разрешается как $K(n) = O(n^{\log 3})$. (Здесь и далее по тексту все логарифмы — по основанию 2.)

Подробно об истории появления первого быстрого метода умножения рассказывает сам его автор в [9, 10].

Аналогичный метод и результат имеют место для многочленов. Полиномиальная аналогия позволяет увидеть в основе метода Карацубы идею интерполяции. Так, умножение многочленов степени 1 выполняется в три приема:

- i) Вычисление значений многочленов в трех точках²: $0, -1, \infty$.
- ii) Перемножение значений в каждой точке.
- iii) Восстановление многочлена, имеющего заданные значения в точках интерполяции, см. формулу (2).

Развитие идеи интерполяции привело к появлению теоретически более быстрых методов умножения.

3. Блочные методы умножения 1960-х

Первый такой метод предложил А. Л. Тоом (тогда студент мехмата МГУ) в 1963 г. [22]. В методе Тоома каждый множитель разбивается на r блоков:

$$A = \sum_{i=0}^{r-1} A_i 2^{iq}, \quad B = \sum_{i=0}^{r-1} B_i 2^{iq}, \quad A_i, B_i < 2^q. \quad (3)$$

Произведение чисел восстанавливается из произведения многочленов $A(X) = \sum A_i X^i$ и $B(X) = \sum B_i X^i$ подстановкой $X = 2^q$. Для умножения многочленов выполняется интерполяция в $2r - 1$ точках: $-r + 1, \dots, r - 1$.

Заметим, что умножения в методе Тоома возникают не только в точках интерполяции, но также и при вычислении значений многочленов $A(X)$ и $B(X)$ в этих точках, и при восстановлении многочлена $A(X)B(X)$ по значениям в точках. В оригинальном методе этап восстановления рассматривается как решение системы линейных уравнений на коэффициенты искомого многочлена.

Метод Тоома практичен при небольших значениях r . При выборе $r = 2$ получается просто вариант метода Карацубы. По сей день для умножения чисел в диапазоне от нескольких десятков до 1000 двоичных разрядов обычно применяются методы Карацубы и троичный ($r = 3$)

²Значение многочлена в точке ∞ полагается равным старшему коэффициенту.

вариант метода Тоома. Но для вывода теоретической оценки сложности следует выбирать r растущим вместе с n , оптимальным является выбор $r = 2^{\Theta(\sqrt{\log n})}$.

Авторская оценка сложности метода имеет вид $O\left(n2^{5\sqrt{\log n}}\right)$. Более тщательный анализ, выполненный Д. Кнудом (см. [11]), привел к уточнению оценки до $O\left(n2^{\sqrt{2\log n}} \log n\right)$.

Адаптированный для умножения многочленов вариант метода Тоома (указан С. Куком [40]) предлагает в качестве точек интерполяции выбирать многочлены малых степеней с коэффициентами 0 и 1. Такой выбор универсален: он позволяет умножать и двоичные многочлены. Рекордные оценки сложности умножения двоичных многочленов степени в пределах одной-двух сотен получаются специальным образом оптимизированными блочными методами, см., например, [37, 46, 73].

Если посмотреть шире, в основе метода Тоома можно увидеть идею перехода к модулярному представлению, поскольку интерполяция — это частный случай этой идеи. В модулярном представлении многочлен записывается как набор остатков по модулям некоторых заданных многочленов $f_i(x)$. Метод Тоома—Кука, как изложен выше, использует многочлены $x^q - \alpha_i$, где α_i — это точки: числа или многочлены.

Развивая модулярную идею, А. Шёнхаге в 1966 г. [78] построил подходящую систему модулей вида $2^{q_i} - 1$ и получил еще один метод умножения чисел с оценкой сложности $O\left(n2^{\sqrt{2\log n}} \log^{3/2} n\right)$.

За год до этого появилась статья Дж. Кули и Дж. Тьюки [41], в которой авторы указали быстрый способ вычисления дискретного преобразования Фурье (ДПФ) и вообще обратили внимание на ДПФ как инструмент быстрых вычислений. С тех пор все новые быстрые алгоритмы умножения опираются на ДПФ.

4. Дискретное преобразование Фурье

Привлечение ДПФ к задаче умножения фактически положило конец дискуссии об оптимальном выборе точек для интерполяции. Умножение при помощи ДПФ использует в качестве точек интерполяции группу корней из единицы. Далее приводятся некоторые сведения о ДПФ, необходимые для описания быстрых методов умножения.

Следуя [53], дадим формальное определение. Пусть K — коммутативное, ассоциативное кольцо с единицей. Элемент $\zeta \in K$ называется *примитивным (первообразным) корнем степени $N \in \mathbb{N}$* , если $\zeta^N = 1$, и никакой из элементов $\zeta^{N/p} - 1$, где p — простой делитель числа N , не является делителем нуля в K . (Напомним, что элемент a называется делителем нуля, если существует ненулевой элемент b , такой, что $ab = 0$.)

Дискретным преобразованием Фурье (ДПФ) порядка N называется $(K^N \rightarrow K^N)$ -преобразование

$$\text{ДПФ}_{N,\zeta}[K](\gamma_0, \dots, \gamma_{N-1}) = (\gamma_0^*, \dots, \gamma_{N-1}^*), \quad \gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}. \quad (4)$$

где ζ — примитивный корень степени N .

Фундаментальное свойство ДПФ формулируется следующим образом:

ЛЕММА 1. Пусть элементы γ_j^* определяются из (4). Тогда

$$\text{ДПФ}_{N,\zeta^{-1}}[K](\gamma_0^*, \dots, \gamma_{N-1}^*) = (N\gamma_0, \dots, N\gamma_{N-1}),$$

где под N в правой части формулы понимается сумма N единиц кольца.

Как следствие, получаем, что если элемент $N = 1 + \dots + 1 \in K$ обратим, то определено обратное к ДПФ преобразование

$$\text{ДПФ}_{N,\zeta}^{-1}[K] = N^{-1} \cdot \text{ДПФ}_{N,\zeta^{-1}}[K].$$

4.1. Полиномиальная интерпретация ДПФ

Рассмотрим многочлен $\Gamma(x) = \gamma_0 + \dots + \gamma_{N-1}x^{N-1}$. Тогда, по определению,

$$\text{ДПФ}_{N,\zeta}[K](\gamma_0, \dots, \gamma_{N-1}) = (\Gamma(\zeta^0), \dots, \Gamma(\zeta^{N-1})),$$

т.е. ДПФ вычисляет значения многочлена $\Gamma(x)$ в точках ζ^i . Смысл обратного преобразования $\text{ДПФ}_{N,\zeta}^{-1}[K]$ заключается в восстановлении коэффициентов единственного многочлена степени $< N$, имеющего заданный набор значений в точках $\zeta^0, \dots, \zeta^{N-1}$.

Формально, связь между ДПФ и интерполяцией описывается следующей леммой:

ЛЕММА 2. Преобразование $\text{ДПФ}_{N,\zeta}[K]$ задает изоморфизм: $K[x]/(x^N - 1) \rightarrow K^N$.

Рассмотренный изоморфизм приводит к эффективному способу умножения многочленов над K .

ТЕОРЕМА 1. Пусть в кольце K определено преобразование $\text{ДПФ}_{N,\zeta}[K]$ и обратное к нему. Тогда умножение двух многочленов по модулю $x^N - 1$ над K можно выполнить при помощи двух преобразований $\text{ДПФ}_{N,\zeta}[K]$, одного $\text{ДПФ}_{N,\zeta}^{-1}[K]$, N умножений в K и N умножений на константы $N^{-1} \in K$.

Если рассматривать многочлены как вектора коэффициентов, то умножение по модулю $x^N - 1$ совпадает с циклической сверткой порядка N .

4.2. Вычисление ДПФ

Эффективность ДПФ обеспечивается семейством алгоритмов быстрого его вычисления. Эти алгоритмы получили название быстрого преобразования Фурье (БПФ). Вообще, под алгоритмами БПФ понимаются такие алгоритмы, в которых используется прием сведения ДПФ составного порядка N к ДПФ порядка множителей числа N . Иногда термин БПФ прилагается к любым алгоритмам сложности $O(N \log N)$.

Самым популярным примером БПФ является метод Кули—Тьюки [41], основанный на следующей лемме.

ЛЕММА 3 ([41]). ДПФ порядка ST реализуется при помощи S ДПФ порядка T , T ДПФ порядка S и $(S-1)(T-1)$ операций умножения на степени ζ — примитивного корня степени ST .

Доказательство леммы опирается на декомпозицию ДПФ на «внешние» ДПФ порядка S и «внутренние» ДПФ порядка T . При любых $s = 0, \dots, S-1$ и $t = 0, \dots, T-1$ справедливо

$$\begin{aligned} \gamma_{sT+t}^* &= \sum_{I=0}^{ST-1} \gamma_I \zeta^{I(sT+t)} = \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{(iS+j)(sT+t)} = \\ &= \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{itS+jST+jt} = \sum_{j=0}^{S-1} (\zeta^T)^{js} \cdot \zeta^{jt} \cdot \gamma_{(j),t}, \quad (5) \end{aligned}$$

где

$$\gamma_{(j),t} = \sum_{i=0}^{T-1} \gamma_{iS+j} (\zeta^S)^{it}.$$

Учитывая, что ДПФ порядка 2 выполняется при помощи сложения и вычитания, рекурсивным применением леммы 3 выводится

ЛЕММА 4. *ДПФ порядка 2^k может быть выполнено за $k2^k$ операций сложения-вычитания и $(k-2)2^{k-1} + 1$ операций скалярного умножения.*

Эта оценка является асимптотически наилучшей из известных верхних оценок сложности ДПФ порядка 2^k .

Для случая, когда N раскладывается на взаимно простые множители, существует более эффективный алгоритм И. Гуда [54], который не требует дополнительных умножений на степени примитивного корня. Этот алгоритм также называют алгоритмом Гуда—Томаса, т.к. он был переоткрыт Л. Томасом [84] несколько лет спустя после работы Гуда.

ЛЕММА 5 ([54]). *Если $\text{НОД}(S, T) = 1$, то для вычисления ДПФ порядка ST достаточно выполнить S ДПФ порядка T и T ДПФ порядка S .*

Доказательство опирается на следующую декомпозицию. Пусть m, n — коэффициенты Безу из равенства $nS + mT = 1$. Предварительно для $I = 0, \dots, ST - 1$ обозначим $\gamma_I = \gamma_{i,j}$, где $i = I \bmod T$ и $j = I \bmod S$, а для $K = 0, \dots, ST - 1$ обозначим $\gamma_K^* = \gamma_{s,t}^*$, где $s = mK \bmod S$ и $t = nK \bmod T$. Заметим, что $I = (inS + jmT) \bmod ST$ и $K = (sT + tS) \bmod ST$. Тогда при любом K справедливо:

$$\begin{aligned} \gamma_K^* = \gamma_{s,t}^* &= \sum_{I=0}^{ST-1} \gamma_I \zeta^{IK} = \sum_{j=0}^{S-1} \sum_{i=0}^{T-1} \gamma_{i,j} \zeta^{(inS+jmT)(sT+tS)} = \\ &= \sum_{j=0}^{S-1} \sum_{i=0}^{T-1} \gamma_{i,j} \zeta^{(intS^2+jmsT^2)} = \sum_{j=0}^{S-1} \sum_{i=0}^{T-1} \gamma_{i,j} (\zeta^S)^{it} (\zeta^T)^{js} = \sum_{j=0}^{S-1} (\zeta^T)^{js} \gamma_{(j),t}, \end{aligned} \quad (6)$$

где

$$\gamma_{(j),t} = \sum_{i=0}^{T-1} \gamma_{i,j} (\zeta^S)^{it}.$$

Сравнивая правые части (5) и (6), видим, что умножения на степени ζ^{jt} во втором случае удается избежать.

В случае, когда число N простое или когда оно не имеет малых делителей, ДПФ порядка N можно свести к свертке методом Л. Блюстайна [34] или методом Ч. Рейдера [76].

Метод Блюстайна требует наличия корня из единицы степени $2N$ в кольце K и состоит в следующем. Пусть, как и выше, ζ — примитивный корень степени N . Положим $\beta = \zeta^{(N-1)/2} \in K$. Заметим, что $\beta^{-2} = \zeta$. Тогда

$$\gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij} = \beta^{-j^2} \sum_{i=0}^{N-1} \beta^{(j-i)^2} \beta^{-i^2} \gamma_i = \beta^{-j^2} \sum_{i+k \equiv j \bmod N} U_k V_i = \beta^{-j^2} C_j,$$

где $U_k = \beta^{k^2}$, $V_i = \beta^{-i^2} \gamma_i$. Если определить многочлены $u(x) = \sum U_i x^i$, $v(x) = \sum V_i x^i$, $c(x) = \sum C_i x^i$, то $c(x) = u(x)v(x) \bmod (x^N - 1)$. Фактически доказана

ЛЕММА 6 ([34]). *ДПФ порядка N может быть выполнено посредством циклической свертки порядка N и $2N - 2$ умножений на корни из единицы кольца K .*

Альтернативой методу Блюстайна служит метод Рейдера. Он применим в случае простого N , но не предъявляет к кольцу дополнительных требований. Сохраним обозначение ζ для примитивного корня степени N в кольце K . Пусть $g \bmod N$ — порождающий элемент мультипликативной группы поля $GF(N)$. Для $k = 1, \dots, N-1$ обозначим $\gamma[k] = \gamma_{g^k \bmod N}$, $\gamma_{[k]}^* = \gamma_{g^{k^*} \bmod N}$, а также $\zeta^{[k]} = \zeta^{g^k}$ при любых k . Тогда

$$\gamma_{[j]}^* = \gamma_0 + \sum_{i=1}^{N-1} \gamma_{[i]} \zeta^{[i+j]}.$$

Суммы в правой части формулы являются компонентами циклической свертки векторов $(\gamma_{[1]}, \dots, \gamma_{[N-1]})$ и $(\zeta^{[N-1]}, \dots, \zeta^{[1]})$. Компонента γ_0^* вычисляется отдельно как $\sum \gamma_i$. Таким образом, справедлива

ЛЕММА 7 ([76]). *ДПФ простого порядка N может быть выполнено посредством циклической свертки порядка $N-1$ и $2N-2$ сложений в кольце K .*

Метод Рейдера обобщается на случай нечетных примарных чисел $N = p^n$ (p — простое число). В этом случае ДПФ сводится к циклической свертке порядка $(p-1)p^{n-1}$, см., например, [2, 14].

Еще один полезный прием предложили Р. Крэндэлл и Б. Фейгин [42]. Он в некоторых случаях позволяет свести ДПФ «неудобного» порядка к ДПФ «удобного» порядка. Например, умножение по модулю простого числа Мерсенна $2^p - 1$ совпадает с циклической сверткой порядка p векторов двоичной записи перемножаемых чисел. Поэтому оно реализуется при помощи ДПФ порядка p с примитивным корнем $2 \in \mathbb{Z}_{2^p-1}$. Но p — тоже простое число, и ДПФ такого порядка, как правило, реализуется не очень эффективно.

Однако, задачу можно свести к приближенному вычислению вещественного ДПФ произвольного порядка N . Разобьем перемножаемое число $X = [x_{p-1}, \dots, x_0]$ на N блоков приблизительно равной длины: $X = [X_{N-1}, \dots, X_0]$. Пусть B_i — позиция начала i -го блока. Запишем X в виде:

$$X = \sum_{i=0}^{N-1} X_i \cdot 2^{B_i} = \sum_{i=0}^{N-1} (X_i \cdot 2^{B_i - ip/N}) 2^{ip/N} = \sum_{i=0}^{N-1} X'_i \cdot 2^{ip/N}.$$

Теперь умножение X на $Y = \sum_{i=0}^{N-1} Y'_i \cdot 2^{ip/N}$ можно выполнить при помощи двух ДПФ порядка N с примитивным корнем $2^{p/N} \in (\mathbb{R} \bmod 2^p - 1)$ и одного обратного ДПФ. Из вектора результата $[Z'_{N-1}, \dots, Z'_0]$ искомое произведение находится как

$$XY = \sum_{i=0}^{N-1} (Z'_i \cdot 2^{ip/N - B_i}) 2^{B_i} \bmod 2^p - 1.$$

При выборе размера блоков близким к длине машинного слова описанный метод эффективно реализуется на стандартных компьютерах.

4.3. Многомерное ДПФ

Понятия ДПФ и алгоритмы БПФ легко распространяются на многомерные пространства. Пусть в кольце K определены ДПФ порядков $n_1, \dots, n_d$ с примитивными корнями соответственно $\zeta_1, \dots, \zeta_d$. В полиномиальной интерпретации входом d -мерного преобразования является некоторый многочлен $\Gamma(x_1, \dots, x_d) \in K[x_1, \dots, x_d]$, а компонентами ДПФ порядка $n_1 \times \dots \times n_d$ над K являются всевозможные значения

$$\Gamma(\zeta_1^{j_1}, \dots, \zeta_d^{j_d}), \quad j_1 \in \{0, \dots, n_1 - 1\}, \dots, j_d \in \{0, \dots, n_d - 1\}.$$

Несложно проверить, что при этом справедлив аналог леммы 2: ДПФ задает изоморфизм колец $K[x_1, \dots, x_d] / ((x_1^{n_1} - 1) \cdot \dots \cdot (x_d^{n_d} - 1))$ и $K^{n_1 \cdot \dots \cdot n_d}$. Обратное ДПФ получается из прямого заменой примитивных корней ζ_i на ζ_i^{-1} и домножением на величину $(n_1 \cdot \dots \cdot n_d)^{-1}$ (имеет место аналог леммы 1).

Вычислять многомерное ДПФ проще всего как композицию одномерных ДПФ по координатам. В случае $d = 2$ запишем $\Gamma(x_1, x_2) = \sum_{j=0}^{n_2-1} \Gamma_j(x_1) \cdot x_2^j$. При помощи n_2 ДПФ порядка n_1 найдем всевозможные значения $\Gamma_j(\zeta_1^i)$. Применим ДПФ порядка n_2 к каждому из многочленов $\Gamma_i'(x_2) = \sum_{j=0}^{n_2-1} \Gamma_j(\zeta_1^i) \cdot x_2^j$. В итоге будут получены все значения $\Gamma(\zeta_1^i, \zeta_2^j)$. Обобщение изложенного способа приводит к следующему результату.

ЛЕММА 8. Пусть $N = n_1 \cdot \dots \cdot n_d$. ДПФ порядка $n_1 \times \dots \times n_d$ можно реализовать посредством N/n_1 ДПФ порядка n_1 , N/n_2 ДПФ порядка n_2 , $\dots$ и N/n_d ДПФ порядка n_d .

Подробнее о вычислении ДПФ см., например, в [2, 3, 5].

5. Умножение при помощи БПФ

Теорема 1 и лемма 4 показывают, что сложность умножения комплексных многочленов степени $n = 2^k$ можно оценить как

$$M_{\mathbb{C}}(n) \leq (9 + o(1))n \log n. \quad (7)$$

Как заметил Шёнхаге [82], такая же оценка справедлива и для произвольных n : в доказательстве нужно от n перейти к ближайшему сверху числу $n' = 2^t r$, где $r = O(\log n)$. На практике предпочтительнее применять ДПФ порядка ближайшей сверху степени двойки $2^{\lceil \log n \rceil}$, усеченное до n компонент, см. [16, 29, 63, 69].

Разумеется, оценка (7) имеет место для умножения над произвольным кольцом, в котором есть примитивные корни из единицы любой степени. Для применения БПФ к умножению над кольцами, не имеющими подходящих корней из единицы, а также для умножения целых чисел потребовались специальные приемы.

Простой метод расширения кольца хорошо работает в случае многочленов с действительными коэффициентами: достаточно перейти к вычислениям над полем $\mathbb{C}$. Более того, поскольку комплексный Фурье-образ вещественного вектора полностью определяется половиной своих компонент (остальные являются комплексно-сопряженными), примерно половину операций можно сэкономить, см., например, [3, 5].

С 1960-х гг. известны алгоритмы вычисления комплексного ДПФ порядка 2^k с вещественной сложностью³ $\sim 4k2^k$. Впервые такая оценка была получена Р. Явне [88] методом, в котором все умножения выполняются на вещественные константы (real-factor FFT), см. также [3]. Однако большую известность приобрели методы «БПФ с расщепленным основанием» (split-radix FFT, см. [3, 32]) — в них все умножения являются умножениями на корни из единицы, что благоприятно для контроля погрешности вычислений. В 2004 г. Дж. ван Бускирку удалось улучшить оценку сложности до $\sim (34/9)k2^k$ (метод опубликован в [66, 68]) при помощи модификации алгоритма с расщеплением основания. Другие практические алгоритмы были предложены в [61, 89], а наилучшая, на сегодняшний день, оценка $\sim 3 \frac{123}{160} \cdot k2^k$ опубликована в [20].

Таким образом, для сложности умножения вещественных многочленов справедлива оценка $M_{\mathbb{R}}(n) \leq (11 \frac{49}{160} + o(1)) n \log n$.

Указанные методы используют $\Theta(k2^k)$ как аддитивных операций, так и скалярных умножений. Однако, известно, что для реализации ДПФ произвольного порядка N достаточно $O(N)$ умножений [87, 62], но соответствующие алгоритмы имеют большую общую сложность.

³Символ $\sim$ означает асимптотическое равенство.

Теория умножения вещественных и комплексных многочленов адаптируется к умножению над полями $GF(q)$ и $GF(q^2)$, где $q = 2^p - 1$ — псевдомерсенново простое число. В поле $GF(q^2) \cong GF(q)[x]/(x^2 + 1)$ имеются примитивные корни порядка 2^k , $k \leq p + 1$, поэтому для умножения многочленов степени $< 2^k$ возможны быстрые алгоритмы. Подробнее см. в [2, 4].

Сразу после появления алгоритмов БПФ их стали пытаться применять к умножению чисел. Согласно [13], первый быстрый алгоритм умножения чисел, основанный на ДПФ, был построен Н. С. Бахваловым — его метод имел сложность $O(n \log^3 n)$.

Затем, в 1971 г. А. Шёнхаге и Ф. Штрассен [79] опубликовали сразу два быстрых метода умножения. Первый из них эксплуатирует естественную идею перехода к вычислениям над полем комплексных чисел $\mathbb{C}$, которое допускает ДПФ произвольного порядка.

5.1. Метод комплексного приближения

Пусть $2N = 2^n q$. В первом методе Шёнхаге—Штрассена [79] перемножаемые N -разрядные числа разбиваются на блоки длины q , как в (3). Полученные многочлены умножаются при помощи комплексного ДПФ порядка 2^n . Вычисления с комплексными числами выполняются с точностью s знаков после запятой. Параметр s подбирается так, чтобы коэффициенты многочлена-произведения, которые на самом деле являются целыми числами, были найдены с ошибкой $< 1/2$; тогда их можно восстановить путем округления. Несложный анализ (см. [79] или [11]) показывает, что достаточно выбрать $s = 2n + 2q + \log n + O(1)$.

Основная сложность алгоритма сосредоточена в ДПФ: $O(2^n n)$ умножений и сложений-вычитаний $O(s)$ -разрядных чисел. Рекуррентное соотношение для сложности метода имеет вид

$$M(N) \leq O(2^n n(M(s) + s))$$

и решается как $M(N) = O(N \log N \log \log N \log \log \log N \dots)$. Такая же оценка сложности (и, вероятно, тем же самым методом) была ранее получена А. А. Карацубой [10], но не опубликована.

5.2. Умножение в кольце-расширении

В основе второго метода Шёнхаге—Штрассена [79] фактически лежит сведение умножения многочленов над кольцом K , не имеющим корней из единицы подходящей степени, к умножению в кольце-расширении. А именно, предлагается использовать расширение $K_{2,n}(x) = K[x]/(x^{2^n} + 1)$, при этом двойка должна быть обратима в K .

В кольце $K_{2,n}(x)$ определено ДПФ порядка 2^{n+1} с примитивным корнем x (для наглядности, здесь и далее вместо элементов фактор-кольца $K_{2,n}(x)$, которыми являются классы эквивалентных по модулю $x^{2^n} + 1$ многочленов, фигурируют многочлены-представители классов).

Из леммы 4 вытекает

ЛЕММА 9. *ДПФ порядка 2^k над кольцом $K_{2,n}(x)$, $k \leq n + 1$, может быть выполнено за $k2^{k+n}$ аддитивных операций в K .*

Для доказательства достаточно заметить, что умножение на степени примитивного корня x в кольце $K_{2,n}(x)$ реализуется «бесплатно».

Кольцо $K_{2,n}(x)$ можно рассмотреть как расширение аналогичного кольца $K_{2,m}(y)$ меньшей размерности: справедлива

ЛЕММА 10. *Пусть $m < n$. Имеет место изоморфизм*

$$K_{2,n}(x) \cong K_{2,m}(y)[x]/(x^{2^{n-m}} - y),$$

порождаемый подстановкой $x^{2^{n-m}} = y$.

Важно заметить, что указанный изоморфизм реализуется простой перестановкой коэффициентов. Например, многочлену $x^3 + 2x^2 - 1 \in K_{2,2}(x)$ соответствует многочлен $yx + (2y - 1) \in K_{2,1}(y)[x]/(x^2 - y)$. Для реализации умножения можно использовать и другие изоморфизмы, см. [32].

В методе Шёнхаге—Штрассена для умножения в кольце $K_{2,n}(x)$ используется изоморфизм леммы 10 с выбором параметра $m = \lceil n/2 \rceil$. При помощи трех ДПФ порядка $2^{n-m+1} = 2^{\lceil n/2 \rceil + 1}$ над кольцом $K_{2,m}(y)$ умножение сводится к умножениям в меньшем кольце. Рекурсивное применение этой процедуры приводит к следующему результату.

ТЕОРЕМА 2. *Умножение в кольце $K_{2,n}(x)$ может быть выполнено при помощи $3 \cdot 2^n n(\log_2 n + O(1))$ аддитивных операций и $O(n2^n)$ операций умножения в K .*

Умножение многочленов над K теперь можно выполнить при помощи подходящей схемы умножения в $K_{2,n}(x)$.

Чтобы получить алгоритм умножения чисел, вместо кольца $K_{2,n}(x)$ рассматривается кольцо вычетов $\mathbb{Z}_{F_n}$ по модулю числа Ферма $F_n = 2^{2^n} + 1$. Двойка играет роль переменной x — она является примитивным корнем порядка 2^{n+1} в кольце Ферма.

Перемножаемые числа разбиваются на блоки длины 2^{m-1} , которые интерпретируются как коэффициенты целочисленных многочленов. Произведение чисел восстанавливается из произведения этих многочленов. Основная часть числового метода следует алгоритму теоремы 2. Многочлены перемножаются как многочлены на кольцом $\mathbb{Z}_{F_m}$, и поэтому коэффициенты произведения исходных многочленов вычисляются не точно, а по модулю $F_m = 2^{2^m} + 1$. В действительности, коэффициенты произведения исходных многочленов могут иметь размер порядка $2^{n-m} \cdot 2^{2^m}$. Поэтому в методе [79] дополнительно вычисляется произведение исходных многочленов над кольцом вычетов по модулю $2^{n-m+O(1)}$. Искомые коэффициенты затем восстанавливаются при помощи Китайской теоремы об остатках.

Сложность метода определяется сложностью умножения над кольцом $\mathbb{Z}_{F_m}$, поэтому в результате для нее справедлива по порядку такая же как в теореме 2 оценка $O(n \log n \log \log n)$.

В том же 1971 г. Дж. Поллард [75] предложил идейно близкую, но более простую и практичную версию алгоритма. В ней числа разбиваются на 2^{k-1} блоков длины m , соответствующей длине машинного слова. Числовое произведение восстанавливается из произведения многочленов, выполняемого по нескольким простым модулям p_i , таким, что $\prod p_i \geq 2^{2m+k}$. Модули выбираются с условием $p_i \equiv 1 \pmod{2^k}$, тогда умножение многочленов выполняется при помощи ДПФ порядка 2^k над $GF(p_i)$.

Исходный метод Шёнхаге—Штрассена не позволяет умножать многочлены над кольцами, в которых необратима двойка, поскольку над такими кольцами не определено ДПФ четного порядка. В работе [80] А. Шёнхаге предложил модифицированный алгоритм умножения для колец, в которых обратима тройка. Для такого кольца K рассматривается расширение $K_{3,n}(x) = K[x]/(x^{2 \cdot 3^n} + x^{3^n} + 1)$ — в нем x является примитивным корнем степени 3^{n+1} . Умножение выполняется в духе теоремы 2, но при помощи ДПФ порядка степеней тройки.

Для сложности указанного метода умножения в кольце $K_{3,n}(x)$ можно указать оценку $13 \cdot 3^n n(\log n + O(1))$, которая в случае кольца характеристики 2 может быть понижена до $10 \cdot 3^n n(\log n + O(1))$ операций в K [6].

Стратегию умножения в случае $2^{-1}, 3^{-1} \notin K$ указывает метод Кантора—Калтофена [36]. Способом теоремы 2 и ее троичного аналога, заменяя обратные преобразования ДПФ N, ζ^{-1} ненормированными преобразованиями ДПФ N, ζ^{-1} , вычисляются «почти произведения»

$$2^{N_1} fg = 2^{N_1} fg \pmod{x^{2^{N_1}} + 1}, \quad 3^{N_2} fg = 3^{N_2} fg \pmod{x^{2 \cdot 3^{N_2}} + x^{3^{N_2}} + 1}$$

при подходящих $n_i, N_i \in \mathbb{N}$, где f, g — перемножаемые многочлены. Окончательно произведение fg можно вычислить как $q2^{N_1} fg + s3^{N_2} fg$, где q, s — коэффициенты Безу из соотношения

$q2^{N_1} + s3^{N_2} = 1$. Впрочем, актуальность разработки быстрых алгоритмов умножения над такими достаточно экзотическими кольцами представляется пока незначительной.

Практичность числового метода Шёнхаге—Штрассена долгое время вызывала сомнения. Тем не менее, метод реализован во многих современных библиотеках быстрой арифметики и обычно вызывается, когда длина перемножаемых чисел превышает несколько тысяч разрядов⁴. Более того, в последнее десятилетие появились приложения, использующие умножение чисел с миллионами знаков и более, в частности, полностью гомоморфное шифрование (FHE). Но вместе с тем возникли и теоретически более быстрые методы умножения.

6. Новейшие методы умножения

Долгое время методы Шёнхаге и Штрассена оставались рекордными, пока в 2007 г. М. Фюрер [49] не предъявил метод умножения n -разрядных чисел сложности $n \log n \cdot 2^{O(\log^* n)}$. В определенном смысле, метод Фюрера получается комбинацией двух методов из [79]. Через год группа индийских математиков [43] предложила модификацию метода Фюрера с аналогичной оценкой сложности.

Любопытно, что Фюрер еще в 1989 г. [48] построил метод, имевший такую сложность в предположении о достаточно высокой плотности распределения простых чисел Ферма — но сегодня более правдоподобной считается гипотеза о конечности множества таких чисел.

В 2014 г. Д. Харви, Ж. ван дер Хувер и Г. Лесер [55, 56] построили семейство алгоритмов умножения как для чисел, так и для многочленов, с теоретической оценкой сложности $O(n \log n \cdot 8^{\log^* n})$. В последующих работах [57, 58] оценки сложности были улучшены до $O(n \log n \cdot 4^{\log^* n})$.

На одной итерации каждого из новых методов умножения выполняется логарифмическая редукция размера задачи: с n до $2^{\log^{O(1)} \log n}$. Это достигается за счет перехода к вычислениям над кольцом, допускающим компактную кодировку элементов и содержащим примитивные корни высокого и гладкого порядка: например, кольцом комплексных многочленов небольшой степени или конечным полем подходящего размера.

В отличие от предыдущих методов умножения, у новых методов основная сложность сосредоточена в преобразованиях Фурье, а не в умножениях Фурье-образов. Более точно, сложность алгоритмов сконцентрирована в скалярных умножениях, возникающих при разложении БПФ в композицию преобразований малого порядка.

6.1. Метод Фюрера

Рассмотрим кольцо $C_p = \mathbb{C}[x]/(x^{2^p} + 1)$. В нем элемент x является примитивным корнем степени 2^{p+1} из единицы. При этом кольцо содержит примитивные корни из единицы произвольной степени $q2^{p+1}$, которые одновременно являются корнями (степени q) из x .

Один из таких примитивных корней $\rho_q(x)$ степени $q2^{p+1}$ можно построить следующим образом. Обозначим $\zeta = e^{i\pi/2^p}$ и $\xi = e^{i\pi/(q2^p)}$. Определим многочлен $\rho_q(x)$ степени $< 2^p$ значениями в точках:

$$\rho_q(\zeta^{2k+1}) = \xi^{2k+1}, \quad k = 0, \dots, 2^p - 1.$$

Как можно проверить, этот многочлен обладает дополнительным важным свойством: модули коэффициентов его степеней $\rho_q^m(x)$ в кольце C_p не превосходят 1.

Таким образом, в кольце C_p определено ДПФ порядка $N = 2^{s(p+1)}$ с примитивным корнем $\rho_{2^s}(x)$, и при реализации методом Кули—Тьюки оно имеет следующую структуру: s слоев,

⁴Возможно, преодолению скептицизма в отношении метода Шёнхаге—Штрассена способствовала его реализация, выполненная самим Шёнхаге и его учениками на эмуляторе многоленточной машины Тьюринга в начале 1990-х гг. [83].

в которых параллельно выполняется по $N2^{-(p+1)}$ ДПФ порядка 2^{p+1} чередуются со слоями, в которых выполняется по N умножений на степени $\rho_{2^s}(x)$.

Схема состоит из $O(N \log N)$ простых операций — сложений-вычитаний и умножений на степени x (циклических сдвигов), при помощи которых выполняются внутренние ДПФ — и $(s-1)N$ сложных операций: умножений на степени примитивного корня.

Пусть для записи действительных и мнимых частей комплексных коэффициентов многочленов из C_p используется E двоичных разрядов. Тогда сложность умножения $M(N, E)$ многочленов из $C_p[y]$ по модулю $y^N - 1$ можно оценить как

$$M(N, E) \leq O(2^p EN \log N) + 3sN \cdot M(1, E).$$

Умножение в кольце C_p естественным образом сводится к умножению $O(2^p(E+p))$ -разрядных чисел.

В силу накопления погрешности (абсолютной величины ошибки) по ходу вычислений, точность, с которой вычисляются коэффициенты произведения, вообще говоря, существенно меньше, чем точность исходных коэффициентов. Однако, используя ограниченность коэффициентов $\rho_{2^s}^m(x)$, несложно проверить, что погрешность возрастает в $A^2 N^{O(1)}$ раз, где A — максимум абсолютных значений комплексных коэффициентов исходных многочленов.

В методе Фюрера используется выбор параметров⁵ $E \asymp \log N$ и $2^p \asymp \log N$. Перемножаемые числа представляются многочленами над C_p степени $< N/2$ следующим образом: они разбиваются на блоки длины $E/3$, которые интерпретируются как целые числа, каждые 2^{p-1} подряд расположенных блоков интерпретируются как коэффициенты многочлена из кольца $\mathbb{C}[x]/(x^{2^p} + 1)$. Параметр точности E выбирается так, чтобы можно было восстановить коэффициенты произведения полученных многочленов простым округлением.

Таким образом, для сложности умножения n -разрядных чисел выводится соотношение

$$M(n) \leq O(2^p EN \log N) + 3sN \cdot M(O(2^p(E+p))),$$

где $N \asymp n/\log^2 n$, $E \asymp \log n$, $2^p \asymp \log n$, $s \asymp \log n / \log \log n$. Оно разрешается как $M(n) \leq n \log n \cdot 2^{O(\log^* n)}$.

Метод [43] развивает идею Фюрера, используя вместо C_p подходящие расширения колец вычетов $\mathbb{Z}_{p^c}$.

6.2. Метод Харви—ван дер Хувена—Лесера

Отметим, что ни метод Фюрера [49], ни его p -адичная версия [43] не допускают адаптацию к умножению многочленов. А семейство методов, предложенных в [55, 56], включает как числовые методы умножения, так и методы умножения многочленов. Рассмотрим новый подход на примере умножения двоичных многочленов.

Умножение двоичных многочленов можно интерпретировать как умножение в кольце $GF(2)[x]/(x^n - 1)$. Вставкой необходимого числа нулевых коэффициентов такое умножение сводится к умножению в кольце $GF(2^k)[y]/(y^N - 1)$, где $kN \asymp n$, $N = N_1 \cdot \dots \cdot N_d \mid 2^k - 1$ — гладкое число.

Существование подходящего гладкого числа N гарантируется следующим теоретико-числовым результатом.

ЛЕММА 11 ([27]). *Минимальное число $\lambda(t)$, такое, что*

$$t \leq \prod_{p \in \mathbb{P}, (p-1) \mid \lambda(t)} p,$$

имеет величину $\lambda(t) = (\log t)^{\Theta(\log \log \log t)}$.

⁵Символы $\asymp$ и $\leq$ означают равенство и неравенство порядков.

Согласно лемме, для заданного порога t найдется число $M \geq t$ — произведение простых чисел $2 < p \leq \lambda(t) + 1$ со свойством $p - 1 \mid \lambda(t)$. Последнее условие по малой теореме Ферма означает, что $p \mid 2^{\lambda(t)} - 1$. Можно проверить, что если $S > \lambda(t)$, то из M можно выделить произведение $N = N_1 \cdot \dots \cdot N_d \in [t, (\lambda(t) + 1)t]$ взаимно простых множителей, $S \leq N_i \leq S^3$.

В рассматриваемом методе выбирается $t \asymp n$ и $S = 2^{\Theta(\log^2 \log n)}$. Параметр k выбирается кратным $\lambda(t)$ и имеет размер порядка $(\log n)^{\Theta(\log \log \log n)}$. По построению, множители N_i имеют величину $2^{\Theta(\log^2 \log n)}$.

Далее, умножение в кольце $GF(2^k)[y]/(y^N - 1)$ выполняется при помощи ДПФ порядка N над $GF(2^k)$. ДПФ порядка N методом Кули—Тьюки (лемма 3) или методом Гуда (лемма 5) сводится к последовательному выполнению ДПФ порядков $N_1, \dots, N_d$. ДПФ порядка N_i методом Блюстайна (лемма 6) сводится к умножению в кольце $GF(2^k)[y]/(y^{N_i} - 1)$.

Такое умножение, в свою очередь, сводится (вставкой нулевых коэффициентов) к умножению в кольце $GF(2)[x]/(x^{n_i} - 1)$, где $n_i \asymp kN_i$. Тем самым задача умножения размерности n сведена к умножениям размерности $n_i = 2^{\Theta(\log^2 \log n)}$.

Используя вытекающую из леммы 5 оценку сложности ДПФ составного порядка N , получаем для сложности $M_{GF(2)}(n)$ умножения в кольце $GF(2)[x]/(x^n - 1)$ рекуррентное соотношение

$$M_{GF(2)}(n) \leq N \sum_{i=1}^d \frac{M_{GF(2)}(n_i)}{N_i} + 2dNM_{GF(2^k)},$$

где $M_{GF(2^k)}$ — сложность умножения в поле $GF(2^k)$ — ее оценим грубо как $O(k \log k \log \log k)$ (метод Шёнхаге [80]).

Обозначим $\mu(n) = \frac{M_{GF(2)}(n)}{n}$. Тогда с учетом $d \asymp \log n / \log^2 \log n$ имеем (при некоторой постоянной c)

$$\mu(n) \leq c \sum_{i=1}^d \mu(n_i) + O(d \log k \log \log k) = c \sum_{i=1}^d \mu(n_i) + o(\log n).$$

Несложно проверить, что это соотношение разрешается как $\mu(n) = \log n \cdot 2^{O(\log^* n)}$.

Для обоснования оценки $\mu(n) \leq \log n \cdot 4^{\log^* n}$ в [56, 57] используются несколько дополнительных приемов и более аккуратный анализ. В частности, применяется адаптированный для расширений конечных полей метод Крэндалла—Фейгина [42].

Аналогичным образом можно выполнять умножение над произвольным конечным полем и, привлекая идею Кантора—Калтофена [36] (см. выше), над произвольным кольцом. Аккуратная оценка [57] гласит, что умножение многочленов степени n над произвольным кольцом K выполняется при помощи $O(n \log n \cdot 4^{\log^* n})$ аддитивных операций и $O(n \cdot 2^{\log^* n})$ мультипликативных операций в K .

Числовые версии [55, 58] метода следуют близкой к приведенной выше общей схеме. Вместо полей $GF(2^k)$ используются или кольца вычетов $\mathbb{Z}_q$ со специальным представлением элементов или поле комплексных чисел, вычисления в котором выполняются с контролируемой точностью, а порядок ДПФ выбирается равным степени двойки.

6.3. Умножение со сложностью $O(n \log n)$

В 2019 г. Д. Харви и Ж. ван дер Хуven [59, 60] построили методы умножения сложности $O(n \log n)$, и вполне возможно, что этот результат по порядку уже неулучшаем. В основе новых методов лежит сведение к многомерной интерполяции.

Действительно, от умножения многочленов степени $< n$ над кольцом K , допускающим лишь БПФ порядка $m \ll n$, несложно путем подстановки Кронекера $x_i = x^{r \cdot 2^i}$ перейти к умножению в кольце многочленов $K[x_1, \dots, x_d]$. Для умножения в этом кольце доступно d -мерное

БПФ на m^d точках. Но для того, чтобы обратная подстановка позволила восстановить произведение, параметр r следует выбирать чуть меньшим чем $m/2$. Потому и размер перемножаемых многочленов вырастает по меньшей мере в 2^d раз. Для построения теоретически быстрых методов умножения такой рост неприемлем.

Роста размерности можно избежать при переходе к многомерному ДПФ с взаимно простыми компонентами. Действительно, пусть $n = n_1 \cdot \dots \cdot n_d$, где $n_1, \dots, n_d$ — попарно взаимно просты. Тогда имеет место изоморфизм $K[x]/(x^n - 1) \cong K[x_1, \dots, x_d]/(x_1^{n_1} - 1, \dots, x_d^{n_d} - 1)$, порождаемый подстановкой $x_1 = x^{n/n_1}, \dots, x_d = x^{n/n_d}$. Таким образом, одномерное ДПФ порядка n с точностью до перестановки компонент совпадает с d -мерным ДПФ порядка $n_1 \times \dots \times n_d$. Эта связь отмечена в работе [28], а метод Гуда—Томаса позволяет свести вычисление такого преобразования к ДПФ порядков n_i . При этом камнем преткновения может стать неэффективность реализации ДПФ с различными порядками n_i .

Такой способ перехода к многомерному ДПФ применяется в методе [59, 60]. Как в методе Фюрера, перемножаемые n -разрядные числа сначала разбиваются на $N = O(n/\log n)$ блоков длины порядка $\log n$, интерпретируемых как комплексные коэффициенты. Далее числа рассматриваются как многочлены над кольцом $C_p = \mathbb{C}[y]/(y^{2^p} + 1)$, где $p = \lceil (1/d) \log N \rceil$. Умножение таких многочленов выполняется как умножение в кольце $C_p[x]/(x^{n_1 \dots n_{d-1}} - 1)$, где $3N > n_1 \cdot \dots \cdot n_{d-1} \cdot 2^p > 2N$, и все n_i — различные простые числа. Последнее умножение, как описано выше, сводится к вычислению ДПФ порядка $n_1 \times \dots \times n_{d-1}$ и умножениям в точках интерполяции. Все вычисления выполняются с запасом точности, который можно определить в $O(\log n)$ разрядов. Пусть для хранения действительных и мнимых частей комплексного коэффициента используется по $E = O(\log n)$ двоичных разрядов.

Для преодоления проблемы неэффективности ДПФ простых порядков n_i авторами [59, 60] предложено два способа. В первом способе в качестве параметров n_i выбираются числа вида $n_i = k_i \cdot 2^p + 1$, где множители k_i не очень велики. Посредством многомерного варианта метода Рейдера ДПФ порядка $n_1 \times \dots \times n_{d-1}$ сводится к циклической свертке более гладкого порядка $(n_1 - 1) \times \dots \times (n_{d-1} - 1)$. На этом пути может быть получена оценка сложности умножения $O(n \log n)$ при условии, что k_i можно выбрать действительно малыми, скажем, $k_i < 2^{\varepsilon p}$, где ε — подходящая константа. Но возможность такого выбора опирается на недоказанную гипотезу о размере простых чисел в арифметической прогрессии. Если гипотеза будет подтверждена, то одновременно будет доказана и оценка сложности $O(n \log n)$ для умножения многочленов степени n , см. [60].

Второй способ работает только в числовом случае. Простые числа n_i выбираются чуть меньшими, чем степени двойки $t_i \in \{2^{p-1}, 2^p\}$, так, что $T = t_1 \cdot \dots \cdot t_{d-1} \leq 2N' = 2n_1 \cdot \dots \cdot n_{d-1}$. Закон распределения простых чисел позволяет это сделать. Ключевым моментом метода является сведение ДПФ порядка $n_1 \times \dots \times n_{d-1}$ к ДПФ порядка $t_1 \times \dots \times t_{d-1}$: естественно, речь идет о построении приближения с достаточно высокой точностью. Возможность быстрого приближенного вычисления ДПФ одного порядка при помощи ДПФ другого порядка неочевидна и малоизвестна. На материале одномерных преобразований вопрос изучался в работе [45]. Авторы [59] обобщили на многомерный случай и несколько усовершенствовали метод [45]. В результате удалось показать, что при определенных соотношениях между n_i и t_i (числа не должны быть слишком близки) и некоторых других выполнимых условиях указанное сведение может быть выполнено со сложностью $o(n \log n)$ и требуемой точностью.

Напомним, что ДПФ порядка степени двойки t_i над кольцом C_p методом Кули—Тьюки вычисляется за $O(t_i \log t_i)$ операций в C_p , т.е. с общей сложностью $O(t_i \log t_i \cdot 2^p E)$. Тогда лемма 8 позволяет оценить сложность ДПФ порядка $t_1 \times \dots \times t_{d-1}$ как $O(N' \log N' \cdot 2^p E) = O(n \log n)$. Используя обозначение $M(N, E)$ из §6.1, приходим к соотношению

$$M(n) \leq M(N', E) + O(n) \leq N' \cdot M(1, E) + O(n \log n) \leq N' \cdot M(O(2^p(E + p))) + O(n \log n), \quad (8)$$

оценивая сложность $M(1, E)$ (приближенного) умножения в кольце C_p через $M(O(2^p(E + p)))$,

как и в §6.1. Ввиду $N' = O(n \cdot 2^{-p} / \log n)$ и $p \sim (1/d) \log n$ соотношение (8) разрешается как $M(n) = O(n \log n)$ при достаточно большом постоянном параметре d .

Такова общая схема вычисления. Анализ погрешности и выбор параметра E выполняется примерно так же, как в методе Фюрера. Основная сложность доказательства приходится на построение приближения многомерного ДПФ. Многомерный случай сводится к одномерному, т.е. вычислению ДПФ порядка s через ДПФ порядка $t > s$, где $(s, t) = 1$. Для этого используется матричное тождество $R \cdot \Pi_s \cdot \Phi_s = \Pi_t \cdot \Phi_t \cdot R'$, где Φ_z — матрицы ДПФ порядка z , Π_z — подходящие матрицы перестановок размера $z \times z$, а R и R' — специальные матрицы размера $t \times s$. При фиксированном векторе аргументов $x \in \mathbb{C}^s$ получается переопределенная система линейных уравнений $A \cdot X = b$ относительно вектора неизвестных $X = \Phi_s \cdot x$, где $A = R \cdot \Pi_s$ и $b = \Pi_t \cdot \Phi_t \cdot R' \cdot x$. Построение приближенного решения системы облегчает особенность матриц R и R' — быстрое убывание их коэффициентов при удалении от некоторой диагонали. Подробнее см. в [59].

7. Аддитивное ДПФ и умножение

Методы, основанные на ДПФ, как правило, не позволяют быстро выполнять умножение многочленов над конечными полями, поскольку конечное поле редко поддерживает ДПФ достаточно большого гладкого порядка. Теоретически быстрые методы не работают в практическом диапазоне размерностей. Однако, оказывается, что можно умножать быстро, используя интерполяцию в точках аддитивных подгрупп конечного поля, при этом основанные на этом методы оказываются практичными.

Частный случай аддитивного метода умножения был предложен Я. Ван и Ш. Цу [85] в 1988 г. Через год Д. Кантор [35] построил быстрый метод умножения над полями порядка q^{q^k} . Позже И. фон цур Гатен и Ю. Герхард [52] распространили метод на поля произвольного порядка.

Пусть в поле $GF(q^k)$ выбран базис $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$. Положим $W_0 = \{0\}$ и обозначим $W_i = \langle \alpha_1, \dots, \alpha_i \rangle$ — линейную оболочку первых i базисных элементов над полем $GF(q)$. Таким образом, W_i является аддитивной подгруппой. По построению,

$$W_i = \bigcup_{c \in GF(q)} \{c\alpha_i + W_{i-1}\}.$$

Аддитивное ДПФ (АДПФ) порядка q^i определяется как множество значений многочлена $\Gamma(x) \in GF(q^k)[x]$ в точках подгруппы W_i . Обратное АДПФ определяется как набор коэффициентов единственного многочлена степени $q^i - 1$, имеющего заданные значения в точках W_i .

Определим многочлены $S_i(x)$ как

$$S_i(x) = \prod_{\beta \in W_i} (x - \beta). \quad (9)$$

Несложно доказывается

ЛЕММА 12. *Имеют место следующие свойства многочленов $S_i(x)$:*

- (i) $S_0(x) \mid S_1(x) \mid \dots \mid S_k(x) = x^{q^k} - x$;
- (ii) $S_{i+1}(x) = S_i^q(x) - S_i^{q-1}(\alpha_{i+1})S_i(x)$;
- (iii) *Многочлен $S_i(x)$ является линейризованным над $GF(q)$, т.е. имеет ненулевые коэффициенты только при степенях x^{q^j} , $0 \leq j \leq i$.*

Для линейризованных многочленов, в частности, для многочленов $S_i(x)$, выполнены свойства линейности: $S_i(\beta + \gamma) = S_i(\beta) + S_i(\gamma)$ при любых $\beta, \gamma \in GF(q^k)$ и $S_i(c\beta) = cS_i(\beta)$ при любых $\beta \in GF(q^k)$ и $c \in GF(q)$.

Можно проверить [52], что как прямое, так и обратное АДПФ порядка q^i над полем $GF(q^k)$ реализуются схемами над $GF(q^k)$ сложности $O(i^2 q^{i+1})$.

7.1. Быстрое АДПФ

Оценки сложности АДПФ могут быть понижены при специальном выборе базиса. Эффективные базисы для АДПФ над полями $GF(q^{q^k})$ предложил Д. Кантор [35]. Элементы базисов Кантора⁶ определяются соотношениями $\alpha_1 = 1$ и $\alpha_{i+1}^q - \alpha_{i+1} = \alpha_i$ при $i > 1$. Такой выбор базиса позволил Кантору в случае простого числа q улучшить оценку сложности до $O(i \log_q \binom{q+1}{2} q^{i+1})$.

Для двоичных полей, которые представляют основной интерес, Ш. Гао и Т. Матир [51, 69] построили более быстрые алгоритмы. Изложим быстрый алгоритм АДПФ над полем $GF(2^{2^k})$.

Базис Кантора в двоичном поле строится по правилам: $\alpha_1 = 1$ и $\alpha_{i+1}^2 + \alpha_{i+1} = \alpha_i$ при $i > 1$. Тогда характеристические многочлены (9) удовлетворяют соотношению $S_{i+1}(x) = S_i^2(x) + S_i(x)$ согласно лемме 12.

Быстрый алгоритм Гао—Матир эффективно использует тот факт, что многие многочлены S_i являются двучленами. А именно, $S_{2^i}(x) = x^{2^{2^i}} + x$ и $W_{2^i} \cong GF(2^{2^i})$. Иначе говоря, последовательность $\{W_i\}$ содержит башню полей

$$GF(2) \subset GF(2^2) \subset \dots \subset GF(2^{2^i}) \subset \dots \subset GF(2^{2^k}).$$

Чтобы проявить аналогию между быстрым алгоритмом АДПФ и БПФ, следует переписать многочлен-прообраз в специальном базисе.

На множестве многочленов степени $< 2^i$ над $GF(2^k)$ определим базис

$$P_i = \{m_b(x) \mid 0 \leq b < 2^i\}$$

так: если в двоичной записи $b = [b_{i-1}, \dots, b_0]$, то $m_b(x) = \prod_{j=0}^{i-1} S_j^{b_j}(x)$. По построению, $P_0 \subset P_1 \subset \dots \subset P_k$. Справедлива

ЛЕММА 13 ([69]). *Переход между представлениями многочлена степени $< 2^m$ в стандартном базисе и базисе P_m в любом направлении может быть выполнен схемой над $GF(2^{2^k})$ из $\leq 2^{m-2} m \log m$ аддитивных операций.*

Алгоритм перехода к базису P_m использует только операции деления с остатком на двучлены, чем обусловлена его малая сложность. Пусть $2^i < m = 2^i + t \leq 2^{i+1}$. Задача размера 2^m сводится к 2^{2^i} задачам размера 2^t и 2^t задачам размера 2^{2^i} . Общая схема такова.

1) Сначала многочлен $f(x)$ переписывается в виде

$$\sum_{j=0}^{2^t-1} f_j(x) S_{2^i}^j(x),$$

$\deg f_j < 2^{2^i}$. Это выполняется методом «деления пополам»: сначала многочлен $f(x)$ делим на $S_{2^i}^{2^{t-1}}$, затем частное и остаток — на $S_{2^i}^{2^{t-2}}$, и т.д.

⁶Базис Кантора является частным случаем базиса Артина—Шрайера.

- 2) Внутренние многочлены $f_j(x)$ переписываются в базисе P_{2^i} .
 3) Полагая $y = S_{2^i}(x)$, результат предыдущего шага можно записать как

$$\sum_{b=0}^{2^{2^i}-1} m_b(x) g_b(y),$$

$\deg g_b < 2^t$. Приведем многочлены g_b к представлению в базисе P_t (относительно переменной y). Заметим, что $S_{2^i+l}(x) = S_l(y)$, поэтому переход завершен.

При переходе от специального базиса P_m к стандартному все действия выполняются в обратном порядке.

Доказательство следующей леммы полностью аналогично доказательству леммы 4.

ЛЕММА 14. *Вычисление значений многочлена $f(x) \in GF(2^{2^k})[x]$, записанного в базисе P_m , в точках $\omega + W_m$, где $\omega \in GF(2^{2^k})$, и обратная задача восстановления многочлена, имеющего заданные значения в указанных точках, выполняется схемой над $GF(2^{2^k})$ из $m2^m$ сложений и $m2^{m-1}$ скалярных умножений. В случае $\omega = 0$ можно дополнительно сэкономить по $2^m - 1$ сложений и скалярных умножений.*

На очередном шаге алгоритма многочлен $f(x)$ степени $2^m - 1$ записывается как

$$f_1(x)S_{m-1}(x) + f_0(x).$$

Поэтому

$$f(\omega + W_{m-1}) = f'(\omega + W_{m-1}), \quad f(\omega + \alpha_m + W_{m-1}) = f''(\omega + \alpha_m + W_{m-1}),$$

где $f' = f_1 S_{m-1}(\omega) + f_0$, $f'' = f_1 S_{m-1}(\omega) + f_0 + f_1$.

При выполнении обратной процедуры многочлены f_0, f_1 восстанавливаются по формулам $f_1 = f'' + f'$, $f_0 = f' + S_{m-1}(\omega)(f'' + f')$.

7.2. Умножение при помощи АДПФ

АДПФ позволяет быстро умножать многочлены над полями $GF(q^k)$, если степень произведения меньше q^k . Если порядок поля мал, то вычисления погружаются в поле большего размера.

Например, для умножения двоичных многочленов многочлены разбиваются на блоки длины 2^{k-1} , которые интерпретируются как элементы поля $GF(2^{2^k})$ при подходящем k .

В результате умножение многочленов степени N сводится к $\Theta(N)$ умножениям в поле степени $O(\log N)$, поэтому теоретическая сложность метода $O(N \log N \log^{1+o(1)} \log N)$ — несколько выше, чем у метода Шёнхаге—Штрассена или метода [56]. Однако практически метод АДПФ имеет приоритет. Еще и по той причине, что многие умножения в быстром алгоритме АДПФ выполняются на элементы подполей.

В работе [33] показано, что указанный метод позволяет умножать двоичные многочлены степени порядка нескольких сотен быстрее, чем любой другой ранее применявшийся метод.

Совсем недавно [65, 67] было обнаружено, что дополнительный выигрыш (в пределе около двух раз, но практически меньше) удастся получить за счет эксплуатации тождества Фробениуса $(a + b)^q = a^q + b^q$, справедливого при любых $a, b \in GF(q)$. В силу этого тождества значение многочлена с коэффициентами из $GF(q)$ в точке $\omega \in GF(q^k)$ автоматически определяет его значения во всех точках ω^{q^l} . Действительно, если $f \in GF(q)[x]$ и $\omega \in GF(q^k)$, то $f(\omega^{q^l}) = (f(\omega))^{q^l}$.

Аutomорфизм Фробениуса $x \rightarrow x^{2^i}$ сохраняет аддитивные подгруппы W_j , определенные для базиса Кантора: если $\omega \in W_j$, то $\omega^{2^i} \in W_j$, как следует из определения базиса. Можно проверить, что группа автоморфизмов Фробениуса при действии на элемент $\omega \in W_j \setminus W_{j-1} \in GF(2^{2^k})$ порождает класс эквивалентности (орбиту) $\{\omega^{2^i} \mid i = 0, \dots, 2^k - 1\}$ мощности $2^{\lceil \log j \rceil}$. Как следствие, множество точек АДПФ порядка 2^m над $GF(2^{2^k})$ распадается на не более чем $2^m / (m - o(1))$ классов эквивалентности.

Этим наблюдением продиктован следующий метод умножения многочленов суммарной степени менее 2^m . Для вычислений используется поле $GF(2^{2^k})$, $k = \lceil \log m \rceil$. Сначала каждый из перемножаемых многочленов $f, g \in GF(2)[x]$, интерпретируемый как многочлен над $GF(2^{2^k})$, приводится к представлению в базисе P_m . Разбиение на блоки и вставка нулевых блоков не требуются. Далее, значения каждого многочлена вычисляются на множестве $\Sigma \subset W_m$ представителей классов эквивалентности. Используется алгоритм леммы 14, адаптированный для многочленов с коэффициентами из подполя $GF(2)$. Обратная процедура восстанавливает произведение по значениям $f(\omega)g(\omega)$, $\omega \in \Sigma$. Подробности см. в [38].

Отметим аналогию с умножением многочленов с вещественными коэффициентами: наличие автоморфизма комплексного сопряжения, сохраняющего подполе $\mathbb{R}$ и множество корней из единицы, позволяет вычислять комплексное ДПФ с вещественным образом или прообразом примерно вдвое быстрее, чем в общем случае.

Идея сокращенного ДПФ над конечным полем, использующего тождество Фробениуса, предложена Ж. ван дер Хувеном и Р. Ларью в [65]. Описанный выше аддитивный аналог метода построен группой математиков из Тайваня в 2018 г. [67]. Полученные с его помощью верхние оценки сложности умножения двоичных многочленов степени от нескольких сотен и выше на момент написания настоящего обзора являются наилучшими из опубликованных.

8. Параллельные схемы для умножения

До сих пор мы качество алгоритмов измеряли общим числом выполняемых операций. Теперь рассмотрим другую важную характеристику — время выполнения алгоритма. В теоретических работах время обычно формализуется понятием глубины.

Глубина — это максимальное число элементов в ориентированной цепи, соединяющей вход и выход схемы. Если сложность соответствует размеру или площади реальной электронной микросхемы, то глубина соответствует быстродействию или времени срабатывания микросхемы. Глубина $D(f)$ функции f (т.е. минимальная глубина схемы, реализующей функцию) характеризует время ее параллельного вычисления. Глубина функции, существенно зависящей от n переменных, в базисе из бинарных операций не может быть меньше $\log n$.

В работе [8] помимо метода Карацубы представлен еще один результат, принадлежащий Ю. П. Офману. Выражаясь современным языком, он говорит о том, что умножение n -разрядных чисел может быть реализовано булевой схемой глубины $O(\log n)$.

Умножение n -коэффициентных многочленов очевидно выполняется с глубиной $\lceil \log n \rceil + 1$ стандартным методом, и эта оценка точная. Вопрос с глубиной умножения чисел обстоит сложнее. В числовом случае не прост даже вопрос о глубине сумматора. Впрочем, В. М. Храпченко [23] разрешил его в асимптотическом смысле, построив сумматор n -разрядных чисел глубины $(1 + o(1)) \log n$. Наилучшая, на сегодняшний день, верхняя оценка глубины сумматора имеет вид $\log n + \log \log n + O(1)$ и принадлежит М. И. Гринчуку [7].

В начале 1960-х гг. сразу в нескольких работах, в том числе в [8], было показано, что умножение n -разрядных чисел выполняется с глубиной $O(\log n)$. В основе доказательства лежит сведение к задаче суммирования n бит. Действительно, если в школьном методе умножения (см. рис. 1) выполнить сложения отдельно в каждом столбце и надлежащим образом сгруп-

пировать биты результатов, умножение сведется к суммированию $\log n$ чисел. Можно продолжить в том же духе, сократив число слагаемых до $\log \log n$ и т.д., пока не останется только два слагаемых, чтобы прийти к соотношению

$$D(M_n) \leq (D(C_n) + D(C_{\log n}) + \dots) + D(A_{2n}) = D(C_n) + \log n + o(\log n), \quad (10)$$

где через M_n , A_n и C_n обозначены соответственно операторы умножения и сложения n -разрядных чисел и оператор суммирования n бит. Последний переход выполнен при условии $D(C_n) = o(n)$. В практическом плане описанная стратегия не идеальна, но она позволяет вывести асимптотически наилучшие известные оценки глубины умножения.

Быстрые методы выполнения многократного сложения основаны на идее компрессоров.

Двоичный (k, l) -компрессор⁷ ширины 1 — это схема, реализующая булев оператор $(x_1, \dots, x_k) \rightarrow (y_1, \dots, y_l)$ по правилу $\sum 2^{a_i} x_i = \sum 2^{b_j} y_j$, где $k > l$, а $a_i, b_j \in \mathbb{Z}$. (k, l) -компрессор произвольной ширины строится из параллельных копий компрессоров ширины 1 — он преобразует k многоразрядных чисел в l чисел, сохраняя сумму.

Действительно, k чисел $x^i = [x_{n-1}^i, \dots, x_0^i]$, $1 \leq i \leq k$, параллельными преобразованиями $(x_{j+a_1}^1, \dots, x_{j+a_k}^k) \rightarrow (y_{j+b_1}^1, \dots, y_{j+b_l}^l)$, $j \in \mathbb{Z}$, переводятся в l чисел $y^i = [y_{n+h}^i, \dots, y_0^i]$, $1 \leq i \leq l$, где $h < \log k$, с сохранением суммы (все не определенные разряды в приведенных формулах полагаются равными нулю).

Простейшим компрессором является $(3, 2)$ -компрессор. Он реализует сумму трех битов по правилу $x_1 + x_2 + x_3 = 2y_2 + y_1$ формулами

$$y_2 = x_1(x_2 \oplus x_3) \oplus x_2x_3, \quad y_1 = x_1 \oplus x_2 \oplus x_3$$

сложности 5 и глубины 3.

Элементарный способ параллельной реализации оператора C_n — построить дерево $(3, 2)$ -компрессоров ширины $\log n$. Дерево имеет n входов, два $\log n$ -разрядных выхода и $\lceil \log_{3/2}(n/2) \rceil$ уровней компрессоров. Остается присоединить к выходам $\log n$ -разрядный сумматор. Ясно, что глубина полученной схемы равна $O(\log n)$.

Приемы быстрого вычисления C_n при помощи компрессоров совершенствовались в работах В. М. Храпченко [24], М. Патерсона, Н. Пиппенджера, У. Цвика [71, 72] (в этих же работах приводится подробная история вопроса). В частности, в [71, 72] установлен способ оптимального размещения заданных компрессоров в схеме. Рекордные, на сегодняшний день, результаты получены одним из авторов настоящего обзора: конструктивная оценка $D(M_n) \lesssim 4.34 \log n$ [17] и неконструктивная оценка $D(M_n) \lesssim 4.02 \log n$ [19]. В доказательстве этих оценок сумма бит восстанавливается из остатков по модулям 2^k и 3^l , и вычисленного с подходящей точностью приближенного значения.

И прикладной, и теоретический интерес представляет построение параллельных версий быстрых методов умножения, не приводящих к значительному росту сложности. Рассмотренные методы умножения многочленов и так имеют по порядку логарифмическую глубину. Известно по меньшей мере два подхода к параллельному перестроению числовых алгоритмов — оба связаны с применением специального кодирования чисел, в котором аддитивные операции выполняются с глубиной $O(1)$. Первый способ использует запись в знаковой четверичной системе счисления и известен с 1960-х гг. [30], см. также [86]. Во втором способе, предложенном А. В. Чашкиным [25], число u кодируется парой чисел (u_1, u_2) , разность которых доставляет истинное значение $u = u_1 - u_2$.

⁷В западной литературе принят термин CSA (carry save adder).

9. Еще о сложности базовых методов умножения

Несмотря на развитие быстрых методов умножения, стандартный метод и его модификации по-прежнему широко используются. На практике перемножаемые числа обычно имеют сравнительно небольшой размер, до нескольких сотен разрядов — для таких размеров стандартный метод эффективен.

Итак, суть стандартного метода — в сведении умножения к многократному сложению чисел. Сложность n -кратного сложения n -разрядных чисел имеет порядок n^2 , что очевидно, исходя из размерности задачи.

Зная, что $5n - 3$ операций необходимо для сложения двух n -разрядных чисел [15], кажется естественным, что сложение m чисел требует примерно $5(m - 1)n$ операций. Тем неожиданнее оказался результат, полученный в работе [44] 2010 г. группой математиков из Санкт-Петербургского отделения МИ РАН: указанная оценка сложности m -кратного сложения может быть улучшена уже при $m = 3$. Предложенная авторами схема основана на новой экономной конструкции компрессора. Используя эту конструкцию, верхнюю оценку сложности стандартного метода умножения можно уточнить до $5.5n^2 - 6.5n - 1 + (n \bmod 2)$ [18].

Для сложности метода Карацубы, в котором многократные сложения-вычитания, диктуемые формулой (2), оптимизированы с учетом результата [44], можно указать оценку $K(2^k) \leq 25 \frac{83}{405} \cdot 3^k - O(2^k)$ [18].

10. Сложность: квадратичная или линейная

Первоначальное предположение о квадратичной сложности умножения оправдывается в вычислительной модели клеточных схем. Содержательно, плоская клеточная схема — это прямоугольник, составленный из квадратных клеток-элементов. На стороне клетки расположено не более одного входа или выхода, при помощи которых клетки соединяются друг с другом. Например, схема может быть составлена из функциональных, коммутационных и разделительных элементов, изображенных на рис. 2 (f символизирует двуместную, а g — одноместную булеву функцию). Входы и выходы схемы расположены по периметру прямоугольника. Сложность клеточной схемы — число элементов в ней. Подробнее см., например, в [26].

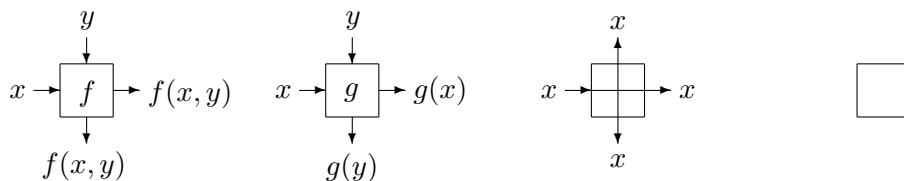


Рис. 2

Н. А. Шкаликова [26] доказала, что порядок сложности умножения n -разрядных чисел при реализации плоскими клеточными схемами равен n^2 . То же верно и для трехмерных клеточных схем. Понятно, что хотя клеточные схемы до некоторой степени подобны реальным электронным схемам, относительный размер проводников (коммутационных элементов) в модели несколько завышен. Нижняя оценка сложности умножения как раз и получается из оценки числа проводников, соединяющих фрагменты схемы. Впрочем, в современной схемотехнике плотность размещения проводников и плотность размещения функциональных элементов сближаются.

Напротив, можно указать вычислительные модели, в которых умножение доказуемо выполняется исключительно быстро, не в пример клеточным схемам. Одна из таких моделей —

это RAM-программы (альтернативное обозначение $\log$ -RAM). RAM-программа выполняет арифметические действия с аргументами длины $\log n$ за единичное время, где n — размер входа, подробнее см. в [1, 21, 50]. Сложность измеряется суммарным временем выполняемых инструкций. Модель вводится для адекватного отображения процесса вычислений на универсальном процессоре с памятью, хотя, конечно, физический процессор не способен поддерживать единичное время выполнения операций при $n \rightarrow \infty$.

А. О. Слисенко [21] и позднее М. Фюрер [50] заметили, что уже первый метод Шёнхаге–Штрассена, основанный на комплексном ДПФ, реализуется RAM-программами линейной сложности. Действительно, метод сводит умножение n -разрядных чисел к ДПФ порядка $\Theta(n/\log n)$ с $O(\log n)$ -разрядными аргументами, которое выполняется за $O(n)$ арифметических операций с такими аргументами.

Впрочем, линейная оценка сложности умножения в модели RAM-программ не должна вводить в заблуждение. Модель принципиально допускает вычисления с сублинейной сложностью. Например, сложение n -разрядных чисел реализуется RAM-программами сложности $O(n/\log n)$.

Около 1979 г. А. Шёнхаге [81] получил линейную сложность умножения в более изощренной вычислительной модели — машин с указателями (storage modification machines), см. также [11, 21].

11. Умножение в реальном времени

В некоторых приложениях возникает потребность в алгоритмах умножения реального времени (или online -умножения). Реальное время означает, что k -й разряд или коэффициент множителя поступает на вход алгоритма только после того, как вычислен $(k-1)$ -й разряд (коэффициент) произведения. Подобная ситуация естественным образом возникает в случае, когда очередные разряды входов зависят от найденных разрядов выхода. Так бывает, в частности, при решении функциональных уравнений итеративной процедурой (см., например, [64]).

Обозначим через $M^{\text{ONLINE}}(n)$ сложность умножения n -разрядных чисел в реальном времени неветвящимися программами⁸. М. Фишер и Л. Стокмайер [47] получили оценку

$$M^{\text{ONLINE}}(2^k) \preceq \sum_{i=0}^{k-1} 2^{k-i} M(2^i) + k2^k$$

через сложность обычного умножения⁹. Из нее в предположении равномерности роста функции $M(n)$ следует $M^{\text{ONLINE}}(n) \preceq M(n) \log n$. Если, например, для внутренних умножений алгоритма использовать метод Карацубы, то полученная online -версия метода Карацубы будет иметь такой же порядок сложности $n^{\log 3}$, как и у исходного метода. Аналогичный результат справедлив для умножения многочленов.

Ж. ван дер Хувер в серии работ (см., например, [64]) показал, что множитель $\log n$ может быть понижен при некоторых дополнительных предположениях о свойствах кольца, над которым выполняется умножение.

Нетривиальная нижняя оценка $M^{\text{ONLINE}}(n) = \Omega(n \log n)$ принадлежит М. Патерсону, М. Фишеру и А. Майеру [70].

⁸Напомним, что неветвящаяся программа — это схема с фиксацией порядка срабатывания элементов.

⁹В работе [47] использовалась вычислительная модель машины Тьюринга, но соотношение справедливо и для неветвящихся программ.

12. Заключение

Итак, на смену пессимистичной гипотезе $M(n) = \Omega(n^2)$ 1950-х гг. поначалу пришли оптимистичные ожидания: в некоторых публикациях ставился вопрос о существовании метода умножения линейной сложности. Сегодня же можно констатировать, что начиная с метода Карацубы и заканчивая методами 2014–2019 гг. магистральная линия развития методов умножения — редукция размера задачи при помощи интерполяции — оставалась неизменной. Этот путь привел к покорению рубежа $O(n \log n)$ в целочисленном варианте задачи; нет сомнений, что в самое ближайшее время аналогичная оценка будет доказана для сложности умножения многочленов. Многие исследователи склоняются к тому, что полученный результат по порядку сложности уже не может быть улучшен.

Впрочем, некоторые надежды связаны с развитием методов умножения линейной мультипликативной сложности. *Мультипликативная сложность* умножения многочленов из $K[x]$ — это число выполняемых при этом не скалярных умножений в K . Вопрос о мультипликативной сложности нетривиален, когда мощность кольца K меньше числа коэффициентов в произведении многочленов, и особенно интересен в экстремальном случае $K = GF(2)$.

Около 1987 г. братья Чудновские [39] предложили теорию для построения методов умножения над любым конечным полем $GF(q)$ с линейной мультипликативной сложностью. Исследования были продолжены в десятках работ других авторов, см., например, обзоры [31, 77]. Все построенные методы используют интерполяцию в группах дивизоров алгебраических кривых и имеют весьма нетривиальное обоснование¹⁰.

Пока основные результаты здесь связаны с уточнением констант в оценках мультипликативной сложности. Например, к сегодняшнему дню доказано, что мультипликативная сложность умножения многочленов степени n над $GF(2)$ не превосходит $(35/3 + o(1))n$ [74]. Но общая сложность соответствующих алгоритмов умножения, по всей видимости, далека от желаемой.

С другой стороны, нелинейная мультипликативная сложность является одним из ограничивающих факторов для известных быстрых алгоритмов умножения, поскольку она определяет размерность линейных преобразований в билинейной структуре алгоритмов. Для сравнения, в методах Шёнхаге и Штрассена выполняется порядка $n \log n$ элементарных не скалярных умножений, в методе [56] — порядка $n \cdot c^{\log^* n}$, а в методе [60] — порядка $n \log^c n$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Ахо А., Хопкрофт Дж., Ульман Дж. Проектирование и анализ вычислительных алгоритмов. — М.: Мир, 1979.
2. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов. — М.: Мир, 1989.
3. Власенко В. А., Лаппа Ю. М., Ярославский Л. П. Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов. — М.: Наука, 1990.
4. Гашков С. Б. Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли // Дискретная математика. 2000. 12, № 3. С. 124–153.
5. Гашков С. Б., Сергеев И. С. Алгоритмы быстрого преобразования Фурье // Дискретная математика и ее приложения. V. — М.: Изд-во ИПМ РАН, 2009. — С. 3–23.

¹⁰Сложность теории подчеркивает тот факт, что во всех первоначальных и во многих последующих работах по методам умножения линейной мультипликативной сложности обнаружены пробелы в рассуждениях.

6. Гашков С. Б., Сергеев И. С. О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2 // Дискретная математика. 2013. 25, № 1. С. 3–32.
7. Гринчук М. И. Уточнение верхней оценки глубины сумматора и компаратора // Дискретный анализ и исследование операций. Серия 1. 2008. 15, № 2. С. 12–22.
8. Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах // Доклады АН СССР. 1962. 145, № 2. С. 293–294.
9. Карацуба А. А. Сложность вычислений // Труды МИАН. 1995. 211. С. 186–202.
10. Карацуба А. А. Комментарии к моим работам, написанные мной самим // Современные проблемы математики. 2013. 17. С. 7–29.
11. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. — М.: Вильямс, 2004.
12. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд. МГУ, 1984.
13. Лупанов О. Б. А. Н. Колмогоров и теория сложности схем // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 5–12.
14. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток. — М.: Радио и связь, 1985.
15. Редькин Н. П. О минимальной реализации двоичного сумматора // Проблемы кибернетики. Вып. 38. — М.: Наука, 1981. — С. 181–216.
16. Сергеев И. С. Регулярные оценки сложности умножения многочленов и усеченного ДПФ // Прикладная дискретная математика. 2011. № 4(14). С. 72–88.
17. Сергеев И. С. Верхние оценки глубины симметрических булевых функций // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2013. № 4. С. 39–44.
18. Сергеев И. С. О схемной сложности стандартного метода умножения чисел и метода Карацубы // Труды XXII Междунар. науч.-техн. конф. “Информационные средства и технологии”. Том 3. — М.: Изд. дом МЭИ, 2014. — С. 180–187.
19. Сергеев И. С. О сложности и глубине формул для симметрических булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. 2016. № 3. С. 53–57.
20. Сергеев И. С. О вещественной сложности комплексного ДПФ // Проблемы передачи информации. 2017. 53, № 3. С. 90–99.
21. Слисенко А. О. Сложностные задачи теории вычислений // Успехи математических наук. 1981. 36, № 6(222). С. 21–103.
22. Тоом А. Л. О сложности схемы из функциональных элементов, реализующей умножение целых чисел // Доклады АН СССР. 1963. 150, № 3. С. 496–498.
23. Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 107–120.

-
24. Храпченко В. М. Некоторые оценки для времени умножения // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 221–227.
 25. Чашкин А. В. Дискретная математика. — М.: Академия, 2012.
 26. Шкаликова Н. А. О сложности реализации некоторых функций клеточными схемами // Сб. работ по матем. кибернетике. Вып. 1. — М.: Изд-во ВЦ АН СССР, 1976. — С. 102–115.
 27. Adleman L. M., Pomerance C., Rumely R. S. On distinguishing prime numbers from composite numbers // The Annals of Mathematics, Second Series. 1983. 117, № 1. P. 173–206.
 28. Agarwal R. C., Cooley J. W. New algorithms for digital convolution // IEEE Trans. on ASSP. 1977. 25, № 5. P. 392–410.
 29. Arnold A. A new truncated Fourier transform algorithm // Proc. Int. Symp. on Symbolic and Algebraic Comp. (Boston, 2013). — NY: ACM, 2013. — P. 15–22.
 30. Avizienis A. Signed-digit number representations for fast parallel arithmetic // IRE Trans. on Electr. Computers. 1961. EC10. P. 389–400.
 31. Ballet S., Chaumine J., Pieltant J., Rolland R. On the tensor rank of multiplication in finite fields. 2011. arXiv:1107.1184.
 32. Bernstein D. J. Fast multiplication and its applications // Algorithmic Number Theory, MSRI Publ. 2008. 44. P. 325–384.
 33. Bernstein D. J., Chou T. Faster binary-field multiplication and faster binary-field MACs // Lecture Notes on Comp. Sci. 2014. 8781. P. 92–111.
 34. Bluestein L. I. A linear filtering approach to the computation of discrete Fourier transform // ECCS Trans. on Audio and Electroacoustics. 1970. 18, № 4. P. 451–455. [NEREM record. 1968. 10. P. 218–219.]
 35. Cantor D. G. On arithmetical algorithms over finite fields // J. Comb. Theory. Series A. 1989. 50. P. 285–300.
 36. Cantor D., Kaltofen E. On fast multiplication of polynomials over arbitrary algebras // Acta Inf. 1991. 28, № 7. P. 693–701.
 37. Cenk M., Hasan M. A. Some new results on binary polynomial multiplication // J. Cryptographic Engineering. 2015. 5, № 4. P. 289–303.
 38. Chen M.-S., Cheng C.-M., Kuo P.-C., Li W.-D., Yang B.-Y. Multiplying boolean polynomials with Frobenius partitions in additive fast Fourier transform. 2018. arXiv:1803.11301.
 39. Chudnovsky D. V., Chudnovsky G. V. Algebraic complexities and algebraic curves over finite fields // J. Complexity. 1988. 4. P. 285–316.
 40. Cook S. On the minimum computation time of functions. Ph.D. Thesis, Harvard Univ., 1966.
 41. Cooley J. W., Tukey J. W. An algorithm for the machine calculation of complex Fourier series // Math. Comp. 1965. 19, № 90. P. 297–301.
 42. Crandall R., Fagin B. Discrete weighted transforms and large-integer arithmetic // Math. Comp. 1994. 62, № 205. P. 305–324.

-
43. De A., Kurur P. P., Saha C., Saptharishi R. Fast integer multiplication using modular arithmetic // SIAM J. Comput. 2013. 42, № 2. P. 685–699.
 44. Demenkov E., Kojevnikov A., Kulikov A., Yaroslavl'tsev G. New upper bounds on the Boolean circuit complexity of symmetric functions // Inf. Proc. Letters. 2010. 110, № 7. P. 264–267.
 45. Dutt A., Rokhlin V. Fast Fourier transforms for nonequispaced data // SIAM J. Sci. Comput. 1993. 14, № 6. P. 1368–1393.
 46. Find M. G., Peralta R. Better circuits for binary polynomial multiplication // IEEE Trans. on Comp. 2019. 68, № 4. P. 624–630.
 47. Fischer M. J., Stockmeyer L. Fast on-line integer multiplication // J. Comput. and System Sci. 1974. 9. P. 317–331.
 48. Fürer M. On the complexity of integer multiplication (extended abstract). Tech. Report CS-89-17. Pennsylvania State Univ., 1989.
 49. Fürer M. Faster integer multiplication // SIAM J. Comput. 2009. 39, № 3. P. 979–1005.
 50. Fürer M. How fast can we multiply large integers on an actual computer? // Proc. Latin Amer. Symp. on Theor. Inf. (Montevideo, 2014). Lecture Notes on Comp. Sci. 2014. 8392. P. 660–670.
 51. Gao S., Mateer T. Additive fast Fourier transforms over finite fields // IEEE Trans. on Information Theory. 2010. 56. P. 6265–6272.
 52. von zur Gathen J., Gerhard J. Arithmetic and factorization of polynomials over $\mathbb{F}_2$ // Proc. Int. Symp. on Symbolic and Algebraic Comp. (Zürich, 1996). — NY: ACM, 1996. — P. 1–9.
 53. von zur Gathen J., Gerhard J. Modern computer algebra. — Cambridge: Cambridge University Press, 1999.
 54. Good I. J. The interaction algorithm and practical Fourier analysis // J. R. Statist. Soc. B. 1958. 20, № 2. P. 361–372; 1960. 22, № 2. P. 372–375.
 55. Harvey D., van der Hoeven J., Lecerf G. Even faster integer multiplication // J. Complexity. 2016. 36. P. 1–30.
 56. Harvey D., van der Hoeven J., Lecerf G. Faster polynomial multiplication over finite fields // J. ACM. 2017. 63, № 6. Article 52.
 57. Harvey D., van der Hoeven J. Faster integer and polynomial multiplication using cyclotomic coefficient rings. 2017. arXiv:1712.03693.
 58. Harvey D., van der Hoeven J. Faster integer multiplication using short lattice vectors // Proc. 13th Algorithm. Number Theory Symp. (Madison, Wisconsin, 2018) — Berkeley: Math. Sci. Publ., 2019. — P. 293–310.
 59. Harvey D., van der Hoeven J. Integer multiplication in time $O(n \log n)$. Tech. report № 02070778. HAL, 2019.
 60. Harvey D., van der Hoeven J. Polynomial multiplication over finite fields in time $O(n \log n)$. Tech. report № 02070816. HAL, 2019.
 61. Haynal S., Haynal H. Generating and searching families of FFT algorithms // J. Satisf., Boolean Modeling and Comput. 2011. 7, № 4. P. 145–187.

62. Heideman M. T. Applications of multiplicative complexity theory to convolution and the discrete Fourier transform. Ph.D. Thesis. Rice Univ., 1986.
63. van der Hoeven J. The truncated Fourier transform and applications // Proc. Int. Symp. on Symbolic and Algebraic Comput. (Santander, 2004). — NY: ACM, 2004. — P. 290–296.
64. van der Hoeven J. Faster relaxed multiplication // Proc. Int. Symp. on Symbolic and Algebraic Comp. (Kobe, 2014). — NY: ACM, 2014. — P. 405–412.
65. van der Hoeven J., Larrieu R. The Frobenius FFT // Proc. Int. Symp. on Symbolic and Algebraic Comp. (Kaiserslautern, 2017). — NY: ACM, 2017. — P. 437–444.
66. Johnson S. F., Frigo M. A modified split-radix FFT with fewer arithmetic operations // IEEE Trans. Signal Process. 2007. 55, № 1. P. 111–119.
67. Li W.-D., Chen M.-S., Kuo P.-C., Cheng C.-M., Yang B.-Y. Frobenius additive fast Fourier transform // Proc. Int. Symp. on Symbolic and Algebraic Comp. (New York, 2018). — NY: ACM, 2018. — P. 263–270.
68. Lundy T. J., van Buskirk J. A new matrix approach to real FFTs and convolutions of length 2^k // Computing. 2007. 80, № 1. P. 23–45.
69. Mateer T. Fast Fourier transform algorithms with applications. Ph.D. thesis, Clemson Univ., 2008.
70. Paterson M. S., Fischer M. J., Meyer A. R. An improved overlap argument for on-line multiplication. Tech. Report 40. Project MAC. MIT, 1974. [Русский перевод: Патерсон М. С., Фишер М. Дж., Мейер А. Р. Улучшенный метод частичного перекрытия для умножения, выполняемого в темпе поступления информации. Кибернетический сборник. Вып. 14. — М.: Мир, 1977. — С. 78–94.]
71. Paterson M. S., Pippenger N., Zwick U. Optimal carry save networks // LMS Lecture Notes Series. Boolean function complexity. Vol. 169. — Cambridge: Cambridge Univ. Press, 1992. — P. 174–201.
72. Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication // Comput. Complexity. 1993. 3. P. 262–291.
73. De Piccoli A., Visconti A., Rizzo O. G. Polynomial multiplication over binary finite fields: new upper bounds. Cryptology ePrint Archive, 2018/901.
74. Pielant J., Randriam H. New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields // Math. Comp. 2015. 84. P. 2023–2045.
75. Pollard J. M. The Fast Fourier Transform in a finite field // Math. Comp. 1971. 25, № 114. P. 365–374. [Русский перевод: Поллард Дж. М. Быстрое преобразование Фурье в конечном поле // В кн. Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. — М.: Радио и связь, 1983. — С. 147–155.]
76. Rader C. M. Discrete Fourier transforms when the number of data samples is prime // Proc. IEEE. 1968. 56. P. 1107–1108. [Русский перевод: Рейдер Ч. М. Дискретное преобразование Фурье, когда число отсчетов простое // В кн. Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. — М.: Радио и связь, 1983. — С. 89–91.]

77. Randriambololona H. Bilinear complexity of algebras and the Chudnovsky—Chudnovsky interpolation method // J. Complexity. 2012. 28, № 4. P. 489–517.
78. Schönhage A. Multiplikation großer Zahlen // Computing. 1966. 1, № 3. P. 182–196.
79. Schönhage A., Strassen V. Schnelle Multiplikation großer Zahlen // Computing. 1971. 7, № 3–4. P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел. Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98.]
80. Schönhage A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2 // Acta Inf. 1977. 7. P. 395–398.
81. Schönhage A. Storage modification machines // SIAM J. Comput. 1980. 9, № 3. P. 490–508.
82. Schönhage A. Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients // Proc. Europ. Comput. Algebra Conf. (Marseille, 1982). Lecture Notes on Comp. Sci. 1982. 144. P. 3–15.
83. Schönhage A., Grotfeld A. F. W., Vetter E. Fast algorithms: a multitape Turing machine implementation. — Mannheim, Leipzig, Wien, Zürich: BI-Wissenschaftsverlag, 1994.
84. Thomas L. H. Using a computer to solve problem in Physics // Application in digital computers. — Boston: Ginn and Co., 1963.
85. Wang Y., Zhu X. A fast algorithm for Fourier transform over finite fields and its VLSI implementation // IEEE Journal on Selected Areas in Communications. 1988. 6, № 3. P. 572–577.
86. Wegener I. The complexity of Boolean functions. — Stuttgart: Wiley-Teubner, 1987.
87. Winograd S. On the multiplicative complexity of the discrete Fourier transform // Advances in Math. 1979. 32, № 2. P. 83–117.
88. Yavne R. An economical method for calculating the discrete Fourier transform // Proc. Fall Joint Computer Conf. (San Francisco, 1968). Part I. — NY: ACM, 1968. — P. 115–125.
89. Zheng W., Li K., Li K. Scaled radix-2/8 algorithm for efficient computation of length- $N = 2^m$ DFTs // IEEE Trans. Signal Process. 2014. 62, № 10. P. 2492–2503.

REFERENCES

1. Aho, A. V., Hopcroft, J. E. & Ullman J. D. 1976, The design and analysis of computer algorithms, Addison-Wesley, Reading, Mass.
2. Blahut, R. E. 1985, Fast algorithms for digital signal processing, Addison-Wesley, Reading, Mass.
3. Vlasenko, V. A., Lappa, Yu. M. & Jaroslavsky L. P. 1990, Metody sinteza bystrykh algoritmov svertki i spektral'nogo analiza signalov [Methods to design the fast convolution algorithms and spectral signal analysis], Nauka, Moscow, USSR (in Russian).
4. Gashkov, S. B. 2000, “Remarks on the fast multiplication of polynomials, and Fourier and Hartley transforms”, Diskret. mat., vol. 12, no. 3, pp. 124–153 (in Russian); 2000, Discrete Math. and Appl., vol. 10, no. 5, pp. 499–528.

5. Gashkov, S. B. & Sergeev, I. S. 2009, “Fast Fourier transform algorithms”, *Diskretnaya matematika i ee prilozheniya* [Discrete mathematics and its applications], vol. V, Keldysh Inst. Appl. Math., Moscow, Russia, pp. 3–23 (in Russian).
6. Gashkov, S. B. & Sergeev, I. S. 2013, “On complexity and depth of Boolean circuits for multiplication and inversion over finite fields of characteristic 2”, *Diskret. mat.*, vol. 25, no. 1, pp. 3–32 (in Russian); 2013, *Discrete Math. and Appl.*, vol. 23., no. 1, pp. 1–37.
7. Grinchuk, M. I. 2008, “Sharpening an upper bound on the adder and comparator depths”, *Diskret. analiz i issled. operatsii. Ser. 1*, vol. 15, no. 2, pp. 12–22 (in Russian); 2009, *J. Appl. and Industr. Math.*, vol. 3, no. 1, pp. 61–67.
8. Karatsuba, A. A. & Ofman, Yu. P. 1962, “Multiplication of multidigit numbers on automata”, *Doklady Akad. nauk SSSR*, vol. 145, no. 2, pp. 293–294 (in Russian); 1963, *Soviet Physics Doklady*, vol. 7, pp. 595–596.
9. Karatsuba, A. A. 1995, “The complexity of computations”, *Trudy MIAN*, vol. 211, pp. 186–202 (in Russian); 1995, *Proc. Steklov Inst. Math.*, vol. 211, pp. 169–183.
10. Karatsuba, A. A. 2013, “Comments to my works, written by myself”, *Sovrem. problemy matem.*, vol. 17, pp. 7–29 (in Russian); 2013, *Proc. Steklov Inst. Math.*, vol. 282, suppl. 1, pp. S1–S23.
11. Knuth, D. E. 1998, *The art of computer programming. Vol. 2. Seminumerical algorithms*, 3rd ed., Addison–Wesley Longman, Reading, Mass.
12. Lupanov, O. B. 1984, *Asimptoticheskie otsenki slozhnosti upravlyayuscshikh sistem* [Asymptotic bounds on the complexity of control systems], Mosk. Gos. Univ., Moscow, USSR (in Russian).
13. Lupanov, O. B. 2008, “A. N. Kolmogorov and the circuit complexity theory”, *Matematicheskie voprosy kibernetiki* [Mathematical issues of cybernetics], vol. 17, Fizmatlit, Moscow, Russia, pp. 5–12 (in Russian).
14. Nussbaumer, H. J. 1982, *Fast Fourier transform and convolution algorithms*, 2nd ed., Springer, Berlin–Heidelberg.
15. Red’kin, N. P. 1981, “On the minimal realization of the binary adder”, *Problemy kibernetiki* [Problems of cybernetics], vol. 38, Nauka, Moscow, USSR, pp. 181–216 (in Russian).
16. Sergeev, I. S. 2011, “Regular estimates for the complexity of polynomial multiplication and truncated Fourier transform”, *Prikladnaya diskretnaya matematika* [Applied discrete mathematics], no. 4(14), pp. 72–88 (in Russian).
17. Sergeev, I. S. 2013, “Upper bounds on the depth of symmetric Boolean functions”, *Vestnik Mosk. univ. Ser. 15. Vychislit. matem. i kibern.*, no. 4, pp. 39–44 (in Russian); 2013, *Moscow Univ. Comput. Math. and Cybernetics*, vol. 37, no. 4, pp. 195–201.
18. Sergeev, I. S. 2014, “On the circuit complexity of the standard and the Karatsuba methods of multiplying integers”, *Trudy XXII Mezhdunar. nauchn.-tekhn. konf. “Informatsionnye sredstva i tekhnologii”* [Proc. 22th Int. Sci.-Tech. Conf. “Information tools and technologies”], vol. 3, Izd. dom MEI, Moscow, Russia, pp. 180–187 (in Russian); 2016, arXiv:1602.02362, available at: <http://arxiv.org/abs/1602.02362>
19. Sergeev, I. S. 2016, “Complexity and depth of formulas for symmetric Boolean functions”, *Vestnik Mosk. univ. Ser. 1. Matem. Mekh.*, no. 3, pp. 53–57 (in Russian); 2016, *Moscow Univ. Math. Bulletin*, vol. 71, no. 3, pp. 127–130.

-
20. Sergeev, I. S. 2017, "On the real complexity of a complex DFT", *Problemy peredachi informatsii*, vol. 53, no. 3, pp. 90–99 (in Russian); 2017, *Problems of Information Transmission*, vol. 53, no. 3, pp. 284–293.
 21. Slisenko A. O. 1981, "Complexity problems in computational theory", *Uspekhi mat. nauk*, vol. 36, no. 6(222), pp. 21–103 (in Russian); 1981, *Russian Math. Surveys*, vol. 36, no. 6, pp. 23–125.
 22. Toom, A. L. 1963, "The complexity of a scheme of functional elements realizing the multiplication of integers", *Doklady Akad. nauk SSSR*, vol. 150, no. 3, pp. 496–498 (in Russian); 1963, *Soviet Math. Doklady*, vol. 3, pp. 714–716.
 23. Khrapchenko, V. M. 1967, "Asymptotic estimation of addition time of a parallel adder", *Problemy kibernetiki* [Problems of cybernetics], vol. 19, Nauka, Moscow, USSR, pp. 107–120 (in Russian); 1970, *Systems Theory Research*, vol. 19, pp. 105–122.
 24. Khrapchenko, V. M. 1978, "Some estimates for the multiplication time", *Problemy kibernetiki* [Problems of cybernetics], vol. 33, Nauka, Moscow, USSR, pp. 221–227 (in Russian).
 25. Chashkin, A. V. 2012, *Diskretnaya matematika* [Discrete mathematics], Akademiya, Moscow, Russia, 2012 (in Russian).
 26. Shkalikova, N. A. 1976, "On the complexity of realization of some functions by cellular circuits", *Sborn. rabot po matem. kibern.* [Selected papers on math. cybernetics], vol. 1, Izd. Vychisl. Ts. AN SSSR, Moscow, USSR, pp. 102–115 (in Russian).
 27. Adleman, L. M., Pomerance, C. & Rumely, R. S. 1983, "On distinguishing prime numbers from composite numbers", *The Annals of Mathematics*, Second Series, vol. 117, no. 1, pp. 173–206.
 28. Agarwal R. C. & Cooley J. W. 1977, "New algorithms for digital convolution", *IEEE Trans. on ASSP*, vol. 25, no. 5, pp. 392–410.
 29. Arnold, A. 2013, "A new truncated Fourier transform algorithm", *Proc. Int. Symp. on Symbolic and Algebraic Comp.* (Boston, 2013), ACM, NY, pp. 15–22.
 30. Avizienis, A. 1961, "Signed-digit number representations for fast parallel arithmetic", *IRE Trans. on Electr. Computers*, vol. EC10, pp. 389–400.
 31. Ballet, S., Chaumine, J., Peltant, J. & Rolland, R. 2011. "On the tensor rank of multiplication in finite fields", arXiv:1107.1184, available at: <http://arxiv.org/abs/1107.1184>
 32. Bernstein, D. J. 2008, "Fast multiplication and its applications", *Algorithmic Number Theory*, MSRI Publ., vol. 44, pp. 325–384.
 33. Bernstein, D. J. & Chou, T. 2014, "Faster binary-field multiplication and faster binary-field MACs", *Lecture Notes on Comp. Sci.*, vol. 8781, pp. 92–111.
 34. Bluestein, L. I. 1970, "A linear filtering approach to the computation of discrete Fourier transform", *ECCC Trans. on Audio and Electroacoustics*, vol. 18, no. 4, pp. 451–455; 1968, *NEREM record*, vol. 10, pp. 218–219.
 35. Cantor, D. G. 1989, "On arithmetical algorithms over finite fields", *J. Comb. Theory. Series A*, vol. 50, pp. 285–300.
 36. Cantor, D. & Kaltofen, E. 1991, "On fast multiplication of polynomials over arbitrary algebras", *Acta Inf.*, vol. 28, no. 7, pp. 693–701.

37. Cenk, M. & Hasan, M. A. 2015, "Some new results on binary polynomial multiplication", *J. Cryptographic Engineering*, vol. 5, no. 4, pp. 289–303.
38. Chen, M.-S., Cheng, C.-M., Kuo, P.-C., Li, W.-D. & Yang, B.-Y. 2018, "Multiplying boolean polynomials with Frobenius partitions in additive fast Fourier transform", arXiv:1803.11301, available at: <http://arxiv.org/abs/1803.11301>
39. Chudnovsky, D. V. & Chudnovsky, G. V. 1988, "Algebraic complexities and algebraic curves over finite fields", *J. Complexity*, vol. 4, pp. 285–316.
40. Cook, S. 1966, On the minimum computation time of functions, Ph.D. Thesis, Harvard Univ., Cambridge, Mass.
41. Cooley, J. W. & Tukey J. W. 1965, "An algorithm for the machine calculation of complex Fourier series", *Math. Comp.*, vol. 19, no. 90, pp. 297–301.
42. Crandall, R. & Fagin, B. 1994, "Discrete weighted transforms and large-integer arithmetic", *Math. Comp.*, vol. 62, no. 205, pp. 305–324.
43. De, A., Kurur, P. P., Saha, C. & Saptharishi, R. 2013, "Fast integer multiplication using modular arithmetic", *SIAM J. Comput.*, vol. 42, no. 2, pp. 685–699.
44. Demenkov, E., Kojevnikov, A., Kulikov, A. & Yaroslavl'tsev G. 2010, "New upper bounds on the Boolean circuit complexity of symmetric functions", *Inf. Proc. Letters*, vol. 110, no. 7, pp. 264–267.
45. Dutt, A. & Rokhlin, V. 1993, "Fast Fourier transforms for nonequispaced data", *SIAM J. Sci. Comput.*, vol. 14, no. 6., pp. 1368–1393.
46. Find, M. G. & Peralta, R. 2019, "Better circuits for binary polynomial multiplication", *IEEE Trans. on Comp.*, vol. 68, no. 4, pp. 624–630.
47. Fischer, M. J. & Stockmeyer, L. 1974, "Fast on-line integer multiplication", *J. Comput. and System Sci.*, vol. 9, pp. 317–331.
48. Fürer, M. 1989, On the complexity of integer multiplication (extended abstract), Tech. Report CS-89-17, Pennsylvania State Univ.
49. Fürer, M. 2009, "Faster integer multiplication", *SIAM J. Comput.*, vol. 39, no. 3, pp. 979–1005.
50. Fürer, M. 2014, "How fast can we multiply large integers on an actual computer?", *Proc. Latin Amer. Symp. on Theor. Inf. (Montevideo, 2014)*, *Lecture Notes on Comp. Sci.*, vol. 8392, pp. 660–670.
51. Gao, S. & Mateer, T. 2010, "Additive fast Fourier transforms over finite fields", *IEEE Trans. on Information Theory*, vol. 56, pp. 6265–6272.
52. von zur Gathen, J. & Gerhard, J. 1996, "Arithmetic and factorization of polynomials over $\mathbb{F}_2$ ", *Proc. Int. Symp. on Symbolic and Algebraic Comp. (Zürich, 1996)*, ACM, NY, pp. 1–9.
53. von zur Gathen, J. & Gerhard, J. 1999, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.
54. Good, I. J. 1958, "The interaction algorithm and practical Fourier analysis", *J. R. Statist. Soc. B.*, vol. 20, no. 2, pp. 361–372; 1960, vol. 22, no. 2, pp. 372–375.

-
55. Harvey, D., van der Hoeven, J. & Lecerf, G. 2016, “Even faster integer multiplication”, J. Complexity, vol. 36, pp. 1–30.
 56. Harvey, D., van der Hoeven, J. & Lecerf, G. 2017, “Faster polynomial multiplication over finite fields”, J. ACM, vol. 63, no. 6, Article 52.
 57. Harvey, D. & van der Hoeven, J. 2017, “Faster integer and polynomial multiplication using cyclotomic coefficient rings”, arXiv:1712.03693, available at: <http://arxiv.org/abs/1712.03693>
 58. Harvey, D. & van der Hoeven, J. 2019, “Faster integer multiplication using short lattice vectors”, Proc. 13th Algorithm. Number Theory Symp. (Madison, Wisconsin, 2018), Math. Sci. Publ., Berkeley, pp. 293–310.
 59. Harvey D. & van der Hoeven J. 2019, “Integer multiplication in time $O(n \log n)$ ”, HAL Tech. report № 02070778, available at: <https://hal.archives-ouvertes.fr/hal-02070778>
 60. Harvey D. & van der Hoeven J. 2019, “Polynomial multiplication over finite fields in time $O(n \log n)$ ”, HAL Tech. report № 02070816, available at: <https://hal.archives-ouvertes.fr/hal-02070816>
 61. Haynal, S. & Haynal, H. 2011, “Generating and searching families of FFT algorithms”, J. Satisf., Boolean Modeling and Comput., vol. 7, no.4, pp. 145–187.
 62. Heideman, M. T. 1986, Applications of multiplicative complexity theory to convolution and the discrete Fourier transform, Ph.D. Thesis, Rice Univ., Houston, Texas.
 63. van der Hoeven, J. 2004, “The truncated Fourier transform and applications”, Proc. Int. Symp. on Symbolic and Algebraic Comput. (Santander, 2004), ACM, NY, pp. 290–296.
 64. van der Hoeven, J. 2014, “Faster relaxed multiplication”, Proc. Int. Symp. on Symbolic and Algebraic Comp. (Kobe, 2014), ACM, NY, pp. 405–412.
 65. van der Hoeven, J. & Larrieu, R. 2017, “The Frobenius FFT”, Proc. Int. Symp. on Symbolic and Algebraic Comp. (Kaiserslautern, 2017), ACM, NY, pp. 437–444.
 66. Johnson, S. F. & Frigo, M. 2007, “A modified split-radix FFT with fewer arithmetic operations”, IEEE Trans. Signal Process., vol. 55, no. 1, pp. 111–119.
 67. Li, W.-D., Chen, M.-S., Kuo, P.-C., Cheng, C.-M. & Yang, B.-Y. 2018, “Frobenius additive fast Fourier transform”, Proc. Int. Symp. on Symbolic and Algebraic Comp. (New York, 2018), ACM, NY, pp. 263–270.
 68. Lundy, T. J. & van Buskirk, J. 2007, “A new matrix approach to real FFTs and convolutions of length 2^k ”, Computing, vol. 80, no. 1, pp. 23–45.
 69. Mateer, T. 2008, Fast Fourier transform algorithms with applications, Ph.D. thesis, Clemson Univ., Clemson, South Car.
 70. Paterson, M. S., Fischer, M. J. & Meyer, A. R. 1974, An improved overlap argument for on-line multiplication, Tech. Report 40, Project MAC, MIT, Boston, Mass.
 71. Paterson, M. S., Pippenger, N. & Zwick, U. 1992, “Optimal carry save networks”, LMS Lecture Notes Series. Boolean function complexity, vol. 169, Cambridge Univ. Press, Cambridge, UK, pp. 174–201.

72. Paterson, M. & Zwick, U. 1993, “Shallow circuits and concise formulae for multiple addition and multiplication”, *Comput. Complexity*, vol. 3, pp. 262–291.
73. De Piccoli, A., Visconti, A. & Rizzo, O. G. 2018, “Polynomial multiplication over binary finite fields: new upper bounds”, *Cryptology ePrint Archive*, 2018/901, available at: <https://eprint.iacr.org/2018/091.pdf>
74. Pielant, J. & Randriam, H. 2015, “New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields”, *Math. Comp.*, vol. 84, pp. 2023–2045.
75. Pollard, J. M. 1971, “The Fast Fourier Transform in a finite field”, *Math. Comp.*, vol. 25, no. 114, pp. 365–374.
76. Rader, C. M. 1968, “Discrete Fourier transforms when the number of data samples is prime”, *Proc. IEEE*, vol. 56, pp. 1107–1108.
77. Randriambololona, H. 2012, “Bilinear complexity of algebras and the Chudnovsky—Chudnovsky interpolation method”, *J. Complexity*, vol. 28, no. 4, pp. 489–517.
78. Schönhage, A. 1966, “Multiplikation großer Zahlen”, *Computing*, vol. 1, no. 3, pp. 182–196.
79. Schönhage, A. & Strassen, V. 1971, “Schnelle Multiplikation großer Zahlen”, *Computing*, vol. 7, no. 3–4, pp. 271–282.
80. Schönhage, A. 1977, “Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2”, *Acta Inf.*, vol. 7, pp. 395–398.
81. Schönhage, A. 1980, “Storage modification machines”, *SIAM J. Comput.*, vol. 9, no. 3, pp. 490–508.
82. Schönhage, A. 1982, “Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients”, *Proc. Europ. Comput. Algebra Conf. (Marseille, 1982)*, *Lecture Notes on Comp. Sci.*, vol. 144, pp. 3–15.
83. Schönhage, A., Grotefeld, A. F. W. & Vetter, E. 1994, *Fast algorithms: a multitape Turing machine implementation*, BI-Wissenschaftsverlag, Mannheim, Leipzig, Wien, Zürich.
84. Thomas, L. H. 1963, “Using a computer to solve problem in Physics”, *Application in digital computers*, Ginn and Co., Boston, Mass.
85. Wang, Y. & Zhu, X. “A fast algorithm for Fourier transform over finite fields and its VLSI implementation”, *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 3, pp. 572–577.
86. Wegener, I. 1987, *The complexity of Boolean functions*, Wiley–Teubner, Stuttgart, FRG.
87. Winograd, S. 1979, “On the multiplicative complexity of the discrete Fourier transform”, *Advances in Math.*, vol. 32, no.2, pp. 83–117.
88. Yavne, R. 1968, “An economical method for calculating the discrete Fourier transform”, *Proc. Fall Joint Computer Conf. (San Francisco, 1968)*. Part I, ACM, NY, pp. 115–125.
89. Zheng, W., Li, K. & Li, K. 2014, “Scaled radix-2/8 algorithm for efficient computation of length- $N = 2^m$ DFTs”, *IEEE Trans. Signal Process.*, vol. 62, no. 10, pp. 2492–2503.

Получено 5.03.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.4

DOI 10.22405/2226-8383-2020-21-1-135-144

Об алгебраических тождествах между фундаментальными матрицами обобщённых гипергеометрических уравнений

В. А. Горелов

Горелов Василий Александрович — кандидат физико-математических наук, доцент кафедры математического моделирования, Национальный исследовательский университет «Московский энергетический институт» (г. Москва).

e-mail: gorelov.va@mail.ru

Аннотация

В настоящей работе получены примеры алгебраических тождеств между фундаментальными матрицами обобщённых гипергеометрических уравнений. В некоторых случаях эти тождества порождают все алгебраические соотношения между компонентами решений гипергеометрических уравнений.

Обобщённые гипергеометрические функции (см. [1–5]) — это функции вида

$${}_l\varphi_q(z) = {}_l\varphi_q(\vec{\nu}; \vec{\lambda}; z) = {}_{l+1}F_q \left(\begin{matrix} 1, \nu_1, \dots, \nu_l \\ \lambda_1, \dots, \lambda_q \end{matrix} \middle| z \right) = \sum_{n=0}^{\infty} \frac{(\nu_1)_n \dots (\nu_l)_n}{(\lambda_1)_n \dots (\lambda_q)_n} z^n,$$

где $0 \leq l \leq q$, $(\nu)_0 = 1$, $(\nu)_n = \nu(\nu+1) \dots (\nu+n-1)$, $\vec{\nu} = (\nu_1, \dots, \nu_l) \in \mathbb{C}^l$, $\vec{\lambda} \in (\mathbb{C} \setminus \mathbb{Z}^-)^q$.

Функция ${}_l\varphi_q(\vec{\nu}; \vec{\lambda}; z)$ удовлетворяет (обобщённому) гипергеометрическому дифференциальному уравнению

$$L(\vec{\nu}; \vec{\lambda}; z) y = (\lambda_1 - 1) \dots (\lambda_q - 1),$$

где

$$L(\vec{\nu}; \vec{\lambda}; z) \equiv \left(\prod_{j=1}^q (\delta + \lambda_j - 1) - z \prod_{k=1}^l (\delta + \nu_k) \right), \quad \delta = z \frac{d}{dz}.$$

В теории трансцендентных чисел одним из основных методов является метод Зигеля-Шидловского (см. [4], [5]), который позволяет доказывать трансцендентность и алгебраическую независимость значений целых функций некоторого класса, включающего в себя функции ${}_l\varphi_q(\alpha z^{q-l})$, при условии алгебраической независимости этих функций над $\mathbb{C}(z)$.

В статье [6] Ф. Бейкерсом, В. Браунвеллом и Г. Хекманом были введены важные для установления алгебраической зависимости и независимости функций понятия коградиентности и контрградиентности дифференциальных уравнений (фактически эти понятия возникли ранее в статье Е. Колчина [7]).

Настоящая работа посвящена подробному доказательству и дальнейшему развитию результатов о коградиентности и контрградиентности, опубликованных в заметках [8] и [9]. В частности, уточняются некоторые результаты статьи [6].

Ключевые слова: гипергеометрические функции, метод Зигеля, алгебраическая независимость.

Библиография: 16 названий.

Для цитирования:

В. А. Горелов. Об алгебраических тождествах между фундаментальными матрицами обобщённых гипергеометрических уравнений // Чебышевский сборник, 2020, т. 21, вып. 1, с. 135–144.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.4

DOI 10.22405/2226-8383-2020-21-1-135-144

On algebraic identities between solution matrices of generalized hypergeometric equations

V. A. Gorelov

Gorelov Vasily Alekzandrovich — candidate of physical and mathematical sciences, associate Professor, National Research University "Moscow Power Engineering Institute" (Moscow).

e-mail: gorelov.va@mail.ru

Abstract

The examples of algebraic identities between solution matrices of generalized hypergeometric equations are found in paper. These identities generate all the algebraic identities between components of solutions of hypergeometric equations in some cases.

Generalized hypergeometric functions (see [1–5]) are defined as

$${}_l\varphi_q(z) = {}_l\varphi_q(\vec{\nu}; \vec{\lambda}; z) = {}_{l+1}F_q \left(\begin{matrix} 1, \nu_1, \dots, \nu_l \\ \lambda_1, \dots, \lambda_q \end{matrix} \middle| z \right) = \sum_{n=0}^{\infty} \frac{(\nu_1)_n \dots (\nu_l)_n}{(\lambda_1)_n \dots (\lambda_q)_n} z^n,$$

where $0 \leq l \leq q$, $(\nu)_0 = 1$, $(\nu)_n = \nu(\nu+1)\dots(\nu+n-1)$, $\vec{\nu} = (\nu_1, \dots, \nu_l) \in \mathbb{C}^l$, $\vec{\lambda} \in (\mathbb{C} \setminus \mathbb{Z}^-)^q$.

The function ${}_l\varphi_q(\vec{\nu}; \vec{\lambda}; z)$ satisfies the (generalized) hypergeometric differential equation

$$L(\vec{\nu}; \vec{\lambda}; z) y = (\lambda_1 - 1) \dots (\lambda_q - 1),$$

where

$$L(\vec{\nu}; \vec{\lambda}; z) \equiv \prod_{j=1}^q (\delta + \lambda_j - 1) - z \prod_{k=1}^l (\delta + \nu_k), \quad \delta = z \frac{d}{dz}.$$

The Siegel-Shidlovskii method (see [4], [5]) is one of the main methods in the theory of transcendental numbers. It permits to establish the transcendency and the algebraic independence of the values of entire functions of some class, which contains the functions ${}_l\varphi_q(\alpha z^{q-l})$, provided that these functions are algebraically independent over $\mathbb{C}(z)$.

F. Beukers, W.D. Brownawell and G. Heckman introduced in paper [6] notions of cogredience and contragredience of differential equations, which are important for determination of algebraic dependence and independence of functions (these notions appeared firstly in paper [7] of E. Kolchin really).

This work contains detailed proof and further development of results connected with cogredience and contragredience, that have been published in notes [8], [9]. Some results in [6] have been revised particularly.

Keywords: hypergeometric functions, Siegel's method, algebraic independence.

Bibliography: 16 titles.

For citation:

V. A. Gorelov, 2020, "On algebraic identities between solution matrices of generalized hypergeometric equations", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 135–144.

1. Введение

Пусть $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$, $\mathbb{Z}^- = \mathbb{Z} \setminus \mathbb{N}$, $\mathbb{C}[z^{\pm 1}] = \mathbb{C}[z, z^{-1}]$, δ_i^j — символ Кронекера, $M(q, K)$ — множество всех матриц размера $q \times q$ с элементами из кольца K , $GL(q, K)$ — полная линейная группа в $M(q, K)$. При $\gamma, \beta \in \mathbb{C}$, $\vec{\mu} = (\mu_1, \dots, \mu_n) \in \mathbb{C}^n$ положим $\gamma\vec{\mu} + \beta = (\gamma\mu_1 + \beta, \dots, \gamma\mu_n + \beta)$. Для векторов $\vec{\mu} = (\mu_1, \dots, \mu_n)$, $\vec{\eta} = (\eta_1, \dots, \eta_n)$ будем писать $\vec{\mu} \sim \vec{\eta}$, если существует перестановка π чисел $1, \dots, n$ такая, что $\mu_i - \eta_{\pi(i)} \in \mathbb{Z}$, $i = 1, \dots, n$.

Если Φ_1, Φ_2 — произвольные фундаментальные матрицы двух линейных однородных дифференциальных уравнений с коэффициентами из $\mathbb{C}(z)$ и выполняется одно из равенств

$$\Phi_1 = gB\Phi_2C, \quad \Phi_1(\Phi_2C)^T = gB,$$

где $C \in GL(q, \mathbb{C})$, $B \in GL(q, \mathbb{C}(z))$, $g = g(z)$ — функция с условием $g'/g \in \mathbb{C}(z)$, то (см. [6]) исходные дифференциальные уравнения называются коградиентными (соответственно контрградиентными).

Явный вид уравнения $L(\vec{\nu}; \vec{\lambda}; \alpha z^p) y = 0$, получаемого из $L(\vec{\nu}; \vec{\lambda}; z) y = 0$ подстановкой $z \rightarrow \alpha z^p$, где $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$, приведён в лемме 1 и (6). Фундаментальную систему решений уравнения $L(\vec{\nu}; \vec{\lambda}; \alpha z^p) y = 0$ при $\lambda_i - \lambda_k \notin \mathbb{Z}$, $i \neq k$ образуют, например, функции (следствие леммы 1)

$$z^{(1-\lambda_k)p} {}_lF_{q-1}(\vec{\nu} + 1 - \lambda_k; \vec{\lambda} + 1 - \lambda_k; \alpha z^p), \quad k = 1, \dots, q. \quad (1)$$

ТЕОРЕМА 1. Пусть $\vec{\nu} \in \mathbb{C}^l$, $\vec{\lambda} \in \mathbb{C}^q$, $q \geq \max(2, l)$, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$, Φ_1, Φ_2 — произвольные фундаментальные матрицы дифференциальных операторов $L(\vec{\nu}; \vec{\lambda}; \alpha z^p)$ и $L(1 - \vec{\nu}; 2 - \vec{\lambda}; (-1)^{q-l} \alpha z^p)$. Тогда:

1°. Существует матрица $C \in GL(q, \mathbb{C})$ такая, что

$$\Phi_1(\Phi_2C)^T = B, \quad (2)$$

где $B = \|b_{i,j}\|_{i,j} \in GL(q, \mathbb{C}[z^{\pm 1}, (1 - \alpha z^p)^\varepsilon])$, $\varepsilon = -\delta_q^l$, причём

$$b_{k,q-k+1} = (-1)^k c_0 z^{1-q} (1 - \alpha z^p)^\varepsilon, \quad c_0 \in \mathbb{C}, \quad k = 1, \dots, q,$$

а выше этих элементов стоят нули.

2°. Если $\lambda_i - \lambda_k \notin \mathbb{N}$, $i, k = 1, \dots, q$, а Φ_1, Φ_2 соответствуют множествам функций (1) и

$$f_k = z^{(\lambda_k-1)p} {}_lF_{q-1}(\lambda_k - \vec{\nu}; \lambda_k + 1 - \vec{\lambda}; (-1)^{q-l} \alpha z^p), \quad k = 1, \dots, q, \quad (3)$$

то в равенстве (2) $C = \text{diag}(c_1, \dots, c_q)$,

$$c_k = (-1)^k \prod_{1 \leq i < j \leq q; i, j \neq k} (\lambda_i - \lambda_j); \quad c_0 = p^{q-1} \prod_{1 \leq i < j \leq q} (\lambda_i - \lambda_j),$$

пустое произведение скобок равно 1.

СЛЕДСТВИЕ. Пусть $q \geq \max(2, l)$, $\lambda_i - \lambda_k \notin \mathbb{N}$, $i, k = 1, \dots, q$, числа c_k определены в теореме 1. Тогда

$$\sum_{k=1}^q c_k {}_lF_{q-1}(\vec{\nu} + 1 - \lambda_k; \vec{\lambda} + 1 - \lambda_k; z) {}_lF_{q-1}(\lambda_k - \vec{\nu}; \lambda_k + 1 - \vec{\lambda}; (-1)^{q-l} z) = 0. \quad (4)$$

Различные формулировки теоремы 1 и несколько следствий из неё были опубликованы автором в 2008 – 2013 гг. ([10], [8], [11, лемма 5]). В 2015 г. Ф. Бейкерс и Ф. Жуэ [12], а в 2016 г. Р. Фенг, А. Кузнецов и Ф. Янг [13] опубликовали результаты, часть из которых вытекает из формул (2) и (4).

Теорема 1 даёт нетривиальные примеры контргradientности дифференциальных уравнений. Из статей [6, 7], где введено это понятие, не было ясно, существует ли контргradientность вообще и насколько она характерна для случая гипергеометрических уравнений.

Если разности соответствующих параметров двух гипергеометрических функций являются целыми числами, то такие функции называются смежными или ассоциированными. Из [11, лемма 12] и [14] следует, что однородные линейные дифференциальные уравнения, соответствующие уравнениям, которым удовлетворяют смежные функции, являются когradientными.

В следующей теореме решается вопрос о том, возможны ли когradientность или контргradientность гипергеометрических уравнений при несовпадающих l .

ТЕОРЕМА 2. Уравнения $L(\vec{\nu}_k; \vec{\lambda}_k; \alpha_k z^{p_k})y = 0$, где $\alpha_k \in \mathbb{C}$, $p_k \in \mathbb{N}$, $\vec{\nu}_k = (\nu_{k,1}, \dots, \nu_{k,l_k}) \in \mathbb{C}^{l_k}$, $\vec{\lambda}_k = (\lambda_{k,1}, \dots, \lambda_{k,q_k}) \in (\mathbb{C} \setminus \mathbb{Z}^-)^{q_k}$, $k = 1, 2$, с условием

$$\begin{aligned} q_1 = q_2 = 2, \quad l_1 = 1, \quad l_2 = 0, \quad p_2 = 2p_1, \quad \alpha_1^2 = 16\alpha_2, \\ \vec{\lambda}_1 - \lambda_{1,j} \sim \pm 2(\vec{\lambda}_2 - \lambda_{2,1}), \quad 1 \leq j \leq 2, \quad 2\nu_{1,1} - \lambda_{1,1} - \lambda_{1,2} \in \mathbb{Z}, \end{aligned} \quad (5)$$

являются когradientными и контргradientными.

2. Вспомогательные утверждения

ЛЕММА 1 (см. [11, лемма 1]). Функция (либо, при $l > q$, формальный степенной ряд) $z^{\gamma} \varphi_q(\vec{\nu}; \vec{\lambda}; \alpha z^p)$, где $\vec{\nu} \in \mathbb{C}^l$, $\vec{\lambda} \in (\mathbb{C} \setminus \mathbb{Z}^-)^q$, $\alpha, \gamma \in \mathbb{C}$, $l, q \in \mathbb{Z}^+$, $l+q \neq 0$, $p \in \mathbb{Z}$, удовлетворяет дифференциальному уравнению

$$\left(\prod_{i=1}^q (\delta + p(\lambda_i - 1) - \gamma) - \alpha p^{q-l} z^p \prod_{i=1}^l (\delta + p\nu_i - \gamma) \right) y = p^q z^{\gamma} \prod_{i=1}^q (\lambda_i - 1),$$

пустое произведение скобок равно 1.

СЛЕДСТВИЕ. Если $\lambda_i - \lambda_k \notin \mathbb{Z}$, $i \neq k$, $q \geq \max(1, l)$, то функции (1) образуют фундаментальную систему решений уравнения $L(\vec{\nu}; \vec{\lambda}; \alpha z^p)y = 0$.

ЛЕММА 2 (см. [11, лемма 2]). Пусть $\vec{\nu} \in \mathbb{C}^l$, $\vec{\lambda} \in \mathbb{C}^q$, $q \geq \max(1, l)$, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$, $f_1, \dots, f_q$ — фундаментальная система решений уравнения

$$L(\vec{\nu} + 1 - \lambda_s; \vec{\lambda} + 1 - \lambda_s; \alpha z^p)y = 0, \quad 1 \leq s \leq q.$$

Тогда функции $z^{(1-\lambda_s)p} f_1, \dots, z^{(1-\lambda_s)p} f_q$ образуют фундаментальную систему решений уравнения $L(\vec{\nu}; \vec{\lambda}; \alpha z^p)y = 0$.

ЛЕММА 3. [9, лемма 1]. Пусть Φ, Φ_1, Φ_2 — фундаментальные матрицы, отвечающие наборам функций $\{v_1, \dots, v_q\}$, $\{z^{\beta} v_1, \dots, z^{\beta} v_q\}$ и $\{e^{\gamma z} v_1, \dots, e^{\gamma z} v_q\}$ соответственно, $\beta, \gamma \in \mathbb{C}$. Тогда

$$\Phi_1 = z^{\beta} B_1 \Phi, \quad \Phi_2 = e^{\gamma z} B_2 \Phi,$$

где $B_1 \in GL(q, \mathbb{C}[z^{-1}])$, $B_2 \in GL(q, \mathbb{C})$, причём матрицы B_1, B_2 являются нижнетреугольными с единицами на главной диагонали и не зависят от $v_1, \dots, v_q$.

Из лемм 2 и 3 вытекает

ЛЕММА 4. Пусть $\vec{\nu} \in \mathbb{C}^l$, $\vec{\lambda} \in \mathbb{C}^q$, $q \geq \max(2, l)$, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$, Φ_1, Φ_2 — произвольные фундаментальные матрицы дифференциальных операторов $L(\vec{\nu}; \vec{\lambda}; \alpha z^p)$ и $L(\vec{\nu} + 1 - \lambda_s; \vec{\lambda} + 1 - \lambda_s; \alpha z^p)$, $1 \leq s \leq q$. Тогда

$$\Phi_1 = z^{(1-\lambda_s)p} B \Phi_2 C,$$

где $C \in GL(q, \mathbb{C})$, B — нижнетреугольная матрица из $SL(q, \mathbb{C}[z^{-1}])$ с единицами на главной диагонали.

ЛЕММА 5. [9, лемма 2]. Пусть $\Phi = \Phi(z)$, $\Psi = \Psi(z)$ — фундаментальные матрицы, отвечающие наборам функций $\{v_1(z), \dots, v_q(z)\}$ и $\{v_1(\alpha z^p), \dots, v_q(\alpha z^p)\}$ соответственно, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$. Тогда

$$\Psi(z) = B\Phi(\alpha z^p),$$

где $B \in M(q, \mathbb{C}[z])$ — нижнетреугольная матрица с определителем $|B| = (\alpha p z^{p-1})^{q(q-1)/2}$, не зависящая от $v_1, \dots, v_q$.

Как следует из леммы 1, уравнение $L(\vec{v}; \vec{\lambda}; \alpha z^p)y = 0$ при $q \geq l$ имеет вид

$$\begin{aligned} (1 - \alpha z^p)^\varepsilon z^q y^{(q)} + \left((\lambda_1 + \dots + \lambda_q - q)p + (q-1)\frac{q}{2} - \varepsilon_1 \alpha p z^p - \right. \\ \left. - \varepsilon \alpha \left((\nu_1 + \dots + \nu_q)p + (q-1)\frac{q}{2} \right) z^p \right) z^{q-1} y^{(q-1)} + \\ + \dots + p^q ((\lambda_1 - 1) \dots (\lambda_q - 1) - \alpha \nu_1 \dots \nu_l z^p) y = 0, \end{aligned} \quad (6)$$

где $\varepsilon = \delta_q^l$, $\varepsilon_1 = \delta_q^{l+1}$.

ЛЕММА 6. Пусть $\vec{v} \in \mathbb{C}^l$, $\vec{\lambda} \in (\mathbb{C} \setminus \mathbb{Z}^-)^q$, $l, q \in \mathbb{Z}^+$, $q \geq \max(1, l)$, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$. Тогда:

1°. Определитель Вронского уравнения $L(\vec{v}; \vec{\lambda}; \alpha z^p)y = 0$ равен

$$W = c z^{-(\lambda_1 + \dots + \lambda_q - q)p - (q-1)q/2} (1 - \alpha z^p)^{(\lambda_1 + \dots + \lambda_q - \nu_1 - \dots - \nu_q - q)\varepsilon} e^{\alpha z^p \varepsilon_1}, \quad (7)$$

где $c \in \mathbb{C} \setminus \{0\}$, $\varepsilon = \delta_q^l$, $\varepsilon_1 = \delta_q^{l+1}$.

2°. Если $\lambda_i - \lambda_k \notin \mathbb{Z}$, $i \neq k$, а W отвечает функциям (1), то

$$c = p^{q(q-1)/2} \prod_{1 \leq i < j \leq q} (\lambda_i - \lambda_j).$$

ДОКАЗАТЕЛЬСТВО. При $\alpha = p = 1$ равенство (7) вытекает из (6) и формулы Лиувилля. Отсюда, сделав подстановку $z \rightarrow \alpha z^p$, с помощью леммы 5 получаем утверждение 1° леммы 6 при произвольных α и p . Для доказательства утверждения 2° в предположении, что $\lambda_1, \dots, \lambda_q \notin \mathbb{Z}$, рассмотрим члены наименьшей степени разложений по z функций (1) и их производных, составляющих определитель W :

$$\begin{aligned} \begin{vmatrix} z^{p-\lambda_1 p} & \dots & z^{p-\lambda_q p} \\ (z^{p-\lambda_1 p})' & \dots & (z^{p-\lambda_q p})' \\ \dots & \dots & \dots \\ (z^{p-\lambda_1 p})^{(q-1)} & \dots & (z^{p-\lambda_q p})^{(q-1)} \end{vmatrix} = z^{-(\lambda_1 + \dots + \lambda_q - q)p - (q-1)q/2} \cdot \\ \cdot \begin{vmatrix} 1 & \dots & 1 \\ p - \lambda_1 p & \dots & p - \lambda_q p \\ \dots & \dots & \dots \\ \prod_{0 \leq i \leq q-2} (p - \lambda_1 p - i) & \dots & \prod_{0 \leq i \leq q-2} (p - \lambda_q p - i) \end{vmatrix}. \end{aligned} \quad (8)$$

В полученном числовом определителе элемент, стоящий в k -й строке и j -м столбце, является многочленом от $-\lambda_j p$ с коэффициентами, не зависящими от j и старшим членом $(-\lambda_j p)^{k-1}$. Поэтому, последовательно вычитая из каждой строки некоторую линейную комбинацию предыдущих, мы получим определитель Вандермонда от $-\lambda_1 p, \dots, -\lambda_q p$, равный c . Если же какое-либо из $\lambda_1, \dots, \lambda_q$ принадлежит $\mathbb{Z}$, то утверждение 2° получается с помощью предельного перехода, так как функции ${}_l F_q(z)$ непрерывно зависят от параметров (см. [3, §§2.1, 2.2]). Лемма 6 доказана.

Напомним, что сопряжённым к дифференциальному уравнению

$$Ly \equiv a_m y^{(m)} + \dots + a_1 y' + a_0 y = 0$$

называется уравнение

$$\bar{L}v \equiv (-1)^m (a_m v)^{(m)} + \dots - (a_1 v)' + a_0 v = 0$$

(см., например, [15, гл. 2, §5]). Таким же образом определяются сопряжённые дифференциальные операторы L и $\bar{L}$.

ЛЕММА 7. [11, лемма 4]. Пусть $\vec{v} - \zeta \in \mathbb{C}^l$, $\vec{\lambda} - \eta \in \mathbb{C}^q$, $\alpha, \gamma \in \mathbb{C}$, $l, q \in \mathbb{Z}^+$, $l + q \neq 0$, $p \in \mathbb{N}$, ζ, η — произвольные аналитические функции. Тогда

$$\overline{z^\gamma L(\vec{v}; \vec{\lambda}; \alpha z^p)} = (-1)^q z^\gamma L\left(1 - \vec{v} + \frac{1 + \gamma}{p}; 2 - \vec{\lambda} + \frac{1 + \gamma}{p}; (-1)^{q-l} \alpha z^p\right).$$

ЛЕММА 8. Пусть $\vec{v} \in \mathbb{C}^l$, $\vec{\lambda} \in \mathbb{C}^q$, $q \geq \max(2, l)$, $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$, Φ_1, Φ_2 — произвольные фундаментальные матрицы дифференциальных операторов $L(\vec{v}; \vec{\lambda}; \alpha z^p)$ и $L(1 - \vec{v}; 2 - \vec{\lambda}; (-1)^{q-l} \alpha z^p)$. Тогда существует матрица $C \in GL(q, \mathbb{C})$ такая, что

$$\Phi_1(\Phi_2 C)^T = B \in GL(q, \mathbb{C}[z^{\pm 1}, (1 - \alpha z^p)^\varepsilon]), \quad \varepsilon = -\delta_q^l.$$

ДОКАЗАТЕЛЬСТВО. Согласно лемме 7, в которой положим $\gamma = -1$, $\zeta \equiv \eta \equiv 0$, свойствам решений сопряжённых дифференциальных уравнений (см., например, [15, гл. 2, §5.2]) и формулам (6), для любой фундаментальной матрицы Φ_1 уравнения $L(\vec{v}; \vec{\lambda}; \alpha z^p)y = 0$ найдётся фундаментальная матрица Φ_2 уравнения $L(1 - \vec{v}; 2 - \vec{\lambda}; (-1)^{q-l} \alpha z^p)y = 0$ такая, что $\Phi_1 \Phi_2^T = B = \|b_{i,j}\|_{i,j}$ является матрицей, у которой

$$b_{k,q-k+1} = (-1)^k a_0^{-1}, \quad a_0 = z^{q-1} (1 - \alpha z^p)^{-\varepsilon}, \quad k = 1, \dots, q,$$

а выше этих элементов стоят нули. Здесь a_0 — старший коэффициент уравнения $z^{-1} L(\vec{v}; \vec{\lambda}; \alpha z^p)y = 0$. Другими словами, если $\vec{v}$ и $\vec{g}$ — фундаментальные системы решений, соответствующие Φ_1, Φ_2 , то для скалярных произведений их производных имеем $(\vec{v}^{(s)}, \vec{g}^{(k)}) = 0$ при $s + k < q - 1$ и $(\vec{v}^{(s)}, \vec{g}^{(k)}) = (-1)^k a_0^{-1}$ при $s + k = q - 1$. Дифференцируя эти скалярные произведения и заменяя с помощью дифференциальных уравнений (6) производные $\vec{v}^{(q)}, \vec{g}^{(q)}$ на линейные комбинации векторов $\vec{v}^{(0)}, \dots, \vec{v}^{(q-1)}$, $\vec{g}^{(0)}, \dots, \vec{g}^{(q-1)}$, получим, что все элементы матрицы B принадлежат $\mathbb{C}[z^{\pm 1}, (1 - \alpha z^p)^\varepsilon]$. Лемма 8 доказана.

3. Доказательство теоремы 1

Первое утверждение теоремы 1 следует из леммы 8 и её доказательства. Перейдём к доказательству второго утверждения теоремы. Предположим, что разность любых двух параметров $\lambda_1, \dots, \lambda_q$ не принадлежит $\mathbb{Z}$. Согласно леммам 1 и 7 функции (3) образуют фундаментальную систему решений оператора $L(1 - \vec{v}; 2 - \vec{\lambda}; (-1)^{q-l} \alpha z^p)$. В качестве Φ_1 и Φ_2 возьмём фундаментальные матрицы, соответствующие множествам функций (1) и (3). Тогда, как уже было сказано, найдётся вектор $\vec{g} = \{g_1, \dots, g_q\}$, где все g_k являются линейными комбинациями функций (3) с коэффициентами из $\mathbb{C}$, такой, что скалярные произведения вектора с компонентами (1) и векторов $\vec{g}, \vec{g}', \dots, \vec{g}^{(q-2)}$ равны нулю. Рассмотрев в этих скалярных произведениях слагаемые, не содержащие дробных степеней z , приходим к выводу, что можно положить $g_k = a_k f_k$, $k = 1, \dots, q$. Числа a_k найдём следующим образом. Рассмотрим вектор,

компоненты которого являются членами наименьшей степени разложений по z соответствующих компонент вектора $\vec{g}$, т. е. вектор $\{a_1 z^{(\lambda_1-1)p}, \dots, a_q z^{(\lambda_q-1)p}\}$. Известно (см. [15, гл. 2, §5.2], что в качестве $\vec{g}$ можно взять вектор $\{A_{q,1}, \dots, A_{q,q}\}(a_0 W)^{-1}$, где $A_{q,k}$ — алгебраические дополнения к элементам последней строки вронскиана W , отвечающего функциям (1), $a_0 = z^{q-1}(1 - \alpha z^p)^{-\varepsilon}$ — старший коэффициент соответствующего уравнения (6), делённого на z . Заменяем каждый элемент фундаментальной матрицы, соответствующей (1), на младший член его разложения по степеням z . В предположении, что $\lambda_1, \dots, \lambda_q \notin \mathbb{Z}$, получаем, что член наименьшей степени разложения по z функции $A_{q,k}$ равен алгебраическому дополнению элемента с такими же индексами определителя в левой части равенства (8). Следовательно,

$$A_{q,k} = (-1)^{q+k} z^{(\lambda_k - \sum \lambda_s + q-1)p - (q-1)(q-2)/2} p^{(q-1)(q-2)/2} \prod_{1 \leq i < j \leq q; i, j \neq k} (\lambda_i - \lambda_j).$$

Умножив члены наименьшей степени разложений по z компонент вектора $\{A_{q,1}, \dots, A_{q,q}\}$ на член наименьшей степени произведения $z^{1-q}(1 - \alpha z^p)^\varepsilon W^{-1}$, получим вектор $\{a_1 z^{(\lambda_1-1)p}, \dots, a_q z^{(\lambda_q-1)p}\}$, где числа a_k совпадают с диагональными элементами матрицы C в формулировке теоремы 1, делёнными на число c , вычисленное в лемме 6. Таким образом, для рассматриваемого случая утверждение 2° теоремы 1 доказано. Если же некоторые из параметров $\lambda_1, \dots, \lambda_q$ совпадают между собой или с целыми числами, то утверждение 2° получается с помощью предельного перехода, так как функции ${}_1F_q(z)$ и, следовательно, все компоненты матрицы $\Phi_1(\Phi_2 C)^T$ непрерывно зависят от параметров (см. [3, §§2.1, 2.2]).

4. Доказательство теоремы 2

Прежде всего заметим, что для дифференциальных уравнений 2-го порядка понятия коградиентности и контрградиентности совпадают (см. [7]).

Рассмотрим гипергеометрические функции Куммера

$$A_{\mu, \nu}(z) = {}_1\varphi_2(\nu; 1, \mu; z) = {}_1F_1\left(\nu \middle| \mu; z\right) = \sum_{n=0}^{\infty} \frac{(\nu)_n}{n!(\mu)_n} z^n,$$

удовлетворяющие уравнениям

$$z^{-2}L(\nu; 1, \mu; z) y \equiv y'' + \left(-1 + \frac{\mu}{z}\right) y' - \frac{\nu}{z} y = 0, \quad (9)$$

и функции

$$K_\lambda(z) = {}_0\varphi_2(1, \lambda + 1; -z^2/4) = {}_0F_1\left(\begin{matrix} - \\ \lambda + 1 \end{matrix} \middle| -\frac{z^2}{4}\right) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(\lambda + 1)_n} \left(\frac{z}{2}\right)^{2n},$$

отличающиеся от функций Бесселя $J_\lambda(z)$ с индексом λ только множителем $(z/2)^\lambda (\Gamma(\lambda + 1))^{-1}$ и удовлетворяющие уравнениям

$$z^{-2}L(1, \lambda + 1; -z^2/4) y \equiv y'' + \frac{2\lambda + 1}{z} y' + y = 0. \quad (10)$$

Имеет место тождество (см., например, [2, п. 7.1, формула (46)])

$$K_\lambda(z) = e^{\mp iz} A_{2\lambda+1, \lambda+1/2}(\pm 2iz). \quad (11)$$

Более того, нетрудно проверить, что для произвольного решения $f(z)$ уравнения (10) функция $e^{z/2} f(\mp iz/2)$ удовлетворяет уравнению (9), где $\mu = 2\lambda + 1$, $\nu = \lambda + 1/2$.

Отсюда с помощью подстановки $z \rightarrow \pm 2iz$ получаем, что фундаментальная матрица уравнения $L(1, \lambda + 1; -z^2/4) e^{\pm iz} y = 0$ является фундаментальной матрицей уравнения $L(\lambda + 1/2; 1, 2\lambda + 1; \pm 2iz) y = 0$. Если Φ_1, Φ_2 — произвольные фундаментальные матрицы операторов $L(\lambda + 1/2; 1, 2\lambda + 1; \pm 2iz)$ и $L(1, \lambda + 1; -z^2/4)$ соответственно, то из этого согласно лемме 3 (и её доказательству из [9]) вытекают тождества

$$e^{\pm iz} \begin{pmatrix} 1 & 0 \\ \pm i & 1 \end{pmatrix} \Phi_2 = \Phi_1 C, \quad \Phi_2 = e^{\mp iz} \begin{pmatrix} 1 & 0 \\ \mp i & 1 \end{pmatrix} \Phi_1 C, \quad C \in GL(q, \mathbb{C}),$$

обобщающие тождество (11). Таким образом, уравнения $L(1, \lambda + 1; -z^2/4) y = 0$ и $L(\lambda + 1/2; 1, 2\lambda + 1; \pm 2iz) y = 0$ коградиентны, что и должно быть согласно теореме 2. Рассмотрим три следующих преобразования: подстановку $z \rightarrow \alpha z^p$, где $\alpha \in \mathbb{C}$, $p \in \mathbb{N}$; переход от набора параметров $\vec{\nu}, \vec{\lambda}$ к $\vec{\nu} + 1 - \lambda_s, \vec{\lambda} + 1 - \lambda_s$, где $1 \leq s \leq q$; изменение любого параметра на целое число. При этих преобразованиях согласно леммам 5, 4 и [11, лемма 12] коградиентность уравнений не нарушается, как и условие (5).

Предположим теперь, что для каких-либо двух гипергеометрических уравнений условие (5) справедливо. Пусть $\vec{\lambda}_1 - \lambda_{1,j} \sim 2(\vec{\lambda}_2 - \lambda_{2,1})$. Поскольку нумерация параметров в нашем распоряжении, будем считать $j = 1$. Ввиду леммы 4 коградиентность уравнений достаточно установить в случае $\lambda_{1,1} = \lambda_{2,1} = 1$, откуда, учитывая [11, лемма 12], $(0, \lambda_{1,2} - 1) = 2(0, \lambda_{2,2} - 1)$ и $\lambda_{1,2} = 2\lambda_{2,2} - 1$. Пусть $\vec{\lambda}_1 - \lambda_{1,j} \sim -2(\vec{\lambda}_2 - \lambda_{2,1})$. Рассуждая аналогично и считая $j = 2$, получим $(1 - \lambda_{1,2}, 0) \sim -2(0, \lambda_{2,2} - 1)$, откуда снова $\lambda_{1,2} = 2\lambda_{2,2} - 1$. В обоих случаях, полагая $\lambda_{2,2} = \lambda + 1$, имеем $\lambda_{1,2} = 2\lambda + 1$, $\nu_{1,1} = \lambda + 1/2$. Сделав подстановку $z^p \rightarrow (\pm 2i/\alpha_1)z$, приходим к гипергеометрическим уравнениям, коградиентность которых установлена выше.

5. Заключение

Условия для коградиентности и контрградиентности гипергеометрических уравнений и, следовательно, для алгебраической зависимости их решений, исследовались в статьях [6] и [16]. Необходимо отметить, что в этих работах, а также в статье автора [11], выпал из рассмотрения описанный в теореме 2 случай алгебраической зависимости между элементами фундаментальных матриц уравнений 2-го порядка. Можно показать, что в остальных случаях теоремы статей [6], [11], [16] справедливы. Таким образом, согласно результатам статьи [11], коградиентность и контрградиентность однородных гипергеометрических уравнений, элементы фундаментальных матриц которых связаны только соотношением Лиувилля, может возникнуть лишь по причинам, описанным в теоремах 1 и 2, лемме 4 и лемме 12 статьи [11] либо при сочетании этих причин.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Люк Ю. Специальные математические функции и их аппроксимации. М: Мир, 1980.
2. Кратцер А., Франц В. Трансцендентные функции. М: ИЛ, 1963.
3. Аски Р., Рой Р., Эндрюс Дж. Специальные функции. М: МЦНМО, 2013.
4. Siegel C.L. Über einige Anwendungen Diophantischer Approximationen // Abh. Preuss. Acad. Wiss., Phys. Math. Kl. 1929 – 1930. № 1. S. 1 – 70.
5. Шидловский А.Б. Трансцендентные числа. М: Наука, 1987.
6. Beukers F., Brownawell W.D., Heckman G. Siegel normality // Annals of Math. 1988. Vol. 127. P. 279 – 308.

7. Kolchin E.R. Algebraic groups and algebraic dependence // Amer. J. Math. 1968. Vol. 90, № 4. P. 1151 – 1164.
8. Горелов В.А. Об алгебраических тождествах между обобщёнными гипергеометрическими функциями // Матем. заметки. 2010. Т. 88, вып. 4. С. 511 – 516.
9. Горелов В.А. Об алгебраических тождествах между фундаментальными матрицами уравнений Бесселя и Куммера // Сибирские электронные математические известия. 2019. Т. 16. С. 258 – 262.
10. Горелов В.А. О новых алгебраических тождествах между обобщёнными гипергеометрическими функциями // Вестник МЭИ. 2008. № 6. С. 129 – 138.
11. Горелов В.А. Об алгебраической независимости значений обобщённых гипергеометрических функций // Матем. заметки. 2013. Т. 94, вып. 1. С. 94 – 108.
12. Beukers F., Jouhet F. Duality relations for hypergeometric series // Bulletin of the London Math. Soc. 2015. Vol. 47. P. 343 – 358.
13. Feng R., Kuznetsov A., Yang F. A short proof of duality relations for hypergeometric functions // J. of Math. Analysis and Applications. 2016. Vol. 443. P. 116 – 122.
14. Горелов В.А. On contiguity relations for generalized hypergeometric functions // Problemy Analiza – Issues of Analysis. 2018. Vol. 7(25), № 2. P. 39 – 46.
15. Сансоне Дж. Обыкновенные дифференциальные уравнения. М: ИЛ, 1953.
16. Черепнёв М.А. Об алгебраической независимости значений гипергеометрических E-функций // Матем. заметки. 1995. Т. 57, вып. 6. С. 896 – 912.

REFERENCES

1. Luke, Y. 1975, *Mathematical functions and their approximations*, Academic Press, New York.
2. Kratzer, A. & Franz, W. 1960, *Transzendente Funktionen*, Akademische Verlagsgesellschaft, Leipzig. (German)
3. Andrews, G., Askey, R. & Roy, R. 2000, *Special Functions*, Cambridge University Press.
4. Siegel C.L. 1929 – 1930, “Über einige Anwendungen Diophantischer Approximationen“, *Abh. Preuss. Acad. Wiss., Phys. – Math. Kl.*, no. 1, pp. 1 – 70. (German)
5. Shidlovskii, A.B. 1989, *Transcendental numbers*, Walter de Gruyter, Berlin–New York.
6. Beukers, F., Brownawell, W.D. & Heckman, G. 1988, “Siegel Normality“, *Annals of Math.*, vol. 127, pp. 279–308.
7. Kolchin, E.R. 1968, “Algebraic groups and algebraic dependence“, *Amer. J. Math.*, vol. 90, no. 4, pp. 1151–1164.
8. Gorelov, V.A. 2010, “On algebraic identities between generalized hypergeometric functions“, *Mathematical Notes*, vol. 88, no. 4, pp. 487–491. DOI: 10.1134/S0001434610090208
9. Gorelov, V.A. 2019, “On algebraic identities between solution matrices of Bessel’s and Kummer’s equations“, *Siberian Electronic Mathematical Reports*, vol. 16, pp. 258–262. DOI: 10.33048/semi.2019.16.017. (Russian)

10. Gorelov, V.A. 2008, "About new algebraic identities between generalized hypergeometric functions", *Vestnik Moskovskogo energeticheskogo instituta*, no. 6, pp. 129-138. (Russian)
11. Gorelov, V.A. 2013, "On the algebraic independence of values of generalized hypergeometric functions", *Mathematical Notes*, vol. 94, no. 1, pp. 82-95. DOI: 10.1134/S0001434613070080
12. Beukers, F. & Jouhet, F. 2015, "Duality relations for hypergeometric series", *Bulletin of the London Math. Soc.*, vol. 47, pp. 343-358.
13. Feng, R., Kuznetsov, A. & Yang, F. 2016, "A short proof of duality relations for hypergeometric functions", *J. of Math. Analysis and Applications*, vol. 443, pp. 116-122.
14. Gorelov, V.A. 2018, "On contiguity relations for generalized hypergeometric functions", *Problemy Analiza – Issues of Analysis*, vol. 7(25), no. 2, pp. 39-46. DOI:10.15393/j3.art.2018.4490
15. Sansone, G. 1948, *Equazioni differenziali nel campo reale*, Bologna. (Italian)
16. Cherepnev, M.A. 1995, "Algebraic independence of values of hypergeometric E-functions", *Mathematical Notes*, vol. 57, no. 6, pp. 630-642.

Получено 17.05.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 519.1

DOI 10.22405/2226-8383-2020-21-1-145-164

О специальных свойствах некоторых квазиметрик

Е. И. Деза, Б. Мханна

Деза Елена Ивановна — доктор педагогических наук, кандидат физико-математических наук, доцент, профессор кафедры теоретической информатики и дискретной математики, Московский педагогический государственный университет (г. Москва).

e-mail: elena.deza@gmail.com

Мханна Батуль — аспирант кафедры теоретической информатики и дискретной математики, Московский педагогический государственный университет (г. Москва).

e-mail: batoolmhanna77@gmail.com

Аннотация

В статье рассмотрены свойства квазиметрики среднего времени первого прохода — обобщенной метрической структуры, тесно связанной с эргодическими однородными цепями Маркова.

Во введении представлена история вопроса, дан обзор основных идей и результатов работы.

В первом разделе собраны основные понятия теории *цепей Маркова* — последовательностей случайных событий с конечным или счетным числом исходов, характеризующихся тем, что, говоря нестрого, при фиксированном настоящем будущее независимо от прошлого. Точнее, математическая модель некоторого случайного процесса представляет собой марковскую цепь, если распределение вероятностей параметров процесса в следующий момент времени зависит только от параметров процесса в предыдущий момент.

Во втором разделе собраны базовые определения, необходимые для рассмотрения роли графовых моделей в представлении и исследовании эргодических однородных цепей Маркова. Марковская цепь может быть изображена в виде ориентированного взвешенного графа переходов, вершины которого соответствуют состояниям цепи, а дуги — переходам между ними. Процесс будет эргодическим, если построенный взвешенный орграф является слабо связным, и наибольший общий делитель длин всех его циклов равен единице. С другой стороны, любой связный граф может служить базой для построения модели простейшей цепи Маркова: если вершина i имеет степень k , то все выходящие из нее ребра превращаются в дуги с весами $\frac{1}{k}$.

В третьем разделе дано определение среднего времени первого прохода для однородной эргодической цепи Маркова. Представлены несколько способов построения соответствующей матрицы M . Подробно проанализирован алгоритм нахождения среднего времени первого прохода с помощью использования сходящихся деревьев ориентированного графа, связанного с матрицей перехода эргодической однородной цепи Маркова. Описана родственная рекуррентная процедура.

В четвертом разделе матрица среднего времени первого прохода рассмотрена как *квазиметрика t среднего времени первого прохода* на множестве вершин $V = \{1, 2, \dots, n\}$ ориентированного графа, соответствующего матрице перехода эргодической однородной цепи Маркова: $t(i, j)$ — ожидаемое количество шагов (дуг) для случайного блуждания на орграфе Γ , начинающегося с i , для достижения j в первый раз. Эта квазиметрика обладает рядом важных теоретических и прикладных свойств. В частности, квазиметрика среднего времени первого прохода для *простого случайного блуждания* по связному невзвешенному графу G , в котором из любой вершины графа существует равная вероятность перемещения в любую соседнюю вершину, является *взвешиваемой квазиметрикой*,

т.е. существует *весовая функция* $w : V \rightarrow \mathbb{R}_{\geq 0}$, такая, что для всех $i, j \in V$ имеет место соотношение $m(i, j) + w_i = m(j, i) + w_j$. Менее изучены, но не менее интересны связи квазиметрики среднего времени первого прохода с другими метрическими структурами на графах, в частности, с α -метрикой леса и ее вариациями.

Наконец, в пятом разделе рассмотрены примеры построения и исследования квазиметрики среднего времени первого прохода. Помимо иллюстрации "графовой" процедуры построения матрицы M , представлены рекуррентные алгоритмы исследования и проанализированы получающиеся при этом обобщенные метрические структуры.

Ключевые слова: цепь Маркова, среднее время первого прохода, остовной входящий корневой лес ориентированного графа, квазиметрика, квазиметрика среднего времени первого прохода, метрика леса.

Библиография: 25 названий.

Для цитирования:

Е. И. Деза, Б. Мханна. О специальных свойствах некоторых квазиметрик // Чебышевский сборник, 2020, т. 21, вып. 1, с. 145–164.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 519.1

DOI 10.22405/2226-8383-2020-21-1-145-164

On special properties of some quasi-metrics

E. I. Deza, B. Mhanna

Deza Elena Ivanovna — doctor of pedagogical Sciences, candidate of physical and mathematical Sciences, associate Professor, Professor of the Department of theoretical Informatics and discrete mathematics, Moscow State Pedagogical University (Moscow).

e-mail: elena.deza@gmail.com

Mhanna Batul — graduate student of the Department of Theoretical Informatics and Discrete Mathematics, Moscow State Pedagogical University (Moscow).

e-mail: batoolmhanna77@gmail.com

Abstract

In this paper we consider some questions of the theory and practice of mean first passage time quasi-metric, a generalized metric structure closely related to ergodic homogeneous Markov chains.

The introduction considers the history of the problem and provides an overview of the main ideas and results presented in the article.

The first section gives the basic concepts of the theory of Markov chains. In fact, a *Markov chain* is a mathematical model of some random process describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event.

The second section collects the basic definitions needed to consider the role of graph models in the presentation and study of ergodic homogeneous Markov chains. The Markov chain can be depicted as an oriented weighted graph of transitions whose vertices correspond to the states of the chain and the arcs correspond to the transitions between them. The process will be ergodic if this weighted oriented graph is weakly connected, and the largest common divisor of the lengths of all its cycles is equal to 1. On the other hand, any connected graph can be used as a basis for building a model of the simplest Markov chain: if a vertex i has degree k , all incident edges are converted into arcs with the weights $\frac{1}{k}$.

In the third section the definition of the mean first passage time for an ergodic homogeneous Markov chain is given. There are several ways to build the corresponding matrix. The algorithm of finding the mean first passage time is analyzed in detail by using converging trees of the oriented graph, related to the transition matrix of the ergodic homogeneous Markov chain. Related recurrent procedure is described.

In the fourth section, a mean first passage time is analyzed as the *quasi-metric* m of *mean first passage time* on the vertices $V = \{1, 2, \dots, n\}$ of the oriented graph corresponding to the transition matrix of a given ergodic homogeneous Markov chain: $m(i, j)$ is the expected number of steps (arcs) for random wandering on the oriented graph Γ , starting at i , to reach j for the first time. In particular, the quasi-metric of mean first passage time for the *simple random walking* on a connected unweighted graph G , in which there is an equal probability of moving from any vertex to any adjacent vertex, is a *weighted quasi-metric*, i.e., there exists a *weight function* $w : V \rightarrow \mathbb{R}_{\geq 0}$, such that $m(i, j) + w_i = m(j, i) + w_j$ for all $i, j \in V$.

We consider also some connections of the mean first passage time quasi-metric to other metric structures on graphs (in particular to α -*metric forest* and its relatives), which are less studied, but not less interesting.

Finally, the fifth section deals with examples of the construction of mean first passage time quasi-metrics. In addition to illustrating the "graphical" procedure of building the matrix M , recurrent research algorithms are presented and the resulting generalized metric structures are analyzed.

Keywords: Markov chain, mean first passage time, spanning rooted forest of an oriented graph, quasi-metric, mean first passage time quasi-metric, forest metric.

Bibliography: 25 titles.

For citation:

E. I. Deza, B. Mhanna, 2020, "On special properties of some quasi-metrics", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 145–164.

1. Введение

Рассмотрим последовательность одинаковых случайных испытаний, в которой вероятность исхода следующего испытания зависит только от исхода испытания, непосредственно предшествующего ему. Такая случайная последовательность называется *цепью Маркова*.

Другими словами, *цепь Маркова* — последовательность случайных событий с конечным или счетным числом исходов, характеризующаяся тем свойством, что, говоря нестрого, при фиксированном настоящем будущее независимо от прошлого.

Марковская цепь может быть изображена в виде ориентированного взвешенного графа переходов, вершины которого соответствуют состояниям цепи, а дуги — переходам между ними. Вес дуги (i, j) , связывающей вершины s_i и s_j , будет равен вероятности p_{ij} перехода из первого состояния во второе.

Процесс будет эргодическим, если построенный взвешенный орграф является слабо связным, и наибольший общий делитель длин всех его циклов равен единице.

С другой стороны, любой связный граф может служить базой для построения модели простейшей цепи Маркова. Для этого достаточно превратить его во взвешенный орграф по следующему закону: если вершина i имеет степень k , то все выходящие из нее ребра превращаются в дуги с весами $\frac{1}{k}$.

Важной характеристикой эргодической однородной цепи Маркова с состояниями $1, 2, \dots, n$ является *среднее время первого прохода* из состояния i в состояние j , определяемое как

$$m_{ij} = E(F_{ij}) = \sum_{k=1}^{\infty} k \Pr(F_{ij} = k),$$

где $E(\cdot)$ — математическое ожидание, а $F_{ij} = \min\{p \geq 1 : X_p = j \mid X_0 = i\}$.

Матрицу M можно получить, пользуясь исследованием ориентированного графа, связанного с матрицей перехода эргодической однородной цепи Маркова. Именно, имеет место следующий результат ([7, 10]).

Пусть $T \in \mathbb{R}^{n \times n}$ — матрица перехода эргодической однородной цепи Маркова с состояниями $1, 2, \dots, n$. Пусть Γ — взвешенный орграф без петель, вершины которого равны $1, 2, \dots, n$, а веса дуг равны соответствующим вероятностям перехода в T . Тогда среднее время первого прохода из состояния i в состояние j в цепи Маркова может быть представлено как

$$m_{ij} = q_j^{-1} \cdot \begin{cases} f_{ij}, & \text{если } i \neq j, \\ q, & \text{если } i = j, \end{cases}$$

где f_{ij} — суммарный вес входящих лесов орграфа Γ , состоящих из двух деревьев, и имеющих одно дерево, содержащее i , а другое дерево, сходящееся к j , q_j — суммарный вес остовных деревьев, сходящихся к j в Γ , а $q = \sum_{k=1}^n q_k$.

Если в определении среднего времени первого прохода использовать требование $p \geq 0$ вместо требования $p \geq 1$, то среднее время первого прохода из состояния i в состояние j в цепи Маркова может быть получено как $m_{ij} = f_{ij}/q_j$, $i, j = 1, 2, \dots, n$. В этом случае можно говорить о *квазиметрике среднего времени первого прохода* m на $V = \{1, 2, \dots, n\}$, такой, что $m(i, j) = m_{ij}$ — ожидаемое количество шагов (дуг) для случайного блуждания на Γ , начинающегося с i , для достижения j в первый раз; это 0 для $i = j$.

Эта квазиметрика обладает рядом важных теоретических и прикладных свойств. Так, она удовлетворяет *геодезическому свойству*: равенство $m(i, j) = m(i, k) + m(k, j)$ выполняется тогда и только тогда, когда все пути в Γ от i до j проходят через k .

Квазиметрика среднего времени первого прохода для *простого случайного блуждания* по связному невзвешенному графу G , в котором из любой вершины графа существует равная вероятность перемещения в любую соседнюю вершину, является *взвешиваемой квазиметрикой*, т. е. существует *весовая функция* $w : V \rightarrow \mathbb{R}_{\geq 0}$, такая, что для всех $i, j \in V$ имеет место соотношение $m(i, j) + w_i = m(j, i) + w_j$. В качестве взвешиваемой квазиметрики, m обладает *ослабленным свойством симметрии*: $m(i, j) + m(j, k) + m(k, i) = m(i, k) + m(k, j) + m(j, i)$.

Менее изучены, но не менее интересны связи квазиметрики среднего времени первого прохода с другими метрическими структурами на графах, в частности, с α -*метрикой леса* и ее вариациями. Особый интерес представляет попытка переноса ряда классических рекуррентных процедур, связанных с указанными метрическими структурами, на ориентированный случай.

2. Основные понятия теории цепей Маркова

Пусть $\langle \Omega, F, \text{Pr} \rangle$ — вероятностное пространство. При изложении теории марковских цепей принято рассматривать дискретные случайные величины, областью значений которых является некоторое конечное множество $E = \{s_1, \dots, s_k\}$.

Последовательность дискретных случайных величин $\{X_n\}_{n \geq 0}$ называется *простой цепью Маркова* (с дискретным временем), если

$$\text{Pr}(X_{n+1} = i_{n+1} \mid X_n = i_n, X_{n-1} = i_{n-1}, \dots, X_0 = i_0) = \text{Pr}(X_{n+1} = i_{n+1} \mid X_n = i_n).$$

Область значений случайных величин X_n называется *пространством состояний* цепи, а номер n — номером шага.

Матрица $P[n]$, где $p_{ij}[n] = \text{Pr}(X_{n+1} = j \mid X_n = i)$, называется *матрицей переходных вероятностей на n -ом шаге*; вектор $p = (p_1, p_2, \dots, p_n)$, где $p_i = \text{Pr}(X_0 = i)$, называется *начальным распределением* цепи Маркова.

Цепь Маркова называется *однородной*, если матрица переходных вероятностей не зависит от номера шага, то есть $\forall n \in \mathbb{N} \quad p_{ij}[n] = p_{ij}$. В дальнейшем будем предполагать, что мы имеем дело с однородными цепями Маркова.

Таким образом, последовательность случайных величин $\xi_1, \xi_2, \dots, \xi_n, \dots$ образует однородную цепь Маркова, если для любых номеров n , а также произвольных $i, j, i_1, \dots, i_{n-2}$ справедливо равенство

$$\Pr(\xi_n = s_i \mid \xi_1 = s_{i_1}, \xi_2 = s_{i_2}, \dots, \xi_{n-2} = s_{i_{n-2}}, \xi_{n-1} = s_j) = \Pr(\xi_n = s_i \mid \xi_{n-1} = s_j) = p_{ij}.$$

Из определения и формулы полной вероятности следует, что $p_{ij} \geq 0$, и $\sum_{i=1}^k p_{ij} = 1$ для всех $j = 1, \dots, k$. Матрицы, обладающие такими свойствами, называются *стохастическими*.

В соответствии с определением марковской цепи и формулой полной вероятности, вероятность $p_{ij}(n) = \Pr(\xi_{n+m} = s_i \mid \xi_m = s_j)$ перехода за n шагов из состояния s_j в состояние s_i вычисляется по рекуррентной формуле $p_{ij}(n) = \sum_{i=1}^k p_{ii} p_{ij}(n-1)$, $p_{ij}(1) = p_{ij}$. Марковская цепь называется *неразложимой*, если для любых $i, j = 1, \dots, k$ найдётся такое n , что $p_{ij}(n) > 0$.

Число $d > 1$ называется *периодом состояния* s_i , если d есть наибольший общий делитель таких чисел n , что $p_{ij}(n) > 0$, т.е. число d — период состояния s_i , если в состояние s_i можно вернуться только за кратное d число шагов. Нетрудно показать, что все состояния неразложимой марковской цепи имеют одинаковый период.

Если все состояния марковской цепи имеют период $d > 1$, то марковская цепь называется *периодической*. В противном случае марковская цепь называется *непериодической*.

Если марковская цепь неразложима и непериодична, то найдётся такое число $n_0 \in \mathbb{N}$, что $p_{ij}(n) > 0$ для всех $n \geq n_0$ и $i, j = 1, \dots, k$.

Эргодическая теорема утверждает, что марковская цепь является неразложимой и непериодической тогда и только тогда, когда для каждого $i = 1, \dots, k$ существует предел $\lim_{n \rightarrow \infty} p_{ij}(n) = \pi_i > 0$, не зависящий от j . Величины π_i называются *стационарными* или *филиальными вероятностями* состояний цепи Маркова, а вектор π — вектором стационарных вероятностей или, чаще в англоязычной специальной литературе, (нормализованным) вектором Перрона.

Нетрудно убедиться в том, что для вектора $\pi = (\pi_1, \dots, \pi_k)$ стационарных вероятностей цепи Маркова имеют место соотношения $\pi = P \cdot \pi$, и $\sum_{i=1}^k \pi_i = 1$. [2], [3], [5]

3. Представления цепей Маркова графовыми моделями

Для обсуждения возможности представления цепей Маркова с помощью графовых моделей, вспомним некоторые базовые понятия теории орграфов. [4], [7], [10]

Ориентированный граф (орграф) — граф, ребрам которого присвоено направление. Направленные ребра называются *дугами*. Граф, ни одному ребру которого не присвоено направление, называется *неориентированным*. Орграф называется (реберно) *взвешенным*, если каждой дуге присвоено некоторое числовое значение — *вес*.

Орграф называется *слабо связным*, если соответствующий неориентированный граф связан. *Слабой компонентой* орграфа называется любой его максимальный слабосвязный подграф.

Вес взвешенного орграфа определяется произведением весов его дуг; вес любого орграфа, который не имеет дуг, равен 1. Вес множества орграфов — это сумма весов его членов.

Сходящееся дерево — слабосвязный оргграф, в котором одна вершина, называемая *корнем*, имеет нулевое значение для входящей степени, а оставшиеся вершины имеют для входящей степени значение 1.

Входящий лес оргграфа Γ — остоновый подграф оргграфа Γ , все слабые компоненты которого являются сходящимися деревьями. Говорят, что входящий лес *сходятся к корням* его сходящихся деревьев. Входящий лес F оргграфа Γ называется *максимальным входящим лесом оргграфа* Γ , если Γ не имеет входящего леса с большим числом дуг, чем в F .

Размерность входящего леса оргграфа Γ — число слабых компонент в любом максимальном входящем лесе. Очевидно, что каждый максимальный входящий лес оргграфа Γ имеет $n - d$ дуг, где d — размерность входящего леса оргграфа Γ . *Подмаксимальный входящий лес оргграфа* Γ — это лес в Γ , имеющий $d + 1$ слабые компоненты; как следствие, он имеет $n - d - 1$ дугу.

Марковская цепь может быть изображена в виде ориентированного взвешенного графа переходов, вершины которого соответствуют состояниям цепи, а дуги — переходам между ними. Вес дуги (i, j) , связывающей вершины s_i и s_j , будет равен вероятности p_{ij} перехода из первого состояния во второе.

Очевидно, что для $i \neq j$ имеет место равенство $p_{ij} = -l_{ij}$, где $L = ((l_{ij})) \in \mathbb{R}^{n \times n}$ — *матрица Лапласа (матрица Кирхгоффа)* взвешенного оргграфа Γ , т. е., по определению, $l_{ij} = -w_{ij}$ для $i \neq j$, и $l_{ii} = -\sum_{j \neq i} l_{ij}$. Другими словами, матрица Лапласа L оргграфа Γ удовлетворяет соотношению $L = I - P$.

Процесс будет эргодическим, если построенный взвешенный оргграф является слабо связным, и наибольший общий делитель длин всех его циклов равен единице.

С другой стороны, любой связный граф может служить базой для построения модели простейшей цепи Маркова. Для этого достаточно превратить его во взвешенный оргграф по следующему закону: если вершина i имеет степень k , то все выходящие из нее ребра превращаются в дуги с весами $\frac{1}{k}$. Другими словами, любое ребро (i, j) превращается в дугу, соответствующую переходу с вероятностью $p_{ij} = \frac{1}{k}$.

4. Среднее время первого прохода для цепей Маркова

Пусть $T = ((t_{ij})) \in \mathbb{R}^{n \times n}$ — матрица перехода эргодической однородной цепи Маркова с состояниями $1, 2, \dots, n$.

Определим *среднее время первого прохода* из состояния i в состояние j как

$$m_{ij} = E(F_{ij}) = \sum_{k=1}^{\infty} k \Pr(F_{ij} = k),$$

где $E(\cdot)$ — математическое ожидание, а $F_{ij} = \min\{p \geq 1 : X_p = j \mid X_0 = i\}$. По [23] (теорема 3.3), матрица $M = ((m_{ij})) \in \mathbb{R}^{n \times n}$ имеет следующее представление:

$$M = (I - L^{\#} + J L_{dg}^{\#}) \Pi^{-1},$$

где I — единичная $n \times n$ матрица, J — $n \times n$ матрица, состоящая из одних единиц, $L = I - T$, $L^{\#}$ — *обратная матрица*, полученная применением операции группового обращения из матрицы L , $L_{dg}^{\#}$ — диагональная матрица, полученная заменой всех недиагональных элементов матрицы $L^{\#}$ нулями, $\Pi = \text{diag}(\pi_1, \dots, \pi_n)$ — диагональная матрица с элементами $\pi_1, \dots, \pi_n$, и $(\pi_1, \dots, \pi_n) = \pi$ — *нормализованный левый вектор Перрона* матрицы T , т. е. вектор из $\mathbb{R}^n$, удовлетворяющий условиям $\pi T = \pi$, $\sum_{i=1}^n \pi_i = 1$.

В развернутой форме мы получаем следующую формулу ([23, 6]):

$$m_{ij} = \begin{cases} \pi_j^{-1}, & \text{если } i = j, \\ \pi_j^{-1}(L_{jj}^\# - L_{ij}^\#), & \text{если } i \neq j. \end{cases}$$

Замечание 1. Если вместо вспомогательного требования $p \geq 1$ в определении среднего времени первого прохода используется вспомогательное требование $p \geq 0$ ([6]), то $m_{jj} = 0$, и

$$m_{ij} = \pi_j^{-1}(L_{jj}^\# - L_{ij}^\#), \quad i, j = 1, 2, \dots, n.$$

Рассмотрим взвешенный оргграф Γ , который соответствует цепи Маркова с матрицей перехода T .

По [9] (предложение 15), для любого взвешенного оргграфа Γ и его матрицы Лапласа L выполняется соотношение

$$L^\# = \sigma_{n-d}^{-1} \left(Q_{n-d-1} - \frac{\sigma_{n-d-1}}{\sigma_{n-d}} Q_{n-d} \right),$$

где σ_k — суммарный вес входящих лесов с k дугами (так что σ_{n-d} и σ_{n-d-1} являются суммарными весами максимальных и подмаксимальных входящих лесов оргграфа Γ , соответственно), Q_k — матрица, в которой ij -элемент q_{ij}^k ($i, j = 1, 2, \dots, n$) представляет собой суммарный вес входящих лесов, имеющих k дуг, у которых вершина i принадлежит дереву, которое сходится к вершине j .

Поскольку рассматриваемая цепь Маркова эргодична, то соответствующий оргграф Γ слабосвязан и, следовательно, имеет остовные сходящиеся деревья. Таким образом, размерность d максимального входящего леса оргграфа Γ равна 1, и каждый максимальный входящий лес, сходящийся к j , является остовным сходящимся деревом, которое содержит i . Другими словами, jj - и ij -элементы матрицы $Q_{n-d} = Q_{n-1} = ((q_{ij}^{(n-1)}))$ одинаковы, а разности между ними равны нулю: $q_{jj}^{(n-1)} - q_{ij}^{(n-1)}$, $i, j = 1, 2, \dots, n$.

Что касается матрицы $Q_{n-d-1} = Q_{n-2} = ((q_{ij}^{(n-2)}))$, разности вида $q_{jj}^{(n-2)} - q_{ij}^{(n-2)} \stackrel{\text{def}}{=} f_{ij}$ между ее jj - и ij -элементами равны весам входящих лесов оргграфа Γ , которые состоят ровно из двух деревьев, сходящихся к j и имеют i и j в разных деревьях.

Таким образом, мы получаем, что $m_{ij} = \frac{f_{ij}}{\sigma_{n-1} \pi_j}$, если $i \neq j$.

Поскольку (см., например, [21, 22, 24]) $\pi_j = \frac{q_j}{\sigma_{n-1}}$, где q_j — суммарный вес деревьев, сходящихся к j в Γ (так что $\sum_{k=1}^n q_k = \sigma_{n-1}$), то мы получаем ([7, 10]) следующее "графовое" представление для среднего времени первого прохода:

$$m_{ij} = q_j^{-1} \cdot \begin{cases} f_{ij}, & \text{если } i \neq j, \\ q, & \text{если } i = j, \end{cases}$$

где f_{ij} — суммарный вес входящих лесов оргграфа Γ , состоящих из двух деревьев, и имеющих одно дерево, содержащее i , а другое дерево, сходящееся к j , q_j — суммарный вес остовных деревьев, сходящихся к j в Γ , а $q = \sum_{k=1}^n q_k$.

Замечание 2. Если в определении среднего времени первого прохода использовать требование $p \geq 0$, то среднее время первого прохода из состояния i в состояние j в цепи Маркова может быть представлено следующим образом: $m_{ij} = f_{ij}/q_j$, $i, j = 1, 2, \dots, n$.

Заметим, что f_{ij} и q_j можно вычислить и с помощью элементарной матричной алгебры, а именно, с помощью следующей рекуррентной процедуры ([9], утверждение 4): для $k = 0, 1, \dots, n-1$ имеет место формула $\sigma_{k+1} = \frac{\text{tr}(LQ_k)}{k+1}$, $Q_{k+1} = -LQ_k + \sigma_{k+1}I$, где $\sigma_0 = 1$, и $Q_0 = I$.

5. Квазиметрика среднего времени первого прохода

Если в определении среднего времени первого прохода использовать требование $p \geq 0$, то можно перейти к исследованию соответствующей квазиметрики ([18, 25, 1, 16]) на множестве вершин орграфа Γ , соответствующего цепи Маркова с матрицей перехода T .

В этом случае мы говорим о *квазиметрике среднего времени первого прохода* t на $V = \{1, 2, \dots, n\}$, такой, что $t(i, j) = m_{ij}$ - ожидаемое количество шагов (дуг) для случайного блуждания на Γ , начинающегося с i , для достижения j в первый раз; это 0 для $i = j$.

На самом деле, мы можем проверить все аксиомы *квазиметрики*: для всех $i, j, k \in V$ $t(i, j) \geq 0$, $t(i, j) > 0$ тогда и только тогда, когда $i \neq j$, и $t(i, j) \leq t(i, k) + t(k, j)$ ([19], теорема 6.2.1).

Более того, ([19], теорема 6.2.1) эта квазиметрика обладает свойством *аддитивности точки-разреза* ([8]), или, что то же, *геодезическим свойством* ([20]): $t(i, j) = t(i, k) + t(k, j)$ тогда и только тогда, когда все пути в Γ от i до j проходят через k .

Метрика коммутирующего времени первого прохода c на V определяется теперь как

$$c(i, j) = t(i, j) + t(j, i).$$

Простейший пример квазиметрики среднего времени первого прохода может быть получен для *простого случайного блуждания* по связному невзвешенному графу G , в котором из любой вершины графа существует равная вероятность перемещения в любую соседнюю вершину.

В этом случае квазиметрика t является *взвешиваемой квазиметрикой* (см. [14, 15, 17] и [16], глава 16), т.е. существует *весовая функция* $w : V \rightarrow \mathbb{R}_{\geq 0}$, такая, что для всех $i, j \in V$ имеет место соотношение $t(i, j) + w_i = t(j, i) + w_j$. В качестве взвешиваемой квазиметрики, t обладает *ослабленным свойством симметрии*: для любых $i, j, k \in V$

$$t(i, j) + t(j, k) + t(k, i) = t(i, k) + t(k, j) + t(j, i).$$

Метрика коммутирующего времени первого прохода c на V имеет теперь форму $c(i, j) = t(i, j) + t(j, i) = 2t(i, j) + w_i - w_j$, в то время как $t(i, j) = \frac{c(i, j) - w_i + w_j}{2}$.

Кроме того, функция p , $p(i, j) = t(i, j) + w_i = \frac{c(i, j) + w_i + w_j}{2}$, является *частичной метрикой* на V ([14]), т.е. для всех $i, j, k \in V$ имеют место следующие соотношения: $p(i, j) \geq 0$; $p(i, j) \geq p(i, i)$ (*саморасстояния малы*); $p(i, i) = p(j, j) = p(i, j) \Rightarrow i = j$; $p(i, j) = p(j, i)$ (*симметрия*); $p(i, j) \leq p(i, k) + p(k, j) - p(k, k)$ (*острое неравенство треугольника*).

Квазиметрика среднего времени первого прохода t тесно связана и с другими метрическими структурами на графах.

При $\alpha > 0$ связный взвешенный неориентированный граф (в общем случае даже *мультиграф*, допускается использование параллельных ребер) $G = (V, E; w)$ с положительной реберной весовой функцией $w = (w(e))_{e \in E}$ обладает α -*метрикой леса* $forest^\alpha$. [13] Ее значение между вершинами u и v определяется как

$$forest^\alpha(u, v) = \frac{1}{2}(q_{uu} + q_{vv} - q_{uv} - q_{vu})$$

для $((g_{ij})) = (I + \alpha L)^{-1}$, где I — тождественная $|V| \times |V|$ матрица, и $L = ((l_{ij}))$ — матрица Лапласа орграфа Γ .

Особую роль в построенном семействе метрик играет *метрика леса forest* ([11]): это случай $\alpha = 1$ для α -метрики леса.

С α -метрикой леса тесно связана *нормализованная α -метрика леса*

$$\rho^\alpha(u, v) = \alpha(q_{uu} + q_{vv} - q_{uv} - q_{vu});$$

она пропорциональна α -метрике леса, но в ряде случаев более удобна для приложений.

Эти метрические структуры обладают рядом интересных и полезных свойств.

Так, можно показать ([12]), что увеличенная в два раза α -метрика леса на G является *метрикой сопротивления* для связного взвешенного (мульти)графа $G' = (V', E'; w')$. Здесь множество вершин $V' = V \cup \{0\}$, множество ребер $E' = E \cup \{u0 : u \in V\}$, а весовая функция удовлетворяет следующим условиям: $w'(e) = \alpha w(e)$ для всех $e \in E$, и $w'(u0) = 1$ для всех $u \in V$.

Известно ([12]), что для $\alpha \rightarrow 0$ мы получаем из d^α *дискретную метрику* d^0 :

$$d^0(i, i) = 0, \quad d^0(i, j) = 1 \quad \text{при } i \neq j.$$

Из метрики ρ^α при стремлении α к нулю получается *недискретная полуметрика* $\rho^0(i, j) \equiv 0$.

Для $\alpha \rightarrow +\infty$ мы получаем (в случае связного графа) из d^α *дискретную полуметрику* $d^0(i, j) \equiv 0$. Из метрики ρ^α при неограниченном росте α получается хорошо известная *метрика сопротивления* ρ : $\rho_{ij} = l_{ii}^+ + l_{jj}^+ - l_{ij}^+ - l_{ji}^+$, где $L^+ = ((l_{ij}^+))$ - преобразование Мура-Пенроуза матрицы Лапласа L .

С точки зрения вопросов, рассматриваемых в нашей статье, очень интересна связь метрики леса с рекуррентной процедурой, родственной описанной выше рекуррентной схеме получения матрицы $((f_{ij}))$. Именно, матрица $\bar{Q} = (1 + L)^{-1}$, используемая для построения метрики леса, может быть получена ([9]) как

$$\bar{Q} = \sigma^{-1} Q, \quad \text{где } \sigma = \sum_{k=0}^{n-d} \sigma_k, \quad Q = \sum_{k=0}^{n-d} Q_k,$$

причем σ_k — общий вес остовных корневых лесов с k дугами (так что σ_{n-d} и σ_{n-d-1} являются суммарными весами максимальных и подмаксимальных остовных корневых лесов графа G , соответственно), а Q_k — матрица, ij -элемент которой $(i, j = 1, \dots, n)$ есть суммарный вес лесов, имеющих k компонент и вершину i , принадлежащую дереву с корнем j . (Соответствующие определения для неориентированного случая представлены в работе [9]; впрочем, заинтересованный читатель легко получит их самостоятельно.)

В случае орграфов мы можем получить аналогичное построение. На самом деле, мы можем попытаться использовать рекуррентную процедуру построения матрицы среднего времени первого прохода в качестве основы для построения q -*метрики леса* $qforest$ на Γ .

Аналогично, матрица $\bar{Q}(\alpha) = (1 + \alpha L)^{-1}$, используемая при построении α -метрики леса, может быть получена ([9]) как

$$\bar{Q}(\alpha) = \sigma^{-1}(\alpha) Q(\alpha), \quad \text{где } \sigma(\alpha) = \sum_{k=0}^{n-d} \sigma_k \alpha^k, \quad Q(\alpha) = \sum_{k=0}^{n-d} Q_k \alpha^k.$$

В случае орграфов мы можем попытаться использовать рекуррентную процедуру построения матрицы среднего времени первого прохода в качестве основы для построения (q, α) -*метрики леса* $qforest^\alpha$ (и *нормализованной* (q, α) -*метрики леса* qr^α) на Γ .

В следующем параграфе мы рассматриваем такие построения на конкретных примерах и изучаем свойства полученных конструкций.

6. Примеры квазиметрики среднего времени первого прохода

6.1. Пример 1.

Рассмотрим простейший симметричный случай случайного блуждания. Пусть

$$T = \begin{bmatrix} 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \\ 1/2 & 1/2 & 0 \end{bmatrix}.$$

Другими словами, мы рассматриваем простое случайное блуждание на простом цикле с тремя вершинами, то есть на неориентированном графе $G = (V, E)$, где $V = \{1, 2, 3\}$, $E = \{12, 23, 31\}$. Поскольку $d(1) = d(2) = d(3) = 2$, то, следуя описанной выше схеме, мы получаем орграф Γ на трех вершинах с весами дуг $w_{ik} = 1/2$, $i, k = 1, 2, 3$, $i \neq k$ (рис. 1).

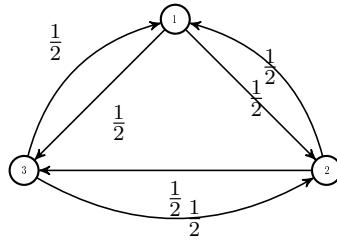
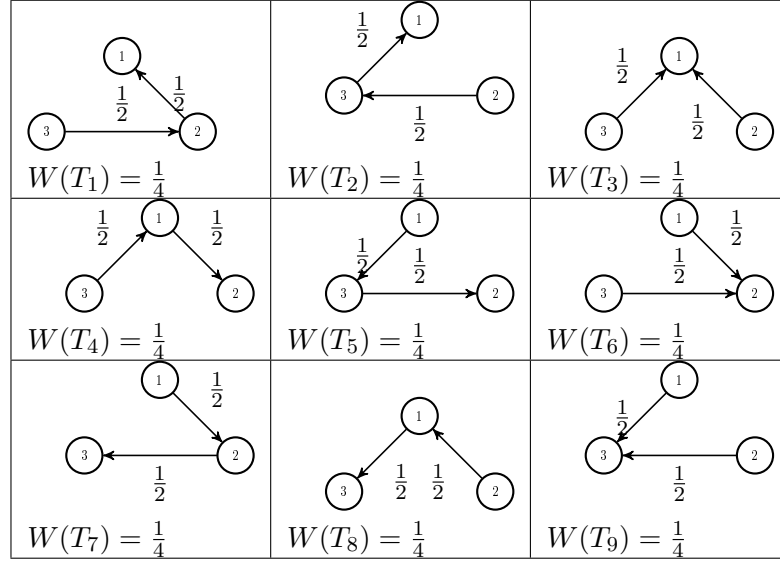


Рис.1. Орграф Γ на трех вершинах.

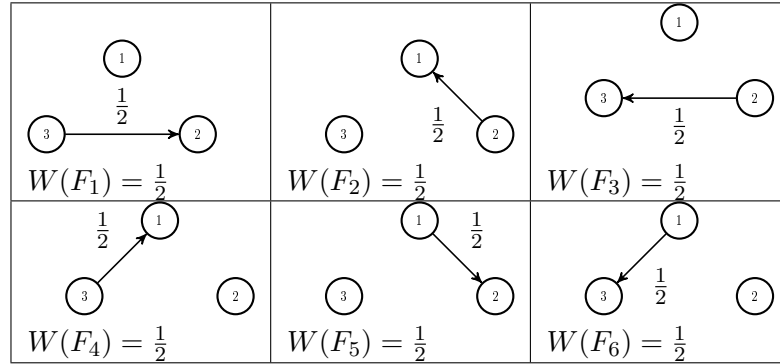
Пользуясь определением q_i (общий вес деревьев, сходящихся к i), и рассматривая 9 сходящихся деревьев орграфа Γ (рис. 2), найдем вектор $(q_1, q_2, q_3) = (3/4, 3/4, 3/4)$. Так как $q = \sum_{i=1}^3 q_i = 9/4$, то $\tilde{q} = (\tilde{q}_1, \tilde{q}_2, \tilde{q}_3) = \frac{q_i}{\sum_{i=1}^3 q_i} = (1/3, 1/3, 1/3)$. Этот вектор совпадает с π , нормированным левым вектором Перрона для T .

На рис. 3 представлены все 6 "2-деревьевых" лесов орграфа Γ (каждый имеет ровно две дуги). Вспоминая, что f_{ij} определяется как общий вес всех таких лесов, у которых i содержится в одном дереве, а второе дерево сходится к j , получаем:

$$\begin{aligned} ((f_{ij})) &= \begin{bmatrix} 0 & \sum w(F_i), i = 1, 4, 6 & \sum w(F_i), i = 2, 3, 5 \\ \sum w(F_i), i = 1, 3, 4 & 0 & \sum w(F_i), i = 2, 5, 6 \\ \sum w(F_i), i = 1, 2, 3 & \sum w(F_i), i = 4, 5, 6 & 0 \end{bmatrix} = \\ &= \begin{bmatrix} 0 & 3/2 & 3/2 \\ 3/2 & 0 & 3/2 \\ 3/2 & 3/2 & 0 \end{bmatrix}. \end{aligned}$$

Рис. 2. Сходящиеся деревья орграфа Γ .

Пользуясь тем, что $m_{ij} = \frac{f_{ij}}{q_j}$, $m_{ii} = \frac{q_1+q_2+q_3}{q_i}$, получим $M = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$.

Рис. 3. Леса орграфа Γ , состоящие из двух деревьев.

Мы можем получить те же результаты, пользуясь рекуррентной процедурой. Начиная с $Q_0 = I$ и $\sigma_0 = 1$ и используя матрицу $L = I - T = \begin{bmatrix} 1 & -1/2 & -1/2 \\ -1/2 & 1 & -1/2 \\ -1/2 & -1/2 & 1 \end{bmatrix}$, мы имеем:

$$\sigma_1 = \frac{\text{tr}(LQ_0)}{1} = 3, \quad Q_1 = -LQ_0 + \sigma_1 I = \begin{bmatrix} 2 & 1/2 & 1/2 \\ 1/2 & 2 & 1/2 \\ 1/2 & 1/2 & 2 \end{bmatrix},$$

$$\sigma_2 = \frac{\text{tr}(LQ_1)}{2} = 9/4, \quad Q_2 = -LQ_1 + \sigma_2 I = \begin{bmatrix} 3/4 & 3/4 & 3/4 \\ 3/4 & 3/4 & 3/4 \\ 3/4 & 3/4 & 3/4 \end{bmatrix}.$$

Обозначая $Q_1 = ((q_{ij}^{(1)}))$, находим $f_{ij} = q_{jj}^{(1)} - q_{ij}^{(1)}$, $i, j = 1, 2, 3$: $((f_{ij})) = \begin{bmatrix} 0 & 3/2 & 3/2 \\ 3/2 & 0 & 3/2 \\ 3/2 & 3/2 & 0 \end{bmatrix}$.

Следуя дальнейшей процедуре, мы вновь получим матрицу M , и, избавляясь от диагональных

членов, квазиметрику среднего времени первого прохода $\begin{bmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{bmatrix}$. В нашем простейшем симметричном случае данная квазиметрика является метрикой. Более того, она совпадает с удвоенной дискретной метрикой.

6.2. Пример 2.

Рассмотрим более интересный пример простого случайного блуждания. Пусть

$$T = \begin{bmatrix} 0 & 1/2 & 1/2 & 0 \\ 1/2 & 0 & 1/2 & 0 \\ 1/3 & 1/3 & 0 & 1/3 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Другими словами, мы рассматриваем простое случайное блуждание на неориентированном графе $G = (V, E)$, где $V = \{1, 2, 3, 4\}$, и $E = \{12, 13, 23, 34\}$.

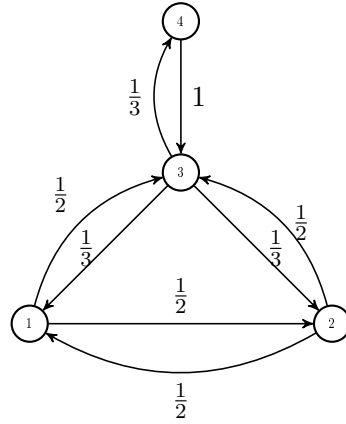


Рис.4. Орграф Γ на четырех вершинах.

Поскольку $d(1) = d(2) = 2$, $d(3) = 3$ и $d(4) = 1$, мы получаем новый орграф Γ (рис. 4) на вершинах 1, 2, 3, 4 с весами дуг $w_{1k} = 0.5$, $k = 2, 3$, $w_{2k} = 0.5$, $k = 1, 3$, $w_{3k} = 1/3$, $k = 1, 2, 4$, и $w_{43} = 1$.

По определению q_i (общий вес деревьев, сходящихся к i), используя 12 сходящихся деревьев орграфа Γ (рис. 5), найдем вектор $(q_1, q_2, q_3, q_4) = 0.25(2, 2, 3, 1)$. Так как $q = \sum_{k=1}^4 q_k = 2$, то $\tilde{q} = (\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4, \tilde{q}_5, \tilde{q}_6) = \frac{q}{\sum_{k=1}^6 q_k} = 0.125(2, 2, 3, 1)$. Этот вектор совпадает с π , нормированным левым вектором Перрона для T .

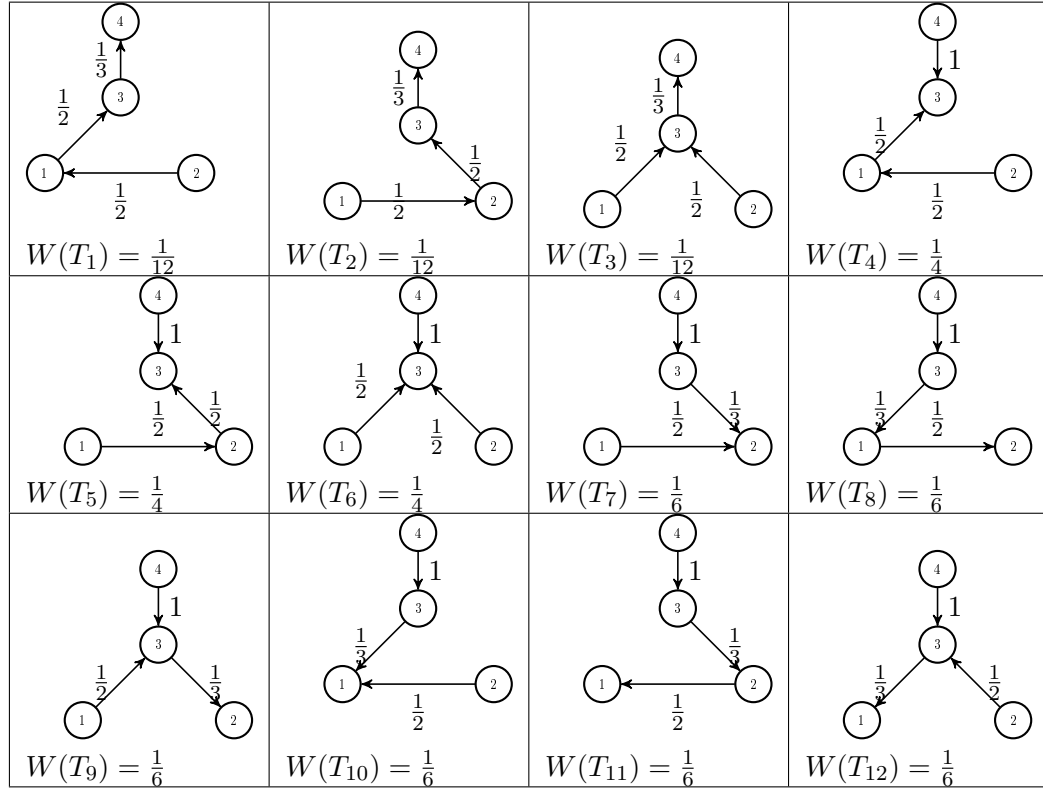
На рис. 6 представлены все 19 "2-деревьевых" лесов орграфа Γ (каждый имеет две дуги).

Величина f_{ij} определяется как общий вес всех таких лесов, у которых i содержится в одном дереве, а второе дерево сходится к j . Следовательно,

$$((f_{ij})) =$$

$$= \begin{bmatrix} 0 & \sum w(F_i), i = 6, 8, 9, 10 & \sum w(F_1), i = 2, 4, 7 & \sum w(F_i), i = 1, 3, 5, 11 - 19 \\ \sum w(F_i), i = 5, 6, 7, 8 & 0 & \sum w(F_i), i = 2, 4, 10 & \sum w(F_i), i = 1, 3, 9, 11 - 19 \\ \sum w(F_i), i = 3 - 7 & \sum w(F_i), i = 1, 2, 8 - 10 & 0 & \sum w(F_i), i = 11 - 19 \\ \sum w(F_i), i = 3 - 7, 12, 15 & \sum w(F_i), i = 1, 8, 9, 10, 13, 14 & \sum w(F_i), i = 11, 16, 19 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 0 & 4/3 & 3/2 & 9/4 \\ 4/3 & 0 & 3/2 & 9/4 \\ 5/3 & 5/3 & 0 & 7/4 \\ 13/6 & 13/6 & 3/4 & 0 \end{bmatrix}.$$

Рис. 5. Сходящиеся деревья орграфа Γ .

Отсюда, пользуясь тем, что $m_{ij} = \frac{f_{ij}}{q_j}$, $m_{ii} = \frac{q_1+q_2+q_3+q_4}{q_i}$, получим:

$$M = \frac{1}{3} \begin{bmatrix} 12 & 8 & 6 & 27 \\ 8 & 12 & 6 & 27 \\ 10 & 10 & 8 & 21 \\ 13 & 13 & 3 & 24 \end{bmatrix}.$$

Мы можем получить те же результаты, пользуясь рекуррентной процедурой. Начиная с $Q_0 = I$ и $\sigma_0 = 1$ и используя матрицу

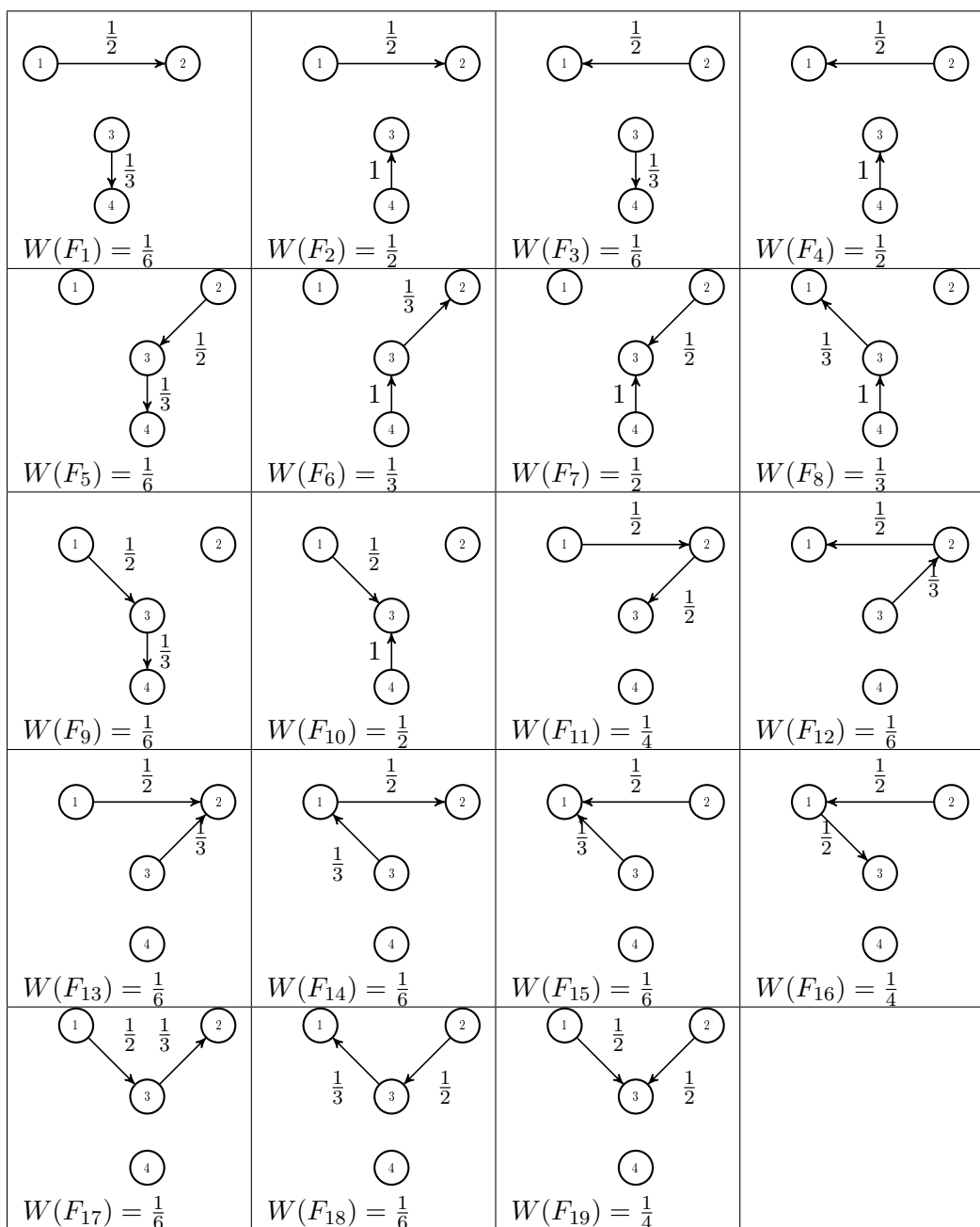
$$L = I - T = \begin{bmatrix} 1 & -1/2 & -1/2 & 0 \\ -1/2 & 1 & -1/2 & 0 \\ -1/3 & -1/3 & 1 & -1/3 \\ 0 & 0 & -1 & 1 \end{bmatrix},$$

мы имеем:

$$\sigma_1 = \frac{\text{tr}(LQ_0)}{1} = 4, \quad Q_1 = -LQ_0 + \sigma_1 I = \begin{bmatrix} 3 & 0.5 & 0.5 & 0 \\ 0.5 & 3 & 0.5 & 0 \\ 1/3 & 1/3 & 3 & 1/3 \\ 0 & 0 & 1 & 3 \end{bmatrix},$$

$$\sigma_2 = \frac{\text{tr}(LQ_1)}{2} = 61/12, \quad Q_2 = -LQ_1 + \sigma_2 I = \begin{bmatrix} 5/2 & 7/6 & 5/4 & 1/6 \\ 7/6 & 5/2 & 5/4 & 1/6 \\ 5/6 & 5/6 & 11/4 & 2/3 \\ 1/3 & 1/3 & 2 & 29/12 \end{bmatrix},$$

$$\sigma_3 = \frac{\text{tr}(LQ_2)}{3} = 2, \quad Q_3 = -LQ_2 + \sigma_3 I = \begin{bmatrix} 1/2 & 1/2 & 3/4 & 1/4 \\ 1/2 & 1/2 & 3/4 & 1/4 \\ 1/2 & 1/2 & 3/4 & 1/4 \\ 1/2 & 1/2 & 3/4 & 1/4 \end{bmatrix}.$$

Рис.6. Леса орграфа Γ , состоящие из двух деревьев.

Обозначая $Q_2 = ((q_{ij}^{(2)}))$, получаем, что $f_{ij} = q_{jj}^{(2)} - q_{ij}^{(2)}$, $i, j = 1, \dots, 4$, и, следовательно,

$$((f_{ij})) = \begin{bmatrix} 0 & 4/3 & 3/2 & 9/4 \\ 4/3 & 0 & 3/2 & 9/4 \\ 5/3 & 5/3 & 0 & 7/4 \\ 13/6 & 13/6 & 3/4 & 0 \end{bmatrix}, \text{ и } M = \frac{1}{3} \begin{bmatrix} 12 & 8 & 6 & 27 \\ 8 & 12 & 6 & 27 \\ 10 & 10 & 8 & 21 \\ 13 & 13 & 3 & 24 \end{bmatrix}.$$

Диагональ матрицы Q_3 вновь дает вектор $(1/2, 1/2, 3/4, 1/4)$.

Нетрудно убедиться в том, что нами получена (все ориентированные неравенства треугольника выполнены) квазиметрика

$$\overline{M} = \frac{1}{3} \begin{bmatrix} 0 & 8 & 6 & 27 \\ 8 & 0 & 6 & 27 \\ 10 & 10 & 0 & 21 \\ 13 & 13 & 3 & 0 \end{bmatrix},$$

обладающая ослабленным свойством симметрии $m_{ij} + m_{jk} + m_{ki} = m_{ik} + m_{kj} + m_{ji}$ и свойством аддитивности точки-разреза: если все пути от i к j идут через k , то $m_{ik} + m_{kj} = m_{ij}$. Более того, это взвешенная квазиметрика: $m_{ij} + w_i = m_{ji} + w_j$ для некоторой весовой функции w . Ее (неотрицательная и определенная с точностью до сдвига) весовая функция определяется вектором $w = \frac{1}{3}(4, 4, 0, 18)$. Соответствующая метрика коммутирующего времени первого прохода c , $c_{ij} = m(i, j) + m(j, i)$, и частичная метрика p , $p(i, j) = \frac{c(i, j) + w_i + w_j}{2}$, задаются матрицами

$$C = \frac{1}{3} \begin{bmatrix} 0 & 16 & 16 & 40 \\ 16 & 0 & 16 & 40 \\ 16 & 16 & 0 & 24 \\ 40 & 40 & 24 & 0 \end{bmatrix}; \quad P = \frac{1}{3} \begin{bmatrix} 4 & 12 & 16 & 31 \\ 12 & 4 & 16 & 31 \\ 16 & 16 & 0 & 38 \\ 31 & 31 & 38 & 18 \end{bmatrix}.$$

Для любой весовой функции w такой, что $m(i, j) \leq w_j$, $i, j = 1, 2, 3, 4$, т.е. начиная с $w = \frac{1}{3}(13, 13, 9, 27)$, функции m , c , p сильны на соответствующем уровне: m — сильная взвешенная квазиметрика, c — сильная взвешенная метрика, и p — сильная частичная метрика ([14]).

Более того, в этом случае функция $c' : V' \times V' \rightarrow \mathbb{R}$, где $V' = \{0, 1, 2, 3, 4\}$, $c'(0, 0) = 0$, $c'(0, i) = c'(i, 0) = w_i$, $c'(i, j) = c(i, j)$, если $i, j = 1, 2, 3, 4$, является метрикой на V' ; в случае $w = \frac{1}{3}(13, 13, 9, 27)$ ее матрица имеет вид

$$C' = \frac{1}{3} \begin{bmatrix} 0 & 13 & 13 & 9 & 27 \\ 13 & 0 & 16 & 16 & 40 \\ 13 & 16 & 0 & 16 & 40 \\ 9 & 16 & 16 & 0 & 24 \\ 27 & 40 & 40 & 24 & 0 \end{bmatrix}.$$

Используя результаты проведенной выше рекуррентной процедуры, мы получим матрицу $Q = ((q_{ij})) = \frac{\sum_{i=0}^3 Q_i}{\sum_{i=0}^3 \sigma_i}$:

$$Q = \frac{Q_0 + Q_1 + Q_2 + Q_3}{\sigma_0 + \sigma_1 + \sigma_2 + \sigma_3} = \frac{12}{145} \begin{bmatrix} 7 & 13/6 & 5/2 & 5/12 \\ 13/6 & 7 & 5/2 & 5/12 \\ 5/3 & 5/3 & 15/2 & 5/4 \\ 5/6 & 5/6 & 15/4 & 20/3 \end{bmatrix}.$$

Симметричная матрица $D = ((q_{ii} + q_{jj} - q_{ij} - q_{ji}))$, получаемая из $Q = ((q_{ij}))$, соответствует метрике леса для неориентированного случая. Она имеет вид

$$D = \frac{12}{145} \begin{bmatrix} 0 & 29/3 & 31/3 & 149/12 \\ 29/3 & 0 & 31/3 & 149/12 \\ 31/3 & 31/3 & 0 & 53/6 \\ 149/12 & 149/12 & 53/6 & 0 \end{bmatrix}.$$

Непосредственная проверка показывает, что для этой матрицы выполняются соотношения $d_{ij} + d_{jk} \geq d_{ik}$, $i, j = 1, 2, 3, 4$, то есть функция $D : V \times V \rightarrow \mathbb{R}$, определенная по закону $D(i, j) = D_{ij}$, является метрикой.

6.3. Пример 3.

Рассмотрим пример, не сводящийся к простому случайному блужданию. Пусть ([7])

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0.8 & 0.2 & 0 \\ 0.4 & 0 & 0.2 & 0.4 \\ 0 & 0 & 0.25 & 0.75 \end{bmatrix}.$$

Весовой оргграф Γ , соответствующий нашей цепи Маркова, показан на рис. 7.

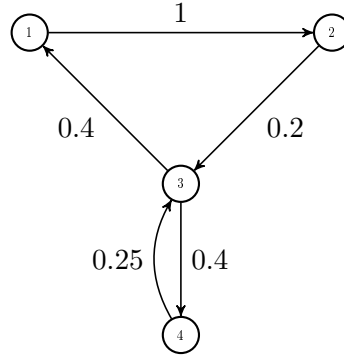


Рис.7. Весовой оргграф Γ , соответствующий матрице T .

Вычисляя q_i как общий вес деревьев, сходящихся к i , находим вектор $(q_1, q_2, q_3, q_4) = (0.02, 0.1, 0.05, 0.08)$. Поскольку $\sum_{k=1}^4 q_i = 0.25$, то $\tilde{q} = (\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4) = \frac{q}{\sum_{k=1}^4 q_i} = (0.08, 0.4, 0.2, 0.32)$. Этот вектор π , нормированный левый вектор Перрона для T .

Определяя f_{ij} как общий вес "2-деревьевых" лесов орграфа Γ , имеющих одно дерево, содержащее i , а другое дерево, сходящееся к j , получим, что

$$((f_{ij})) = \begin{bmatrix} 0 & 0.1 & 0.3 & 1.16 \\ 0.23 & 0 & 0.25 & 1.08 \\ 0.13 & 0.75 & 0 & 0.68 \\ 0.21 & 1.15 & 0.2 & 0 \end{bmatrix}, \text{ и } M = \begin{bmatrix} 12.5 & 1 & 6 & 14.5 \\ 11.5 & 2.5 & 5 & 13.5 \\ 6.5 & 7.5 & 5 & 8.5 \\ 10.5 & 11.5 & 4 & 3.125 \end{bmatrix}.$$

Пользуясь рекуррентной процедурой для вычисления f_{ij} и q_j , начиная с $Q_0 = I$, $\sigma_0 = 1$, мы имеем:

$$\sigma_1 = \frac{\text{tr}(LQ_0)}{1} = 2.25, Q_1 = \begin{bmatrix} 1.25 & 1 & 0 & 0 \\ 0 & 2.05 & 0.2 & 0 \\ 0.4 & 0 & 1.45 & 0.4 \\ 0 & 0 & 0.25 & 2 \end{bmatrix},$$

$$\sigma_2 = \frac{\text{tr}(LQ_1)}{2} = 1.56, Q_2 = \begin{bmatrix} 0.31 & 1.05 & 0.2 & 0 \\ 0.08 & 1.15 & 0.25 & 0.08 \\ 0.18 & 0.4 & 0.5 & 0.48 \\ 0.1 & 0 & 0.3 & 1.16 \end{bmatrix},$$

$$\sigma_3 = \frac{\text{tr}(LQ_2)}{3} = 0.25, Q_3 = \begin{bmatrix} 0.02 & 0.1 & 0.05 & 0.08 \\ 0.02 & 0.1 & 0.05 & 0.08 \\ 0.02 & 0.1 & 0.05 & 0.08 \\ 0.02 & 0.1 & 0.05 & 0.08 \end{bmatrix}.$$

Вычисляя f_{ij} по формуле $f_{ij} = q_{jj}^{(2)} - q_{ij}^{(2)}$, $i, j = 1, 2, \dots, 4$, мы приходим к тем же результатам. При этом (см. диагональ матрицы Q_3) мы вновь получаем вектор $(0.02, 0.1, 0.05, 0.08)$.

Непосредственная проверка показывает, что в данном случае соответствующая квазиметрика среднего времени первого прохода не будет взвешиваемой.

Используя описанную выше рекуррентную процедуру, мы можем получить и матрицу $Q = \frac{1}{\sigma_0 + \sigma_1 + \sigma_2 + \sigma_3}(Q_0 + Q_1 + Q_2 + Q_3)$:

$$Q = \frac{1}{5.06} \begin{bmatrix} 2.58 & 2.15 & 0.255 & 0.08 \\ 0.1 & 0.43 & 0.5 & 0.16 \\ 0.6 & 0.5 & 3 & 0.96 \\ 0.12 & 0.01 & 0.6 & 4.24 \end{bmatrix}.$$

Симметричная матрица $D = ((q_{ii} + q_{jj} - q_{ij} - q_{ji}))$, получаемая из $Q = ((q_{ij}))$, соответствует метрике леса для неориентированного случая. Она имеет вид

$$D = \frac{1}{5.06} \begin{bmatrix} 0 & 0.76 & 4.725 & 6.63 \\ 0.76 & 0 & 2.43 & 4.5 \\ 4.725 & 2.43 & 0 & 5.68 \\ 6.63 & 4.5 & 5.68 & 0 \end{bmatrix}.$$

К сожалению, в данном общем случае эта матрица метрику не определяет, поскольку неравенство треугольника нарушается (например, $d_{32} + d_{21} < d_{31}$). Однако следует заметить, что неравенство треугольника нарушено только на парах, содержащих 12. Это связано с тем, что вероятность перехода из вершины 1 в вершину 2 в соответствующем орграфе равна 1, то есть слишком велика.

7. Заключение

В статье представлены материалы, связанные с поведением специальной квазиметрики, тесно связанной со стохастическими дискретными процессами. Помимо короткого обзора теоретических оснований проблематики, подробно рассмотрены и проиллюстрированы на примерах "графовый" и рекуррентный алгоритмы построения квазиметрики среднего времени первого прохода; прокомментированы особые свойства этой квазиметрики в случае простого случайного блуждания по связному неориентированному графу. Осуществлена попытка рекуррентного построения и анализа других обобщенных структур, в том числе симметричных, связанных с теорией цепей Маркова.

В этой связи интерес представляет задача построения и исследования свойств конусов и многогранников рассматриваемых обобщенных (квази)метрик, заданных на малом числе точек; ее можно реализовать в рамках классической схемы (см., например, [15], [17]).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Деза М. М., Деза Е. И., Дютур Сикирич М. Полиэдральные конструкции, связанные с квази-метриками // Чебышевский сборник. 2015. Том 16, выпуск 2. С. 79 — 92.
2. Кудряшов Б. Д. Теория информации: Учебник для вузов. — СПб.: Петир, 2009.
3. Потапов В. Н. Теория информации. Кодирование дискретных вероятностных источников. — Новосибирск: НГУ, 1999.
4. Харари Ф. Теория графов. — М.: УРСС, 2003.
5. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.
6. Catral M., Neumann M., Xu H. Proximity in group inverses of M-matrices and inverses of diagonally dominant M-matrices // Linear Algebra and its Applications. 2005. Vol. 409. P. 32–50.
7. Chebotarev P. A graph theoretic interpretation of the mean first passage times // arXiv preprint arXiv:math.PR/0701359. 2007.
8. Chebotarev P. Studying new classes of graph metrics / in F. Nielsen and F. Barbaresco, editors, Proceedings of the SEE Conference "Geometric Science of Information" (GSI-2013) // Lecture Notes in Computer Science. 2013. LNCS 8085. P. 207–214.
9. Chebotarev P., Agaev R. Forest matrices around the Laplacian matrix // Linear Algebra and its Applications. 2002. Vol. 356. P. 253–274.
10. Chebotarev P., Deza E. Hitting time quasi-metric and its forest representation // Optimization Letters. 2020. Vol. 14. P. 291–307. <https://doi.org/10.1007/s11590-018-1314-2>
11. Chebotarev P. Y., Shamis E. V. On proximity measures for graph vertices // Automation and Remote Control. 1998. Vol. 59. P. 1443–1459.
12. Chebotarev P., Shamis E. Matrix forest theorems // arXiv:0602575v1. 2006.
13. Chebotarev P., Shamis E. The forest metric for graph vertices // arXiv:060257v1. 2006.
14. Deza E., Deza M., Dutour Sikirić Generalizations of Finite Metrics and Cuts. — World Scientific, 2016.
15. Deza M., Deza E. Cones of partial metrics // Contributions to Discrete Mathematics. 2011. Vol. 6. P. 26–47.
16. Deza M. M., Deza E. Encyclopedia of Distances. — Springer: Berlin-Heidelberg, 2016.
17. Deza M., Deza E., Vidali J. Cones of weighted and partial metrics / in Proceedings of the Internat. Conference on Algebra 2010 // Advances in Algebraic Structures. 2012. P. 177–197.
18. Hausdorff F. Grundzuge der Mengenlehre. — Walter de Gruyter: Berlin, 1927.
19. Kirkland S. J., Neumann M. Group inverses of M-matrices and their applications. — CRC Press, 2012.
20. Klein D., Zhu H. Distances and volumina for graphs // Journal of Mathematical Chemistry. 1998. Vol. 23. P. 179–195.

21. Leighton T., Rivest R. L. The Markov chain tree theorem // Computer Science Technical Report MIT/LCS/TM-249, Laboratory of Computer Science, MIT, Cambridge, Mass. 1983.
22. Leighton T., Rivest R. L. Estimating a probability using finite memory // IEEE Transactions on Information Theory. 1986. Vol. 32. P. 733–742.
23. Meyer Jr., C. D. The role of the group generalized inverse in the theory of finite Markov chains // SIAM Review. 1975. Vol. 17. P. 443–464.
24. Wentzell A. D., Freidlin M. I. On small random perturbations of dynamical systems // Russian Mathematical Surveys. 1970. Vol. 25. P. 1–55.
25. Wilson W. On quasi-metric spaces // American Journal of Mathematics. 1931. Vol. 53. P. 675–684.

REFERENCES

1. Deza, M.M., Deza, E.I., Dutour Sikirić, M. 2015, "Polyhedral structures associated with quasi-metrics", *Chebyshevskii sbornik*, Vol. 16 (2), P. 79–92.
2. Kudryashov, B.D. 2009, "Information Theory", *StPb.: Petir*.
3. Potapov, V.N. 1999, "Information Theory. Coding of discrete probabilistic sources", *Novosibirsk: NSU center*.
4. Harari, F. 2003, "Graph Theory", *M.: URSS*.
5. Shannon, K. 1963, "Works on Information theory and Cybernetics", *M.: IL*.
6. Catral, M., Neumann, M., Xu J. 2005, "Proximity in group inverses of M-matrices and inverses of diagonally dominant M-matrices", *Linear Algebra and its Applications*, Vol. 409, P. 32–50.
7. Chebotarev, P. 2007, "A graph theoretic interpretation of the mean first passage times", *arXiv preprint arXiv:math.PR/0701359*.
8. Chebotarev, P. 2013, "Studying new classes of graph metrics", in *F. Nielsen and F. Barbaresco, editors, Proceedings of the SEE Conference "Geometric Science of Information" (GSI-2013), Lecture Notes in Computer Science*, LNCS 8085, P. 207–214.
9. Chebotarev, P., Agaev, R. 2002, "Forest matrices around the Laplacian matrix", *Linear Algebra and its Applications*, Vol. 356, P. 253–274.
10. Chebotarev, P., Deza, E. 2020, "Hitting time quasi-metric and its forest representation", *Optimization Letters*, Vol. 14, P. 291–307. <https://doi.org/10.1007/s11590-018-1314-2>
11. Chebotarev, P.Y., Shamis E.V. 1998, "On proximity measures for graph vertices", *Automation and Remote Control*, Vol. 59, P. 1443–1459.
12. Chebotarev, P., Shamis E. 2006, "Matrix forest theorems", *arXiv:0602575v1*.
13. Chebotarev, P., Shamis, E. 2006, "The forest metric for graph vertices", *arXiv:060257v1*.
14. Deza, E., Deza, M., Dutour Sikirić, M. 2016, "Generalizations of Finite Metrics and Cuts", *World Scientific*.

15. Deza, M., Deza, E. 2011, "Cones of partial metrics", *Contributions to Discrete Mathematics*, Vol. 6, P. 26–47.
16. Deza, M. M., Deza, E. 2016, "Encyclopedia of Distances", *Springer, Berlin - Heidelberg*.
17. Deza, M., Deza, E., Vidali, J. 2012, "Cones of weighted and partial metrics", in *Proceedings of the Internat. Conference on Algebra 2010: Advances in Algebraic Structures*, P. 177–197.
18. Hausdorff, F. 1927, "Grundzuge der Mengenlehre", *Walter de Gruyter, Berlin*.
19. Kirkland, S. J., Neumann, M. 2012, "Group inverses of M-matrices and their applications", *CRC Press*.
20. Klein, D., Zhu, H. 1998, "Distances and volumina for graphs", *Journal of Mathematical Chemistry*, Vol. 23, P. 179–195.
21. Leighton, T., Rivest, R.L. 1983, "The Markov chain tree theorem", *Computer Science Technical Report MIT/LCS/TM-249, Laboratory of Computer Science, MIT, Cambridge, Mass*.
22. Leighton, T., Rivest, R.L. 1986, "Estimating a probability using finite memory", *IEEE Transactions on Information Theory*, Vol. 32, P. 733–742.
23. Meyer, Jr., C. D. 1975, "The role of the group generalized inverse in the theory of finite Markov chains", *SIAM Review*, Vol. 17, P. 443–464.
24. Wentzell, A. D., Freidlin, M.I. 1970, "On small random perturbations of dynamical systems", *Russian Mathematical Surveys*, Vol. 25, P. 1–55.
25. Wilson, W. 1931, "On quasi-metric spaces", *American Journal of Mathematics*, Vol. 53, P. 675–684.

Получено 15.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.3

DOI 10.22405/2226-8383-2019-21-1-165-185

Обратная задача для моноида с экспоненциальной последовательностью простых¹

Н. Н. Добровольский, И. Ю. Реброва, Н. М. Добровольский

Добровольский Николай Николаевич — кандидат физико-математических наук, доцент кафедры прикладной математики и информатики, Тульский государственный университет; доцент кафедры алгебры, математического анализа и геометрии, Тульский государственный педагогический университет им. Л. Н. Толстого, г. Тула.

e-mail: nikolai.dobrovolsky@gmail.com

Реброва Ирина Юрьевна — кандидат физико-математических наук, доцент, декан факультета математики, физики и информатики, Тульский государственный педагогический университет им. Л. Н. Толстого, г. Тула.

e-mail: i_rebrova@mail.ru

Добровольский Николай Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры, математического анализа и геометрии, Тульский государственный педагогический университет им. Л. Н. Толстого, г. Тула.

e-mail: dobrovol@tsput.ru

Аннотация

В работе для произвольного моноида $M(PE)$ с экспоненциальной последовательностью простых чисел PE типа q решается обратная задача, то есть нахождение асимптотики для функции распределения элементов моноида $M(PE)$, исходя из асимптотики распределения простых чисел последовательности простых чисел PE типа q .

Для решения этой задачи вводится понятие произвольной экспоненциальной последовательности натуральных чисел типа q и рассматривается моноид, порожденный этой последовательностью. С помощью двух гомоморфизмов таких моноидов задача о распределении плотности сводится к аддитивной задаче Ингама.

Показано, что для этого класса моноидов понятие степенной плотности не работает. Введено новое понятие C логарифмической θ -степенной плотности.

Показано, что любой моноид $M(PE)$ для произвольной экспоненциальной последовательности простых PE типа q имеет C логарифмическую θ -степенную плотность с $C = \pi \sqrt{\frac{2}{3 \ln q}}$ и $\theta = \frac{1}{2}$.

Ключевые слова: дзета-функция Римана, ряд Дирихле, дзета-функция моноида натуральных чисел, эйлерово произведение, экспоненциальная последовательность простых, C логарифмическая θ -степенная плотность.

Библиография: 28 названий.

Для цитирования:

Н. Н. Добровольский, И. Ю. Реброва, Н. М. Добровольский. Обратная задача для моноида с экспоненциальной последовательностью простых // Чебышевский сборник. 2020. Т. 21, вып. 1, С. 165–185.

¹Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-41-710004_p_a.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.3

DOI 10.22405/2226-8383-2019-21-1-165-185

Inverse problem for a monoid with an exponential sequence of primes²

N. N. Dobrovol'skii, I. Yu. Rebrova, N. M. Dobrovol'skii

Dobrovol'skii Nikolai Nikolaevich — candidate of physical and mathematical sciences, associate Professor of the department of applied mathematics and computer science, Tula State University; associate Professor of the department of algebra, mathematical analysis and geometry, Tula State L. N. Tolstoy Pedagogical University, Tula.

e-mail: nikolai.dobrovolsky@gmail.com

Rebrova Irina Yuryevna — candidate of physical and mathematical Sciences, associate professor, dean of the faculty of mathematics, physics and computer science, Tula State L. N. Tolstoy Pedagogical University, Tula.

e-mail: i_rebrova@mail.ru

Dobrovol'skii Nikolai Mihailovich — doctor of physical and mathematical sciences, professor, head of the department of algebra, mathematical analysis and geometry, Tula State L. N. Tolstoy Pedagogical University, Tula.

e-mail: dobrovol@tspu.ru

Abstract

In this paper, for an arbitrary monoid $M(PE)$ with an exponential sequence of primes PE of type q , the inverse problem is solved, that is, finding the asymptotic for the distribution function of elements of the monoid $M(PE)$, based on the asymptotic distribution of primes of the sequence of primes PE of type q .

To solve this problem, we introduce the concept of an arbitrary exponential sequence of natural numbers of the type q and consider the monoid generated by this sequence. Using two homomorphisms of such monoids, the density distribution problem is reduced to the additive Ingham problem.

It is shown that the concept of power density does not work for this class of monoids. A new concept of C logarithmic θ -power density is introduced.

It is shown that any monoid $M(PE)$ for an arbitrary exponential sequence of primes PE of type q has C logarithmic θ -power density with $C = \pi \sqrt{\frac{2}{3 \ln q}}$ and $\theta = \frac{1}{2}$.

Keywords: Riemann zeta function, Dirichlet series, zeta function of the monoid of natural numbers, Euler product, exponential sequence of primes, C logarithmic θ -power density.

Bibliography: 28 titles.

For citation:

N. N. Dobrovol'skii, I. Yu. Rebrova, N. M. Dobrovol'skii, 2020, "Inverse problem for a monoid with an exponential sequence of Prime numbers", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 165–185.

*Посвящается 80-летию академика РАН,
профессора Владимира Петровича Платонова*

²Acknowledgments: The reported study was funded by RFBR, project number 19-41-710004_r_a.

1. Введение

В работе [14] дано следующее определение экспоненциальной последовательности простых чисел.

ОПРЕДЕЛЕНИЕ 1. Пусть $q \geq 2$ — произвольное натуральное число, тогда бесконечная последовательность простых чисел $p_1 < p_2 < \dots < p_n < \dots$ называется экспоненциальной типа q , если выполняются соотношения $q \leq p_1 < q^2$, $q^\nu < p_\nu < q^{\nu+1}$ ($\nu \geq 2$).

В силу постулата Бертрана, доказанного П. Л. Чебышёвым (см. [26]), для любого $q \geq 2$ существует бесконечно много экспоненциальных последовательностей простых чисел типа q .

В работе [14] было дано определение

ОПРЕДЕЛЕНИЕ 2. Для любого множества A натуральных чисел дзета-функция $\zeta(A|\alpha)$ определяется равенством

$$\zeta(A|\alpha) = \sum_{x \in A} \frac{1}{x^\alpha} \quad (\alpha = \sigma + it, \sigma > \sigma_A). \quad (1)$$

Если множество A конечное, то равенство (1) задает дзета-функцию $\zeta(A|\alpha)$ на всей комплексной α -плоскости. Если множество A бесконечное, то равенство (1) задает дзета-функцию $\zeta(A|\alpha)$ только при $\sigma > \sigma_A$, при этом обязательно в точке $\alpha = \sigma_A$ будет полюс первого порядка и $0 \leq \sigma_A \leq 1$, так как это следует из свойств дзета-ряда для дзета-функции $\zeta(\alpha)$ (см. [24], [26]). Отметим, что при $\sigma > \sigma_A$ ряд абсолютно сходится, а при $\sigma \geq \sigma_0$ для любого $\sigma_0 > \sigma_A$ ряд равномерно сходится.

Пусть $PE = \{p_1, p_2, \dots, p_n, \dots\}$ — экспоненциальная последовательность простых чисел типа q и $M(PE)$ — моноид натуральных чисел, образованный с помощью PE . В работе [14] доказана следующая теорема.

ТЕОРЕМА 1. Для любого $q \geq 2$ и любой экспоненциальной последовательности простых чисел $PE = \{p_1, p_2, \dots, p_n, \dots\}$ типа q дзета-ряд для дзета-функции $\zeta(M(PE)|\alpha)$ абсолютно сходится для любого α в полуплоскости $\sigma > 0$ и равномерно в полуплоскости $\sigma \geq \sigma_0$ для любого $\sigma_0 > 0$.

В работе [18] была высказана гипотеза о "заградительном ряде" для дзета-функции $\zeta(M(PE)|\alpha)$, которая была доказана в работе [17]. Тем самым было установлено, что для этой дзета-функции её область голоморфности совпадает с правой полуплоскостью $\sigma > 0$.

В работе [15] доказана теорема о количестве простых элементов в моноиде $M(A)$, не превосходящих x , которое будем обозначать через $\pi_{M(A)}(x)$. В общем случае это непростая задача, однако для случая любой экспоненциальной последовательности простых чисел $PE = \{p_1, p_2, \dots, p_n, \dots\}$ типа q и моноида $M(PE)$ можно дать удовлетворительный ответ.

ТЕОРЕМА 2. Для любого $q \geq 2$ и любой экспоненциальной последовательности простых чисел $PE = \{p_1, p_2, \dots, p_n, \dots\}$ типа q для количества простых элементов в моноиде $M(PE)$, не превосходящих x , справедливо равенство

$$\pi_{PE}(x) = \frac{\ln x}{\ln q} - \theta_{PE}(x),$$

где $0 \leq \theta_{PE}(x) = \left\{ \frac{\ln x}{\ln q} - \frac{\ln p_n}{\ln q} \right\} + \left\{ \frac{\ln p_n}{\ln q} \right\} < 2$ при $q^n \leq x < q^{n+1}$.

В работе [16] было дано определение σ -последовательности $\mathbb{P}_\sigma$ простых чисел.

ОПРЕДЕЛЕНИЕ 3. Последовательность $\mathbb{P}_\sigma$ простых чисел называется σ -последовательностью, если

$$\mathbb{P}_\sigma = \{p_1 < p_2 < \dots < p_n < \dots\}$$

и найдется N_σ такое, что для любого $n > N_\sigma$ выполняются неравенства

$$n^\sigma \leq p_n < (n+1)^\sigma. \quad (2)$$

Нам потребуется теорема Ингама о простых числах в следующей формулировке (см. [25], стр. 66).

ТЕОРЕМА 3. Существует $X_I > 1$ такое, что для любого $x > X_I$ найдется простое число p_x , для которого выполнены неравенства

$$x^3 \leq p_x \leq (x+1)^3. \quad (3)$$

Из этой теоремы сразу следует следующее утверждение.

Пусть $\sigma > 3$ и $X_{I,\sigma} = X_I^{\frac{3}{\sigma}}$, тогда для любого $x > X_{I,\sigma}$ найдется простое число $p_{x,\sigma}$, для которого выполнены неравенства

$$x^\sigma \leq p_{x,\sigma} \leq (x+1)^\sigma. \quad (4)$$

Из следствия из теоремы Ингама следует, что σ -последовательности простых чисел существуют для любого $\sigma \geq 3$.

Остановимся на вопросе о распределении простых чисел в σ -последовательности $\mathbb{P}_\sigma$ простых чисел. Обозначим количество простых чисел в σ -последовательности $\mathbb{P}_\sigma$ простых чисел, не превосходящих x через $\pi_{\mathbb{P}_\sigma}(x)$. В работе [16] доказана следующая теорема.

ТЕОРЕМА 4. При $x > N_\sigma$: σ для функции $\pi_{\mathbb{P}_\sigma}(x)$ справедливы равенства

$$\pi_{\mathbb{P}_\sigma}(x) = x^{\frac{1}{\sigma}} + \theta(x), \quad (5)$$

где $-2 < \theta(x) < -1$.

Теоремы 2 и 4 непосредственно связаны с тематикой работ Б. М. Бредихина [2]–[10]. Следуя этим работам, определим функции $\nu_{M(PE)}(x)$ и $\nu_{M(\mathbb{P}_\sigma)}(x)$ с помощью равенств:

$$\nu_{M(PE)}(x) = \sum_{n \in M(PE), n \leq x} 1, \quad \nu_{M(\mathbb{P}_\sigma)}(x) = \sum_{n \in M(\mathbb{P}_\sigma), n \leq x} 1.$$

Целью данной и следующих работ будет решение обратной задачи для функций $\nu_{M(PE)}(x)$ и $\nu_{M(\mathbb{P}_\sigma)}(x)$, т. е. нахождение асимптотики для этих функций, зная асимптотики для функций $\pi_{PE}(x)$ и $\pi_{\mathbb{P}_\sigma}(x)$.

2. Вспомогательные леммы

Пусть M — произвольный моноид натуральных чисел с однозначным разложением на простые элементы, $P(M)$ — множество его простых элементов и функции $\nu_M(x)$, $\pi_{P(M)}(x)$ заданы равенствами

$$\nu_M(x) = \sum_{n \in M, n \leq x} 1, \quad \pi_{P(M)}(x) = \sum_{q \in P(M), q \leq x} 1.$$

ЛЕММА 1. *Справедливо равенство*

$$\nu_M(x) \ln x = \int_1^x \nu_M(u) \frac{du}{u} + \sum_{k \geq 1} \sum_{q \in P(M), q \leq x} \nu_M\left(\frac{x}{q^k}\right) \ln q. \quad (6)$$

ДОКАЗАТЕЛЬСТВО. Обозначим через $\Pi_M(x)$ произведение всех элементов из моноида M , непревосходящих x :

$$\Pi_M(x) = \prod_{n \in M, n \leq x} n,$$

тогда, в силу однозначности разложения на простые элементы в моноиде M , получим

$$\Pi_M(x) = \prod_{q \in P(M), q \leq x} q^{\beta_{M,q}(x)},$$

где $\beta_{M,q}(x)$ — показатель степени, с которым простым элементом q входит в произведение $\Pi_M(x)$.

По аналогии с формулой для факториала имеем:

$$\beta_{M,q}(x) = \sum_{k \geq 1} \nu_M\left(\frac{x}{q^k}\right).$$

Отсюда после логарифмирования получим

$$\sum_{n \in M, n \leq x} \ln n = \sum_{q \in P(M), q \leq x} \sum_{k \geq 1} \nu_M\left(\frac{x}{q^k}\right) \ln q. \quad (7)$$

Применяя теорему Абеля (см. [26], стр. 106) при $M = \{1 = \lambda_1 < \lambda_2 < \dots\}$, $a_n = 1$, $\varphi(x) = \ln x$, $A(x) = \sum_{\lambda_n \leq x} a_n = \nu_M(x)$ к левой части последнего равенства, получим

$$\sum_{n \in M, n \leq x} \ln n = \nu_M(x) \ln x - \int_1^x \nu_M(t) \frac{dt}{t}. \quad (8)$$

Заменяя левую часть в (8) на правую часть из (7), получим утверждение леммы

$$\nu_M(x) \ln x = \int_1^x \nu_M(u) \frac{du}{u} + \sum_{k \geq 1} \sum_{q \in P(M), q \leq x} \nu_M\left(\frac{x}{q^k}\right) \ln q.$$

□

ЛЕММА 2. Пусть $q \geq 2$ и $PE = \{p_1, p_2, \dots, p_n, \dots\}$ — экспоненциальная последовательность простых чисел типа q . Справедливо неравенство³

$$\prod_{p_j \leq x} \left(1 - \frac{1}{p_j}\right)^{-1} = \exp \left(\frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1}\right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - O \left(\ln \left(1 - \frac{1}{p_1}\right) \right) \right), \quad (9)$$

где $x \geq p_1 > 1$.

³Здесь и далее, как обычно, $\exp(x) = e^x$.

ДОКАЗАТЕЛЬСТВО. Действительно,

$$\prod_{p_j \leq x} \left(1 - \frac{1}{p_j}\right)^{-1} = \exp \left(\sum_{k \geq 1} \sum_{p_j \leq x} \frac{1}{k p_j^k} \right).$$

Применяя к внутренней сумме по p_j теорему Абеля, получим

$$\sum_{p_j \leq x} \frac{1}{k p_j^k} = \frac{\pi_{PE}(x)}{k x^k} + \int_{p_1}^x \frac{\pi_{PE}(t)}{t^{k+1}} dt.$$

Применим теорему 2, получим

$$\sum_{p_j \leq x} \frac{1}{k p_j^k} = \frac{\frac{\ln x}{\ln q} - \theta_{PE}(x)}{k x^k} + \int_{p_1}^x \frac{\frac{\ln t}{\ln q} - \theta_{PE}(t)}{t^{k+1}} dt.$$

Отсюда следует, что

$$\begin{aligned} \sum_{k \geq 1} \sum_{p_j \leq x} \frac{1}{k p_j^k} &= \left(\frac{\ln x}{\ln q} - \theta_{PE}(x) \right) \ln \left(1 - \frac{1}{x} \right)^{-1} + \frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} - \frac{\ln x}{\ln q} \ln \left(1 - \frac{1}{x} \right)^{-1} + \\ &+ \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2} \left(\frac{1}{p_1^k} - \frac{1}{x^k} \right) - \theta_1 \ln \frac{1 - \frac{1}{p_1}}{1 - \frac{1}{x}} = \frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - \\ &- O \left(\ln \left(1 - \frac{1}{p_1} \right) + \frac{1}{x} \right) \rightarrow \frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - O \left(\ln \left(1 - \frac{1}{p_1} \right) \right) \quad (x \rightarrow \infty), \end{aligned}$$

где $0 \leq \theta_1 < 2$. $\square$

ЛЕММА 3. Пусть $q \geq 2$ и $PE = \{p_1, p_2, \dots, p_n, \dots\}$ — экспоненциальная последовательность простых чисел типа q . Справедливо неравенство

$$\nu_{M(PE)}(x) \leq x \exp \left(\frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - O \left(\ln \left(1 - \frac{1}{p_1} \right) \right) \right), \quad (10)$$

где $x \geq p_1 > 1$.

ДОКАЗАТЕЛЬСТВО. Действительно,

$$\sum_{n \in M(PE), n \leq x} \frac{1}{n} \leq \prod_{p_j \leq x} \left(1 - \frac{1}{p_j} \right)^{-1}.$$

Отсюда и из леммы 2 следует, что

$$\sum_{n \in M(PE), n \leq x} \frac{1}{n} \leq \exp \left(\frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - O \left(\ln \left(1 - \frac{1}{p_1} \right) \right) \right).$$

По теореме Абеля

$$\sum_{n \in M(PE), n \leq x} \frac{1}{n} = \frac{\nu_{M(PE)}(x)}{x} + \int_1^x \frac{\nu_{M(PE)}(t)}{t^2} dt.$$

Следовательно,

$$\nu_{M(PE)}(x) \leq x \exp \left(\frac{\ln p_1}{\ln q} \ln \left(1 - \frac{1}{p_1} \right)^{-1} + \frac{1}{\ln q} \sum_{k \geq 1} \frac{1}{k^2 p_1^k} - O \left(\ln \left(1 - \frac{1}{p_1} \right) \right) \right).$$

□

Мы видим, что в данном случае подход Б. М. Бредихина не работает, так как мы заведомо имеем случай для моноида $M(PE)$, когда отсутствует степенная θ -плотность, так как при степенной плотности невозможна асимптотическая формула из теоремы 2. Далее мы будем опираться на аддитивную теорему Ингама, но нам удастся получить только две асимптотические оценки сверху и снизу.

3. О двух гомоморфизмах моноида с экспоненциальной последовательностью простых

Пусть G — произвольная свободная коммутативная мультипликативная полугруппа с нейтральным элементом e и со счетным числом образующих элементов $\omega_1, \omega_2, \dots, \omega_\nu, \dots$, множество которых будем обозначать через $\Omega(G)$.

Рассмотрим произвольный гомоморфизм $N(g)$ полугруппы G в мультипликативный моноид $\mathbb{N}$ натуральных чисел, обладающий тем свойством, что в полугруппе G имеется только конечное число элементов g с $N(g) \leq x$ для любого вещественного x . Обозначим через M его образ. Это будет мультипликативный моноид натуральных чисел $M = N(G)$. Вслед за Б. М. Бредихиным (см. [2]), рассмотрим дзета-функцию полугруппы G

$$\zeta_G(\alpha) = \sum_{g \in G} \frac{1}{N^\alpha(g)}, \quad \alpha = \sigma + it, \quad \sigma > \sigma_G,$$

где σ_G — абсцисса абсолютной сходимости ряда Дирихле для дзета-функции полугруппы G .

В силу мультипликативности гомоморфизма имеет место разложение в эйлерово произведение

$$\zeta_G(\alpha) = P_G(\alpha) = \prod_{\nu=1}^{\infty} \left(1 - \frac{1}{N^\alpha(\omega_\nu)} \right)^{-1}$$

в правой полуплоскости $\sigma > \sigma_G$.

Рассмотрим дзета-функцию моноида $M = N(G)$

$$\zeta(M|\alpha) = \sum_{n \in M} \frac{1}{n^\alpha}, \quad \alpha = \sigma + it, \quad \sigma > \sigma_M,$$

где σ_M — абсцисса абсолютной сходимости ряда Дирихле для дзета-функции моноида $M = N(G)$.

Вообще говоря, $\zeta_G(\alpha) \neq \zeta(M|\alpha)$. Дело в том, что

$$\zeta_G(\alpha) = \sum_{g \in G} \frac{1}{N^\alpha(g)} = \sum_{n \in M} \frac{|N^{-1}(n)|}{n^\alpha},$$

где $N^{-1}(n) = \{g \in G | N(g) = n\}$ — прообраз натурального числа n при гомоморфизме $N(g)$ полугруппы G в мультипликативный моноид $\mathbb{N}$ натуральных чисел, а $|N^{-1}(n)|$ — количество элементов в этом прообразе, которое конечно в силу ограничений на гомоморфизм $N(g)$.

Таким образом, равенство дзета-функций возможно только в случае изоморфизма G и $M = N(G)$.

Следующее важное обстоятельство связано с тем, что $P(M)$ — множество простых элементов мультипликативного моноида M , вообще говоря, не совпадает с образом множества образующих элементов полугруппы G : $P(M) \subset N(\Omega(G))$.

Напомним, что если через $P(M|\alpha)$ обозначается эйлерово произведение:

$$P(M|\alpha) = \prod_{r \in P(M)} \left(1 - \frac{1}{r^\alpha}\right)^{-1},$$

тогда для произвольного моноида M натуральных чисел с однозначным разложением на простые элементы справедливо равенство

$$\zeta(M|\alpha) = P(M|\alpha).$$

Таким образом, возможны следующие ситуации:

$$\zeta(M|\alpha) \neq P(M|\alpha), \quad P(M|\alpha) \neq P_G(\alpha) = \prod_{r \in P(M)} \left(1 - \frac{1}{r^\alpha}\right)^{-|N^{-1}(r)|}.$$

Рассмотрим в качестве G мультипликативный моноид $M(PE)$, порожденный экспоненциальной системой простых чисел PE типа q , где $q \geq 2$ — любое натуральное число. Определим два гомоморфизма мультипликативного моноида $M(PE)$ в мультипликативный моноид $\mathbb{N}$ натуральных чисел:

$$\begin{aligned} N_1 : M(PE) &\rightarrow \mathbb{N} : N_1 \left(\prod_{\nu=1}^n p_{j_\nu}^{\beta_\nu} \right) = q^{\sum_{\nu=1}^n j_\nu \beta_\nu}, \\ N_2 : M(PE) &\rightarrow \mathbb{N} : N_2 \left(\prod_{\nu=1}^n p_{j_\nu}^{\beta_\nu} \right) = q^{\sum_{\nu=1}^n (j_\nu+1) \beta_\nu}. \end{aligned}$$

Обозначим через $M_1(q)$ образ мультипликативного моноида $M(PE)$ при гомоморфизме N_1 , а через $M_2(q)$ при гомоморфизме N_2 . Непосредственно из определения следует, что

$$M_1(q) = \{1, q, q^2, \dots\}, \quad M_2(q) = \{1, q^2, q^3, \dots\}.$$

Отсюда сразу следует, что $P(M_1(q)) = \{q\}$ и $P(M_2(q)) = \{q^2, q^3\}$.

Определим функции $\nu_{M(PE),1}(x)$ и $\nu_{M(PE),2}(x)$ с помощью равенств:

$$\nu_{M(PE),1}(x) = \sum_{n \in M(PE), N_1(n) \leq x} 1, \quad \nu_{M(PE),2}(x) = \sum_{n \in M(PE), N_2(n) \leq x} 1.$$

ЛЕММА 4. *Справедливы неравенства:*

для любого $n \in M(PE)$ имеем $N_1(n) \leq n \leq N_2(n)$,

$$\nu_{M(PE),2}(x) \leq \nu_{M(PE)}(x) \leq \nu_{M(PE),1}(x).$$

ДОКАЗАТЕЛЬСТВО. Пусть $n = \prod_{\nu=1}^n p_{j_\nu}^{\beta_\nu}$, тогда, так как $q^{j_\nu} \leq p_{j_\nu} \leq q^{j_\nu+1}$, имеем неравенства

$$N_1(n) = q^{\sum_{\nu=1}^n j_\nu \beta_\nu} \leq n \leq q^{\sum_{\nu=1}^n (j_\nu+1) \beta_\nu} = N_2(n).$$

Отсюда сразу вытекает двустороннее неравенство для функции $\nu_{M(PE)}(x)$. $\square$

Обозначим через $p_1(n)$ количество решений в неотрицательных целых числах $x_1, x_2, \dots, x_r, \dots$ диофантова уравнения

$$n = 1 \cdot x_1 + 2 \cdot x_2 + \dots + r \cdot x_r + \dots,$$

а через $p_2(n)$ количество решений диофантова уравнения

$$n = 2 \cdot x_2 + \dots + r \cdot x_r + \dots$$

Положим

$$P_1(x) = \sum_{n \leq x} p_1(n), \quad P_2(x) = \sum_{n \leq x} p_2(n).$$

ЛЕММА 5. *Справедливы равенства*

$$\nu_{M(PE),1}(x) = P_1\left(\frac{\ln x}{\ln q}\right), \quad \nu_{M(PE),2}(x) = P_2\left(\frac{\ln x}{\ln q}\right).$$

ДОКАЗАТЕЛЬСТВО. Действительно, если $N_1(n) = q^m$, то $m = \sum_{\nu=1}^n j_\nu \beta_\nu$. Отсюда следует, что количество $n \in M(PE)$, таких что $N_1(n) = q^m$, в точности равно $p_1(m)$. Так как из $N_1(n) = q^m \leq x$ следует, что $m \leq \frac{\ln x}{\ln q}$, то первое равенство доказано. Второе равенство доказывается аналогично. $\square$

4. Об экспоненциальных последовательностях

Дадим следующее определение.

ОПРЕДЕЛЕНИЕ 4. Пусть $q \geq 2$ — произвольное натуральное число, тогда бесконечная последовательность натуральных чисел $q_1 < q_2 < \dots < q_n < \dots$ называется экспоненциальной последовательностью типа q , если выполняются соотношения $q \leq q_1 < q^2$, $q^\nu \leq q_\nu < q^{\nu+1}$ ($\nu \geq 2$).

Таким образом, минимальной экспоненциальной последовательностью натуральных чисел типа q будет геометрическая прогрессия $\{q, q^2, \dots, q^n, \dots\}$ со знаменателем q , а максимальной — сдвинутая геометрическая прогрессия $\{q^2 - 1, q^3 - 1, \dots, q^n - 1, \dots\}$ со знаменателем q . Если QE — произвольная экспоненциальная последовательность натуральных чисел типа q , то через $M(QE)$ будем обозначать минимальный мультипликативный моноид натуральных чисел, порождённый последовательностью QE . Таким образом,

$$M(QE) = \left\{ n = \prod_{\nu=1}^m q_{j_\nu}^{\beta_\nu} \mid \beta_\nu > 0 (\nu = 1, \dots, m), m \geq 0 \right\}.$$

Нетрудно задать гомоморфизм N произвольной коммутативной свободной полугруппы G с нейтральным элементом e и системой образующих $\Omega(G)$ в мультипликативный моноид $M(QE)$, положив

$$N(e) = 1, \quad N(\omega_\nu) = q_\nu \quad (\nu = 1, 2, \dots).$$

Тогда для любого $g \in G$ имеем:

$$g = \prod_{\nu=1}^m \omega_{j_\nu}^{\beta_\nu}, \quad N(g) = \prod_{\nu=1}^m q_{j_\nu}^{\beta_\nu}.$$

Если $M(QE)$ моноид с однозначным разложением на образующие элементы, то по аналогии со случаем мультипликативного моноида $M(PE)$ можно определить два гомоморфизма N_1 и N_2 мультипликативного моноида QE в мультипликативные моноиды $M_1(q)$ и $M_2(q)$, соответственно.

Определим функции $\nu_{M(QE),1}(x)$ и $\nu_{M(QE),2}(x)$ с помощью равенств:

$$\nu_{M(QE),1}(x) = \sum_{n \in M(QE), N_1(n) \leq x} 1, \quad \nu_{M(QE),2}(x) = \sum_{n \in M(QE), N_2(n) \leq x} 1,$$

а функции $\nu_{M(QE),1}^*(x)$ и $\nu_{M(QE),2}^*(x)$ с помощью равенств:

$$\nu_{M(QE),1}^*(x) = \sum_{g \in G, N_1(N(g)) \leq x} 1, \quad \nu_{M(QE),2}^*(x) = \sum_{g \in G, N_2(N(g)) \leq x} 1.$$

Необходимо различать две функции $\nu_{M(QE)}(x)$ и $\nu_{M(QE)}^*(x)$, которые задаются равенствами

$$\nu_{M(QE)}(x) = \sum_{n \in M(QE), n \leq x} 1, \quad \nu_{M(QE)}^*(x) = \sum_{g \in G, N(g) \leq x} 1.$$

Ясно, что $\nu_{M(QE)}(x) \leq \nu_{M(QE)}^*(x)$, так как при гомоморфизме $N(g)$ некоторые элементы могут "склеиваться". Таким образом, $\nu_{M(QE)}^*(x)$ подсчитывает элементы в $M(QE)$ с учетом кратности, а $\nu_{M(QE)}(x)$ — без учёта кратности.

ЛЕММА 6. *Справедливы неравенства:*

для любого $n \in M(QE)$ имеем $N_1(n) \leq n \leq N_2(n)$,

$$\nu_{M(QE),2}(x) \leq \nu_{M(QE)}(x) \leq \nu_{M(QE),1}(x), \quad \nu_{M(QE),2}^*(x) \leq \nu_{M(QE)}^*(x) \leq \nu_{M(QE),1}^*(x).$$

ДОКАЗАТЕЛЬСТВО. Дословно повторяет доказательство леммы 4. $\square$

Аналогом леммы 5 будет следующая лемма.

ЛЕММА 7. *Справедливы равенства*

$$\nu_{M(PE),1}^*(x) = P_1 \left(\frac{\ln x}{\ln q} \right), \quad \nu_{M(PE),2}^*(x) = P_2 \left(\frac{\ln x}{\ln q} \right).$$

ДОКАЗАТЕЛЬСТВО. Действительно, если $N_1(N(g)) = q^m$, то $m = \sum_{\nu=1}^n j_\nu \beta_\nu$. Отсюда следует, что количество $g \in G$, таких что $N_1(N(g)) = q^m$, в точности равно $p_1(m)$. Так как из $N_1(N(g)) = q^m \leq x$ следует, что $m \leq \frac{\ln x}{\ln q}$, то первое равенство доказано. Второе равенство доказывается аналогично. $\square$

Обозначим через $\mathbb{PE}_q$ множество всех экспоненциальных последовательностей простых типа q , а через $\mathbb{QE}_q$ множество всех экспоненциальных последовательностей типа q .

ЛЕММА 8. *Для мощностей множеств $\mathbb{PE}_q$ и $\mathbb{QE}_q$ справедливо равенство*

$$|\mathbb{PE}_q| = |\mathbb{QE}_q| = \mathfrak{c}.$$

ДОКАЗАТЕЛЬСТВО. Действительно, рассмотрим множество Δ всех бесконечных последовательностей из 0 и 1. Как известно, его мощность — континуум: $|\Delta| = \mathfrak{c}$. Каждой последовательности $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n, \dots) \in \Delta$ поставим в соответствие экспоненциальную последовательность QE_ε типа q , заданную равенством

$$QE_\varepsilon = \{q + \varepsilon_1, q^2 + \varepsilon_2, \dots, q^n + \varepsilon_n, \dots\}.$$

Так как все такие последовательности различные, то мощность множества всех экспоненциальных последовательностей типа q — континуум.

Из асимптотического закона распределения простых чисел вытекает, что для любого натурального $q \geq 2$ найдутся две экспоненциальные последовательности простых типа q , пусть это

$$PE_1 = \{p_{1,1} < p_{1,2} < \dots < p_{1,n} < \dots\}, \quad PE_2 = \{p_{2,1} < p_{2,2} < \dots < p_{2,n} < \dots\},$$

такие, что начиная с некоторого номера n_0 имеем $p_{1,n} \neq p_{2,n}$ при $n \geq n_0$. Каждой последовательности $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n, \dots) \in \Delta$ поставим в соответствие экспоненциальную последовательность простых PE_ε типа q , заданную равенством

$$PE_\varepsilon = \{\varepsilon_1 p_{1,1} + (1 - \varepsilon_1) p_{2,1}, \varepsilon_2 p_{1,2} + (1 - \varepsilon_2) p_{2,2}, \dots, \varepsilon_n p_{1,n} + (1 - \varepsilon_n) p_{2,n}, \dots\}.$$

Так как любые две такие последовательности различные, если существует $n \geq n_0$ такое, что элементы ε для этого номера различные, то мощность множества всех экспоненциальных последовательностей простых типа q — континуум. $\square$

Для дальнейшего нам потребуется экспоненциальная последовательность $QE_1(q, a)$ типа q , заданная равенством

$$QE_1(q, a) = \left\{ q + q \left\{ \frac{a}{q} \right\}, q^2 + q^2 \left\{ \frac{a}{q^2} \right\}, \dots, q^n + q^n \left\{ \frac{a}{q^n} \right\}, \dots \right\},$$

и последовательность $QE_2(q, a)$ типа q , заданная равенством

$$QE_2(q, a) = \left\{ q^2 - q \left\{ \frac{a}{q} \right\}, q^3 - q^2 \left\{ \frac{a}{q^2} \right\}, \dots, q^{n+1} - q^n \left\{ \frac{a}{q^n} \right\}, \dots \right\},$$

Заметим, что при $n > \frac{\ln a}{\ln q}$ справедливо равенство $q^n + q^n \left\{ \frac{a}{q^n} \right\} = q^n + a$ и равенство $q^{n+1} - q^n \left\{ \frac{a}{q^n} \right\} = q^{n+1} - a$.

5. Следствия из аддитивной теоремы Ингама

Нам потребуется следующая аддитивная теорема Ингама (см. [23], стр. 180).

ТЕОРЕМА 5. Пусть $0 < \lambda_1 < \lambda_2 < \dots$ — данная последовательность вещественных чисел, причём

$$N(u) = Bu^\beta + R(u), \quad B > 0, \quad \beta > 0,$$

где $N(u)$ — количество чисел λ_ν , не превосходящих u , и

$$\int_0^u \frac{R(v)}{v} dv = b \ln u + c + o(1)$$

при $u \rightarrow \infty$. Для вещественного l пусть будет $p(l)$ — количество решений уравнения

$$l = r_1 \lambda_1 + r_2 \lambda_2 + \dots$$

в целых $r_\nu \geq 0$.

Обозначим для вещественного u и $h > 0$

$$P(u) = \sum_{l < u} p(l),$$

где суммирование ведётся по дискретному множеству чисел l , для которых $p(l) \neq 0$, и

$$P_h(u) = \frac{P(u) - P(u - h)}{h}.$$

Тогда при $u \rightarrow \infty$

$$P(u) \sim \left(\frac{1-\alpha}{2\pi} \right)^{\frac{1}{2}} e^c M^{-(b+\frac{1}{2})\alpha} u^{(b+\frac{1}{2})(1-\alpha)-\frac{1}{2}} e^{\frac{1}{\alpha}(Mu)^\alpha},$$

где

$$\alpha = \frac{\beta}{\beta+1}, \quad M = (B\beta\Gamma(\beta+1)\zeta(\beta+1))^{\frac{1}{\beta}}.$$

Также

$$P_h(u) \sim \left(\frac{1-\alpha}{2\pi} \right)^{\frac{1}{2}} e^c M^{-(b-\frac{1}{2})\alpha} u^{(b-\frac{1}{2})(1-\alpha)-\frac{1}{2}} e^{\frac{1}{\alpha}(Mu)^\alpha},$$

где h — такая положительная константа, что $P_h(u)$ есть неубывающая функция и (если h принадлежит к данной последовательности λ_ν , то это условие выполняется).

СЛЕДСТВИЕ 1. При $x \rightarrow \infty$ справедливы соотношения

$$P_1(x) \sim \frac{1}{2\pi\sqrt{2x}} e^{\pi\sqrt{\frac{2}{3}x}}, \quad \nu_{M(PE),1}(x) \sim \frac{1}{2\pi\sqrt{2\frac{\ln x}{\ln q}}} e^{\pi\sqrt{\frac{2}{3}\frac{\ln x}{\ln q}}}.$$

ДОКАЗАТЕЛЬСТВО. Положим $\lambda_\nu = \nu$ ($\nu = 1, 2, \dots$), тогда $N(u) = [u]$, $R(u) = [u] - u$, $B = \beta = 1$, $\alpha = \frac{1}{2}$, $M = \zeta(2) = \frac{\pi^2}{6}$ и (см. [23], стр. 181)

$$\int_0^u \frac{R(v)}{v} dv = -\frac{1}{2} \ln u - \frac{1}{2} \ln 2\pi + o(1).$$

Таким образом, $b = -\frac{1}{2}$, $c = -\frac{1}{2} \ln 2\pi$. Поэтому по аддитивной теореме Ингама получим

$$P_1(x) \sim \left(\frac{1}{4\pi} \right)^{\frac{1}{2}} e^{-\frac{\ln 2\pi}{2}} x^{-\frac{1}{2}} e^{2\left(\frac{\pi^2}{6}x\right)^{\frac{1}{2}}} = \frac{1}{2\pi\sqrt{2x}} e^{\pi\sqrt{\frac{2}{3}x}}.$$

Отсюда следует, что

$$\nu_{M(PE),1}(x) = P_1\left(\frac{\ln x}{\ln q}\right) \sim \frac{1}{2\pi\sqrt{2\frac{\ln x}{\ln q}}} e^{\pi\sqrt{\frac{2}{3}\frac{\ln x}{\ln q}}}.$$

□

СЛЕДСТВИЕ 2. При $x \rightarrow \infty$ справедливы соотношения

$$P_2(x) \sim \frac{1}{4\sqrt{3}x} e^{\pi\sqrt{\frac{2}{3}x}}, \quad \nu_{M(PE),2}(x) \sim \frac{\ln q}{4\sqrt{3}\ln x} e^{\pi\sqrt{\frac{2}{3}\frac{\ln x}{\ln q}}}.$$

ДОКАЗАТЕЛЬСТВО. Положим $\lambda_\nu = \nu + 1$ ($\nu = 1, 2, \dots$), $f(u) = [u] - 1$, тогда

$$N(u) = \begin{cases} 0, & \text{при } 0 \leq u \leq 1, \\ f(u), & \text{при } u \geq 1, \end{cases} \quad R(u) = \begin{cases} -u, & \text{при } 0 \leq u \leq 1, \\ f(u) - u, & \text{при } u \geq 1, \end{cases}$$

$B = \beta = 1$, $\alpha = \frac{1}{2}$, $M = \zeta(2) = \frac{\pi^2}{6}$ и

$$\int_0^u \frac{R(v)}{v} dv = -\frac{3}{2} \ln u - \frac{1}{2} \ln 2\pi + o(1).$$

Таким образом, $b = -\frac{3}{2}$, $c = -\frac{1}{2} \ln 2\pi$. Поэтому по аддитивной теореме Ингама получим

$$P_2(x) \sim \left(\frac{1}{4\pi}\right)^{\frac{1}{2}} e^{-\frac{\ln 2\pi}{2}} \left(\frac{\pi^2}{6}\right)^{\frac{1}{2}} x^{-1} e^{2\left(\frac{\pi^2}{6}x\right)^{\frac{1}{2}}} = \frac{1}{4\sqrt{3}x} e^{\pi\sqrt{\frac{2}{3}x}}.$$

Отсюда следует, что

$$\nu_{M(PE),2}(x) = P_2\left(\frac{\ln x}{\ln q}\right) \sim \frac{\ln q}{4\sqrt{3} \ln x} e^{\pi\sqrt{\frac{2}{3} \frac{\ln x}{\ln q}}}.$$

□

СЛЕДСТВИЕ 3. При $x \rightarrow \infty$ справедливы соотношения

$$\nu_{M(QE_1(q,1))}(x) \sim \frac{\sqrt{\ln q}}{2\pi e^{c(q)} \sqrt{2 \ln x}} e^{\pi\sqrt{\frac{2}{3} \frac{\ln x}{\ln q}}}.$$

ДОКАЗАТЕЛЬСТВО. Положим $\lambda_\nu = \ln(q^\nu + 1) = \nu \ln q + \ln\left(1 + \frac{1}{q^\nu}\right)$ ($\nu = 1, 2, \dots$), тогда

$$N(u) = \frac{u}{\ln q} + R(u) = \begin{cases} 0, & \text{при } 0 \leq u < \lambda_1, \\ \nu, & \text{при } \lambda_\nu \leq u < \lambda_{\nu+1}, \end{cases} \quad R(u) = \begin{cases} -\frac{u}{\ln q}, & \text{при } 0 \leq u < \lambda_1, \\ \nu - \frac{u}{\ln q}, & \text{при } \lambda_\nu \leq u < \lambda_{\nu+1}, \end{cases}$$

$B = \frac{1}{\ln q}$, $\beta = 1$, $\alpha = \frac{1}{2}$, $M = \frac{\zeta(2)}{\ln q} = \frac{\pi^2}{6 \ln q}$ и при $\lambda_n \leq u < \lambda_{n+1}$

$$\begin{aligned} \int_0^u \frac{R(v)}{v} dv &= -\frac{u}{\ln q} + \sum_{\nu=1}^{n-1} \nu \ln \frac{\lambda_{\nu+1}}{\lambda_\nu} + n \ln \frac{u}{\lambda_n} = -\frac{u}{\ln q} - \sum_{\nu=1}^n \ln \lambda_\nu + n \ln u = \\ &= n \ln u - \frac{u}{\ln q} - \sum_{\nu=1}^n \left(\ln \nu + \ln \ln q + \ln \left(1 + \frac{\ln\left(1 + \frac{1}{q^\nu}\right)}{\nu \ln q} \right) \right). \end{aligned}$$

Заметим, что $u = n \ln q + \theta(u)$, $\ln\left(1 + \frac{1}{q^n}\right) \leq \theta(u) < \ln q + \ln\left(1 + \frac{1}{q^{n+1}}\right)$, $\ln u = \ln n + \ln \ln q + \ln\left(1 + \frac{\theta(u)}{n \ln q}\right)$,

$$\ln n + \ln \ln q + \ln\left(1 + \frac{\ln\left(1 + \frac{1}{q^n}\right)}{n \ln q}\right) \leq \ln u < \ln n + \ln\left(1 + \frac{1}{n}\right) + \ln \ln q + \ln\left(1 + \frac{\ln\left(1 + \frac{1}{q^{n+1}}\right)}{(n+1) \ln q}\right). \quad (11)$$

Применим формулу Стирлинга

$$\sum_{\nu=1}^n \ln \nu = \frac{1}{2} (\ln 2\pi + \ln n) + n \ln n - n + \frac{1}{12n + \theta_n},$$

где $0 < \theta_n < 1$. Получим

$$\begin{aligned} \int_0^u \frac{R(v)}{v} dv &= n \ln n + n \ln \ln q + n \ln\left(1 + \frac{\theta(u)}{n \ln q}\right) - n - \frac{\theta(u)}{\ln q} - \\ &- \left(\frac{1}{2} (\ln 2\pi + \ln n) + n \ln n - n + \frac{1}{12n + \theta_n} \right) - n \ln \ln q - \sum_{\nu=1}^n \ln\left(1 + \frac{\ln\left(1 + \frac{1}{q^\nu}\right)}{\nu \ln q}\right) = \\ &= n \ln\left(1 + \frac{\theta(u)}{n \ln q}\right) - \frac{\theta(u)}{\ln q} - \frac{1}{2} \ln 2\pi - \frac{\ln n}{2} - \frac{1}{12n + \theta_n} - \sum_{\nu=1}^n \ln\left(1 + \frac{\ln\left(1 + \frac{1}{q^\nu}\right)}{\nu \ln q}\right). \end{aligned}$$

Так как $n \ln \left(1 + \frac{\theta(u)}{n \ln q}\right) - \frac{\theta(u)}{\ln q} = O\left(\frac{\theta^2(u)}{n \ln^2 q}\right)$, $\frac{\ln n}{2} = \frac{\ln u}{2} - \frac{\ln \ln q}{2} + O\left(\frac{1}{n}\right)$, сходится ряд

$$c(q) = \sum_{\nu=1}^{\infty} \ln \left(1 + \frac{\ln \left(1 + \frac{1}{q^\nu}\right)}{\nu \ln q}\right)$$

и для остаточного ряда справедливо асимптотическое равенство

$$\sum_{\nu=n+1}^{\infty} \ln \left(1 + \frac{\ln \left(1 + \frac{1}{q^\nu}\right)}{\nu \ln q}\right) = O\left(\frac{1}{n q^n}\right),$$

то справедливо асимптотическое равенство

$$\int_0^u \frac{R(v)}{v} dv = -\frac{\ln u}{2} + \frac{\ln \ln q}{2} - \frac{1}{2} \ln 2\pi - c(q) + O\left(\frac{1}{n}\right).$$

Таким образом, $b = -\frac{1}{2}$, $c = \frac{\ln \ln q}{2} - \frac{1}{2} \ln 2\pi - c(q)$. Поэтому по аддитивной теореме Ингама получим

$$P(x) \sim \left(\frac{1}{4\pi}\right)^{\frac{1}{2}} e^{\frac{\ln \ln q}{2} - \frac{\ln 2\pi}{2} - c(q)} x^{-\frac{1}{2}} e^{2\left(\frac{\pi^2}{6 \ln q} x\right)^{\frac{1}{2}}} = \frac{\sqrt{\ln q}}{2\pi e^{c(q)} \sqrt{2x}} e^{\pi \sqrt{\frac{2}{3 \ln q} x}}.$$

Отсюда следует, что, так как для $q_\nu = q^\nu + 1$ неравенство

$$\prod_{\nu=1}^m q_{j_\nu}^{\beta_\nu} \leq x$$

равносильно неравенству

$$\sum_{\nu=1}^m \lambda_{j_\nu} \beta_\nu \leq \ln x,$$

то $\nu_{M(QE_1(q,1))}(x) = P(\ln x)$ и

$$\nu_{M(QE_1(q,1))}(x) = P(\ln x) \sim \frac{\sqrt{\ln q}}{2\pi e^{c(q)} \sqrt{2 \ln x}} e^{\pi \sqrt{\frac{2}{3} \frac{\ln x}{\ln q}}}.$$

□

СЛЕДСТВИЕ 4. При $x \rightarrow \infty$ справедливы соотношения

$$\nu_{M(QE_2(q,1))}(x) \sim \frac{\sqrt{\ln^3 q}}{2\pi e^{c_1(q)} \sqrt{2x}} e^{\pi \sqrt{\frac{2}{3} \frac{\ln x}{\ln q}}}.$$

ДОКАЗАТЕЛЬСТВО. Положим $\lambda_\nu = \ln(q^{\nu+1} - 1) = (\nu + 1) \ln q + \ln\left(1 - \frac{1}{q^{\nu+1}}\right)$ ($\nu = 1, 2, \dots$), тогда

$$N(u) = \frac{u}{\ln q} + R(u) = \begin{cases} 0, & \text{при } 0 \leq u < \lambda_1, \\ \nu, & \text{при } \lambda_\nu \leq u < \lambda_{\nu+1}, \end{cases} \quad R(u) = \begin{cases} -\frac{u}{\ln q}, & \text{при } 0 \leq u < \lambda_1, \\ \nu - \frac{u}{\ln q}, & \text{при } \lambda_\nu \leq u < \lambda_{\nu+1}, \end{cases}$$

$B = \frac{1}{\ln q}$, $\beta = 1$, $\alpha = \frac{1}{2}$, $M = \frac{\zeta(2)}{\ln q} = \frac{\pi^2}{6 \ln q}$ и при $\lambda_n \leq u < \lambda_{n+1}$

$$\begin{aligned} \int_0^u \frac{R(v)}{v} dv &= -\frac{u}{\ln q} + \sum_{\nu=1}^{n-1} \nu \ln \frac{\lambda_{\nu+1}}{\lambda_\nu} + n \ln \frac{u}{\lambda_n} = -\frac{u}{\ln q} - \sum_{\nu=1}^n \ln \lambda_\nu + n \ln u = \\ &= n \ln u - \frac{u}{\ln q} - \sum_{\nu=1}^n \left(\ln(\nu + 1) + \ln \ln q + \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{\nu+1}}\right)}{(\nu + 1) \ln q}\right) \right). \end{aligned}$$

Заметим, что $u = (n+1) \ln q + \theta(u)$, $\ln \left(1 - \frac{1}{q^{n+1}}\right) \leq \theta(u) < \ln q + \ln \left(1 - \frac{1}{q^{n+2}}\right)$, $\ln u = \ln(n+1) + \ln \ln q + \ln \left(1 + \frac{\theta(u)}{(n+1) \ln q}\right)$,

$$\ln(n+1) + \ln \ln q + \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{n+1}}\right)}{(n+1) \ln q}\right) \leq \ln u < \ln(n+1) + \ln \left(1 + \frac{1}{n+1}\right) + \ln \ln q + \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{n+2}}\right)}{(n+2) \ln q}\right).$$

Применим формулу Стирлинга

$$\sum_{\nu=1}^n \ln(\nu+1) = \frac{1}{2} (\ln 2\pi + \ln(n+1)) + (n+1) \ln(n+1) - (n+1) + \frac{1}{12(n+1) + \theta_{n+1}},$$

где $0 < \theta_{n+1} < 1$. Получим

$$\begin{aligned} \int_0^u \frac{R(v)}{v} dv &= n \ln(n+1) + n \ln \ln q + n \ln \left(1 + \frac{\theta(u)}{(n+1) \ln q}\right) - (n+1) - \frac{\theta(u)}{\ln q} - \\ &- \left(\frac{1}{2} (\ln 2\pi + \ln(n+1)) + (n+1) \ln(n+1) - (n+1) + \frac{1}{12(n+1) + \theta_{n+1}}\right) - n \ln \ln q - \\ &- \sum_{\nu=1}^n \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{\nu+1}}\right)}{(\nu+1) \ln q}\right) = n \ln \left(1 + \frac{\theta(u)}{(n+1) \ln q}\right) - \frac{\theta(u)}{\ln q} - \frac{1}{2} \ln 2\pi - \frac{3 \ln(n+1)}{2} - \\ &- \frac{1}{12(n+1) + \theta_{n+1}} - \sum_{\nu=1}^n \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{\nu+1}}\right)}{(\nu+1) \ln q}\right). \end{aligned}$$

Так как $n \ln \left(1 + \frac{\theta(u)}{(n+1) \ln q}\right) - \frac{\theta(u)}{\ln q} = O\left(\frac{\theta(u)}{n \ln q}\right)$, $\frac{3 \ln(n+1)}{2} = \frac{3 \ln u}{2} - \frac{3 \ln \ln q}{2} + O\left(\frac{1}{n}\right)$, сходится ряд

$$c_1(q) = \sum_{\nu=1}^{\infty} \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{\nu+1}}\right)}{(\nu+1) \ln q}\right)$$

и для остаточного ряда справедливо асимптотическое равенство

$$\sum_{\nu=n+1}^{\infty} \ln \left(1 + \frac{\ln \left(1 - \frac{1}{q^{\nu+1}}\right)}{(\nu+1) \ln q}\right) = O\left(\frac{1}{n q^n}\right),$$

то справедливо асимптотическое равенство

$$\int_0^u \frac{R(v)}{v} dv = -\frac{3 \ln u}{2} + \frac{3 \ln \ln q}{2} - \frac{1}{2} \ln 2\pi - c_1(q) + O\left(\frac{1}{n}\right).$$

Таким образом, $b = -\frac{3}{2}$, $c = \frac{3 \ln \ln q}{2} - \frac{1}{2} \ln 2\pi - c_1(q)$. Поэтому по аддитивной теореме Ингама получим

$$P(x) \sim \left(\frac{1}{4\pi}\right)^{\frac{1}{2}} e^{\frac{3 \ln \ln q}{2} - \frac{\ln 2\pi}{2} - c_1(q)} x^{-1} e^{2\left(\frac{\pi^2}{6 \ln q} x\right)^{\frac{1}{2}}} = \frac{\sqrt{\ln^3 q}}{2\pi e^{c_1(q)} \sqrt{2x}} e^{\pi \sqrt{\frac{2}{3 \ln q} x}}.$$

Отсюда следует, что, так как для $q_\nu = q^{\nu+1} - 1$ неравенство

$$\prod_{\nu=1}^m q_{j_\nu}^{\beta_\nu} \leq x$$

равносильно неравенству

$$\sum_{\nu=1}^m \lambda_{j_\nu} \beta_\nu \leq \ln x,$$

то $\nu_{M(QE_2(q,1))}(x) = P(\ln x)$ и

$$\nu_{M(QE_2(q,1))}(x) = P(\ln x) \sim \frac{\sqrt{\ln^3 q}}{2\pi e^{c_1(q)} \sqrt{2x}} e^{\pi \sqrt{\frac{2}{3} \frac{\ln x}{\ln q}}}.$$

□

Перейдём к изучению более сложного случая поведения функции $\nu_{M(PE)}(x)$.

Через λ_ν обозначим $\ln p_\nu$, где простые числа p_ν образуют экспоненциальную систему PE типа q . Ясно, что величина $N(u)$ выражается через величину $\pi_{PE}(x)$ по следующей формуле

$$N(u) = \pi_{PE}(e^u).$$

Действительно, $\lambda_\nu < u$ тогда и только тогда, когда $p_\nu = e^{\lambda_\nu} < e^u$.

Из теоремы 2 получаем, что

$$N(u) = \frac{u}{\ln q} + R(u), \quad R(u) = -\left\{ \frac{u}{\ln q} - \frac{\ln p_n}{\ln q} \right\} - \left\{ \frac{\ln p_n}{\ln q} \right\}$$

при $n \ln q \leq u < (n+1) \ln q$. Следовательно, $B = \frac{1}{\ln q}$, $\beta = 1$. Нам необходимо изучить поведение интеграла $\int_0^u \frac{R(v)}{v} dv$. Сложность заключается в том, что $\nu \ln q \leq \lambda_\nu < (\nu+1) \ln q$ и более тесных границ для произвольной экспоненциальной последовательности простых задать нельзя. Анализируя доказательства предыдущих следствий, мы видим, что существенную роль играет поведение величин $\delta_\nu = \frac{\lambda_\nu - \nu \ln q}{\nu \ln q}$, $\frac{\ln(1 + \frac{1}{q^\nu})}{\nu \ln q} \leq \delta_\nu \leq \frac{\ln q + \ln(1 - \frac{1}{q^{\nu+1}})}{\nu \ln q}$ и суммы

$$S_n(PE, q) = \sum_{\nu=1}^n \ln(1 + \delta_\nu), \quad c(q) - O\left(\frac{1}{n}\right) \leq S_n(PE, q) \leq \ln n + O(1).$$

ЛЕММА 9. *Справедливо равенство*

$$\int_0^u \frac{R(v)}{v} dv = -\frac{\ln u}{2} + \frac{\ln \ln q}{2} - \frac{1}{2} \ln 2\pi + O\left(\frac{1}{n}\right) - S_n(PE, q).$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим поведение функции $R(v)$ на различных интервалах изменения.

При $0 \leq v < \lambda_1 = \ln p_1$ имеем $N(v) = 0$,

$$R(v) = \begin{cases} -\frac{v}{\ln q}, & \text{при } 0 \leq v < \ln q, \\ -1 - \left\{ \frac{v}{\ln q} \right\} = -\frac{v}{\ln q}, & \text{при } \ln q \leq v < \lambda_1, \end{cases} \quad \int_0^u \frac{R(v)}{v} dv = -\frac{u}{\ln q}.$$

При $\lambda_n \leq v < \lambda_{n+1}$ ($n = 1, 2, \dots$) имеем $N(v) = n$, $R(v) = -\frac{v}{\ln q} + n$. Отсюда следует, что

при $\lambda_n \leq u < \lambda_{n+1}$ имеем:

$$\begin{aligned} \int_0^u \frac{R(v)}{v} dv &= -\frac{\lambda_1}{\ln q} + \sum_{\nu=1}^{n-1} \int_{\lambda_\nu}^{\lambda_{\nu+1}} \frac{R(v)}{v} dv + \int_{\lambda_n}^u \frac{R(v)}{v} dv = -\frac{\lambda_1}{\ln q} - \sum_{\nu=1}^{n-1} \left(\frac{\lambda_{\nu+1} - \lambda_\nu}{\ln q} - \nu \ln \frac{\lambda_{\nu+1}}{\lambda_\nu} \right) - \\ &- \left(\frac{u - \lambda_n}{\ln q} - n \ln \frac{u}{\lambda_n} \right) = -\frac{u}{\ln q} - \sum_{\nu=1}^n \ln \lambda_\nu + n \ln u = n \ln u - \frac{u}{\ln q} - \sum_{\nu=1}^n (\ln \nu + \ln \ln q) - \\ &- \sum_{\nu=1}^n \ln(1 + \delta_\nu) = F(u) - S_n(PE, q), \quad F(u) = n \ln u - \frac{u}{\ln q} - \sum_{\nu=1}^n (\ln \nu + \ln \ln q). \end{aligned}$$

Заметим, что $u = n \ln q + \theta(u)$, $0 < \lambda_n - n \ln q \leq \theta(u) < \lambda_{n+1} - n \ln q < \ln q$, $\ln u = \ln n + \ln \ln q + \ln \left(1 + \frac{\theta(u)}{n \ln q}\right)$, поэтому как и при доказательстве следствия 3 получим

$$F(u) = n \ln \left(1 + \frac{\theta(u)}{n \ln q}\right) - \frac{\theta(u)}{\ln q} - \frac{1}{2} \ln 2\pi - \frac{\ln n}{2} - \frac{1}{12n + \theta_n}.$$

Так как $n \ln \left(1 + \frac{\theta(u)}{n \ln q}\right) - \frac{\theta(u)}{\ln q} = O\left(\frac{\theta^2(u)}{n \ln^2 q}\right)$, $\frac{\ln n}{2} = \frac{\ln u}{2} - \frac{\ln \ln q}{2} + O\left(\frac{1}{n}\right)$, то

$$\begin{aligned} F(u) &= -\frac{\ln u}{2} + \frac{\ln \ln q}{2} - \frac{1}{2} \ln 2\pi + O\left(\frac{1}{n}\right), \\ \int_0^u \frac{R(v)}{v} dv &= -\frac{\ln u}{2} + \frac{\ln \ln q}{2} - \frac{1}{2} \ln 2\pi + O\left(\frac{1}{n}\right) - S_n(PE, q). \end{aligned}$$

□

Из доказанной леммы следует, что мы не можем непосредственно применить аддитивную теорему Ингама для получения асимптотики величины $\nu_{M(PE)}(x)$ для произвольной экспоненциальной последовательности простых PE типа q .

СЛЕДСТВИЕ 5. При $x \rightarrow \infty$ справедливы соотношения

$$\ln \nu_{M(PE)}(x) \sim \pi \sqrt{\frac{2 \ln x}{3 \ln q}}.$$

ДОКАЗАТЕЛЬСТВО. Согласно лемме 4

$$\nu_{M(PE),2}(x) \leq \nu_{M(PE)}(x) \leq \nu_{M(PE),1}(x).$$

Следовательно,

$$\ln \nu_{M(PE),2}(x) \leq \ln \nu_{M(PE)}(x) \leq \ln \nu_{M(PE),1}(x).$$

Из следствия 1 вытекает, что

$$\ln \nu_{M(PE),1}(x) \sim \pi \sqrt{\frac{2 \ln x}{3 \ln q}}.$$

Из следствия 2 вытекает, что

$$\ln \nu_{M(PE),2}(x) \sim \pi \sqrt{\frac{2 \ln x}{3 \ln q}}.$$

Объединяя оба доказанных соотношения, получаем утверждение следствия. □

6. Заключение

В работе [6] и ряде последующих Б. М. Бредихин работал с понятием степенной плотности последовательности. Из следствий 1–5 видно, что это понятие не работает в случае моноидов, образованных произвольной экспоненциальной последовательностью простых. Естественно дать новое определение.

ОПРЕДЕЛЕНИЕ 5. *Последовательность M натуральных чисел имеет C логарифмическую θ -степенную плотность, если для функции $\nu_M(x)$, заданной равенством*

$$\nu_M(x) = \sum_{n \in M, n \leq x} 1,$$

справедливо равенство

$$\lim_{x \rightarrow \infty} \frac{\ln \nu_M(x)}{\ln^\theta x} = C, \quad C > 0, \quad \theta > 0.$$

Из следствия 5 следует, что любой моноид $M(PE)$ для произвольной экспоненциальной последовательности простых PE типа q имеет C логарифмическую θ -степенную плотность с $C = \pi \sqrt{\frac{2}{3 \ln q}}$ и $\theta = \frac{1}{2}$.

В заключение авторы выражают свою благодарность профессору В. Н. Чубарикову за полезные обсуждения и внимание к работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Э. Бомбьери, А. Гош Вокруг функции Дэвенпорта–Хейльбронна // УМН, 2011. Т. 66, вып. 2(398). С. 15–66.
2. Б. М. Бредихин, “Остаточный член в асимптотической формуле для функции $\nu_G(x)$ ”, Изв. вузов. Матем., 1960, 6, 40–49.
3. Б. М. Бредихин, “Элементарное решение обратных задач о базисах свободных полугрупп”, Матем. сб., 50(92):2 (1960), 221–232.
4. Б. М. Бредихин, “Свободные числовые полугруппы со степенными плотностями”, Докл. АН СССР, 118:5 (1958), 855–857.
5. Б. М. Бредихин, “О степенных плотностях некоторых подмножеств свободных полугрупп”, Изв. вузов. Матем., 1958, 3, 24–30.
6. Б. М. Бредихин, “Свободные числовые полугруппы со степенными плотностями”, Матем. сб., 46(88):2 (1958), 143–158.
7. Б. М. Бредихин, “Пример конечного гомоморфизма с ограниченной сумматорной функцией”, УМН, 11:4(70) (1956), 119–122.
8. Б. М. Бредихин, Некоторые вопросы теории характеров коммутативных полугрупп, Труды 3-го Всесоюз. матем. съезда, т. I, Москва, Изд. АН СССР (1956), 3.
9. Б. М. Бредихин, О сумматорных функциях характеров числовых полугрупп, ДАН 94 (1954), 609 — 612.
10. Б. М. Бредихин, О характерах числовых полугрупп с достаточно редкой базой, ДАН 90 (1953), 707 — 710.

11. Воронин С. М., Карацуба А. А. Дзета-функция Римана. — М.: Физ-матлит, 1994. — 376 с.
12. Гурвиц А., Курант Р. Теория функций. — М.: Наука, 1968. — 618 с.
13. Демидов С. С., Морозова Е. А., Чубариков В. Н., Реброва И. Ю., Балаба И. Н., Добровольский Н. Н., Добровольский Н. М., Добровольская Л. П., Родионов А. В., Пихтилькова О. А. Теоретико-числовой метод в приближенном анализе // Чебышевский сб. 2017. — Т. 18, вып. 4. — С. 6–85.
14. Н. Н. Добровольский Дзета-функция моноидов натуральных чисел с однозначным разложением на простые множители // Чебышевский сб. 2017. Т. 18, вып. 4. С. 187–207.
15. Добровольский Н. Н. О моноидах натуральных чисел с однозначным разложением на простые элементы // Чебышевский сб. 2018. — Т. 19, вып. 1. — С. 79–105.
16. Добровольский Н. Н. Дзета-функция моноидов с заданной абсциссой абсолютной сходимости // Чебышевский сб. 2018. — Т. 19, вып. 2. — С. 142–150.
17. Добровольский Н. Н. Одна модельная дзета-функция моноида натуральных чисел // Чебышевский сборник. 2019. — Т. 20, вып. 1, С. 148–163.
18. Добровольский Н. Н., Добровольский М. Н., Добровольский Н. М., Балаба И. Н., Реброва И. Ю. Гипотеза о "заградительном ряде" для дзета-функций моноидов с экспоненциальной последовательностью простых // Чебышевский сб. 2018. — Т. 19, вып. 1. — С. 106–123.
19. Н. Н. Добровольский, М. Н. Добровольский, Н. М. Добровольский, И. Н. Балаба, И. Ю. Реброва. Алгебра рядов Дирихле моноида натуральных чисел // Чебышевский сборник. 2019. Т. 20, вып. 1, С. 180–196.
20. Н. Н. Добровольский, Н. М. Добровольский, И. Ю. Реброва, А. В. Родионов. Моноиды натуральных чисел в теоретико-числовом методе в приближенном анализе // Чебышевский сборник. 2019. Т. 20, вып. 1. С. 164–179.
21. Добровольский Н. Н., Калинина А. О., Добровольский М. Н., Добровольский Н. М. О количестве простых элементов в некоторых моноидах натуральных чисел // Чебышевский сборник. 2018. — Т. 19, вып. 2. — С. 123–141.
22. Добровольский Н. Н., Калинина А. О., Добровольский М. Н., Добровольский Н. М. О моноиде квадратичных вычетов // Чебышевский сборник. 2018. — Т. 19, вып. 3. — С. 95–108.
23. А. Г. Постников Введение в аналитическую теорию чисел. — М.: Наука, 1971. — 416 с.
24. Е. К. Титчмарш Теория дзета-функции Римана. — М.: И-Л, 1952. — 407 с.
25. Э. Трост Простые числа — М.: ФИЗМАТЛИТ, 1959. — 136 с.
26. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974. — 188 с.
27. Чудаков Н. Г. Введение в теорию L -функций Дирихле. — М. – Л.: ОГИЗ, 1947. — 204 с.
28. Н. Davenport, Н. Heilbronn On the zeros of certain Dirichlet series // J. London Math. Soc. 1936. Vol. 11. P. 181–185.

REFERENCES

1. Bombieria E., Ghoshb A., 2011, "Around the Davenport–Heilbronn function", *Uspekhi Mat. Nauk*, 66:2(398) pp. 15–66.
2. Bredikhin, B.M., 1960, "The remainder term in the asymptotic formula for the function $\nu_G(x)$ ", *Izvestiya vuzov Matematika*, no. 6, pp. 40–49.
3. Bredikhin, B.M., 1960, "An elementary solution of inverse problems on bases of free semigroups", *matematicheskiiy sbornik*, 50(92):2, pp. 221–232.
4. Bredikhin, B.M., 1958, "Free numerical semigroups with power densities", *Doklady Akademii nauk SSSR*, 118:5, pp. 855–857.
5. Bredikhin, B.M., 1958, "On power densities of some subsets of free semigroups", *Izvestiya vuzov Matematika*, no. 3, pp. 24–30.
6. Bredikhin, B.M., 1958, "Free numerical semigroups with power densities", *matematicheskiiy sbornik*, 46(88):2, pp. 143–158.
7. Bredikhin, B.M., 1956, "An example of a finite homomorphism with a bounded adder function", *UMN*, 11:4(70), pp. 119–122.
8. Bredikhin, B.M., 1956, "Some questions of the theory of characters of commutative semigroups", *Trudy 3-go Vsesoyuznogo matematicheskogo s'yezda*, vol. 1, Moskva, izdatel'stvo akademii nauk SSSR, no. 3.
9. Bredikhin, B.M., 1954, "On adder functions of characters of numerical semigroups", *DAN* 94, pp. 609 – 612.
10. Bredikhin, B.M., 1953, "On the characters of numerical semigroups with a rather rare base", *DAN* 90, pp. 707–710.
11. Voronin S. M., Karacuba A. A., 1994, *Dzeta-funkcija Rimana*, Izd-vo Fiz-matlit, Moskva, 376 p.
12. Gurvic A., Kurant R., 1968, *Teoriya funkciy*, Izd-vo Nauka, Moskva, 618 p.
13. Demidov S. S., Morozova E. A., Chubarikov V. N., Rebrov I. Yu., Balaba I. N., Dobrovol'skii N. N., Dobrovol'skii N. M., Dobrovol'skaya L. P., Rodionov A. V., Pikhtil'kova O. A., 2017, "Number-theoretic method in approximate analysis" *Chebyshevskii Sbornik* vol. 18, № 4, pp. 6–85.
14. Dobrovolsky N. N., 2017, "The zeta-function is the monoid of natural numbers with unique factorization", *Chebyshevskii Sbornik*, vol 18, № 4 pp. 188–208.
15. N. N. Dobrovol'skii, 2018, "On monoids of natural numbers with unique factorization into prime elements", *Chebyshevskii sbornik*, vol. 19, no. 1, pp. 79–105.
16. N. N. Dobrovol'skii, 2018, "The zeta function of monoids with a given abscissa of absolute convergence", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 142–150.
17. N. N. Dobrovol'skii, M. N. Dobrovol'skii, N. M. Dobrovol'skii, I. N. Balaba, I. Yu. Rebrova, 2018, "About «zagrobelna the series» for the zeta function of monoids with exponential sequence of simple", *Chebyshevskii sbornik*, vol. 19, no. 1, pp. 106–123.

18. N. N. Dobrovol'skii, M. N. Dobrovol'skii, N. M. Dobrovol'skii, I. N. Balaba, I. Yu. Rebrova, 2019, "Dirichlet series algebra of a monoid of natural numbers", *Chebyshevskii sbornik*, vol. 20, no. 1, pp. 180–196.
19. N. N. Dobrovol'skii, N. M. Dobrovol'skii, I. Yu. Rebrova, A. V. Rodionov, 2019, "Monoids of natural numbers in the numerical-theoretical method in the approximate analysis", *Chebyshevskii sbornik*, vol. 20, no. 1, pp. 164–179.
20. N. N. Dobrovol'skii, A. O. Kalinina, M. N. Dobrovol'skii, N. M. Dobrovol'skii 2018, "On the number of prime elements in certain monoids of natural numbers", *Chebyshevskii sbornik*, vol. 19, no. 2, pp. 123–141.
21. N. N. Dobrovol'skii, A. O. Kalinina, M. N. Dobrovol'skii, N. M. Dobrovol'skii 2018, "On the monoid of quadratic residues", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 95–108.
22. Dobrovol'skaya L. P., Dobrovol'sky M. N., Dobrovol'skii N. M., Dobrovol'sky N. N., 2014, "On Hyperbolic Zeta Function of Lattices", *In: Continuous and Distributed Systems. Solid Mechanics and Its Applications*, Vol. 211. pp. 23–62. DOI:10.1007/978-3-319-03146-0_2.
23. Postnikov, A. G., 1971, *Introduction to analytical number theory* Izd-vo "Nauka", Moskva, 416 p.
24. Titchmarsh E. K., 1952, *Teorija dzeta-funkcii Rimana* Izd-vo I-L, Moskva, 407 p.
25. Trost E., 1959, "Prime numbers", *Izd-vo Fiz-matlit, Moskva*, 136 p.
26. Chandrasekharan K., 1974, *Vvedenie v analiticheskuyu teoriju chisel*, Izd-vo Mir, Moskva, 188 p.
27. Chudakov N. G., 1947, *Introduction to the theory of L-Dirichlet functions* — M.-L.: OGIZ, — 204 p.
28. Davenport H., Heilbronn H., 1936, "On the zeros of certain Dirichlet series", *J. London Math. Soc.* Vol. 11. pp. 181–185.

Получено 18.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512+512.5+512.54+512.54.03

DOI 10.22405/2226-8383-2020-21-1-186-199

Об элементарных теориях алгебраически замкнутых групп

В. Г. Дурнев, О. В. Зеткина, А. И. Зеткина

Дурнев Валерий Георгиевич — доктор физико-математических наук, профессор, Ярославский государственный университет имени П. Г. Демидова (г. Ярославль).

e-mail: durnev@uniyar.ac.ru

Зеткина Оксана Валерьевна — кандидат экономических наук, доцент, Ярославский государственный университет имени П. Г. Демидова (г. Ярославль).

e-mail: ovzetkina@yandex.ru

Зеткина Алена Игоревна — ассистент, Ярославский государственный университет имени П. Г. Демидова (г. Ярославль).

e-mail: ovzetkina@yandex.ru

Аннотация

В статье доказана алгоритмическая неразрешимость позитивных $\forall^2\exists^{24}$ -теории и $\forall^3\exists^2$ -теории любой алгебраически замкнутой группы и класса всех алгебраически замкнутых групп. Установлена разрешимость в любой алгебраически замкнутой группе G каждого уравнения вида

$$w(x_1, \dots, x_n) = g,$$

где $w(x_1, \dots, x_n)$ — непустое несократимое групповое слово от неизвестных $x_1, \dots, x_n$, а g — произвольный элемент группы G .

Ключевые слова: алгебраически замкнутая группа, позитивная теория, уравнение.

Библиография: 8 названий.

Для цитирования:

В. Г. Дурнев, О. В. Зеткина, А. И. Зеткина. Об элементарных теориях алгебраически замкнутых групп // Чебышевский сборник, 2020, т. 21, вып. 1, с. 186–199.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512+512.5+512.54+512.54.03

DOI 10.22405/2226-8383-2020-21-1-186-199

On elementary theories of algebraically closed groups

V. G. Durnev, O. V. Zetkina, A. I. Zetkina

Durnev Valery Georgievch — doctor of physics and mathematics, professor, P. G. Demidov Yaroslavl' University (Yaroslavl').

e-mail: durnev@uniyar.ac.ru

Zetkina Oksana Valerievna — candidate of economic sciences, associate professor, P. G. Demidov Yaroslavl' University (Yaroslavl').

e-mail: ovzetkina@yandex.ru

Zetkina Alena Igorevna — assistant, P. G. Demidov Yaroslavl' University (Yaroslavl').

e-mail: ovzetkina@yandex.ru

Abstract

In paper for any algebraically closed group G , as well as for the class of the algebraically closed groups, we prove algorithmic undecidability of the positive $\forall^2\exists^{24}$ -theory and $\forall^3\exists^2$ -theory. For an arbitrary $g \in G$, we also prove the decidability of the equation of the type

$$w(x_1, \dots, x_n) = g,$$

where $w(x_1, \dots, x_n)$ is a non-empty irreducible word in the unknowns $x_1, \dots, x_n \in G$.

Keywords: algebraically closed group, positive theory, equation.

Bibliography: 8 titles.

For citation:

V. G. Durnev, O. V. Zetkina, A. I. Zetkina, 2020, "On elementary theories of algebraically closed groups", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 186–199.

1. Введение

Понятие *алгебраически замкнутая группа* было введено в работе У. Скотта [1]: группа G называется *алгебраически замкнутой* (*algebraically closed*), если любая система уравнений и неравенств над этой группой

$$\bigwedge_{i=1}^m w_i(x_1, \dots, x_n, g_1, \dots, g_k) = e \text{ и } \bigwedge_{j=1}^p u_j(x_1, \dots, x_n, g_1, \dots, g_k) \neq e,$$

где $w_i(x_1, \dots, x_n, g_1, \dots, g_k)$ ($i = 1, \dots, m$) и $u_j(x_1, \dots, x_n, g_1, \dots, g_k)$ ($j = 1, \dots, p$) — групповые слова от переменных $x_1, \dots, x_n$ и произвольных элементов $g_1, \dots, g_k$ группы G , имеющая решение в некотором расширении этой группы, имеет решение уже в самой группе G . В работе А. Макинтайра [3] такие группы называются *экзистенциально замкнутыми*.

Изучение алгебраически замкнутых групп было начато в работах У. Скотта [1] и Б. Неймана [2]. Особую роль в этих исследованиях сыграла работа А. Макинтайра [3]. Еще в работе Б. Неймана было установлено, что любая алгебраически замкнутая группа является *простой*, поэтому, в частности, *любая нетривиальная вербальная подгруппа алгебраически замкнутой группы совпадает со всей группой*.

В работе У. Скотта [1] наряду с понятием *алгебраически замкнутая группа* (*algebraically closed group*) было введено понятие *слабо алгебраически замкнутая группа* (*weakly algebraically closed group*):

группа G называется *слабо алгебраически замкнутой* (*weakly algebraically closed*), если любая система уравнений над этой группой

$$\bigwedge_{i=1}^m w_i(x_1, \dots, x_n, g_1, \dots, g_k) = e,$$

где $w_i(x_1, \dots, x_n, g_1, \dots, g_k)$ ($i = 1, \dots, m$) — групповые слова от переменных $x_1, \dots, x_n$ и произвольных элементов $g_1, \dots, g_k$ группы G , имеющая решение в некотором расширении $G \leq H$ этой группы, имеет решение уже в самой группе G .

Б. Нейман в работе [2] доказал, что *любая неединичная слабо алгебраически замкнутая группа является алгебраически замкнутой*, т. е. *экзистенциально замкнутой*. При доказательстве Б. Нейман рассматривал достаточно сложную систему уравнений над группой G . Используя результаты работы А. Макинтайра [3], мы предлагаем более прозрачное, на наш взгляд, доказательство этого результата Б. Неймана.

2. Простое доказательство теоремы Б. Неймана

В работе А. Макинтайра [3] доказано, что если G — произвольная группа, а h и g — любые два ее элемента, то

$$G \models (h = e \longrightarrow g = e) \iff \text{существует такое расширение } H \text{ группы } G \\ (G \leq H), \text{ в котором для подходящих элементов } x \text{ и } y \\ \text{выполняется равенство } g = xhx^{-1} \cdot yhy^{-1}.$$

Пусть G — произвольная неединичная *слабо алгебраически замкнутая группа*, а g — ее неединичный элемент.

Рассмотрим произвольную систему Ψ уравнений и неравенств над этой группой

$$\big\&_{i=1}^m w_i(x_1, \dots, x_n, g_1, \dots, g_k) = e \& \big\&_{j=1}^p u_j(x_1, \dots, x_n, g_1, \dots, g_k) \neq e,$$

где $w_i(x_1, \dots, x_n, g_1, \dots, g_k)$ ($i = 1, \dots, m$) и $u_j(x_1, \dots, x_n, g_1, \dots, g_k)$ ($j = 1, \dots, p$) — групповые слова от переменных $x_1, \dots, x_n$ и произвольных элементов $g_1, \dots, g_k$ этой группы. Полагаем

$$\Psi^+ = \big\&_{i=1}^m w_i(x_1, \dots, x_n, g_1, \dots, g_k) = e, \quad \Psi^- = \big\&_{j=1}^p u_j(x_1, \dots, x_n, g_1, \dots, g_k) \neq e.$$

Тогда $\Psi = \Psi^+ \& \Psi^-$.

Полагаем

$$\overline{\Psi} = \Psi^+ \& \overline{\Psi^-},$$

где

$$\overline{\Psi^-} = \big\&_{j=1}^p (y_j u_j(x_1, \dots, x_n, g_1, \dots, g_k) y_j^{-1}) \cdot (z_j u_j(x_1, \dots, x_n, g_1, \dots, g_k) z_j^{-1}) = g.$$

Предположим, что в некотором расширении $G \leq H$ группы G система Ψ имеет решение $h_1, h_2, \dots, h_n$. Тогда

$$H \models \big\&_{i=1}^m w_i(h_1, \dots, h_n, g_1, \dots, g_k) = e \& \big\&_{j=1}^p u_j(h_1, \dots, h_n, g_1, \dots, g_k) \neq e.$$

В силу указанного выше результата из работы [3] А. Макинтайра существует такое расширение $H \leq S$ группы H и элементы $s_1, l_1, \dots, s_p$ и l_p , что

$$S \models \big\&_{i=1}^m w_i(h_1, \dots, h_n, g_1, \dots, g_k) = e \& \\ \big\&_{j=1}^p (s_j u_j(h_1, \dots, h_n, g_1, \dots, g_k) s_j^{-1}) \cdot (l_j u_j(h_1, \dots, h_n, g_1, \dots, g_k) l_j^{-1}) = g.$$

Т.е. в расширении $G \leq S$ группы G система равенств $\overline{\Psi}$ имеет решение $h_1, \dots, h_n, s_1, l_1, \dots, s_p$ и l_p . В силу слабой алгебраической замкнутости группы G система равенств $\overline{\Psi}$ имеет решение $h'_1, \dots, h'_n, s'_1, l'_1, \dots, s'_p$ и l'_p в самой группе G . Значит

$$G \models \big\&_{i=1}^m w_i(h'_1, \dots, h'_n, g_1, \dots, g_k) = e \& \\ \big\&_{j=1}^p (s'_j u_j(h'_1, \dots, h'_n, g_1, \dots, g_k) (s'_j)^{-1}) \cdot (l'_j u_j(h'_1, \dots, h'_n, g_1, \dots, g_k) (l'_j)^{-1}) = g.$$

Так как g — неединичный элемент группы G , то

$$G \models \bigwedge_{i=1}^m w_i(h'_1, \dots, h'_n, g_1, \dots, g_k) = e \text{ и } \bigwedge_{j=1}^p u_j(h'_1, \dots, h'_n, g_1, \dots, g_k) \neq e.$$

Значит $h'_1, \dots, h'_n$ — решение системы уравнений и неравенств Ψ в G . Поэтому группа G является алгебраически замкнутой по У. Скотту или экстенционально замкнутой по А. Макинтайру.

Доказательство использованного выше утверждения в работе А. Макинтайра [3] проводится в рамках комбинаторной теории групп путем рассмотрения нескольких случаев, определяемых возможными порядками элементов g и h . Для предложенного нами выше доказательства результата Б. Неймана достаточно более слабого утверждения: если G — произвольная группа, а h и g — любые два ее неединичных элемента, то *существует такое расширение H группы G ($G \leq H$), в котором для подходящих элементов x, y и z выполняется равенство $g = xhx^{-1} \cdot yhy^{-1} \cdot zhz^{-1}$.*

Для полноты изложения приведем простое доказательство этого факта из монографии Р. Линдона и П. Шуппа [4]. В свободном произведении $G * \langle\langle u \rangle\rangle$ группы G и бесконечной циклической группы $\langle\langle u \rangle\rangle$ элементы

$$guhu^{-1} \text{ и } huhu^{-1}$$

имеют бесконечный порядок. Поэтому группа

$$H = \langle\langle G * \langle\langle u \rangle\rangle, t | guhu^{-1} = t \cdot huhu^{-1} \cdot t^{-1} \rangle\rangle$$

является HNN расширением группы $G * \langle\langle u \rangle\rangle$, а значит группа H — расширение группы G . В группе H выполняется требуемое равенство

$$g = (tht^{-1}) \cdot ((tu)h(tu)^{-1}) \cdot (uhu^{-1}).$$

3. Универсальные формулы на алгебраически замкнутых группах

Для произвольной конечно определенной группы

$$G = \langle\langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle\rangle$$

и любого группового слова $w(a_1, \dots, a_n)$ в алфавите $\{a_1, \dots, a_n\}$ справедлива эквивалентность

$$w(a_1, \dots, a_n) \stackrel{G}{=} e \iff G \models (\forall x_1) \dots (\forall x_n) ((\bigwedge_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e).$$

Поэтому, если для конечно определенной группы G алгоритмически неразрешима проблема равенства, то неразрешима и ее $\forall$ -теория (универсальная теория), а значит и $\exists$ -теория (экстенциональная теория). Однако позитивная теория этой группы может быть разрешима. Например, если GN — конечно определенной группа с алгоритмически неразрешимой проблемой равенства, а F_2 — свободная группа ранга 2, то для конечно определенной группы $GN * F_2$, свободного произведения группы GN и F_2 , проблема равенства алгоритмически неразрешима, а значит неразрешима и ее $\forall$ -теория. Однако, так как среди гомоморфных образов этой группы есть свободная группа F_2 , то из известного результата Ю.И. Мерзлякова [7] следует, что позитивная теория этой группы совпадает с позитивной теорией класса всех групп и с позитивной теорией любой свободной нециклической группы, которая, как доказал Г.С. Макин [5] является алгоритмически разрешимой. Используя результат работы Г.С. Сакердота

[8] вместо конечно определенной группы $GN * F_2$ можно взять и конечно определенную группу $GN * \langle \langle a | a^2 = e \rangle \rangle$ — свободное произведение группы GN и циклической группы второго порядка $\langle \langle a | a^2 = e \rangle \rangle$. Если группа GN имеет задание

$$GN = \langle \langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle \rangle,$$

то группа $GN * \langle \langle a | a^2 = e \rangle \rangle$ имеет “почти такое же” задание:

$$GN * \langle \langle a | a^2 = e \rangle \rangle = \langle \langle a_1, a_2, \dots, a_n, a | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e, a^2 = e \rangle \rangle.$$

Покажем, что *универсальная теория любой алгебраически замкнутой группы GAC совпадает с универсальной теорией класса всех групп*, которая, как хорошо известно, алгоритмически неразрешима. Это достаточно доказать для универсальных формул Φ вида

$$(\forall x_1, \dots, x_n) \left(\bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e \vee \bigvee_{j=1}^q u_j(x_1, \dots, x_n) \neq e \right),$$

так как для любой группы G справедлива эквивалентность:

$$G \models (\forall x_1, \dots, x_n) \left(\bigwedge_{i=1}^m \Psi_i \right) \iff \bigwedge_{i=1}^m G \models (\forall x_1, \dots, x_n) \Psi_i.$$

Универсальную формулу Φ вида

$$(\forall x_1, \dots, x_n) \left(\bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e \vee \bigvee_{j=1}^q u_j(x_1, \dots, x_n) \neq e \right)$$

будем для краткости называть $\forall^n$ -*формулой типа* (p, q) . Часто эти формулы записываются в равносильной форме

$$(\forall x_1, \dots, x_n) \left(\bigwedge_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e \right).$$

Напомним, что $\forall^n$ -*формулы типа* $(1, q)$ называются *квазитождествами*.

Достаточно доказать, что если универсальная формула истинна на алгебраически замкнутой группе GAC , то она истинна и на любой группе.

Предположим противное, т. е. что некоторая универсальная формула указанного вида истинна на алгебраически замкнутой группе GAC , но ложна на некоторой группе G . Тогда

$$G \models (\exists x_1, \dots, x_n) \left(\bigwedge_{i=1}^p w_i(x_1, \dots, x_n) \neq e \wedge \bigwedge_{j=1}^q u_j(x_1, \dots, x_n) = e \right).$$

Значит

$$G * GAC \models (\exists x_1, \dots, x_n) \left(\bigwedge_{i=1}^p w_i(x_1, \dots, x_n) \neq e \wedge \bigwedge_{j=1}^q u_j(x_1, \dots, x_n) = e \right).$$

Но $G * GAC$ — расширение алгебраически замкнутой группы GAC , поэтому

$$GAC \models (\exists x_1, \dots, x_n) \left(\bigwedge_{i=1}^p w_i(x_1, \dots, x_n) \neq e \wedge \bigwedge_{j=1}^q u_j(x_1, \dots, x_n) = e \right),$$

т. е. на группе GAC истинна формула Ψ и ее отрицание $\neg\Psi$. Полученное противоречие показывает, что *универсальная теория любой алгебраически замкнутой группы GAC совпадает с универсальной теорией класса всех групп*. Значит *универсальная теория любой алгебраически замкнутой группы GAC алгоритмически неразрешима*.

Отметим, что мы показали справедливость следующего используемого в дальнейшем утверждения: *если G — произвольная группа, GAC — алгебраически замкнутая группа, а*

$(\exists x_1, \dots, x_n)\Psi$ — замкнутая формула (Ψ — бескванторная часть) и $G \models (\exists x_1, \dots, x_n)\Psi$, то $GAC \models (\exists x_1, \dots, x_n)\Psi$.

Покажем, что для произвольной конечно определенной группы

$$G = \langle \langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle \rangle,$$

любого группового слова $w(a_1, \dots, a_n)$ в алфавите $\{a_1, \dots, a_n\}$ и любой алгебраически замкнутой группы GAC справедлива эквивалентность

$$w(a_1, \dots, a_n) \stackrel{G}{=} e \iff GAC \models (\forall x_1) \dots (\forall x_n) ((\bigotimes_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e).$$

Если $w(a_1, \dots, a_n) \stackrel{G}{=} e$ и $h_1, \dots, h_n$ — такие элементы алгебраически замкнутой группы GAC , для которых

$$GAC \models \bigotimes_{i=1}^m R_i(h_1, \dots, h_n) = e,$$

то подгруппа $gr(h_1, \dots, h_n)$ группы GAC , порожденная элементами $h_1, \dots, h_n$, является гомоморфным образом группы G относительно отображения φ , задаваемого равенствами

$$\varphi(a_1) = h_1, \dots, \varphi(a_n) = h_n.$$

Поэтому из равенства $w(a_1, \dots, a_n) \stackrel{G}{=} e$ следует равенство $w(h_1, \dots, h_n) \stackrel{GAC}{=} e$. Значит

$$GAC \models (\forall x_1) \dots (\forall x_n) ((\bigotimes_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e).$$

Если же $w(a_1, \dots, a_n) \stackrel{G}{\neq} e$, то

$$G \models (\exists x_1) \dots (\exists x_n) ((\bigotimes_{i=1}^m R_i(x_1, \dots, x_n) = e) \& w(x_1, \dots, x_n) \neq e).$$

Но тогда, как отмечалось выше,

$$GAC \models (\exists x_1) \dots (\exists x_n) ((\bigotimes_{i=1}^m R_i(x_1, \dots, x_n) = e) \& w(x_1, \dots, x_n) \neq e).$$

Значит формула

$$(\forall x_1) \dots (\forall x_n) ((\bigotimes_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e)$$

ложна на группе GAC .

Взяв в качестве группы G группу

$$GN = \langle \langle a_1, a_2 | R_1(a_1, a_2) = e, \dots, R_m(a_1, a_2) = e \rangle \rangle$$

с неразрешимой проблемой равенства, получим для любой алгебраически замкнутой группы GAC алгоритмически неразрешима ее $\forall^2$ -теория, а значит и $\exists^2$ -теория.

Покажем, что для любой алгебраически замкнутой группы GAC справедлива эквивалентность:

$$GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e) \iff \bigvee_{i=1}^p GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow w_i(x_1, \dots, x_n) = e).$$

Предварительно установим для произвольной алгебраически замкнутой группы GAC эквивалентность:

$$\begin{aligned} GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e) &\iff \\ \langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models \bigvee_{i=1}^p w_i(a_1, \dots, a_n) = e &\iff \\ \bigvee_{i=1}^p \langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models w_i(a_1, \dots, a_n) = e. \end{aligned}$$

Предположим, что

$$\langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models \bigvee_{i=1}^p w_i(a_1, \dots, a_n) = e.$$

Тогда при некотором i_0

$$\langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models w_{i_0}(a_1, \dots, a_n) = e.$$

Поэтому

$$GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow w_{i_0}(x_1, \dots, x_n) = e),$$

а значит,

$$GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e).$$

Для доказательства обратного предположим, что

$$\langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models \neg(\bigvee_{i=1}^p w_i(a_1, \dots, a_n) = e).$$

Тогда

$$\begin{aligned} \langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models \\ (\exists x_1, \dots, x_n) ((\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e) \& (\bigvee_{i=1}^p w_i(x_1, \dots, x_n) \neq e)). \end{aligned}$$

Значит

$$GAC \models (\exists x_1, \dots, x_n) ((\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e) \& (\bigvee_{i=1}^p w_i(x_1, \dots, x_n) \neq e)),$$

т. е.

$$GAC \models \neg(\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e).$$

В итоге получаем для произвольной алгебраически замкнутой группы GAC цепочку эквивалентностей:

$$\begin{aligned} GAC \models (\forall x_1, \dots, x_n) (\bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e \vee \bigvee_{j=1}^q u_j(x_1, \dots, x_n) \neq e) &\iff \\ GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow \bigvee_{i=1}^p w_i(x_1, \dots, x_n) = e) &\iff \\ \bigvee_{i=1}^p \langle \langle a_1, \dots, a_n | u_1(a_1, \dots, a_n) = e, \dots, u_q(a_1, \dots, a_n) = e \rangle \rangle \models w_i(a_1, \dots, a_n) = e &\iff \\ \bigvee_{i=1}^p GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow w_i(x_1, \dots, x_n) = e) &\iff \\ \bigvee_{i=1}^p GAC \models (\forall x_1, \dots, x_n) (w_i(x_1, \dots, x_n) = e \vee (\bigvee_{j=1}^q u_j(x_1, \dots, x_n) \neq e)) &\iff \\ \bigvee_{i=1}^p GAC \models (\forall x_1, \dots, x_n) (\bigotimes_{j=1}^q u_j(x_1, \dots, x_n) = e \longrightarrow w_i(x_1, \dots, x_n) = e). \end{aligned}$$

Заметим, $\forall^n$ -формулы типа $(1, 0)$ — это тождества, а $\forall^n$ -формулы типа $(1, q)$ при $q \geq 1$ — это квазитожества. В силу классического результата В. Магнуса [4] о разрешимости проблемы равенства для групп с одним определяющим соотношением *существует алгоритм, позволяющий по произвольной $\forall^n$ -формуле типа $(1, 1)$ определить, истинна ли она на произвольной алгебраически замкнутой группе*, в тоже время в силу результата В. В. Борисова [6] о существовании 2-порожденной группы с 12 определяющими соотношениями и с неразрешимой проблемой равенства *для $\forall^n$ -формул типа $(1, 12)$ такой алгоритм построить невозможно*.

4. Позитивные формулы на алгебраически замкнутых группах

Хорошо известно [3], что $\forall^\infty \exists^\infty$ -теории любых двух алгебраически замкнутых групп совпадают.

Так как любая алгебраически замкнутая группа является *полной*, т. е. для любого ее элемента g и произвольного натурального числа n уравнение $x^n = g$ разрешимо в этой группе, то на любой алгебраически замкнутой группе GAC истинна, например, простая позитивная формула $(\forall y)(\exists x)y = x^2$, которая, конечно, ложна на некоторых группах.

Покажем, что *позитивная $\forall^2 \exists^{24}$ -теория любой алгебраически замкнутой группы GAC алгоритмически неразрешима*.

Выше было установлено, что для произвольной конечно определенной группы

$$G = \langle \langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle \rangle,$$

любого группового слова $w(a_1, \dots, a_n)$ в алфавите $\{a_1, \dots, a_n\}$ и любой алгебраически замкнутой группы GAC справедлива эквивалентность

$$w(a_1, \dots, a_n) \stackrel{G}{=} e \iff GAC \models (\forall x_1) \dots (\forall x_n) ((\bigwedge_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e).$$

Возьмем в качестве группы G группу

$$GN = \langle \langle a_1, a_2 | R_1(a_1, a_2) = e, \dots, R_{12}(a_1, a_2) = e \rangle \rangle$$

с двумя образующими и двенадцатью определяющими соотношениями [6] с неразрешимой проблемой равенства и воспользуемся доказанным в работе [3] А. Макинтайра утверждением:

если G — произвольная группа, а $h_1, h_2, \dots, h_n$ и g — любые ее элементы, то

$$G \models ((\bigwedge_{i=1}^n h_i = e) \longrightarrow g = e) \iff$$

существует такое расширение H группы G ($G \leq H$),

в котором для подходящих элементов $u_1, v_1, u_2, v_2, \dots, u_n, v_n$

$$\text{выполняется равенство } g = \prod_{i=1}^n u_i h u_i^{-1} \cdot v_i h v_i^{-1}$$

получим, что для любой алгебраически замкнутой группы GAC и любого группового слова $w(a_1, a_2)$ в алфавите $\{a_1, a_2\}$ справедлива эквивалентность

$$w(a_1, a_2) \stackrel{GN}{=} e \iff$$

$$GAC \models (\forall x_1)(\forall x_2)(\exists u_1, v_1, \dots, u_{12}, v_{12})(w(x_1, x_2) = \prod_{i=1}^{12} u_i R_i(x_1, x_2) u_i^{-1} \cdot v_i R_i(x_1, x_2) v_i^{-1}).$$

Из этой эквивалентности следует справедливость теоремы.

ТЕОРЕМА 1. *Позитивная $\forall^2\exists^{24}$ -теория любой алгебраически замкнутой группы и класса всех алгебраически замкнутых групп алгоритмически неразрешима.*

В рассматриваемых в предыдущей теореме позитивных формулах одна переменная кванторов, а общее число кванторов 26. Следующая теорема уменьшает общее число кванторов до 5 сохраняя позитивность формул и одну переменную кванторов. При этом уменьшается число кванторов существования с 24-х до 2-х, но число кванторов общности увеличивается с 2-х до 3-х.

ТЕОРЕМА 2. *Позитивная $\forall^3\exists^2$ -теория любой алгебраически замкнутой группы и класса всех алгебраически замкнутых групп алгоритмически неразрешима.*

ДОКАЗАТЕЛЬСТВО. Воспользуемся доказанной выше эквивалентностью: для произвольной конечно определенной группы

$$G = \langle \langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle \rangle,$$

любого группового слова $w(a_1, \dots, a_n)$ в алфавите $\{a_1, \dots, a_n\}$ и любой алгебраически замкнутой группы GAC справедлива эквивалентность

$$w(a_1, \dots, a_n) \stackrel{G}{=} e \iff GAC \models (\forall x_1) \dots (\forall x_n) ((\bigwedge_{i=1}^m R_i(x_1, \dots, x_n) = e) \longrightarrow w(x_1, \dots, x_n) = e).$$

Покажем, что для произвольной конечно определенной группы

$$G = \langle \langle a_1, a_2, \dots, a_n | R_1(a_1, \dots, a_n) = e, \dots, R_m(a_1, \dots, a_n) = e \rangle \rangle,$$

любого группового слова $w(a_1, \dots, a_n)$ в алфавите $\{a_1, \dots, a_n\}$ и любой алгебраически замкнутой группы GAC справедлива эквивалентность

$$\begin{aligned} w(a_1, \dots, a_n) \stackrel{G}{=} e \iff \\ GAC \models (\forall x_1, \dots, x_n) (\forall y) (\exists u, v) ((\bigvee_{i=1}^m y = (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \vee \\ w(x_1, \dots, x_n) = e). \end{aligned}$$

Заметим, что для любой алгебраически замкнутой группы GAC

$$GAC \models (\forall x) (\exists u, v) ((uxu^{-1}) \cdot (v xv^{-1}) = e).$$

Если g — произвольный элемент алгебраически замкнутой группы GAC , то так как элементы g и g^{-1} имеют одинаковый порядок, то на HNN-расширении

$$\langle \langle GAC, t | tgt^{-1} = g^{-1} \rangle \rangle$$

группы GAC истинна формула $(\exists u, v) (ugu^{-1}) \cdot (vgv^{-1}) = e$, значит

$$GAC \models (\exists u, v) ((ugu^{-1}) \cdot (vgv^{-1}) = e).$$

Так как g — произвольный элемент алгебраически замкнутой группы GAC , то

$$GAC \models (\forall x) (\exists u, v) ((uxu^{-1}) \cdot (v xv^{-1}) = e).$$

Кроме того справедлива эквивалентность

$$g \stackrel{GAC}{\neq} e \iff GAC \models (\forall y) (\exists u, v) y = (ugu^{-1}) \cdot (vgv^{-1}).$$

Предположим, что $w(a_1, \dots, a_n) \stackrel{G}{=} e$. Покажем, что тогда

$$GAC \models (\forall x_1, \dots, x_n)(\forall y)(\exists u, v)((\bigvee_{i=1}^m y = (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \vee w(x_1, \dots, x_n) = e).$$

Пусть $g_1, \dots, g_n$ — произвольные элементы группы GAC . Покажем, что

$$GAC \models (\forall y)(\exists u, v)((\bigvee_{i=1}^m y = (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \vee w(g_1, \dots, g_n) = e).$$

Рассмотрим произвольный элемент g группы GAC . Покажем, что

$$GAC \models (\exists u, v)((\bigvee_{i=1}^m g = (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \vee w(g_1, \dots, g_n) = e).$$

Если $g = e$, то

$$GAC \models (\exists u, v)e = (uR_1(g_1, \dots, g_n)u^{-1}) \cdot (vR_1(g_1, \dots, g_n)v^{-1}),$$

а значит и

$$GAC \models (\exists u, v)((\bigvee_{i=1}^m e = (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \vee w(g_1, \dots, g_n) = e).$$

Пусть $g \neq e$. Если при некотором j выполняется неравенство $R_j(g_1, \dots, g_n) \neq e$, то

$$GAC \models (\exists u, v)g = (uR_j(g_1, \dots, g_n)u^{-1}) \cdot (vR_j(g_1, \dots, g_n)v^{-1}),$$

поэтому

$$GAC \models (\exists u, v)((\bigvee_{i=1}^m g = (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \vee w(g_1, \dots, g_n) = e).$$

Если же при любом i выполняется равенство $R_i(g_1, \dots, g_n) = e$ в группе GAC , то тогда в этой группе, как уже отмечалось выше, выполняется и равенство $w(g_1, \dots, g_n) = e$. Значит и в этом случае

$$GAC \models (\exists u, v)((\bigvee_{i=1}^m g = (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \vee w(g_1, \dots, g_n) = e).$$

Для доказательства обратного, предположим, что $w(a_1, \dots, a_n) \stackrel{G}{\neq} e$ и покажем, что тогда

$$GAC \models \neg(\forall x_1, \dots, x_n)(\forall y)(\exists u, v)((\bigvee_{i=1}^m y = (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \vee w(x_1, \dots, x_n) = e),$$

т. е.

$$GAC \models (\exists x_1, \dots, x_n)(\exists y)(\forall u, v)((\bigwedge_{i=1}^m y \neq (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \& w(x_1, \dots, x_n) \neq e),$$

Так как

$$G \models (\bigwedge_{i=1}^m R_i(a_1, \dots, a_n) = e) \& w(a_1, \dots, a_n) \neq e),$$

то

$$G \models (\exists x_1, \dots, x_n) (\bigwedge_{i=1}^m R_i(x_1, \dots, x_n) = e) \& w(x_1, \dots, x_n) \neq e.$$

Поэтому, как отмечалось выше,

$$GAC \models (\exists x_1, \dots, x_n) (\bigwedge_{i=1}^m R_i(x_1, \dots, x_n) = e) \& w(x_1, \dots, x_n) \neq e.$$

Пусть $g_1, \dots, g_n$ — такие элементы группы GAC , что

$$GAC \models (\bigwedge_{i=1}^m R_i(g_1, \dots, g_n) = e) \& w(g_1, \dots, g_n) \neq e,$$

а g — неединичный элемент группы GAC . Тогда

$$GAC \models (\forall u, v) ((\bigwedge_{i=1}^m g \neq (uR_i(g_1, \dots, g_n)u^{-1}) \cdot (vR_i(g_1, \dots, g_n)v^{-1})) \& w(g_1, \dots, g_n) \neq e).$$

Поэтому

$$GAC \models (\exists x_1, \dots, x_n) (\exists y) (\forall u, v) ((\bigwedge_{i=1}^m y \neq (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \& w(x_1, \dots, x_n) \neq e),$$

а значит

$$GAC \models \neg (\forall x_1, \dots, x_n) (\forall y) (\exists u, v) ((\bigwedge_{i=1}^m y = (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \vee w(x_1, \dots, x_n) = e).$$

Это завершает доказательство эквивалентности

$$w(a_1, \dots, a_n) \stackrel{G}{=} e \iff GAC \models (\forall x_1, \dots, x_n) (\forall y) (\exists u, v) ((\bigwedge_{i=1}^m y = (uR_i(x_1, \dots, x_n)u^{-1}) \cdot (vR_i(x_1, \dots, x_n)v^{-1})) \vee w(x_1, \dots, x_n) = e).$$

Для завершения доказательства теоремы достаточно применить доказанную эквивалентность к конечно определенной группе

$$GN = \langle \langle a_1, a_2 \mid R_1(a_1, a_2) = e, \dots, R_{12}(a_1, a_2) = e \rangle \rangle$$

с двумя образующими и двенадцатью определяющими соотношениями [6] с неразрешимой проблемой равенства

$$w(a_1, a_2) \stackrel{GN}{=} e \iff GAC \models (\forall x_1, x_2) (\forall y) (\exists u, v) ((\bigwedge_{i=1}^{12} y = (uR_i(x_1, x_2)u^{-1}) \cdot (vR_i(x_1, x_2)v^{-1})) \vee w(x_1, x_2) = e).$$

□

5. Уравнения специального вида в алгебраически замкнутых группах

Хорошо известно, что любая алгебраически замкнутая группа является *полной*, т. е. для любого ее элемента g и произвольного натурального числа n уравнение $x^n = g$ разрешимо в этой группе.

Нетрудно показать, что для произвольного элемента g любой алгебраически замкнутой группы GAC в этой группе разрешимо уравнение $[x, y] = g$, где $[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов x и y , т. е. любой элемент алгебраически замкнутой группы является коммутатором. Нам не встречались явные упоминания этого факта в доступной литературе. Приведем простое доказательство. Так как в группе $GAC * \langle\langle a, b \rangle\rangle$ элементы ag и $b^{-1}ab$ имеют бесконечный порядок, то группа

$$\langle\langle GAC * \langle\langle a, b \rangle\rangle, t | ag = t^{-1}(b^{-1}ab)t \rangle\rangle$$

является HNN-расширением группы GAC и в ней выполняются равенства

$$g = a^{-1}(bt)^{-1}a(bt) = [a, bt],$$

значит в группе GAC разрешимо уравнение

$$g = x^{-1}y^{-1}xy = [x, y].$$

Следующая теорема существенно усиливает эти утверждения.

ТЕОРЕМА 3. *В любой алгебраически замкнутой группе GAC каждое уравнение вида*

$$w(x_1, \dots, x_n) = g, \quad (1)$$

где $w(x_1, \dots, x_n)$ — непустое несократимое групповое слово от неизвестных $x_1, \dots, x_n$, а g — произвольный элемент группы GAC , имеет решение.

ДОКАЗАТЕЛЬСТВО. Рассмотрим два возможных случая.

1) g — элемент бесконечного порядка алгебраически замкнутой группы GAC . В этом случае $w(x_1, \dots, x_n)$ и g — элементы бесконечного порядка группы $GAC * \langle\langle x_1, \dots, x_n \rangle\rangle$. Поэтому группа GAC является подгруппой HNN-расширения

$$\langle\langle GAC * \langle\langle x_1, \dots, x_n \rangle\rangle, t | tw(x_1, \dots, x_n)t^{-1} = g \rangle\rangle,$$

в котором выполняется равенство $w(tx_1t^{-1}, \dots, tx_nt^{-1}) = g$. Поэтому уравнение (1) разрешимо в группе GAC .

2) g — элемент конечного порядка m алгебраически замкнутой группы GAC .

В свободной группе $\langle\langle x_1, \dots, x_n \rangle\rangle$ элемент $w(x_1, \dots, x_n)$ равен элементу вида $u^k(x_1, \dots, x_n)$, где k — натуральное число, а $u(x_1, \dots, x_n)$ не является собственной степенью в этой группе. Тогда $u(x_1, \dots, x_n)$ — элемент порядка km [4] в группе

$$\langle\langle x_1, \dots, x_n | u^{km}(x_1, \dots, x_n) = 1 \rangle\rangle.$$

Поэтому $u^k(x_1, \dots, x_n)$ и g — элементы порядка m в группе

$$GAC * \langle\langle x_1, \dots, x_n | u^{km}(x_1, \dots, x_n) = 1 \rangle\rangle.$$

Значит группа GAC является подгруппой группы

$$\langle\langle G * \langle\langle x_1, \dots, x_n | u^{km}(x_1, \dots, x_n) = 1 \rangle\rangle, t | t u^k(x_1, \dots, x_n) t^{-1} = g \rangle\rangle,$$

в которой выполняется равенство $w(tx_1t^{-1}, \dots, tx_nt^{-1}) = g$. Поэтому уравнение (1) разрешимо в группе GAC . $\square$

Доказанная теорема означает, что в алгебраически замкнутой группе ширина любой вербальной подгруппы равна единице. Конечно, каждая вербальная подгруппа группы GAC совпадает со всей группой, так как GAC — простая группа.

6. Заключение

Установлена алгебраическая неразрешимость “достаточно простых” фрагментов элементарной теории любой алгебраически замкнутой группы и класса всех алгебраически замкнутых групп — доказана алгоритмическая неразрешимость позитивной $\forall^2\exists^{24}$ -теории и позитивной $\forall^3\exists^2$ -теории любой алгебраически замкнутой группы и класса всех алгебраически замкнутых групп. Установлена разрешимость в любой алгебраически замкнутой группе *GAC* каждого разрешенного относительно неизвестных уравнения, по другой терминологии — бескоэффициентного уравнения, т. е. уравнения вида

$$w(x_1, \dots, x_n) = g,$$

где $w(x_1, \dots, x_n)$ — непустое несократимое групповое слово от неизвестных $x_1, \dots, x_n$, а g — произвольный элемент группы *GAC*.

В связи с полученными в работе результатами представляет интерес вопрос о разрешимости позитивной $\forall\exists^\infty$ -теории и позитивной $\exists\forall^\infty$ -теории произвольной алгебраически замкнутой группы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Scott W. R. Algebraically closed groups // *Proc. Amer. Math. Soc.* 1951. Vol. 2. P. 118-121.
2. Neumann B. H. A note on algebraically closed groups // *J. London. Math. Soc.* 1952. Vol. 27. P. 227-242.
3. Macintyre A. On algebraically closed groups // *Ann. of Math.* 1972. Vol. 96. P. 53-97.
4. Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир, 1980.
5. Маканин Г. С. Разрешимость универсальной и позитивной теорий свободной группы // *Изв. АН СССР. Серия матем.* 1984. № 4. С. 735-749.
6. Борисов В. В. Простые примеры групп с неразрешимой проблемой тождества // *Матем. заметки.* 1969. Т. 6. Вып. 5. С. 521-532.
7. Мерзляков Ю. И. Позитивные формулы на свободных группах // *Алгебра и логика.* 1966. Т. 5, № 4. С. 25-42.
8. Sacerdote G. S. Almost all free products of groups have the same positive theory // *J. Algebra.* 1973. Vol. 27, № 3. P. 475-485.

REFERENCES

1. Scott, W. R. 1951, “Algebraically closed groups”, *Proc. Amer. Math. Soc.*, vol. 2, pp. 118-121.
2. Neumann, B. H. 1952, “A note on algebraically closed groups”, *J. London. Math. Soc.* vol. 27. pp. 227-242.
3. Macintyre, A. 1972, “On algebraically closed groups”, *Ann. of Math.* vol. 96. pp. 53-97.
4. Lyndon, R. C. & Schupp, P. E. Combinatorial group theory. Springer, 2015.
5. Makanin, G. S. 1984, “Decidability of the universal and positive theories of a free group”, *Math. USSR-Izv.*, vol. 25, no. 1, pp. 75-88.

6. Borisov, V. V. 1969, "Simple examples of groups with unsolvable word problem", *Math. Notes.*, vol. 6, no. 5, pp. 768-775.
7. Merzlyakov, Yu. I. 1966, "Positive formulae over free groups", *Algebra i logika.*, vol. 5, no. 4, pp. 25-42 (in Russian).
8. Sacerdote, G. S. 1973, "Almost all free products of groups have the same positive theory", *J. Algebra.*, vol. 27, no. 3, pp. 475-485.

Получено 21.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.361

DOI 10.22405/2226-8383-2020-21-1-200-212

О линейных приближающих формах

П. Л. Иванков

Иванков Павел Леонидович — доктор физико-математических наук, профессор кафедры математического моделирования, Московский государственный технический университет им. Н. Э. Баумана (г. Москва).

e-mail: ivankovpl@mail.ru

Аннотация

Обобщенная гипергеометрическая функция определяется суммой степенного ряда, коэффициентами которого являются произведения значений некоторой дробной рациональной функции. Взятые со знаком минус корни числителя и знаменателя этой рациональной функции называются параметрами соответствующей гипергеометрической функции. Для исследования арифметической природы значений гипергеометрических функций и их производных (включая производные по параметру) часто используют метод Зигеля. Соответствующее рассуждение, как правило, начинается с построения функциональной линейной приближающей формы. Если параметры гипергеометрической функции рациональны, то для построения этой формы можно применить принцип Дирихле. При этом построение возможно не только для самих гипергеометрических функций, но и для произведений их степеней. Этим объясняется общность результатов, получаемых таким методом. Если, однако, среди параметров имеются иррациональные числа, то применение принципа Дирихле невозможно, и для проведения соответствующего исследования приходится привлекать дополнительные соображения.

Одним из способов преодоления затруднения, связанного с наличием иррациональных чисел среди параметров гипергеометрической функции является применение эффективного построения линейной приближающей формы, с которой начинается рассуждение. Первоначально эффективные конструкции построения таких приближений появились для функций специального вида (числитель рациональной функции, с помощью которой определяются коэффициенты гипергеометрической функции должен был равняться единице). Изучение свойств этих приближений показало, что они могут оказаться полезными и в случае рациональных параметров: получаемые с помощью эффективных методов количественные результаты оказались точнее их аналогов, полученных методом Зигеля. В дальнейшем методы эффективного построения линейной приближающей формы обобщались в различных направлениях.

В данной работе предлагается новая эффективная конструкция линейной приближающей формы для случая, когда для гипергеометрических функций рассматриваются также и производные по параметру. Эта конструкция используется для уточнения оценки снизу меры линейной независимости значений соответствующих функций.

Ключевые слова: гипергеометрические функции, линейная независимость, дифференцирование по параметру, оценки линейных форм.

Библиография: 25 названий.

Для цитирования:

П. Л. Иванков. О линейных приближающих формах // Чебышевский сборник, 2020, т. 21, вып. 1, с. 200–212.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.361

DOI 10.22405/2226-8383-2020-21-1-200-212

On linear approximating forms

P. L. Ivankov

Ivankov Pavel Leonidovich — doctor of physical and mathematical sciences, Professor, Bauman Moscow State Technical University (Moscow).

e-mail: ivankovpl@mail.ru

Abstract

Generalized hypergeometric function is defined as a sum of the power series whose coefficients are the products of the values of some fractional rational function. Taken with a minus sign roots of a numerator and denominator of this rational function are called parameters of the corresponding hypergeometric function. For the investigation of the arithmetic nature of the values of hypergeometric functions and their derivatives (including derivatives with respect to parameter) one often makes use of Siegel's method. The corresponding reasoning begins as a rule by the construction of the functional linear approximating form. If parameters of the hypergeometric function are rational one is able to use pigeonhole principle for the construction of this form. In addition the construction is feasible not only for the hypergeometric functions themselves but also for the products of their powers. By this is explained the generality of results obtained by such method. But if there are irrational numbers among the parameters the application of a pigeonhole method is impossible and for carrying out the corresponding investigation it is necessary to employ some additional considerations.

One of the methods of surmounting the difficulty connected with the irrationality of some parameters of a hypergeometric function consists in the application of the effective construction of the linear approximating form from which the reasoning begins. Primarily effective constructions of such approximations appeared for the functions of a special kind (the numerator of the rational function by means of which the coefficients of hypergeometric functions are defined was to be equal to unity). The investigation of the properties of these approximations revealed the fact that they can be useful in case of rational parameters as well for the quantitative results obtained by effective methods turned out to be more precise than their analogs obtained by Siegel's method. Subsequently the methods of effective construction of linear approximating forms were generalized in diverse directions.

In this paper we propose a new effective construction of approximating form in case when for the hypergeometric functions derivatives with respect to parameter are also considered. This construction is made use of for the sharpening of the lower estimates of the linear independence measure of the values of corresponding functions.

Keywords: hypergeometric functions, linear independence, differentiation with respect to parameter, estimates of linear forms.

Bibliography: 25 titles.

For citation:

P. L. Ivankov, 2020, "On linear approximating forms", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 200–212.

1. Введение

Для исследования арифметической природы значений гипергеометрических функций с рациональными параметрами часто применяют метод Зигеля. При этом рассуждение начинается с построения с помощью принципа Дирихле функциональной линейной приближающей формы, имеющей достаточно высокий порядок нуля в начале координат. Для продифференцированных по параметру функций этот метод также применим; соответствующие примеры см. в [1, глава 7]. Отметим также работы [2]–[17].

Если функциональная линейная приближающая форма строится эффективно, то возможности метода Зигеля расширяются: удастся исследовать значения функций с иррациональными параметрами, и уточняются соответствующие количественные результаты. Примеры исследований такого рода см. в [18]–[21]. В данной работе предлагается эффективная конструкция линейной приближающей формы для функций вида (1), и затем с помощью этой конструкции уточняется оценка меры линейной независимости значений этих функций в ненулевой рациональной точке.

2. Результаты

Пусть $t, \tau_1, \dots, \tau_t$ — натуральные числа. Рассмотрим функции

$$F_{klkj}(z) = \sum_{\nu=0}^{\infty} z^{\nu} \chi_{kj}(\nu) \prod_{x=1}^{\nu} \frac{a(x)}{b(x)} \cdot \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)}, \quad (1)$$

где $k = 1, \dots, t$, $l_k = 0, 1, \dots, \tau_k - 1$, $j = 1, \dots, m + 2$; $a(x) = (x + \alpha_1) \dots (x + \alpha_r)$, $b(x) = (x + \beta_1) \dots (x + \beta_m)$, $0 \leq r \leq m + 1$; $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_m, A, \lambda_1, \dots, \lambda_t$ — некоторые рациональные числа, причем $a(x)b(x)(x + \lambda_k)(x + A - \lambda_k) \neq 0$ при $x = 1, 2, \dots$;

$$\chi_{kj}(\nu) = \prod_{u=1}^{j-1} (\nu + \beta_u), \quad k = 1, \dots, t, \quad j = 1, \dots, m + 1, \quad \chi_{k,m+2}(\nu) = (\nu + \lambda_k) \chi_{k,m+1}(\nu). \quad (2)$$

Предположим, что

$$\alpha_i - \beta_j, \alpha_i - \lambda_k, \alpha_i + \lambda_k - A, \quad i = 1, \dots, r, \quad j = 1, \dots, m, \quad k = 1, \dots, t,$$

не являются целыми числами; предположим также, что целыми числами не являются

$$\lambda_k - \lambda_{k'}, \lambda_k + \lambda_{k'} - A, 2\lambda_k - A, \quad k, k' = 1, \dots, t, \quad k \neq k'.$$

Положительная постоянная γ , встречающаяся в приведенных ниже теоремах, зависит от параметров функций (1) и от числа ξ ; в дальнейшем такие постоянные будем обозначать $\gamma_1, \gamma_2, \dots$.

ТЕОРЕМА 1. Пусть выполнены перечисленные выше условия. Предположим также, что функции (1) линейно независимы вместе с функцией, тождественно равной единице, над полем рациональных дробей. Тогда для любого отличного от нуля рационального числа ξ и для любого нетривиального набора целых чисел

$$h_{klkj}, \quad k = 1, \dots, t, \quad l_k = 0, 1, \dots, \tau_k - 1, \quad j = 1, \dots, m + 2, \quad (3)$$

при любом целом h_0 выполняется неравенство

$$\left| h_0 + \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} \sum_{j=1}^{m+2} h_{klkj} F_{klkj}(\xi) \right| > H^{-T(m+2) - \frac{\gamma}{\ln(H+2)}},$$

где H есть максимум модулей чисел (3), $T = \tau_1 + \dots + \tau_t$, а положительная постоянная γ не зависит от H .

Аналогичная теорема справедлива и в однородном случае.

ТЕОРЕМА 2. *Предположим, что выполнены все перечисленные выше условия, и пусть $b(0) = 0$. Тогда*

$$\left| \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} \sum_{j=1}^{m+2} h_{klkj} F_{klkj}(\xi) \right| > H^{1-T(m+2)-\frac{\gamma}{\ln \ln(H+2)}},$$

где T, h_{klkj}, H определяются, как в теореме 1.

3. Вспомогательная функция

Будем считать, что условия теоремы 1 выполнены. Пусть $n \geq 1$ и $\nu \geq 0$ — целые числа. Рассмотрим вспомогательную функцию

$$\Phi(\nu) = \frac{(n!)^m}{2\pi i} \int_{\Gamma} \prod_{x=1}^{\nu} \frac{1}{(\zeta+x)(A-\zeta-N_1+x)} \times \\ \times \frac{(A-\zeta-N_1+N_2) \prod_{x=1}^{N_2-1} (\zeta+x)(A-\zeta-N_1+x)}{\prod_{k=1}^t \prod_{\sigma=0}^{N_1} ((\zeta-\lambda_k+\sigma)(\zeta-A+\lambda_k+\sigma))^{\tau_k}} d\zeta, \quad (4)$$

где $N_1 = (m+2)(n+1) - 1$, $N_2 = n + T(m+2)(n+1) - 1$, Γ — положительно ориентированный простой замкнутый кусочно гладкий контур, внутри которого лежат все особые точки подынтегральной функции вида

$$\lambda_k - \sigma \text{ и } A - \lambda_k - \sigma, \quad k = 1, \dots, t, \quad \sigma = 0, 1, \dots, N_1, \quad (5)$$

и при этом все другие особые точки подынтегральной функции лежат в его внешности. Такой контур существует при всех $n \geq \gamma_1$. При $\tau_1 = \dots = \tau_t = 1$ и $A = 0$ аналогичная вспомогательная функция использовалась в [22].

ЛЕММА 1. *Функция $\Phi(\nu)$ обладает при $n \geq \gamma_1$ следующими свойствами:*

- 1) $\Phi(\nu) = 0$ при $\nu = n+1, \dots, N_2-1$;
- 2) $\Phi(N_2) \neq 0$;

$$3) \quad \Phi(\nu) = \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} B_{klk}(\nu) \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k+x)(A-\lambda_k+x)}, \quad (6)$$

где

$$B_{klk}(\nu) = \frac{(n!)^m}{l_k!(\tau_k - l_k - 1)!} \sum_{\sigma=0}^{N_1} \left(\frac{\partial^{\tau_k - l_k - 1}}{\partial \zeta^{\tau_k - l_k - 1}} \left(Q_{\sigma}(\nu, \zeta) (\zeta + A - \lambda_k - \sigma)^{\tau_k} \right) \Big|_{\zeta=\lambda_k-\sigma} + \right. \\ \left. + (-1)^{l_k} \frac{\partial^{\tau_k - l_k - 1}}{\partial \zeta^{\tau_k - l_k - 1}} \left(Q_{\sigma}(\nu, \zeta) (\zeta - A + \lambda_k + \sigma)^{\tau_k} \right) \Big|_{\zeta=A-\lambda_k-\sigma} \right), \quad (7)$$

$$Q_{\sigma}(\nu, \zeta) = \prod_{x=1}^{\sigma} \frac{\zeta + \nu + x}{\zeta + x} \prod_{x=1}^{N_1-\sigma} \frac{A - \zeta - N_1 + \nu + x}{A - \zeta - N_1 + x} \times \\ \times \frac{(A - \zeta - N_1 + N_2) \prod_{x=1}^{N_2-1} (\zeta + x)(A - \zeta - N_1 + x)}{\prod_{k'=1}^t \prod_{\sigma'=0}^{N_1} ((\zeta - \lambda_{k'} + \sigma')(\zeta - A + \lambda_{k'} + \sigma'))^{\tau_{k'}}}$$

Доказательство. Первое свойство справедливо потому, что при указанных значениях ν контур Γ охватывает все полюсы подынтегральной функции, и при этом степень знаменателя более чем на две единицы превосходит степень числителя. Для доказательства второго свойства достаточно заметить, что при $\nu = N_2$ правая часть (4) равна (с точностью до знака) вычету подынтегральной функции при $\zeta = -N_2$; этот вычет отличен от нуля, что проверяется непосредственно.

Докажем третье свойство. При выполнении условий теоремы 1 особые точки (5) подынтегральной функции являются полюсами кратности τ_k ; все прочие особые точки лежат во внешности Γ .

При каждом σ , $0 \leq \sigma \leq N_1$, подынтегральную функцию можно записать в виде

$$\prod_{x=1}^{\nu} \frac{1}{(\zeta + \sigma + x)(A - \zeta - \sigma + x)} \cdot Q_{\sigma}(\zeta, \nu).$$

После применения теоремы о вычетах получаем

$$\begin{aligned} \Phi(\nu) = & \sum_{k=1}^t \frac{1}{(\tau_k - 1)!} \times \\ & \times \sum_{\sigma=0}^{N_1} \left(\frac{\partial^{\tau_k-1}}{\partial \zeta^{\tau_k-1}} \left(\prod_{x=1}^{\nu} \frac{1}{(\zeta + \sigma + x)(A - \zeta - \sigma + x)} Q_{\sigma}(\nu, \zeta) (\zeta - \lambda_k + \sigma)^{\tau_k} \right) \Big|_{\zeta=\lambda_k-\sigma} + \right. \\ & \left. + \frac{\partial^{\tau_k-1}}{\partial \zeta^{\tau_k-1}} \left(\prod_{x=1}^{\nu} \frac{1}{(\zeta + \sigma + x)(A - \zeta - \sigma + x)} Q_{\sigma}(\nu, \zeta) (\zeta - A + \lambda_k + \sigma)^{\tau_k} \right) \Big|_{\zeta=A-\lambda_k-\sigma} \right). \end{aligned}$$

Последнее выражение преобразуем, используя правило дифференцирования произведения. Имеем

$$\begin{aligned} \frac{\partial^l}{\partial \zeta^l} \prod_{x=1}^{\nu} \frac{1}{(\zeta + x)(A - \zeta + x)} = & \sum_{\substack{k_1 + \dots + k_{\nu} = l, \\ k_x \geq 0, x=1, \dots, \nu}} \frac{l!}{k_1! \dots k_{\nu}!} \times \\ & \times \prod_{x=1}^{\nu} \frac{k_x!}{A + 2x} \left(\frac{(-1)^{k_x}}{(\zeta + x)^{k_x+1}} + \frac{1}{(A - \zeta + x)^{k_x+1}} \right). \end{aligned}$$

Отсюда следуют равенства

$$\frac{\partial^l}{\partial \zeta^l} \prod_{x=1}^{\nu} \frac{1}{(\zeta + \sigma + x)(A - \zeta - \sigma + x)} \Big|_{\zeta=\lambda_k-\sigma} = \frac{\partial^l}{\partial \lambda_k^l} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)},$$

и

$$\frac{\partial^l}{\partial \zeta^l} \prod_{x=1}^{\nu} \frac{1}{(\zeta + \sigma + x)(A - \zeta - \sigma + x)} \Big|_{\zeta=A-\lambda_k-\sigma} = (-1)^l \frac{\partial^l}{\partial \lambda_k^l} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)},$$

справедливые при $l = 0, 1, \dots$. Применим эти равенства и в результате получим требуемое. Лемма доказана. $\square$

4. Тождество

Определим в дополнение к многочленам (2) многочлены

$$\chi_{k,m+3}(\zeta) = (\zeta + A - \lambda_k) \chi_{m+2}(\zeta), \quad k = 1, \dots, t.$$

Далее, определим при $k = 1, \dots, t$ числа $c_{k1}, \dots, c_{k,m+2}$ так, чтобы тождественно по ζ выполнялось равенство

$$a(\zeta) = c_{k1}\chi_{k1}(\zeta - 1) + \dots + c_{k,m+2}\chi_{k,m+2}(\zeta - 1),$$

и пусть

$$V_{kjs}(\zeta) = \begin{cases} a(\zeta + 1), & s = 0, j = 1, \dots, m + 2, \\ c_{k1}\chi_{k1}(\zeta) + \dots + c_{kj}\chi_{kj}(\zeta), & s = 1, \dots, n, j = 1, \dots, m + 2. \end{cases}$$

ЛЕММА 2. Пусть $W(\nu)$ — многочлен степени не выше N_1 . Тогда при выполнении условий теоремы 1 для чисел

$$w_{kjs} = \frac{1}{2\pi i} \int_{\Gamma} \frac{V_{kjs}(\zeta - s)}{\chi_{k,j+1}(\zeta - s)} \times \\ \times \frac{W(\zeta) d\zeta}{\prod_{x=0}^{s-1} b(\zeta - x)(\zeta + \lambda_k - x)(\zeta + A - \lambda_k - x) \prod_{x=1}^{n-s+1} a(\zeta - n + x)} \quad (8)$$

тождественно по ν выполняется равенство

$$\sum_{j=1}^{m+2} \sum_{s=0}^n w_{kjs} \chi_{kj}(\nu - s) \prod_{x=0}^{s-1} b(\nu - x)(\nu + \lambda_k - x)(\nu + A - \lambda_k - x) \prod_{x=1}^{n-s} a(\nu - n + x) = W(\nu). \quad (9)$$

Простой замкнутый кусочно гладкий положительно ориентированный контур Γ в правой части (8) выбирается так, что он охватывает все нули многочлена от переменной ζ

$$\prod_{x=0}^n b(\zeta - x)(\zeta + \lambda_k - x)(\zeta + A - \lambda_k - x)$$

и точку ν , а все нули многочлена от переменной ζ

$$\prod_{x=1}^n a(\zeta - n + x)$$

лежат в его внешности.

ДОКАЗАТЕЛЬСТВО. Приведем лишь схему доказательства; подробное доказательство аналогичной леммы дано в [23]. Существование контура Γ из правой части (8) с указанными свойствами обеспечивается условиями теоремы 1. Доказательство леммы 2 основано на использовании тождества

$$\frac{1}{\zeta - \nu} \prod_{x=1}^n \frac{a(\nu - n + x)}{a(\zeta - n + x)} = \sum_{s=0}^n \sum_{j=1}^{m+2} \frac{V_{kjs}(\zeta - s) \chi_{kj}(\nu - s)}{\chi_{k,j+1}(\zeta - s)} \times \\ \times \prod_{x=0}^{s-1} \frac{b(\nu - x)(\nu + \lambda_k - x)(\nu + A - \lambda_k - x)}{b(\zeta - x)(\zeta + \lambda_k - x)(\zeta + A - \lambda_k - x)} \frac{\prod_{x=1}^{n-s} a(\nu - n + x)}{\prod_{x=1}^{n-s+1} a(\zeta - n + x)} + \\ + \frac{1}{\zeta - \nu} \prod_{x=0}^n \frac{b(\nu - x)(\nu + \lambda_k - x)(\nu + A - \lambda_k - x)}{b(\zeta - x)(\zeta + \lambda_k - x)(\zeta + A - \lambda_k - x)}, \quad (10)$$

которое является обобщением известного тождества из теории интерполирования (см., например, [24, формула (4.4:7), с. 450]). Чтобы получить (10), следует записать [23, равенство (2.21)] при $q = n$ для случая, когда фигурирующий там многочлен $b(z)$ заменен на

$b(z)(z + \lambda_k)(z + A - \lambda_k)$. Для доказательства (9) надо умножить (10) на $W(\zeta)/(2\pi i)$ и проинтегрировать получившееся равенство по контуру Γ . Т. к.

$$\frac{1}{2\pi i} \int_{\Gamma} \frac{W(\zeta)}{\zeta - \nu} \prod_{x=1}^n \frac{a(\nu - n + x)}{a(\zeta - n + x)} d\zeta = W(\nu),$$

$$\text{и} \quad \frac{1}{2\pi i} \int_{\Gamma} \frac{W(\zeta)}{\zeta - \nu} \prod_{x=0}^n \frac{b(\nu - x)(\nu + \lambda_k - x)(\nu + A - \lambda_k - x)}{b(\zeta - x)(\zeta + \lambda_k - x)(\zeta + A - \lambda_k - x)} d\zeta = 0,$$

то отсюда получим (8) и (9). Из двух последних равенств первое очевидно (поскольку контур интегрирования содержит лишь один полюс $\zeta = \nu$ подынтегральной функции), а второе справедливо потому, что контур интегрирования охватывает все полюсы подынтегральной функции, и при этом степень многочлена $W(\zeta)$ не превышает N_1 . $\square$

Рассмотрим многочлены

$$P_{klkj}(z) = \sum_{s=0}^n p_{klkjs} z^s, \quad k = 1, \dots, t, \quad l_k = 0, 1, \dots, \tau_k - 1, \quad j = 1, \dots, m + 2, \quad (11)$$

с неопределенными коэффициентами. Пусть

$$\sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} \sum_{j=1}^{m+2} P_{klkj}(z) F_{klkj}(z) = \sum_{\nu=0}^{\infty} C_{\nu} z^{\nu}. \quad (12)$$

ЛЕММА 3. При $\nu \geq n$ справедливо равенство

$$C_{\nu} = \frac{\prod_{x=1}^{\nu-n} a(x)}{\prod_{x=1}^{\nu} b(x)} \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} G_{klk}(\nu) \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)}, \quad (13)$$

где

$$G_{klk}(\nu) = \sum_{\mu=l_k}^{\tau_k-1} \sum_{s=0}^n \sum_{j=1}^{m+2} \binom{\mu}{l_k} p_{k\mu js} \chi_{kj}(\nu - s) \prod_{x=0}^{s-1} b(\nu - x) \prod_{x=1}^{n-s} a(\nu - n + x) \times$$

$$\times \frac{\partial^{\mu-l_k}}{\partial \lambda_k^{\mu-l_k}} \left(\prod_{x=0}^{s-1} (\nu + \lambda_k - x)(\nu + A - \lambda_k - x) \right) \quad (14)$$

ДОКАЗАТЕЛЬСТВО. Запишем и преобразуем выражение для C_{ν} , $\nu \geq n$, которое непосредственно вытекает из (1), (11) и (12); имеем

$$C_{\nu} = \sum_{k=1}^t \sum_{\mu=0}^{\tau_k-1} \sum_{s=0}^n \sum_{j=1}^{m+2} p_{k\mu js} \chi_{kj}(\nu - s) \prod_{x=1}^{\nu-s} \frac{a(x)}{b(x)} \frac{\partial^{\mu}}{\partial \lambda_k^{\mu}} \prod_{x=1}^{\nu-s} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)} =$$

$$= \frac{\prod_{x=1}^{\nu-n} a(x)}{\prod_{x=1}^{\nu} b(x)} \sum_{k=1}^t \sum_{\mu=0}^{\tau_k-1} \sum_{s=0}^n \sum_{j=1}^{m+2} p_{k\mu js} \chi_{kj}(\nu - s) \prod_{x=0}^{s-1} b(\nu - x) \prod_{x=1}^{n-s} a(\nu - n + x) \times$$

$$\times \frac{\partial^{\mu}}{\partial \lambda_k^{\mu}} \left(\prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)} \prod_{x=0}^{s-1} (\nu + \lambda_k - x)(\nu + A - \lambda_k - x) \right).$$

Последнюю частную производную заменим выражением

$$\sum_{l_k=0}^{\mu} \binom{\mu}{l_k} \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \prod_{x=1}^{\nu} \frac{1}{(\lambda_k + x)(A - \lambda_k + x)} \frac{\partial^{\mu-l_k}}{\partial \lambda_k^{\mu-l_k}} \left(\prod_{x=0}^{s-1} (\nu + \lambda_k - x)(\nu + A - \lambda_k - x) \right),$$

полученным с помощью правила Лейбница. После этого перегруппируем слагаемые, заменив $\sum_{\mu=0}^{\tau_k-1} \sum_{l_k=0}^{\mu}$ на $\sum_{l_k=0}^{\tau_k-1} \sum_{\mu=l_k}^{\tau_k-1}$. В результате получим требуемое. Лемма доказана. $\square$

Подберем теперь коэффициенты p_{kl_kjs} многочленов (11) так, чтобы тождественно по ν выполнялись равенства

$$B_{kl_k}(\nu) = G_{kl_k}(\nu), \quad k = 1, \dots, t, \quad l_k = 0, 1, \dots, \tau_k - 1; \quad (15)$$

многочлены, входящие в эти равенства, определяются соответственно формулами (7) и (14). Выполнения (15) можно добиться, рассуждая по индукции с использованием леммы 2. Зафиксируем k и определим сначала коэффициенты многочленов $P_{k,\tau_k-1,j}(z)$ с помощью равенства

$$\begin{aligned} \sum_{s=0}^n \sum_{j=1}^u p_{k,\tau_k-1,j} \chi_{kj}(\nu-s) \prod_{x=0}^{s-1} b(\nu-x)(\nu+\lambda_k-x)(\nu+A-\lambda_k-x) \prod_{x=1}^{n-s} a(\nu-n+x) = \\ = B_{k,\tau_k-1}(\nu), \end{aligned}$$

которое должно выполняться тождественно по ν . Из леммы 2 следует, что требуемые коэффициенты существуют, и их можно записать в виде интегралов (8), в которых следует $W(\zeta)$ заменить на $B_{k,\tau_k-1}(\zeta)$. В результате получим, учитывая (14) при $l_k = \tau_k - 1$, что при таком выборе коэффициентов $p_{k,\tau_k-1,j}$ требуемое равенство $B_{k,\tau_k-1}(\nu) = G_{k,\tau_k-1}(\nu)$ выполняется. Пусть теперь $0 \leq l_k < \tau_k - 1$, и пусть уже определены коэффициенты многочленов $P_{k,\tau_k-1,j}(z), \dots, P_{k,l_k+1,j}(z)$, $j = 1, \dots, m+2$ так, что (15) выполняется при $l_k = \tau_k - 1, \dots, \mu+1$. Потребуем, чтобы тождественно по ν выполнялось равенство

$$\begin{aligned} B_{k\mu}(\nu) - \sum_{l_k=\mu+1}^{\tau_k-1} \sum_{j=1}^s \sum_{s=0}^n p_{kl_kjs} \chi_j(\nu-s) \prod_{x=0}^{s-1} b(\nu-x) \prod_{x=1}^{n-s} a(\nu-n+x) \binom{l_k}{\mu} \times \\ \times \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \left(\prod_{x=0}^{s-1} (\nu+\lambda_k-x)(\nu+A-\lambda_k-x) \right) = \sum_{s=0}^n \sum_{j=1}^{m+2} p_{k\mu js} \chi_j(\nu-s) \times \\ \times \prod_{x=0}^{s-1} b(\nu-x)(\nu+\lambda_k-x)(\nu+A-\lambda_k-x) \prod_{x=1}^{n-s} a(\nu-n+x). \end{aligned}$$

Все коэффициенты p_{kl_kjs} , входящие в левую часть, определены по индуктивному предположению, а коэффициенты $p_{k\mu js}$ из правой части определяются с помощью леммы 2. Таким образом, все неопределенные коэффициенты многочленов (11) определены с помощью индукции.

Из (15), (13) и (6) следует, что

$$C_\nu = \frac{\prod_{x=1}^{\nu-n} a(x)}{\prod_{x=1}^{\nu} b(x)} \Phi(\nu), \quad (16)$$

при условии, что коэффициенты многочленов (11) определены указанным выше способом.

5. Доказательства теорем

В предыдущем разделе мы подобрали многочлены (11) так, что коэффициент при z^ν , $\nu = n+1, \dots, N_2-1$, в разложении по степеням z линейной формы (12) равен нулю. Это следует из (16) и первого свойства функции $\Phi(\nu)$ из леммы 1. Рассмотрим неоднородную линейную форму

$$R(z) = P_0(z) + \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} \sum_{j=1}^u P_{kl_kj}(z) F_{kl_kj}(z), \quad (17)$$

причем зададим многочлен $P_0(z) = \sum_{\nu=0}^n p_{0\nu} z^\nu$ так, чтобы эта форма имела при $z = 0$ порядок нуля, равный N_2 . Для этого, очевидно, следует положить

$$p_{0\nu} = - \sum_{k=1}^t \sum_{l_k=0}^{\tau_k-1} \sum_{j=1}^{m+2} \sum_{s=0}^{\nu} p_{kl_kjs} \chi_j(\nu-s) \prod_{x=0}^{\nu-s} \frac{a(x)}{b(x)} \frac{\partial^{l_k}}{\partial \lambda_k^{l_k}} \prod_{x=1}^{\nu-s} \frac{1}{(\lambda_k+x)(A-\lambda_k+x)}. \quad (18)$$

При этом получившаяся линейная форма не будет равняться нулю тождественно, поскольку коэффициент при z^{N_2} отличен от нуля в силу второго свойства функции $\Phi(\nu)$ из леммы 1. Таким образом, мы имеем эффективно построенную функциональную линейную приближающую форму для функций (1), имеющую при $z = 0$ порядок нуля, лишь на константу отличающийся от максимально возможного. Для дальнейшего важно получить оценку сверху модуля неоднородной линейной формы (17), а также оценку сверху модулей многочленов $P_{kl_kj}(z)$ при $z = \xi$; для многочленов $P_0(z)$ и $P_{kl_kj}(z)$ потребуется еще и оценка сверху общего наименьшего знаменателя их коэффициентов. Получение таких оценок является стандартной вычислительной процедурой, основанной на равенстве (16) и на указанных выше явных формулах для коэффициентов рассматриваемых многочленов. Приведем здесь лишь окончательные результаты:

$$|R(\xi)| \leq e^{\gamma_2 n} (n!)^{-T(m+2)(m+2-r)}; \quad |P_{kl_kj}(\xi)| \leq e^{\gamma_3 n} (n!)^{m+2-r}.$$

При получении оценки сверху общего наименьшего знаменателя коэффициентов многочленов основным моментом является рациональность параметров функций (1); при выполнении этого условия указанный общий наименьший знаменатель не превосходит $e^{\gamma_4 n}$.

Дальнейшие рассуждения скопируем с доказательства первой основной теоремы из [1, с. 91]. Для этого заметим сначала, что функции (1) при $j = 1$, $l_k = 0$, $k = 1, \dots, t$, удовлетворяют уравнению

$$(\delta + \lambda_k)(\delta + A - \lambda_k)b(\delta)y = a(\delta)zy + \lambda_k(A - \lambda_k)b(0), \quad \text{где } \delta = z \frac{d}{dz}.$$

Дифференцируя последнее соотношение по λ_k , получим уравнения, которым удовлетворяют функции (1) при различных значениях l_k . Добавим к функциям (1) функцию, тождественно равную единице, и занумеруем получившиеся функции в произвольном порядке, обозначив их

$$f_1(z), \dots, f_M(z), \quad (19)$$

$M = T(m+2) + 1$. Из сказанного следует, что функции (18) удовлетворяют системе дифференциальных уравнений

$$y'_v = \sum_{i=1}^M q_{vi} y_i, \quad v = 1, \dots, M, \quad q_{vi} \in \mathbb{C}(z).$$

Обозначим через $q = q(z)$ общий наименьший знаменатель рациональных функций $Q_{vi}(z)$. В нашем случае $q(z)$ есть некоторая степень z . Новые обозначения введены для того, чтобы было удобнее следовать рассуждениям, доказывающим первую основную теорему из [1, с. 91]. Мы имеем форму (16), которую запишем в виде

$$R(z) = R_1(z) = \sum_{i=1}^M P_{1i}(z) f_i(z).$$

Далее, как и при доказательстве упомянутой первой основной теоремы из [1], положим

$$R_k = qR'_{k-1}, \quad k = 2, 3, \dots$$

В результате получим совокупность приближающих линейных форм для функций (18). Из леммы 9, [1, с. 106] следует, что определитель

$$\Delta(z) = |P_{vi}(z)|_{v,i=1,\dots,M}$$

отличен от тождественного нуля и имеет вид

$$\Delta(z) = z^{Mn-\gamma_5} \Delta_1(z),$$

причем определитель $\Delta_1(z)$ не равен нулю тождественно. При доказательстве этого утверждения существенно используется линейная независимость функций (18) над полем рациональных дробей. Затем осуществим переход к числовым формам. Из леммы 10, [1, с. 107] следует, что матрица

$$(P_{vi}(\xi))_{\substack{v=1,\dots,M+\gamma_6 \\ i=1,\dots,M}}$$

имеет ранг M . Повторяя с очевидными изменениями рассуждения, доказывающие лемму 16 из [1, с. 118-119], получаем аналог этой леммы для нашего случая.

ЛЕММА 4. *Существуют целые числа g_{vi} , $v, i = 1, \dots, M$, такие, что выполняются следующие условия*

- 1) *определитель $|g_{vi}|_{v,i=1,\dots,M}$ отличен от нуля;*
- 2) $\left| \sum_{i=1}^M g_{vi} f_i(\xi) \right| \leq e^{\gamma n} (n!)^{-T(m+2)(m+2-r)}, v = 1, \dots, M;$
- 3) $|g_{vi}| \leq e^{\gamma n} (n!)^{m+2-r}, v, i = 1, \dots, M.$

Пользуясь последней леммой, нетрудно доказать теорему 1. Оценка получится точнее, чем в упомянутой теореме из [1]. Причина этого заключается в том, что построенная эффективно линейная приближающая форма (17) имеет более высокий порядок нуля при $z = 0$, чем построенная с помощью принципа Дирихле приближающая форма, используемая при доказательстве теоремы 1 из [1, с. 354].

Доказательство теоремы 2 мало отличается от доказательства теоремы 1. Поэтому ограничимся лишь указанием основных отличий. Рассмотрим вспомогательную функцию вида (4), но число N_2 , входящее в правую часть формулы (4), заменим на $T(m+2)(n+1) - 1$. Функциональной линейной приближающей формой здесь служит (12), а не (17), и в связи с этим возникает еще одно отличие, состоящее в том, что если $0 \leq \nu \leq n$, то при вычислении коэффициентов линейной формы (12) индекс s изменяется от нуля до ν ; см. левую часть равенства (14). Однако после вынесения за знаки суммирования произведения $\prod_{x=1}^{\nu} (b(x))^{-1}$ это ν можно заменить на n , используя условие $b(0) = 0$. В остальном доказательство теоремы 2 вполне аналогично доказательству теоремы 1.

Заключение

Эффективно построенную в данной работе приближающую функциональную форму можно применить и для решения других задач, относящихся к арифметической природе значений функций (1). Можно, например, применить эту конструкцию для функций вида (1), не все параметры которых рациональны. При этом, по-видимому, придется заменить многочлен $a(x)$ на тождественную единицу и ввести другие ограничения. Не исключено также, что в неоднородном случае потребуются привлечь сведения из теории делимости в полях алгебраических чисел, как это сделано в работе [25].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Шидловский А. Б. Трансцендентные числа. М.: Наука, 1987.
2. Белогривов И. И. О трансцендентности и алгебраической независимости значений некоторых E -функций // Вестник МГУ. Сер. 1: Математика, механика. 1967. № 2. С. 55–62.
3. Белогривов И. И. О трансцендентности и алгебраической независимости значений E -функций одного класса // Сибирский математический журнал. 1973. Т. 14. № 1. С. 16–35.
4. Шидловский А. Б. О трансцендентности и алгебраической независимости значений целых функций некоторых классов. Ученые записки МГУ. 1959, вып. 186. Математика, 9. С. 11–70.
5. Шидловский А. Б. О трансцендентности и алгебраической независимости значений некоторых функций // Труды Московского матем. общества. 1959. Т. 8. С. 283–320.
6. Шидловский А. Б. О трансцендентности и алгебраической независимости значений целых функций некоторых классов // ДАН СССР. 1954. Т. 96, № 4. С. 697–700.
7. Шидловский А. Б. О трансцендентности и алгебраической независимости значений E -функций, удовлетворяющих линейным неоднородным дифференциальным уравнениям второго порядка // ДАН СССР. 1966. Т. 169, № 1. С. 42–45.
8. Шидловский А. Б. Об алгебраической независимости значений некоторых гипергеометрических E -функций. // Труды Московского математического общества. 1967. Т. 18, № 4. С. 55–64.
9. Белогривов И. И. О трансцендентности и алгебраической независимости значений некоторых гипергеометрических E -функций // ДАН СССР. 1967. Т. 174, № 2. С. 267–270.
10. Чирский В. Г. Об арифметических свойствах значений гипергеометрических функций с иррациональными параметрами // Вестник МГУ. Серия 1, математика, механика. 1978, № 5. С. 3–8.
11. Салихов В. Х. Неприводимость гипергеометрических уравнений и алгебраическая независимость значений E -функций // Acta Arithm. 1990. **53**:5. Р. 453–471.
12. Черепнев М. А. Об алгебраической независимости значений гипергеометрических E -функций // Математические заметки. 1995. **57**:6. С. 896–912.
13. Салихов В. Х. Критерий алгебраической независимости значений гипергеометрических E -функций (четный случай) // Математические заметки. 1998. **64**:2. С. 273–284.
14. Горелов В. А. Об алгебраической независимости значений обобщенных гипергеометрических функций // Математические заметки. 2013. **94**:1. С. 94–108.
15. Горелов В. А. Об алгебраических свойствах решений неоднородных гипергеометрических уравнений // Математические заметки. 2016. **99**:5. С. 658–672.
16. Mahler K. Application of a theorem by A.B.Shidlovski // Proc. Roy. Soc. Ser. A. 1968. V. 305. Р. 149–173.
17. Väinänen K. On the algebraic independence of the values of some E -functions. // Ann. Acad. Sci. Fennicae. Ser. A. Math. 1975. V. 1. Р. 93–109.

18. Иванков П. Л. О дифференцировании гипергеометрической функции по параметру // *Фундаментальная и прикладная математика*. 2010. Т. 16, вып. 6 С. 91–94.
19. Иванков П. Л. О дифференцировании по параметру // *Чебышевский сборник*. 2015. Т. 16, вып. 3. С. 285–294.
20. Иванков П. Л. О дифференцировании по параметру некоторых функций // *Наука и образование. Электронное научно-техническое издание* 2012, № 5. С. 141 – 154. DOI: 10.7463/0512.0398478.
21. Иванков П. Л. О значениях продифференцированных по параметру гипергеометрических функций // *Чебышевский сборник* 2012. Т. 13, вып. 2. С. 64–70.
22. Иванков П. Л. Об арифметических свойствах значений гипергеометрических функций с различными параметрами // *Математические заметки*. 1992. Т. 52, выпуск 6. С. 25-31.
23. Иванков П. Л. Об арифметических свойствах значений гипергеометрических функций // *Математический сборник*. 1991. Т. 182, № 2. С. 283–302.
24. Маркушевич А. И. Теория аналитических функций, т. 1. М.: Наука, 1967.
25. Галочкин А. И. Об арифметических свойствах значений некоторых целых гипергеометрических функций // *Сибирский матем. журнал*. 1976. Т. 17, № 6. С. 1220-1235.

REFERENCES

1. Shidlovskii, A. B. 1987, "Transcendentnye chisla"[Transcendental numbers] "*Nauka*", 448 pp. (Russian).
2. Belogrivov, I. I. 1967, "Transcendentality and algebraic independence of values of certain E-functions *Vestnik Moskov. Univ. Ser. 1 Math. Mech.*, vol. 22, no. 2, pp. 55-62. (Russian).
3. Belogrivov, I. I. 1973, "The transcendence and algebraic independence of the values of a certain class of E-functions *Sibirsk. Math. Zh.*, vol. 14, pp. 16-35. (Russian).
4. Shidlovskii, A. B. 1959, "Transcendence and algebraic independence of the values of entire functions of certain class *Moskov. Gos. Univ. Uch. Zap.*, no. 186, pp. 11-70. (Russian).
5. Shidlovskii, A. B. 1959, "On transcendence and algebraic independence of the values of certain functions *Trudy Moskov. Math. Obsh.*, vol. 8, pp. 283-320. (Russian).
6. Shidlovskii, A. B. 1954, "On transcendentality and algebraic independence of the values of entire functions of certain class *Dokl. Akad. Nauk SSSR*, vol. 96, № 4. pp. 697-700. (Russian).
7. Shidlovskii, A. B. 1954, "Transcendence and algebraic independence of values of *E*-functions satisfying linear nonhomogeneous differential equations of the second order *Dokl. Akad. Nauk SSSR*, vol. 169, № 1. pp. 42-45. (Russian).
8. Shidlovskii, A. B. 1968, "Algebraic independence of the values of certain hypergeometric *E*-functions *Trudy Moskov. Mat. Obsh.*, vol. 18, № 4. pp. 55-64. (Russian).
9. Belogrivov I.I., 1967, "On transcendence and algebraic independence of values of certain hypergeometric *E*-functions *Dokl. Akad. Nauk SSSR*, vol. 174, № 2. pp. 267-270. (Russian).
10. Chirsky V.G., 1978, "On arithmetic properties of the values of hypergeometric functions with irrational parameters *Vestnik Moskov. Univ. Ser. 1. Mat. Meh.* no. 5, pp. 3-8.

11. Salikhov V.Kh., 1990, "Irreducibility of hypergeometric equations and algebraic independence of values of E -functions 1990, *Acta Arithm.*, **53**:5, pp. 453-471.
12. Cherepnev M.A., 1995, "On algebraic independence of values of hypergeometric E -functions *Mat. Zametki*, vol. 57, no. 6, pp. 896-912.
13. Salikhov V.Kh., 1998, "Criterion for the algebraic independence of the values of hypergeometric E -functions (even case) *Mat. Zametki*, vol. 64, no. 2, pp. 273-284.
14. Gorelov V.A., 2013, "On algebraic independence of the values of hypergeometric functions *Mat. Zametki*, vol. 94, no. 1, pp. 94-108.
15. Gorelov V.A., 2016, "On algebraic properties of the solutions of nonhomogeneous hypergeometric equations *Mat. Zametki*, vol. 99, no. 5, pp. 658-672.
16. Mahler, K. 1968, "Application of a theorem by A. B. Shidlovskii *Proc. Roy. Soc. Ser. A*, v. 305, pp. 149-173.
17. Väinänen, K. 1975, "On the algebraic independence of the values of some E -functions *Ann. Acad. Sci. Fennicae. Ser. A. Math.*, v. 1. pp. 93-109.
18. Ivankov, P. L. 2010, "On differentiation of a hypergeometric function with respect to parameter *Fundamentalnaya i Prikladnaya Matematika*, v. 18, issue 6, pp. 91-94. (Russian).
19. Ivankov, P. L. 2015, "On differentiation with respect to parameter", *Chebyshev. Sbornik*, v. 16, issue 3, pp. 285-294. (Russian).
20. Ivankov, P. L. 2012, "On differentiation with respect to parameter of certain functions *Science and Education of the Bauman MSTU*, no. 5, pp. 285-294. DOI: 10.7463/0512.0398478 (Russian).
21. Ivankov, P. L. 2012, "On the values of the differentiated with respect to parameter hypergeometric functions *Chebyshevsky Sbornik*, v. 13, issue 2, pp. 64-70. (Russian).
22. Ivankov, P. L. 1992, "Arithmetic properties of the values of hypergeometric functions with different parameters *Mathematical Notes*, vol. 52, no. 6, pp. 1188-1192.
23. Ivankov, P. L. 1991, "On arithmetic properties of the values of hypergeometric functions *Math. Sbornik*, v. 182, no. 2, pp. 283-302. (Russian).
24. Markushevich, A.I. 1967, "Theory of analytic functions v. I. *Nauka*", 486 pp. (Russian).
25. Galochkin, A.I. 1976, "On arithmetic properties of the values of certain entire hypergeometric functions *Sibirsk. Matem. Zhurnal*, v. 17, no. 6, pp. 1220-1235. (Russian).

Получено 23.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.42

DOI 10.22405/2226-8383-2020-21-1-213-220

**Интервалы малой длины, содержащие
алгебраическое число заданной высоты**

Н. И. Калоша, И. А. Корлюкова, Е. В. Гусева

Калоша Николай Иванович — кандидат физико-математических наук, научный сотрудник, Институт математики НАН Беларуси (г. Минск).

e-mail: kalosha@im.bas-net.by

Корлюкова Ирина Александровна — кандидат физико-математических наук, доцент, декан факультета довузовской подготовки, Гродненский государственный университет имени Янки Купалы (г. Гродно).

e-mail: korlyukova_ia@grsu.by

Гусева Елена Васильевна — аспирант, Институт математики НАН Беларуси (г. Минск).

e-mail: elena.guseva.96@yandex.by

Аннотация

Рациональные числа распределены равномерно, хотя расстояния между соседними рациональными числами в последовательности Фарея могут сильно разниться. Для алгебраических чисел это свойство не выполняется. В 2013 г. Д. Коледа [6, 7] нашел функцию плотности распределения действительных алгебраических чисел любой степени при их естественном упорядочивании.

Можно доказать, что количество действительных алгебраических чисел α степени n и высоты $H(\alpha) \leq Q$ асимптотически равно $c_1(n)Q^{n+1}$. Недавно было доказано, что существуют интервалы длины $Q^{-\gamma}$, $\gamma > 1$, свободные от алгебраических чисел α , $H(\alpha) \leq Q$, однако уже при $0 \leq \gamma < 1$ их не менее чем $c_2(n)Q^{n+1-\gamma}$.

В работе показано, что специальные интервалы длины $Q^{-\gamma}$ и при больших γ могут содержать алгебраические числа, однако их количество не превосходит $c_3Q^{n+1-\gamma}$. Ранее аналогичный результат был получен А. Гусаковой [16] лишь для случая $\gamma = \frac{3}{2}$.

Ключевые слова: алгебраические числа, диофантовы приближения, равномерное распределение, теорема Дирихле.

Библиография: 17 названий.

Для цитирования:

Н. И. Калоша, И. А. Корлюкова, Е. В. Гусева Интервалы малой длины, содержащие алгебраическое число заданной высоты // Чебышевский сборник, 2020, т. 21, вып. 1, с. 213–220.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.42

DOI 10.22405/2226-8383-2020-21-1-213-220

**Intervals of small measure containing
an algebraic number of given height**

N. I. Kalosha, I. A. Korlyukova, E. V. Guseva

Kalosha Nikolai Ivanovich — Ph. D., researcher, Institute of mathematics of the National Academy of Sciences of Belarus (Minsk).

e-mail: kalosha@im.bas-net.by

Korlyukova Irina Alexandrovna — Ph.D., associate professor, Dean of the Faculty of Pre-University Training (Grodno).

e-mail: korlyukova_ia@grsu.by

Guseva Elena Vasilyevna — Ph. D. student, Institute of mathematics of the National Academy of Sciences of Belarus (Minsk).

e-mail: elena.guseva.96@yandex.by

Abstract

Rational numbers are uniformly distributed, even though distances between rational neighbors in a Farey sequence can be quite different. This property doesn't hold for algebraic numbers. In 2013 D. Koleda [6, 7] found the distribution function for real algebraic numbers of an arbitrary degree under their natural ordering.

It can be proved that the quantity of real algebraic numbers α of degree n and height $H(\alpha) \leq Q$ asymptotically equals $c_1(n)Q^{n+1}$. Recently it was proved that there exist intervals of length $Q^{-\gamma}$, $\gamma > 1$, free of algebraic numbers α , $H(\alpha) \leq Q$, however for $0 \leq \gamma < 1$ there exist at least $c_2(n)Q^{n+1-\gamma}$ algebraic numbers in such intervals.

In this paper we show that special intervals of length $Q^{-\gamma}$ may contain algebraic numbers even for large values of γ , however their quantity doesn't exceed $c_3Q^{n+1-\gamma}$. An earlier result by A. Gusakova [16] was proved only for the case $\gamma = \frac{3}{2}$.

Keywords: algebraic number, Diophantine approximation, uniform distribution, Dirichlet's theorem.

Bibliography: 17 titles.

For citation:

N. I. Kalosha, I. A. Korlyukova, E. V. Guseva, 2020, "Intervals of small measure containing an algebraic number of given height *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 213–220.

1. Введение

Распределение рациональных чисел является хорошо изученным. Математикам известно много фактов о распределении рациональных чисел, как в одномерном, так и в многомерном случаях. Многие из них следуют из свойств рядов Фарея [9] — например, теорема Дирихле, которая лежит в основе теории диофантовых приближений [5, 9].

Пусть $Q > 1$ — натуральное число, $\alpha \in \mathbb{R}$. Тогда неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qQ} \quad (1)$$

имеет решение в рациональных числах $(p, q) \in \mathbb{Z} \times \mathbb{N}$, $1 \leq q \leq Q$.

Из неравенства (1) нетрудно получить другое утверждение, которое также называют теоремой Дирихле.

Для любого $\alpha \in \mathbb{R}$ неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2} \quad (2)$$

имеет бесконечное число решений в натуральных $q > 1$. Целое число p в (2) определяется однозначно, поскольку для $q \geq 2$ для правой части справедливо $q^{-2} < 1/2q^{-1}$.

Более того, используя ряды Фарея можно доказать теорему Гурвица [9]: для любого иррационального $\beta \in \mathbb{R}$ неравенство

$$\left| \beta - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2} \quad (3)$$

имеет бесконечно много решений в $(p, q) \in \mathbb{Z} \times \mathbb{N}$; однако при любом $\varepsilon > 0$ и $q > q_0(\varepsilon)$ уже существуют $\beta_1 \in \mathbb{R}$, для которых верно неравенство

$$\left| \beta_1 - \frac{p}{q} \right| > \frac{1}{(\sqrt{5} + \varepsilon)q^2}.$$

Например, можно взять $\beta_1 = \frac{\sqrt{5}-1}{2}$. Заметим, что неравенства (2), (3) значительно сильнее неравенств $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q}$, справедливых для произвольного q и используемых в приближённых вычислениях.

Сделаем еще одно замечание о кажущейся простоте последовательностей Фарея. Существует теорема о том, что свойство “равномерности” рядов Фарея эквивалентно одной из самых знаменитых нерешенных проблем — проблеме о нулях дзета-функции Римана.

Задача приближения действительных чисел значительно усложняется, если в качестве приближающих элементов взять алгебраические числа. Рассмотрим неравенство, аналогичное (2):

$$|\xi - \alpha| < H(\alpha)^{-v}, \quad v > 0. \quad (4)$$

В неравенстве (4) число β — произвольное действительное число, α — алгебраическое число степени $\deg \alpha = n$ и высоты $H(\alpha)$. В 1961 году Вирзинг [15] сформулировал следующую проблему: имеет ли неравенство (4) бесконечное число решений в алгебраических числах α , $\deg \alpha \leq n$, при любом ξ и $v \leq n + 1$? Им была доказана лишь разрешимость неравенства (4) при $v = \frac{n}{2} + \gamma_n$, где $\gamma_n \rightarrow 2$, $n \rightarrow \infty$. Шмидт и Дэвенпорт доказали гипотезу Вирзинга при $n = 2$ [14]. Наилучшие до настоящего времени неравенства для v получены в работах белорусских математиков [1, 13]. Совсем недавно еще один белорусский математик Д. Бодягин в соавторстве с Й. Шлейшитцем [17] доказал гипотезу Вирзинга с $v = \frac{n}{\sqrt{3}} = 0,577n$.

2. Основная задача

Рассмотрим последовательность действительных алгебраических чисел α степени $\deg \alpha = n$ и высоты $H(\alpha) \leq Q$, где $Q > 1$ — натуральное число. Малер предположил, что распределение такой последовательности стремится к равномерному распределению, о чем и написал в письме к Спринджуку в 1985 году. Однако эта гипотеза оказалась неверной. В 2013 году Д. Коледа нашел функцию распределения действительных алгебраических чисел при их естественном упорядочении, а затем получил несколько обобщений своего результата [6, 7].

Несколько результатов о распределении алгебраических чисел доказано в [2, 3]. При этом во всех результатах важна зависимость длины интервалов от высоты. Зависимость от степени выходит на второй план. Важно только, что эту зависимость можно вычислить.

ТЕОРЕМА 1. *Существуют интервалы I длины $|I| = 0,5Q^{-1}$, не содержащие алгебраических чисел α любой степени $n \geq 1$ при ограничении $H(\alpha) \leq Q$.*

ТЕОРЕМА 2. *При некотором $c_1 > c_0(n)$ интервал $I_1, |I_1| > c_1Q^{-v}, 0 \leq v < 1$, содержит c_2Q^{n+1-v} алгебраических чисел α , $\deg \alpha \leq n$, $H(\alpha) \leq Q$.*

Теорему 1 легко доказать, если рассмотреть интервалы вида $(\xi, \xi + 0,5Q^{-1})$, где ξ — рациональное число с малым знаменателем (например, $\xi = 0$).

Доказательство теоремы 2 заметно сложнее. Оно основано на современных результатах метрической теории диофантовых приближений — в частности, доказанной Спринджукон проблеме Малера [8]. С помощью принципа Дирихле можно доказать, что при любом $x \in \mathbb{R}$ и $Q > 1$ неравенство

$$|P(x)| < Q^{-n} \quad (5)$$

разрешимо в $P(x) \in \mathbb{Z}[x]$, $\deg P \leq n$, $H(P) \leq Q$.

Добавим к (5) неравенство

$$|P'(x)| < \delta_0 Q. \quad (6)$$

Обозначим через $B_1 \subset I$ множество $x \in I$, для которых разрешима система неравенств (5), (6). Оказывается [9, 10], что при достаточно малом δ_0 верно неравенство

$$\mu B_1 < \frac{1}{4}|I|,$$

где μB_1 — мера Лебега множества B_1 . Поэтому для множества $B_2 = I \setminus B_1$ справедливо неравенство

$$\mu B_2 \geq \frac{3}{4}|I|. \quad (7)$$

ЛЕММА 1. [12, 8] *Если α_1 — ближайший к x корень многочлена $P_1(x)$, то справедливо неравенство*

$$|x - \alpha_1| < n|P(x)||P'(x)|^{-1} < n\delta_0^{-1}Q^{-n-1}.$$

Воспользуемся для $x_1 \in B_2$ леммой 1 и найдем алгебраическое число α_1 , $\deg \alpha_1 \leq n$, $H(\alpha_1) \leq Q$, на интервале I_1 длины $|I_1| = 2n\delta_0^{-1}Q^{-n-1}$. Исключим интервал I_1 из множества B_2 и обозначим $B_3 = I \setminus (B_1 \cup B_2)$. Возьмем $x_2 \in B_3$, для которого найдем алгебраическое число α_2 — корень полинома $P_2(x)$ из неравенства

$$|x_2 - \alpha_2| < n\delta_0^{-1}Q^{-n-1}. \quad (8)$$

Интервал (8) обозначим I_2 .

Этот процесс можно продолжать, пока мы не исчерпаем интервалами длины $n\delta_0^{-1}Q^{-n-1}$ все точки множества B_2 . Учитывая (7), можно построить не менее чем

$$\frac{3}{8}n^{-1}\delta_0Q^{n+1}|I| > 2^{-2}n^{-1}\delta_0Q^{n+1}|I|$$

алгебраических чисел α , $\deg \alpha \leq n$, $H(\alpha) \leq Q$.

При оценках сверху для количества алгебраических чисел на интервале I , $|I| = Q^{-\gamma}$, будем снова использовать принцип ящиков Дирихле. Если в данном интервале достаточно много алгебраических чисел, то можно построить полиномы небольшой степени, принимающие на I малые значения. Далее применим следующие леммы.

ЛЕММА 2. [4, 8] Пусть

$$P(x) = \prod_{j=1}^k T_j^{a_j}(x), \quad 1 \leq k \leq n, \quad -$$

разложение приводимого полинома $P(x)$ на степени неприводимых полиномов, и $H(T_j)$ — высоты полиномов $T_j(x)$. Тогда существуют положительные величины c и c' , зависящие только от n , такие что

$$cH(P) < \prod_{j=1}^k H(T_j)^{a_j} < c'H(P).$$

Лемма 2 утверждает, что высоты полиномов обладают почти мультипликативным свойством.

ЛЕММА 3. [11] Пусть $P_1(x)$ и $P_2(x)$ — целочисленные полиномы без общих корней такие, что

$$\deg P_1 \leq n, \quad \deg P_2 \leq n, \quad H(P_1) \leq Q, \quad H(P_2) \leq Q.$$

Предположим, что для всех точек интервала I , $|I| = Q^{-\eta}$, $\eta > 0$ выполняется неравенство

$$\max(|P_1(x)|, |P_2(x)|) < Q^{-\tau}, \quad \tau > 0.$$

Тогда для любого $\delta > 0$ и достаточно большого $Q > Q_0(\delta)$ справедливо неравенство

$$\tau + 1 + 2 \max(\tau + 1 - \eta, 0) < 2n + \delta.$$

Когда все полиномы $P_j(x)$ имеют общий множитель, применение леммы 2 на определенном ранее интервале I сопряжено с некоторыми трудностями. Ниже будет показано, как их можно преодолеть.

Интервал I длины $|I| = Q^{-\gamma}$ будем называть (k, v) интервалом, если ему принадлежит алгебраическое число β степени $\deg \beta = k$, $1 \leq k \leq n$, и высоты $H(\beta) = Q^v$. Его минимальный многочлен обозначим $T(x)$. Обозначим через $\#\mathcal{P}_n(Q, \gamma)$ количество алгебраических чисел α — корней полиномов из $\mathcal{P}_n(Q)$.

ТЕОРЕМА 3. При условии

$$\gamma > v \frac{n^2}{n - k + 1} + 1$$

интервалу I принадлежит не более $cQ^{n+1-\gamma}$ алгебраических чисел α , $\deg \alpha = n$, $H(\alpha) \leq Q$.

ДОКАЗАТЕЛЬСТВО. Предположим противное:

$$\#\mathcal{P}_n(Q, \gamma) > cQ^{n+1-\gamma},$$

где $c = c(n)$ — произвольно большая константа. Рассмотрим n -мерные кубы со стороной Q^{v_1} , $0 \leq v_1 \leq 1$, и покроем куб $[-Q, Q]^n$ объединением кубов

$$\bigcup_{k=1}^n \bigcup_{-Q^{1-v_1} \leq i_k \leq Q^{1-v_1}-1} S_{\overline{k}, \overline{i_k}} = \bigcup_{k=1}^n \bigcup_{-Q^{1-v_1} \leq i_k \leq Q^{1-v_1}-1} [i_k Q^{v_1}, (i_k + 1) Q^{v_1}].$$

Количество кубов $S_{\overline{k}, \overline{i_k}}$ не превосходит $(2Q^{1-v_1} + 1)^n < 2^{n+1} Q^{(1-v_1)n}$ при достаточно большом Q . Если

$$2^{n+1} Q^{(1-v_1)n} < cQ^{n+1-\gamma}, \quad (9)$$

то по принципу Дирихле найдется n -мерный куб S' со стороной Q^{v_1} и два полинома $P_1(x), P_2(x) \in \mathcal{P}_n(Q)$, коэффициенты которых $\bar{a} = (a_1, \dots, a_n)$ лежат в S' . Рассмотрим полином

$$R(x) = P_2(x) - P_1(x) \quad (10)$$

с коэффициентами $\bar{b} = (b_0, b_1, \dots, b_n)$. Из (10) теперь следует, что $|b_j| \leq Q^{v_1}, 1 \leq j \leq n$. Разложим каждый из полиномов $P_i(x), i = 1, 2$, в ряд Тейлора на интервале I в окрестности своего корня $\alpha_i = \alpha_1(P_i)$:

$$P_i(x) = P(\alpha_1) + P'(\alpha_1)(x - \alpha_1) + \sum_{j=2}^n P^{(j)}(\alpha_i)(x - \alpha_i)^j. \quad (11)$$

Так как в (11)

$$P(\alpha_1) = 0, \quad P'(\alpha_1) < n^2 Q, \quad |x - \alpha_1| < Q^{-\gamma},$$

то, оценив все слагаемые в разложении (11), получим оценку

$$|P_i(x)| < n^3 Q^{1-\gamma}, \quad |R(x)| < 2n^3 Q^{1-\gamma}. \quad (12)$$

Из (12) можно оценить и свободный коэффициент b_0 многочлена $R(x)$: $|b_0| < 2Q^{v_1}$, откуда

$$H(R) < 2Q^{v_1}. \quad (13)$$

Разрешим неравенство (13) относительно v_1 . Поскольку при $1 - v_1 = 1 + \frac{1-\gamma}{n}$ мы имеем $v_1 = \frac{\gamma-1}{n}$, то при достаточно большой величине s можно добиться выполнения неравенства

$$H(R) < cQ^v, \quad \frac{\gamma-1}{n} \leq v. \quad (14)$$

Многочлен $R(x)$ по лемме 1 не может иметь с многочленом $T(x)$ общих корней. Рассмотрим модуль результата полиномов $T(x)$ и $R(x)$ с корнями $\beta_1, \dots, \beta_k, \alpha_1, \dots, \alpha_n$ и коэффициентами $b_k, \dots, b_0$ и $a_n, \dots, a_0$

$$1 \leq |\text{Res}(T, R)| = |a_n^k b_k^n| \prod_{1 \leq i \leq n, 1 \leq j \leq k} |\alpha_i - \beta_j| < cQ^{\frac{\gamma-1}{n}k + vn} |\alpha_1 - \beta|,$$

где β — корень многочлена $T(x)$, лежащий в I . По лемме 1 из неравенства (12) следует

$$|x - \alpha_1| < 2n^3 Q^{1-\gamma} a_n^{-1} < cQ^{1-\gamma-\frac{\gamma-1}{n}}.$$

Подставляя β вместо x , получаем следующую оценку для результата:

$$1 \leq |\text{Res}(T, R)| < cQ^{vn + \frac{\gamma-1}{n}k - \gamma + 1 - \frac{\gamma-1}{n}}.$$

Данное неравенство противоречиво при

$$\gamma > v \frac{n^2}{n+1-k} + 1, \quad (15)$$

что доказывает теорему. $\square$

В заключение отметим, что добиться выполнения условия (15) несложно: можно взять, например, $\gamma = 3, k = \frac{n}{2} + 1, v = n^{-1}$ или $\gamma = 10, k = \frac{n}{10} + 1, v = 0,8$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Берник, В. И. Целочисленные многочлены с перепадами высот коэффициентов и гипотеза Вирзинга / В. И. Берник, К. И. Тищенко // Докл. АН Беларуси. — 1993. Т. 37. — №5. — С. 9–11.
2. Берник, В. И. Распределение действительных алгебраических чисел произвольной степени в коротких интервалах / В. И. Берник, Ф. Гётце // Изв. РАН Сер. матем. — 2014. Т. 79. — №1. — С. 21–42.
3. Берник, В. И. Распределение действительных алгебраических чисел произвольной степени в коротких интервалах (исправленный вариант) / В. И. Берник, Ф. Гётце // Изв. РАН. Сер. матем. — 2015 — Т. 79. — С. 21–42.
4. Гельфонд, А. О. Об алгебраической независимости трансцендентных чисел некоторых классов / А. О. Гельфонд. // УМН. — 1949. — Т.4. — №5. — С. 14–48.
5. Касселс, Дж. В. С. Введение в теорию диофантовых приближений / Дж. В. С. Касселс. — Москва: Изд-во Иностран. Литер., 1961. — 213 с.
6. Коледа, Д. В. О распределении действительных алгебраических чисел второй степени / Д. В. Коледа // Весці НАН Беларусі. Сер. фіз.-мат. навук. — 2013. — № 3. — С. 54–63.
7. Koleda, D. V. On the density function of the distribution of real algebraic numbers / D. V. Koleda // J. Théor. Nombres Bordeaux. — 2017. — Vol. 29, no. 1. — P. 179–200.
8. Спринджук, В. Г. Проблема Малера в метрической теории чисел / В. Г. Спринджук. — Минск : Наука и техника. 1967. — 181 с.
9. Beresnevich, V. Rational Points near Manifolds and Metric Diophantine Approximation / V. Beresnevich // Annals of Mathematics, Second Series. — 2012. — Vol. 175, no. 1. — P. 187–235.
10. Beresnevich, V. V. Integral polynomials with small discriminants and resultants / V. V. Beresnevich, V. I. Bernik, F. Goetze // Adv. Math. — 2016. — Vol. 298. — P. 393–412.
11. Берник, В. И. Применение размерности Хаусдорфа в теории диофантовых приближений / В. И. Берник // Acta Arithmetica. — 1983. — № 42. — С. 219–253.
12. Dodson, M. M. Metric Diophantine approximation on manifolds / M. M. Dodson, V. I. Bernik // Cambridge Tracts in Mathematics. — 1999. — №.137, 172 p.
13. Tishchenko, K. On approximation to real numbers by algebraic numbers / K. Tishchenko // Acta Arithmetica. — 2000. — №94 — Vol. 1. — P. 1–24.
14. Davenport, H. Dirichlet's theorem on diophantine approximation / H. Davenport, W. M. Schmidt // Symposia Mathematica. — 1970. — Vol. 4. — N. Y.—London. — P. 113–132.
15. Wirsing, E. Approximation mit algebraischen Zahlen beschränkten Grades. / E. Wirsing // Journal für die reine und angewandte Mathematik. — 1961. — Vol. 206. — P. 67–77.
16. Гетце, Ф. Алгебраические числа в коротких интервалах / Ф. Гетце, А. Г. Гусакова // Доклады Национальной академии наук Беларуси. — 2015. — Т. 59, № 4. — С. 11–16.
17. Badziahin, D. An improved bound in Wirsing's problem / D. Badziahin, J. Schleischitz // <https://arxiv.org/abs/1912.09013>.

REFERENCES

1. Берник, В. И., Тищенко К. И. 1993, “Целочисленные многочлены с перепадами высот коэффициентов и гипотеза Вирзинга”, *Докл. АН Беларуси.*, Т. 37, № 5, С. 9–11.
2. Берник, В. И., Гётце, Ф. 2014, “Распределение действительных алгебраических чисел произвольной степени в коротких интервалах”, *Изв. РАН Сер. матем.*, Т. 79, № 1, С. 21–42.
3. Берник, В. И., Гётце, Ф. 2015, “Распределение действительных алгебраических чисел произвольной степени в коротких интервалах” (исправленный вариант), *Изв. РАН. Сер. матем.*, Т. 79, № 1, С. 21–42.
4. Гельфонд, А. О. 1949, “Об алгебраической независимости трансцендентных чисел некоторых классов”, *УМН*, Т.4, № 5, С. 14–48.
5. Касселс, Дж. В. С. 1961, “Введение в теорию диофантовых приближений”, *Изд-во Иностран. Литер.*, Москва, 213 с.
6. Коледа, Д. В. 2013, “О распределении действительных алгебраических чисел второй степени”, *Весті НАН Беларусі. Сер. фіз.-мат. навук*, № 3, С. 54–63.
7. Koleda, D. V. 2017 “On the density function of the distribution of real algebraic numbers”, *J. Théor. Nombres Bordeaux*, Vol. 29, no. 1 (2017), p. 179–200.
8. Спринджук, В. Г., 1967 “Проблема Малера в метрической теории чисел”, *«Наука» и техника*, Минск, 181 с.
9. Beresnevich, V. 2012 “Rational Points near Manifolds and Metric Diophantine Approximation.”, *Annals of Mathematics, Second Series*, Vol. 175, no. 1, p. 187-235.
10. Beresnevich, V. V., Bernik, V. I., Goetze, F. 2016 “Integral polynomials with small discriminants and resultants”, *Adv. Math.*, Vol. 298, p. 393–412.
11. Берник, В. И., 1983 “Применение размерности Хаусдорфа в теории диофантовых приближений”, *Acta Arithmetica*, № 42, С. 219–253.
12. Dodson, M. M., Bernik, V. I., 1999 “Metric Diophantine approximation on manifolds”, *Cambridge Tracts in Mathematics*, №.137, 172 p.
13. Tishchenko, K., 2000 “On approximation to real numbers by algebraic numbers”, *Acta Arithmetica*, №94, Vol. 1, p. 1–24.
14. Davenport, H., Schmidt, W.M., 1970 “Dirichlet’s theorem on diophantine approximation”, *Symposia Mathematica*, Vol. 4, N. Y.—London, p. 113–132.
15. Wirsing, E., 1961 “Approximation mit algebraischen Zahlen beschränkten Grades” *Journal für die reine und angewandte Mathematik*, Vol. 206, p. 67–77.
16. Гетце, Ф., Гусакова, А. Г., 2015 “Алгебраические числа в коротких интервалах”, *Доклады Национальной академии наук Беларуси*, Т. 59, № 4, С. 11–16.
17. Badziahin, D. Schleischitz, J., 2019 “An improved bound in Wirsing’s problem”, <https://arxiv.org/abs/1912.09013>.

Получено 17.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.321

DOI 10.22405/2226-8383-2020-21-1-221-232

Суммы Kloostermana по простым числам
и разрешимость одного сравнения с обратными вычетами — II

М. А. Королев

Королев Максим Александрович — доктор физико-математических наук, ведущий научный сотрудник, Математический институт им. В. А. Стеклова РАН (г. Москва).

e-mail: korolevma@mi-ras.ru

Аннотация

В настоящей статье продолжены исследования, связанные с распределением обратных вычетов по заданному модулю. Ранее автором был получен ряд нетривиальных оценок коротких сумм Kloostermana с простыми числами, отвечающих произвольному модулю q . Следствием таких оценок стали результаты о распределении вычетов $\bar{p}$, обратных простым числам “короткого” промежутка: $p\bar{p} \equiv 1 \pmod{q}$, $1 < p \leq N$, $N \leq q^{1-\delta}$, $\delta > 0$, и, более общо, о распределении по модулю q величин $g(p) = a\bar{p} + bp$, где a, b — целые числа, $(ab, q) = 1$.

Еще одно приложение найденных оценок связано с задачей о представимости произвольного заданного вычета $m \pmod{q}$ суммой $g(p_1) + \dots + g(p_k)$ при фиксированных a, b и $k \geq 3$, и простых $1 < p_1, \dots, p_k \leq N$. Для количества таких представлений автором была найдена формула, поведение предполагаемого главного члена которой определяется аналогом “сингулярного ряда” классического кругового метода, т.е. некоторой величиной κ , зависящей от q и набора k, a, b, m . При фиксированных k, a, b, m она является мультипликативной функцией q . В случае, когда модуль q не делится на 2 или 3, эта величина строго положительна, так что формула для искомого числа представлений является асимптотической.

В настоящей работе исследуется поведение κ в случае, когда $q = 3^n$. Оказывается, что при любых $n \geq 1$, $k \geq 3$ существуют “исключительные” тройки a, b, m , для которых $\kappa = 0$. Цель работы состоит в описании всех таких троек и нижней оценки величины κ для “неисключительных” троек.

Ключевые слова: сравнения, разрешимость, обратные вычеты, суммы Kloostermana, простые числа, сингулярный ряд.

Библиография: 17 названий.

Для цитирования:

М. А. Королев. Суммы Kloostermana по простым числам и разрешимость одного сравнения с обратными вычетами — II // Чебышевский сборник, 2020, т. 21, вып. 1, с. 221–232.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.321

DOI 10.22405/2226-8383-2020-21-1-221-232

Kloosterman sums with primes and the solvability of one congruence with inverse residues — II¹

M. A. Korolev

Korolev Maxim Aleksandrovich — doctor of physical and mathematical sciences, the leading researcher of the Department of Number Theory of Steklov Mathematical Institute of RAS (Moscow).

e-mail: korolevma@mi-ras.ru

Abstract

In the paper, we continue to study the distribution of inverse residues to given modulus. Earlier, the author obtained a series of non-trivial estimates for incomplete Kloosterman sums over prime numbers with an arbitrary modulus q . One of the applications of such estimates are some assertions concerning the distribution of inverse residues $\bar{p}$ to prime numbers lying in a “short” segment: $p\bar{p} \equiv 1 \pmod{q}$, $1 < p \leq N$, $N \leq q^{1-\delta}$, $\delta > 0$, and, more general, concerning the distribution of the quantities $g(p) = a\bar{p} + bp$ with respect to modulus q , where a, b are some integers, $(ab, q) = 1$.

Another application is connected with the problem of the representation of a given residue $m \pmod{q}$ by the sum $g(p_1) + \dots + g(p_k)$ for fixed a, b and $k \geq 3$, in primes $1 < p_1, \dots, p_k \leq N$. For the number of such representations, the author have found the formula, where the behavior of the expected main term is controlled by some analogous of the “singular series” that appears in classical circle method, that is, by some function κ depending on q and the tuple k, a, b, m . For fixed k, a, b, m , this function is multiplicative with respect to q . In the case when q is not divisible by 2 or 3, this function is strictly positive, and therefore the formula for the number of the representations becomes asymptotic.

In this paper, we study the behavior of κ for $q = 3^n$. It appears that, for any $n \geq 1$, $k \geq 3$, there exist the “exceptional” triples a, b, m such that $\kappa = 0$. The main purpose is to describe all such triples and to obtain the lower estimate for κ for all non-exceptional triples.

Keywords: congruences, solvability, inverse residues, Kloosterman sums, prime numbers, singular series.

Bibliography: 17 titles.

For citation:

M. A. Korolev, 2020, "Kloosterman sums with primes and the solvability of one congruence with inverse residues — II *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 221–232.

To academician V. P. Platonov in occasion with his 80th anniversary.

¹This work was supported by the Russian Science Foundation under grant 19-11-00001.

1. Introduction

In the present paper, we continue the study of the solvability of some congruences with inverse residues to modulo q started in [1] and [2]. As in [2], the main subject now is the congruence

$$g(p_1) + \dots + g(p_k) \equiv m \pmod{q}, \quad (1)$$

where $q \geq 2$ is an arbitrary integer, $g(x) \equiv a\bar{x} + bx \pmod{q}$, k, a, b, m are any fixed integers satisfying the conditions $k \geq 3$, $1 \leq a, b, m \leq q$, $(ab, q) = 1$. The variables $p_1, \dots, p_k$ run through prime numbers from the interval $(1, N]$. This interval is assumed to be “short”, that is, we are interested in the case when $N \leq q^{1-\delta}$ for some positive δ .

The key role in such problems is played by the estimates of Kloosterman sums with primes, that is, of the exponential sums of the type

$$W_q(a, b; X) = \sum_{p \leq X, p \nmid q} \exp\left(\frac{2\pi i}{q}(a\bar{p} + bp)\right),$$

(for such estimates and their applications, see: [3]-[16]). The estimates given in [1], [2] lead to the following assertion (see [2]):

THEOREM A. *Let $0 < \varepsilon < 0.01$ be an arbitrary fixed constant and let $k \geq 3$ be any fixed integer. Suppose that $q \geq q_0(\varepsilon, k)$. Further, let $(ab, q) = 1$ and $g(x) \equiv a\bar{x} + bx \pmod{q}$. Finally, let*

$$\gamma_k = \frac{2(k+33)}{3k+64} \quad \text{if } 3 \leq k \leq 16 \quad \text{and} \quad \gamma_k = \frac{3k+50}{4(k+12)} \quad \text{if } k \geq 17,$$

and suppose that $q^{\gamma_k + \varepsilon} \leq N \leq q$. Then the number $I_k(N) = I_k(N, q, a, b, m)$ of solutions of (1) in primes $p_j \leq N$, $(p_j, q) = 1$, satisfies the relation

$$I_k(N) = \frac{\pi^k(N)}{q} (\varkappa_k(q) + O(\Delta_k)). \quad (2)$$

Here $\varkappa_k(q) = \varkappa_k(a, b, m; q)$ is some non-negative multiplicative function of q for any fixed tuple k, a, b and m . Moreover,

a) for any $k \geq 7$ we have $\Delta_k = (\ln \ln N)^B (\ln N)^{-A}$,

$$A = \frac{1}{2} + \frac{29}{2}(k-7), \quad B = 2^k - 1;$$

b) for any $k \geq 3$ we have $\Delta_k = q^{-\varepsilon}$, if Generalized Riemann hypothesis is true.

REMARK. One can check that $\gamma_k \leq 1 - \frac{1}{73}$ for any $k \geq 3$.

The ascertaining of the conditions of when (2) becomes the asymptotic formula is connected with the detailed study of the multiplicative function $\varkappa_k(q) = \varkappa_k(a, b, m; q)$. In this direction, in [2], we prove the following assertion:

THEOREM B. *Suppose that q is coprime to 6 and let $k \geq 3$ be any fixed integer. Then, for any triple (a, b, m) with the conditions $1 \leq a, b, m \leq q$, $(ab, q) = 1$ the following inequalities hold:*

$$\varkappa_k(a, b, m; q) \geq \begin{cases} c_1 \exp\left(-\frac{c_2 \sqrt{\ln q}}{\ln \ln q}\right), & \text{if } k = 3, \\ c_3 (\ln \ln q)^{-6}, & \text{if } k = 4, \\ 10^{-5}, & \text{for any } k \geq 5 \end{cases}$$

where the constants c_j , $j = 1, 2, 3$, are absolute.

REMARK. The exponent (-6) (for $k = 4$) and constant 10^{-5} (for $k \geq 5$) are not optimal.

Now the purpose is to study the behavior of $\kappa_k(q)$ in the case when $q = 3^n$. Unlike the case $(q, 6) = 1$, for any pair k, n there exists the set $\Omega_k(3^n)$ of “exceptional triples” (a, b, m) such that $\kappa_k(a, b, m; 3^n) = 0$. In what follows, we shall refer these sets as “exceptional sets”.

The main results of this paper is the description of all exceptional sets $\Omega_k(3^n)$, $k \geq 3$, $n \geq 1$. Namely, we prove here the following assertion:

THEOREM. *In the cases $k \geq 8$, $n \geq 1$ and $3 \leq k \leq 7$, $n = 1$, the set $\Omega_k(3^n)$ consists of the triples satisfying the conditions*

$$1 \leq a, b, m \leq 3^n, \quad (ab, 3) = 1, \quad a + b \equiv 0 \pmod{3}, \quad m \not\equiv 0 \pmod{3}. \quad (3)$$

In particular, $|\Omega_k(3^n)| = 4 \cdot 3^{3(n-1)}$.

In the case $3 \leq k \leq 7$, the set $\Omega_k(3^2)$ consists of the triples listed in (13)-(16); in particular, $|\Omega_k(3^2)| = 18(14 - k)$;

Finally, in the case $3 \leq k \leq 7$, $n \geq 3$, the set $\Omega_k(3^n)$ consists of the triples coinciding modulo 3^2 with the triples from the set $\Omega_k(3^2)$; in particular, $|\Omega_k(3^n)| = 2 \cdot 3^{3n-4}(14 - k)$.

At the same time, for any $k \geq 3$, $n \geq 1$ and for any “non-exceptional” triple $(a, b, m) \notin \Omega_k(3^n)$ one has

$$\kappa_k(a, b, m; 3^n) > \frac{1}{50}.$$

2. Complete Kloosterman sums to prime power moduli

In [2], we establish the following formula for $\kappa_k(p^n) = \kappa_k(a, b, m; p^n)$:

$$\kappa_k(p^n) = 1 + A_k(p) + A_k(p^2) + \dots + A_k(p^n).$$

Here

$$A_k(p^n) = A_k(a, b, m; p^n) = \frac{1}{\varphi^k(p^n)} \sum_{f=1}^{p^n} e^{-2\pi i \frac{fm}{p^n}} S^k(fa, fb; p^n),$$

and $S(a, b; q)$ is a complete Kloosterman sum, that is,

$$S(a, b; q) = \sum_{\substack{x=1 \\ (x, q)=1}}^q \exp\left(\frac{2\pi i}{q}(a\bar{x} + bx)\right).$$

To study the properties of $\kappa_k(q)$, we need some explicit expressions and the estimates for the quantities $S(a, b; p^n)$, $A_k(a, b, m; 3^n)$, $n \geq 2$.

LEMMA 2.1. *Let $p \geq 3$ and $(ab, p) = 1$. If ab is a quadratic non-residue modulo p then $S(a, b; p^n) = 0$ for any $n \geq 2$. Otherwise, setting q for p^n and ν for any solution of the congruence $ab \equiv \nu^2 \pmod{q}$, we have*

$$S(a, b; q) = S(\nu, \nu; q) = \begin{cases} 2\sqrt{q} \cos \frac{4\pi\nu}{q} & \text{for even } n, \\ 2\sqrt{q} \left(\frac{\nu}{q}\right) \cos\left(\frac{4\pi\nu}{q} + \frac{\pi s}{2}\right) & \text{for odd } n, \end{cases}$$

where $s = 0$ for $p \equiv 1 \pmod{4}$ and $s = 1$ for $p \equiv 3 \pmod{4}$.

For the proof, see [17].

COROLLARY. Under the conditions of Lemma 2.1, for any $n \geq 2$ and $q = p^n$ we have

$$|S(a, b; q)| < 2\sqrt{q}.$$

LEMMA 2.2. For any a, b coprime to 3 the following equalities hold:

$$S(a, b; 3) = \begin{cases} 2, & \text{if } a + b \equiv 0 \pmod{3}, \\ -1, & \text{otherwise;} \end{cases}$$

$$S(a, b; 3^2) = \begin{cases} 3(-1)^b \cos \frac{\pi}{9}(4a + b), & \text{if } b - a \equiv 0 \pmod{3}, \\ 0, & \text{otherwise.} \end{cases}$$

PROOF. Setting $\omega = e^{2\pi i/3}$ we get

$$S(a, b; 3) = \sum_{x=1}^2 \omega^{a\bar{x}+bx} = \omega^{a+b} + \omega^{2(a+b)} = \begin{cases} 2, & \text{if } a + b \equiv 0 \pmod{3}, \\ -1, & \text{otherwise.} \end{cases}$$

Further, setting $x = y + 3z$ in the sum $S(a, b; 3^2)$ we obtain

$$S(a, b; 3^2) = \sum_{y=1}^3 e^{\frac{2\pi i}{3^2}(a\bar{y}+by)} \sum_{z=1}^3 \omega^{z(b-a)}.$$

So, $S(a, b; 3^2) = 0$ for $b - a \not\equiv 0 \pmod{3}$. Finally, if $a = b + 3n$ for some integer n then

$$S(a, b; 3^2) = 3 \left(e^{\frac{2\pi i}{3^2}(a+b)} + e^{\frac{2\pi i}{3^2}(5a+2b)} \right) = 3e^{\frac{2\pi i}{3^2}\left(3a+\frac{3b}{2}\right)} \cos \frac{\pi}{9}(4a + 9).$$

Since

$$\frac{2}{9} \left(3a + \frac{3b}{2} \right) = \frac{2}{9} \left(3b + \frac{3b}{2} + 9n \right) = b + 2n \equiv b \pmod{2},$$

we arrive at the assertion of the lemma. $\square$

In this section, we use the explicit formulas for Kloosterman sums $S(a, b; p^n)$, $p \geq 3$, $n \geq 1$ to provide the explicit formulas for the values

$$A_k(p^n) = A_k(a, b, m; p^n) = \frac{1}{\varphi^k(p^n)} \sum_{f=1}^{p^n} e^{-2\pi i \frac{fm}{p^n}} S^k(fa, fb; p^n).$$

LEMMA 2.3. Suppose that $(ab, 3) = 1$. If $a + b \equiv 0 \pmod{3}$ then

$$A_k(3) = \begin{cases} 2, & \text{when } m \equiv 0 \pmod{3}, \\ -1, & \text{when } m \not\equiv 0 \pmod{3}; \end{cases} \quad A_k(3^n) = 0 \quad \text{for } n \geq 2.$$

If $a + b \not\equiv 0 \pmod{3}$ then

$$A_k(3) = \frac{(-1)^{k+m}}{2^{k-1}} \cos \frac{\pi m}{3} = \frac{(-1)^k}{2^{k-1}} \cos \frac{2\pi m}{3},$$

$$A_k(3^2) = \sum_{f=1}^{3^2} (-1)^{kbf} \cos \frac{2\pi mf}{9} \cos^k \frac{\pi f}{9} (4a + b).$$

PROOF. In the case $a + b \equiv 0 \pmod{3}$, Lemma 2.2 implies that

$$A_k(3) = \frac{1}{2^k} \cdot 2^k \sum_{f=1}^2 \omega^{-mf} = \begin{cases} 2, & \text{when } m \equiv 0 \pmod{3}, \\ -1, & \text{when } m \not\equiv 0 \pmod{3}. \end{cases}$$

It is easy to check that the conditions $a + b \equiv 0 \pmod{3}$ and $\left(\frac{ab}{3}\right) = -1$ are equivalent, so we have $A_k(3^n) = 0$ for any $n \geq 2$ by Lemma 2.1. In the case $a + b \not\equiv 0 \pmod{3}$, Lemma 2.2 implies:

$$\begin{aligned} A_k(3) &= \frac{1}{2^k} \sum_{f=1}^2 \omega^{-mf} (-1)^k = \frac{(-1)^k}{2^k} (\omega^{-m} + \omega^{-2m}) = \frac{(-1)^k}{2^k} e^{-\pi m} (e^{\frac{\pi i m}{3}} + e^{-\frac{\pi i m}{3}}) = \\ &= \frac{(-1)^{k+m}}{2^k} \cos \frac{\pi m}{3}. \end{aligned}$$

Finally we have

$$\begin{aligned} A_k(3^2) &= \frac{1}{6^k} \cdot 6^k \sum_{f=1}^{3^2} e^{-2\pi i \frac{mf}{9}} (-1)^{kbf} \cos^k \frac{\pi f}{9} (4a + b) = \\ &= \sum_{f=1}^{3^2} (-1)^{kbf} \cos \frac{2\pi mf}{9} \cos^k \frac{\pi f}{9} (4a + b). \end{aligned}$$

Lemma is proved. $\square$

LEMMA 2.4. Suppose that $s \geq n \geq 2$, $k \geq 5$. Then the following inequality holds:

$$\left| \sum_{r=n}^s A_k(3^r) \right| < \frac{2 \cdot 3^{k+n-kn/2-1}}{1 - 3^{1-k/2}}.$$

LEMMA 2.5. Suppose that $n \geq 5$. Then, for any $s \geq n$ and for any a, b satisfying the condition $\left(\frac{ab}{3}\right) = 1$ the following inequality holds:

$$\left| \sum_{r=n}^s A_3(3^r) \right| \leq \begin{cases} \frac{3}{16} \cdot 3^{(8-n)/2}, & \text{when } n \equiv 0 \pmod{2}, \\ \frac{5}{16} \cdot 3^{(7-n)/2}, & \text{when } n \equiv 1 \pmod{2}; \end{cases}$$

LEMMA 2.6. Suppose that $n \geq 4$. Then

$$\left| \sum_{r=n}^s A_4(3^r) \right| \leq \frac{1}{8} \cdot 3^{5-n}.$$

LEMMA 2.7. Suppose $n \geq 3$. Then, for any $s \geq n$, the following inequalities hold:

$$\left| \sum_{r=n}^s A_5(3^r) \right| \leq \begin{cases} \frac{35}{416} \cdot 3^{3(4-n)/2}, & \text{when } n \equiv 0 \pmod{2}, \\ \frac{55}{416} \cdot 3^{(11-3n)/2}, & \text{when } n \equiv 1 \pmod{2}; \end{cases}$$

Lemmas 2.4, 2.5, 2.6 and 2.7 are particular cases of Lemmas 6.1, 6.3–6.5 from [2], respectively.

3. The singular series $\varkappa_k(a, b, m; q)$ for $q = 3^n$

In the cases $q = 2^n, 3^n$, $n = 1, 2, 3, \dots$, the behavior of the series $\varkappa_k(a, b, m; q)$ is more sophisticated than in the case $(q, 6) = 1$. In particular, for “small” k and any n there exist some “exceptional” set $\Omega_k(q)$ of triples (a, b, m) such that $\varkappa_k(a, b, m) = 0$. These exceptional sets can be completely described in the case $q = 3^n$ and partially in the case $q = 2^n$. In what follows, we consider only the case $p = 3$ which is more easy.

LEMMA 3.1. *Suppose that $(ab, 3) = 1$, $a + b \equiv 0 \pmod{3}$. Then, for any $n \geq 1$ and $q = 3^n$ we have*

$$\varkappa_k(a, b, m; q) = \begin{cases} 0, & \text{when } m \not\equiv 0 \pmod{3}, \\ 3, & \text{when } m \equiv 0 \pmod{3}. \end{cases}$$

PROOF. Obviously, the conditions $(ab, 3) = 1$, $a + b \equiv 0 \pmod{3}$ are equivalent to the condition $\left(\frac{ab}{3}\right) = -1$. In view of Lemma 2.1, in this case we have $\varkappa_k(q) = 1 + A_k(3)$. By Lemma 2.3, $A_k(3) = -1$ for $m \not\equiv 0 \pmod{3}$ and $A_k(3) = 2$ for $m \equiv 0 \pmod{3}$. Thus lemma follows. $\square$

COROLLARY. *For any $n \geq 1$, the set $\Omega_k(3^n)$ contains all the triples (a, b, m) satisfying the following conditions: $1 \leq a, b, m \leq 3^n$, $(ab, 3) = 1$, $a + b \equiv 0 \pmod{3}$, $m \not\equiv 0 \pmod{3}$. The number of such triples is equal $4 \cdot 3^{3(n-1)}$.*

LEMMA 3.2. *Suppose that $k \geq 8$, $(ab, 3) = 1$ and $a + b \not\equiv 0 \pmod{3}$. Then, for any $n \geq 1$, $q = 3^n$ and for any m , $1 \leq m \leq q$, one has $\varkappa_k(a, b, m; q) > \frac{1}{50}$.*

PROOF. Suppose first that $n = 1$. Since $\bar{x} \equiv x \pmod{3}$ for any $x \in \mathbb{Z}_3^*$ then $g(x)$ becomes a linear function: $g(x) \equiv a\bar{x} + bx \equiv (a + b)x$. Hence, the congruence (1) is equivalent to

$$(a + b)(x_1 + \dots + x_k) \equiv m \pmod{3}$$

or to

$$x_1 + \dots + x_k \equiv \mu \pmod{3}, \quad \mu \equiv m(a + b)^* \equiv m(a + b) \pmod{3}. \quad (4)$$

At the same time, the number of solutions $(x_1, \dots, x_k)$ of (4) such that $(x_j, 3) = 1$, $j = 1, \dots, k$, is equal to

$$\begin{aligned} V_k(3) &= \frac{1}{3} \sum_{c=1}^3 \sum_{x_1, \dots, x_k=1}^2 e^{2\pi i \frac{c}{3}(x_1 + \dots + x_k - \mu)} = \frac{1}{3} \sum_{c=1}^3 \left(\sum_{x=1}^2 e^{2\pi i \frac{cx}{3}} \right)^k e^{-2\pi i \frac{c\mu}{3}} = \\ &= \frac{1}{3} \sum_{c=1}^3 \omega^{-c\mu} (\omega^c + \omega^{2c})^k = \frac{1}{3} \left(2^k + (-1)^k \sum_{c=1}^2 \omega^{-c\mu} \right) = \frac{1}{3} (2^k + (-1)^k \delta), \end{aligned}$$

where $\omega = e^{2\pi i/3}$,

$$\delta = \begin{cases} 2, & \text{when } m \equiv 0 \pmod{3}, \\ -1, & \text{when } m \not\equiv 0 \pmod{3}. \end{cases}$$

Thus we obtain

$$V_k(3) = \frac{\varphi^k(3)}{3} \left(1 + \frac{(-1)^k \delta}{2^k} \right), \quad \varkappa_k(3) = 1 + \frac{(-1)^k \delta}{2^k} \geq 1 - \frac{1}{2^{k-1}} \geq 1 - \frac{1}{16} = \frac{15}{16}.$$

Further, let $n = 2$. Since $\left(\frac{ab}{3}\right) = 1$, then Lemma 2.2 implies

$$\varkappa_k(3^2) = 1 + \frac{(-1)^{k+m}}{2^k} \cos \frac{\pi m}{3} + \sum_{f=1}^{3^2}{}' (-1)^{kbf} \cos \left(\frac{2\pi mf}{3} \right) \cos^k \frac{\pi f}{3^2} (4a + b). \quad (5)$$

The direct tabulation over all triples (a, b, m) , $1 \leq a, b, m \leq 9$, $(ab, 3) = 1$ shows that

$$\varkappa_k(3^2) > 0.0351562 \dots \text{ for } k = 8, 9, \quad (6)$$

$$\varkappa_k(3^2) > 0.0966797 \dots \text{ for } k = 10, 11, \quad (7)$$

$$\varkappa_k(3^2) > 0.171387 \dots \text{ for } k = 12. \quad (8)$$

Moreover, (4) implies the inequality

$$|\varkappa_k(3^2) - 1| \leq \frac{1}{2^k} + \sum_{f=1}^{3^2} \left| \cos \frac{\pi f}{3^2} (4a + b) \right|^k.$$

The condition $a + b \not\equiv 0 \pmod{3}$ implies that $4a + b \not\equiv 0 \pmod{3}$, that is, $(4a + b, 3) = 1$. Hence, both the quantities f and $(4a + b)f$ run through the reduced residual system modulo 3^2 . Thus,

$$|\varkappa_k(3^2) - 1| \leq \frac{1}{2^k} + \sum_{f=1}^{3^2} \left| \cos \frac{\pi f}{3^2} \right|^k = \frac{1}{2^k} + 2 \left(\cos^k \frac{\pi}{9} + \cos^k \frac{2\pi}{9} + \cos^k \frac{4\pi}{9} \right). \quad (9)$$

Denote the right-hand-side of (9) by $g(k)$. Since $g(k)$ is decreasing function of k then for any $k \geq 13$ we have

$$|\varkappa_k(3^2) - 1| = g(k) \leq g(13) = 0.953621 \dots, \quad \varkappa_k(3^2) > 0.0463788 \dots > \frac{1}{22}.$$

The last inequality together with (6)-(8) yields:

$$\varkappa_k(3^2) > 0.0463788 \dots > \frac{1}{22} \text{ for any } k \geq 8.$$

Finally, let $n \geq 3$. Then, for $k \geq 10$, Lemma 2.4 implies the inequality

$$\left| \sum_{r=3}^n A_k(3^r) \right| < \frac{18 \cdot 3^{-k/2}}{1 - 3^{1-k/2}}.$$

Setting $h(k)$ for right-hand-side and using (9) we find

$$|\varkappa_k(q) - 1| \leq g(k) + h(k)$$

for any $n \geq 3$ and $q = 3^n$. Since $h(k) \leq h(13) < 0.0142895 \dots$ for any $k \geq 13$, we get

$$|\varkappa_k(q) - 1| \leq g(13) + h(13) < 0.967911 \dots, \quad \varkappa_k(q) > 0.0320892 \dots > \frac{1}{32}.$$

For $10 \leq k \leq 12$, the inequalities (7), (8) together with the bound

$$\varkappa_k(3^n) > \varkappa_k(3^2) - h(k)$$

imply

$$\begin{aligned} \varkappa_{10}(3^n) &> 0.0966797 \dots - 0.075 > 0.021 > \frac{1}{50}, \\ \varkappa_{11}(3^n) &> 0.0966797 \dots - 0.0430737 > 0.053606 > \frac{1}{19}, \\ \varkappa_{12}(3^n) &> 0.171387 \dots - 0.0247934 > 0.1465936 > \frac{1}{7}. \end{aligned}$$

To conclude the proof, it remains to consider the cases $k = 8, 9$. By Lemma 2.4,

$$\varkappa_k(3^n) = \varkappa_k(3^2) + \sum_{r=4}^n A_k(3^r) \geq \varkappa_k(3^2) - \frac{54 \cdot 3^{-k}}{1 - 3^{1-k/2}}.$$

The direct calculation with all triples (a, b, m) , $1 \leq a, b, m \leq 3^3$, $(ab, 3) = 1$, $a + b \not\equiv 0 \pmod{3}$ shows that

$$\varkappa_k(3^2) > 0.0347222\dots, \quad k = 8, 9.$$

Therefore,

$$\begin{aligned} \varkappa_8(3^n) &> 0.0347222\dots - 0.00854701 > 0.026175 > \frac{1}{39}, \\ \varkappa_9(3^n) &> 0.0347222\dots - 0.00280343 > 0.031918 > \frac{1}{32}. \end{aligned}$$

This proves the lemma. $\square$

COROLLARY. *For any $k \geq 8$, the exceptional set $\Omega_k(3^n)$ consists precisely of the triples pointed in Corollary of Lemma 3.1.*

Now we proceed to study the values of $\varkappa_k(a, b, m; 3^n)$ for $3 \leq k \leq 7$ and $n \geq 2$. In view of Corollary to Lemma 3.1, we will assume that $a + b \not\equiv 0 \pmod{3}$ or, that is the same, $a \equiv b \pmod{3}$.

LEMMA 3.3. *Suppose that $3 \leq k \leq 7$. Then the set $\Omega_k(3^2)$ contains $18(8 - k)$ triples (a, b, m) , $a \equiv b \pmod{3}$, $(ab, 3) = 1$ listed in (10)-(13).*

PROOF. Indeed, let $\mathcal{G} = \mathcal{G}_{a,b} = \mathcal{G}_{b,a}$ be the set of values of the function $g(x) = a\bar{x} + bx$ on $\mathbb{Z}_9^*$. The direct computation shows that

$$\begin{aligned} \mathcal{G} &= \{1, 8\} \quad \text{for the pairs } (a; b) \in \mathcal{E}_1, \quad \mathcal{E}_1 = \{(1; 7), (7; 1), (2; 8), (8; 2), (4; 4), (5; 5)\}, \\ \mathcal{G} &= \{2, 7\} \quad \text{for the pairs } (a; b) \in \mathcal{E}_2, \quad \mathcal{E}_2 = \{(1; 1), (2; 5), (5; 2), (4; 7), (7; 4), (8; 8)\}, \\ \mathcal{G} &= \{4, 5\} \quad \text{for the pairs } (a; b) \in \mathcal{E}_3, \quad \mathcal{E}_3 = \{(1; 4), (4; 1), (2; 2), (5; 8), (8; 5), (7; 7)\}. \end{aligned}$$

Also, the direct computation shows that the sets $k\mathcal{G} = \underbrace{\mathcal{G} + \dots + \mathcal{G}}_{k \text{ times}}$ do not coincide with complete residual system $\mathbb{Z}_9$ for $3 \leq k \leq 7$. Thus, the sets $3\mathcal{G}$ have the forms

$$\mathbb{Z}_9 \setminus \{0, 2, 4, 5, 7\}, \quad \mathbb{Z}_9 \setminus \{0, 1, 4, 5, 8\}, \quad \mathbb{Z}_9 \setminus \{0, 1, 2, 7, 8\}$$

respectively, the sets $4\mathcal{G}$ have the form

$$\mathbb{Z}_9 \setminus \{1, 3, 6, 8\}, \quad \mathbb{Z}_9 \setminus \{2, 3, 6, 7\}, \quad \mathbb{Z}_9 \setminus \{3, 4, 5, 6\},$$

respectively, the sets $5\mathcal{G}$ have the form

$$\mathbb{Z}_9 \setminus \{0, 2, 7\}, \quad \mathbb{Z}_9 \setminus \{0, 4, 5\}, \quad \mathbb{Z}_9 \setminus \{0, 1, 8\},$$

respectively, the sets $6\mathcal{G}$ have the form

$$\mathbb{Z}_9 \setminus \{1, 8\}, \quad \mathbb{Z}_9 \setminus \{2, 7\}, \quad \mathbb{Z}_9 \setminus \{4, 5\},$$

respectively, and, finally, all the sets $7\mathcal{G}$ coincide with $\mathbb{Z}_9 \setminus \{0\}$. Hence, $\varkappa_3(3^2) = 0$ for the triples

$$\begin{aligned} (a, b, 0), (a, b, 2), (a, b, 4), (a, b, 5), (a, b, 7) & \quad (a; b) \in \mathcal{E}_1, \\ (a, b, 0), (a, b, 1), (a, b, 4), (a, b, 5), (a, b, 8) & \quad (a; b) \in \mathcal{E}_2, \\ (a, b, 0), (a, b, 1), (a, b, 2), (a, b, 7), (a, b, 8) & \quad (a; b) \in \mathcal{E}_3, \end{aligned} \tag{10}$$

$\varkappa_4(3^2) = 0$ for the triples

$$\begin{aligned} (a, b, 1), (a, b, 3), (a, b, 6), (a, b, 8), \quad (a; b) \in \mathcal{E}_1, \\ (a, b, 2), (a, b, 3), (a, b, 6), (a, b, 7), \quad (a; b) \in \mathcal{E}_2, \\ (a, b, 3), (a, b, 4), (a, b, 5), (a, b, 6), \quad (a; b) \in \mathcal{E}_3, \end{aligned} \quad (11)$$

$\varkappa_5(3^2) = 0$ for the triples

$$\begin{aligned} (a, b, 0), (a, b, 2), (a, b, 7), \quad (a; b) \in \mathcal{E}_1, \\ (a, b, 0), (a, b, 4), (a, b, 5), \quad (a; b) \in \mathcal{E}_2, \\ (a, b, 0), (a, b, 1), (a, b, 8), \quad (a; b) \in \mathcal{E}_3, \end{aligned} \quad (12)$$

$\varkappa_6(3^2) = 0$ for the triples

$$\begin{aligned} (a, b, 1), (a, b, 8), \quad (a; b) \in \mathcal{E}_1, \\ (a, b, 2), (a, b, 7), \quad (a; b) \in \mathcal{E}_2, \\ (a, b, 4), (a, b, 5), \quad (a; b) \in \mathcal{E}_3, \end{aligned} \quad (13)$$

and, finally, $\varkappa_7(3^2) = 0$ for the triples $(a, b, 0)$, where $(a; b) \in \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$. It is not difficult to check that the number of such triples coincides with $18(8 - k)$ in each case. This proves the lemma. $\square$

COROLLARY. For any k , $3 \leq k \leq 7$, we have

$$|\Omega_k(3^2)| = 18(14 - k).$$

PROOF. This assertion easily follows from the above lemma and the Corollary of Lemma 3.1. $\square$

Suppose now that $n \geq 3$ and the triple (a, b, m) with the conditions $1 \leq a, b, m \leq 3^n$, $(ab, 3) = 1$ is congruent with some exceptional triple $(a', b', m') \in \Omega_k(3^2)$ modulo 3^2 . Then the triple (a, b, m) is contained in the exceptional set $\Omega_k(3^n)$. Indeed, if the congruence

$$g(x_1) + \dots + g(x_k) \equiv m \pmod{3^n}, \quad g(x) = a\bar{x} + bx,$$

is solvable, then the congruence

$$g'(x_1) + \dots + g'(x_k) \equiv m \pmod{3^2}, \quad g'(x) = a'x^* + b'x,$$

is also solvable, and that is impossible (here $x\bar{x} \equiv 1 \pmod{3^n}$, $xx^* \equiv 1 \pmod{3^2}$, so $\bar{x} \equiv x^* \pmod{3^2}$). The below lemma shows that there are no other triples in $\Omega_k(3^n)$.

LEMMA 3.4. Suppose that $n \geq 3$, $3 \leq k \leq 7$. Then there exists an absolute constant $c_4 > 0$ such that the inequality

$$\varkappa_k(3^n) = \varkappa_k(a, b, m, 3^n) > c_4$$

holds for any triple (a, b, m) , $1 \leq a, b, m \leq 3^n$, $(ab, 3) = 1$, that does not coincide with some exceptional triple from the set $\Omega_k(3^2)$ modulo 3^2 .

PROOF. By Lemma 2.4,

$$|\varkappa_k(3^n) - \varkappa_k(3^3)| < \frac{54 \cdot 3^{-k}}{1 - 3^{1-k/2}} \quad \text{and therefore} \quad \varkappa_k(3^n) > \varkappa_k(3^3) - \frac{54 \cdot 3^{-k}}{1 - 3^{1-k/2}}.$$

In particular,

$$\kappa_6(3^n) > \kappa_6(3^3) - \frac{1}{12}, \quad \kappa_7(3^n) > \kappa_7(3^3) - \frac{27 + \sqrt{3}}{33^2} > \kappa_7(3^3) - \frac{1}{37}. \quad (14)$$

The direct calculation with all triples (a, b, m) , $1 \leq a, b, m \leq 3^3$, $(ab, 3) = 1$, that are not congruent with triples from $\Omega_k(3^k)$ modulo 3^2 ($k = 6, 7$) shows that the least values of $\kappa_6(3^3)$ and $\kappa_7(3^3)$ are equal to $\frac{25}{192}$ and $\frac{13}{192}$. Thus, by (14) we conclude that

$$\kappa_6(3^n) > \frac{25}{192} - \frac{1}{12} = \frac{3}{64}, \quad \kappa_7(3^n) > \frac{13}{192} - \frac{1}{37} > \frac{1}{25}.$$

The calculations also shows that

$$\kappa_5(3^n) \geq \frac{1}{4} \quad \text{for } n = 3, \quad (15)$$

$$\kappa_4(3^n) \geq \frac{7}{16} \quad \text{for } n = 3, \quad (16)$$

$$\kappa_3(3^n) \geq \frac{3}{4} \quad \text{for } n = 3, 4, 5 \quad (17)$$

for any triple (a, b, m) , $1 \leq a, b, m \leq 3^n$, $(ab, 3) = 1$ that does not coincide with some triple from the set $\Omega_k(3^2)$ modulo 3^2 ($3 \leq k \leq 5$). At the same time, the inequalities of Lemmas 2.7, 2.6 and 2.5 imply that

$$|\kappa_5(3^n) - \kappa_5(3^3)| \leq \frac{35}{416} \quad \text{for } n \geq 4, \quad (18)$$

$$|\kappa_4(3^n) - \kappa_4(3^3)| \leq \frac{3}{8} \quad \text{for } n \geq 4, \quad (19)$$

$$|\kappa_3(3^n) - \kappa_3(3^5)| \leq \frac{9}{16} \quad \text{for } n \geq 6. \quad (20)$$

Thus the relations (15)-(20) yield:

$$\kappa_5(3^n) \geq \kappa_5(3^3) - \frac{35}{416} \geq \frac{1}{4} - \frac{35}{416} > \frac{1}{7} \quad \text{for } n \geq 4,$$

$$\kappa_4(3^n) \geq \kappa_4(3^3) - \frac{3}{8} \geq \frac{7}{16} - \frac{3}{8} > \frac{1}{16} \quad \text{for } n \geq 4,$$

$$\kappa_3(3^n) \geq \kappa_3(3^5) - \frac{9}{16} \geq \frac{3}{4} - \frac{9}{16} > \frac{3}{16} \quad \text{for } n \geq 6.$$

Taking $c_4 = \frac{1}{37}$, we arrive at the assertion of the lemma. $\square$

COROLLARY. For any $3 \leq k \leq 7$, $n \geq 2$ one has

$$|\Omega_k(3^n)| = 3^{3(n-2)} \cdot 18(14 - k) = 2 \cdot 3^{3n-4}(14 - k).$$

This assertion finishes the description of the quantities $\kappa_k(3^n)$, $k \geq 3$, $n \geq 1$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Korolev M.A. 2019, *Kloosterman sums with primes to composite moduli*, [arXiv:1911.09981 \[math.NT\]](#).

2. Changa M.E., Korolev M.A. 2019, *Kloosterman sums with primes and the solvability of one congruence with inverse residues* - I, [arXiv:1911.12589 \[math.NT\]](#).
3. Karatsuba A.A. 1996, "Sums of fractional parts of functions of a special form", *Dokl. Math.*, vol. 54, no. 1, p. 541.
4. Fouvry É., Michel P. 1998, "Sur certaines sommes d'exponentielles sur les nombres premiers", *Ann. sci. Éc. norm. supér.*, vol. 31, no. 1, pp. 93–130.
5. Bourgain J. 2005, "More on the sum-product phenomenon in prime fields and its applications", *Int. J. Number Theory*, vol. 1, no. 1, pp. 1–32.
6. Garaev M.Z. 2010, "Estimation of Kloosterman sums with primes and its application", *Math. Notes*, vol. 88, no. 3, pp. 330–337.
7. Fouvry É., Shparlinski I.E. 2011, "On a ternary quadratic form over primes", *Acta arith.*, vol. 150, no. 3, pp. 285–314.
8. Baker R.C. 2012, "Kloosterman sums with prime variable", *Acta arith.*, vol. 156, no. 4, pp. 351–372.
9. Irving A.J. 2014, "Average bounds for Kloosterman sums over primes", *Funct. Approximatio. Comment. Math.*, vol. 51, no. 2, pp. 221–235.
10. Bourgain J., Garaev M.Z., "Sumsets of reciprocals in prime fields and multilinear Kloosterman sums", *Izv. Math.*, vol. 78, no. 4, pp. 656–707.
11. Korolev M.A. 2017, "Generalized Kloosterman sum with primes", *Proc. Steklov Inst. Math.*, vol. 296, pp. 154–171.
12. Korolev M.A. 2018, "New estimate for a Kloosterman sum with primes for a composite modulus", *Sb. Math.*, vol. 209, no. 5, pp. 652–659.
13. Korolev M.A. 2018, "Divisors of a quadratic form with primes", *Proc. Steklov Inst. Math.*, vol. 303, pp. 154–170.
14. Korolev M.A. 2018, "Elementary Proof of an Estimate for Kloosterman Sums with Primes", *Math. Notes*, vol. 103, no. 5, pp. 761–768.
15. Korolev M.A. 2019, "Short Kloosterman sums with primes", *Math. Notes*, vol. 106, no. 1, pp. 89–97.
16. Changa M.E., Korolev M.A. 2020, "New estimate for Kloosterman sum with primes", to appear in: *Math. Notes*.
17. Salie H. 1931, Über die Kloostermanschen Summen $S(u, v; q)$. *Math. Z.*, vol. 34, pp. 91–109.

Получено 23.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.3

DOI 10.22405/2226-8383-2020-21-1-233-246

**Пространство рядов Дирихле для многомерных решёток
и алгебра рядов Дирихле решёток,
повторяющихся умножением¹**

Н. В. Максименко

Максименко Наталья Викторовна — аспирант кафедры алгебры и дискретной математики, Оренбургский государственный университет (г. Оренбург).

e-mail: white.background.invisible@mail.ru

Аннотация

В теоретико-числовом методе приближенного анализа важную роль играют гиперболические дзета-функции решёток. Каждая такая гиперболическая дзета-функция решётки является рядом Дирихле по усечённому норменному спектру решётки. Поэтому возникает задача об аналитическом продолжении этого класса рядов Дирихле. Как показали Н. М. Добровольский и его соавторы для любой декартовой решётки такое аналитическое продолжение на всю комплексную плоскость за исключением точки $\alpha = 1$, в которой полюс порядка s , существует. Вопрос о существовании аналитического продолжения для произвольных решёток остается открытым.

Поэтому, естественно, рассмотреть множество всевозможных рядов Дирихле, порожденных заданной решёткой, и изучить свойства этого функционального пространства над полем комплексных чисел.

Алгебраические решётки и соответствующие алгебраические сетки вошли в науку в 1976 году в работах К. К. Фролова. Каждая такая решётка является решёткой, повторяющейся умножением, а её норменный спектр будет моноидом натуральных чисел. Поэтому можно рассмотреть алгебру рядов Дирихле, соответствующих этому моноиду натуральных чисел.

Такая постановка является новой и ранее не встречалась в литературе.

Принципиальный вопрос, который связан с такой постановкой, заключается в следующем: *Какими аналитическими свойствами обладают ряды Дирихле из соответствующего пространства и соответствующей алгебры?*

Ключевые слова: дзета-функция Римана, ряд Дирихле, дзета-функция моноида натуральных чисел, эйлерово произведение.

Библиография: 24 названия.

Для цитирования:

Н. В. Максименко. Пространство рядов Дирихле для многомерных решёток и алгебра рядов Дирихле решёток, повторяющихся умножением // Чебышевский сборник. 2020. Т. 21, вып. 1, С. 233–246.

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-41-710004_p_a.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.3

DOI 10.22405/2226-8383-2020-21-1-233-246

**The space of Dirichlet series to multivariate lattices
and the algebra of Dirichlet series of grids,
repetitive multiplication²**

N. V. Maksimenko

Maksimenko Natalia Viktorowna — postgraduate student of the Department of algebra and discrete mathematics, Orenburg state University (Orenburg).

e-mail: white.background.invisible@mail.ru

Abstract

Hyperbolic Zeta functions of lattices play an important role in the numerical-theoretic method of approximate analysis. Each such hyperbolic Zeta function of the lattice is a Dirichlet series over the truncated normal spectrum of the lattice. Therefore, the problem of analytic continuation of this class of Dirichlet series arises. As shown by N. M. Dobrovolsky and his co-authors, for any Cartesian lattice, such an analytical continuation over the entire complex plane except for the point $\alpha = 1$, in which the pole of order s exists. The question of the existence of an analytic continuation for arbitrary lattices remains open.

Therefore, it is natural to consider the set of possible Dirichlet series generated by a given lattice, and to study the properties of this functional space over the field of complex numbers.

Algebraic lattices and corresponding algebraic grids entered science in 1976 in the works of K. K. Frolov. Each such lattice is a lattice repeated by multiplication, and its normal spectrum will be a monoid of natural numbers. Therefore, we can consider the algebra of Dirichlet series corresponding to this monoid of natural numbers.

This setting is new and has not been seen before in the literature.

The fundamental question that is associated with this statement is the following: *What analytical properties do Dirichlet series have from the corresponding space and the corresponding algebra?*

Keywords: Riemann zeta function, Dirichlet series, zeta function of the monoid of natural numbers, Euler product.

Bibliography: 24 titles.

For citation:

N. V. Maksimenko, 2020, "The space of Dirichlet series to multivariate lattices and the algebra of Dirichlet series of grids, repetitive multiplication", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 233–246.

1. Введение

Рассмотрим класс $\mathfrak{A}_s$ всех периодических функций $f(\vec{x})$ с периодом 1 по каждой переменной, у которых их ряд Фурье

$$f(\vec{x}) = \sum_{\vec{m} \in \mathbb{Z}^s} C(\vec{m}) e^{2\pi i(\vec{m}, \vec{x})}, \quad C(\vec{m}) = \int_0^1 \dots \int_0^1 f(\vec{x}) e^{-2\pi i(\vec{m}, \vec{x})} d\vec{x}$$

²Acknowledgments: The reported study was funded by RFBR, project number 19-41-710004 _r _a.

абсолютно сходится. Пространство $\mathfrak{A}_s$ относительно нормы

$$\|f(\vec{x})\|_{l_1} = \sum_{\vec{m} \in \mathbb{Z}^s} |C(\vec{m})| < \infty$$

является сепарабельным банаховым пространством, изоморфным пространству l_1 — всех абсолютно суммируемых комплексно-значных последовательностей (см. [14]).

Н. М. Коробов ввёл в рассмотрение широкий класс периодических функций $E_s^\alpha(C)$ ($\alpha > 1$) с быстро убывающими коэффициентами Фурье. Через $E_s^\alpha(C)$ обозначается множество функций из E_s^α с нормой, не превосходящей C , то есть шар в банаховом пространстве E_s^α радиуса C с центром в нуле.

Банахово пространство периодических функций $E_s^\alpha \subset \mathfrak{A}_s$ состоит из функций $f(x_1, \dots, x_s)$, у которых для коэффициентов Фурье выполняется оценка³

$$C(\vec{m}) = O\left(\frac{1}{(\bar{m}_1 \dots \bar{m}_s)^\alpha}\right).$$

Таким образом, эти функции удовлетворяют условиям

$$\sup_{\vec{m} \in \mathbb{Z}^s} |C(m_1, \dots, m_s)| (\bar{m}_1 \dots \bar{m}_s)^\alpha = \|f(\vec{x})\|_{E_s^\alpha} < \infty. \quad (1)$$

Ясно, что для этих функций ряды Фурье сходятся абсолютно, так как

$$\|f(\vec{x})\|_{l_1} \leq \|f(\vec{x})\|_{E_s^\alpha} (1 + 2\zeta(\alpha))^s,$$

а поэтому для любого $\alpha > 1$ они представляют непрерывные функции. Здесь и далее, как обычно, $\zeta(\alpha)$ — дзета-функция Римана.

О свойствах класса $E_s^\alpha(C)$ подробно можно узнать в [20] и [21] (так же см. [14]).

Для дальнейшего мы будем рассматривать класс $E_s = \bigcup_{\alpha > 1} E_s^\alpha$. Очевидно $E_s \subset \mathfrak{A}_s$. Ясно, что класс E_s незамкнут в пространстве $\mathfrak{A}_s$ относительно нормы $\|f(\vec{x})\|_{l_1}$, но является всюду плотным множеством.

Пространства E_s^α ($\alpha > 1$) — несепарабельные банаховы пространства, изоморфные пространству $l_{s,\infty}$ — ограниченных комплекснозначных функций на фундаментальной решётке $\mathbb{Z}^s$, которое в силу счётности $\mathbb{Z}^s$ изоморфно пространству l_∞ — ограниченных последовательностей комплексных чисел.

Действительно, этот изоморфизм φ_α нормированных пространств E_s^α и $l_{s,\infty}$ задается равенствами для коэффициентов Фурье

$$C(\vec{m}) = \frac{c(\vec{m})}{(\bar{m}_1 \dots \bar{m}_s)^\alpha}, \quad \vec{m} \in \mathbb{Z}^s, \quad \|c(\vec{m})\|_\infty = \sup_{\vec{m} \in \mathbb{Z}^s} |c(m_1, \dots, m_s)| < \infty.$$

Таким образом, если $\vec{x} \in \mathbb{R}^s$ — произвольная точка, а $c(\vec{m}) \in l_{s,\infty}$, то значение функции $\varphi_\alpha(c(\vec{m}))$ в точке $\vec{x}$ задается с помощью ряда Дирихле

$$\varphi_\alpha(c(\vec{m}))(\vec{x}) = \sum_{\vec{m} \in \mathbb{Z}^s} \frac{c(\vec{m}) e^{2\pi i(\vec{x}, \vec{m})}}{(\bar{m}_1 \dots \bar{m}_s)^\alpha} = \sum_{n=1}^{\infty} \frac{a(\vec{x}, n)}{n^\alpha},$$

где

$$a(\vec{x}, n) = \sum_{\bar{m}_1 \dots \bar{m}_s = n} c(\vec{m}) e^{2\pi i(\vec{x}, \vec{m})}.$$

³Здесь и далее для вещественных m полагаем $\bar{m} = \max(1, |m|)$.

Рассмотрим *квадратурную формулу с весами*

$$\int_0^1 \dots \int_0^1 f(x_1, \dots, x_s) dx_1 \dots dx_s = \frac{1}{N} \sum_{k=1}^N \rho_k f[\xi_1(k), \dots, \xi_s(k)] - R_N[f]. \quad (2)$$

Здесь через $R_N[f]$ обозначена погрешность, получающаяся при замене интеграла

$$\int_0^1 \dots \int_0^1 f(x_1, \dots, x_s) dx_1 \dots dx_s$$

средним взвешенным значением функции $f(x_1, \dots, x_s)$, вычисленным в точках

$$M_k = (\xi_1(k), \dots, \xi_s(k)) \quad (k = 1, \dots, N).$$

Совокупность M точек M_k называется *сеткой M* , а сами точки — *узлами квадратурной формулы*. Величины $\rho_k = \rho(M_k)$ называются весами квадратурной формулы. Будем использовать равноправные обозначения $|M| = N$. В этой работе будем везде предполагать, что все веса вещественнозначные.

ОПРЕДЕЛЕНИЕ 1. *Тригонометрической суммой сетки с весами (M, ρ) для произвольного целочисленного вектора $\vec{m}$ называется выражение*

$$S(\vec{m}, (M, \rho)) = \sum_{\vec{x} \in M} \rho(\vec{x}) e^{2\pi i(\vec{m}, \vec{x})}, \quad (3)$$

а нормированной тригонометрической суммой сетки с весами —

$$S^*(\vec{m}, (M, \rho)) = \frac{1}{|M|} S(\vec{m}, (M, \rho)).$$

Справедлива следующая обобщенная теорема Коробова о погрешности квадратурных формул (см. [13]).⁴

ТЕОРЕМА 1. *Пусть ряд Фурье функции $f(\vec{x})$ сходится абсолютно, $C(\vec{m})$ — ее коэффициенты Фурье и $S_{M, \vec{\rho}}(\vec{m})$ — тригонометрические суммы сетки с весами, тогда справедливо равенство*

$$\begin{aligned} R_N[f] &= C(\vec{0}) \left(\frac{1}{N} S_{M, \vec{\rho}}(\vec{0}) - 1 \right) + \frac{1}{N} \sum'_{m_1, \dots, m_s = -\infty}^{\infty} C(\vec{m}) S_{M, \vec{\rho}}(\vec{m}) = \\ &= C(\vec{0}) \left(S_{M, \vec{\rho}}^*(\vec{0}) - 1 \right) + \sum'_{m_1, \dots, m_s = -\infty}^{\infty} C(\vec{m}) S_{M, \vec{\rho}}^*(\vec{m}) \end{aligned} \quad (4)$$

и при $N \rightarrow \infty$ погрешность $R_N[f]$ будет стремиться к нулю тогда и только тогда, когда взвешенные узлы квадратурной формулы равномерно распределены в единичном s -мерном кубе.

В работе [15] дано следующее определение дзета-функции сетки M с весами $\vec{\rho}$.

⁴Здесь и далее $\sum'$ означает суммирование по системам $(m_1, \dots, m_s) \neq (0, \dots, 0)$.

ОПРЕДЕЛЕНИЕ 2. Дзета-функцией сетки M с весами $\vec{\rho}$ называется функция $\zeta(\alpha|M, \vec{\rho})$, заданная в правой полуплоскости $\alpha = \sigma + it$ ($\sigma > 1$) рядом Дирихле

$$\zeta(\alpha|M, \vec{\rho}) = \sum_{m_1, \dots, m_s = -\infty}^{\infty'} \frac{|S_{M, \vec{\rho}}^*(\vec{m})|}{(\bar{m}_1 \dots \bar{m}_s)^\alpha} = \sum_{n=1}^{\infty} \frac{S^*(M, \vec{\rho}, n)}{n^\alpha}, \quad (5)$$

где

$$S^*(M, \vec{\rho}, n) = \sum_{\vec{m} \in N(n)} |S_{M, \vec{\rho}}^*(\vec{m})| \quad (6)$$

и $N(n)$ — норменная поверхность, заданная равенством $N(n) = \{\vec{m} \in \mathbb{Z}^s | \bar{m}_1 \dots \bar{m}_s = n\}$.

Справедливы две обобщенные теоремы Коробова о погрешности квадратурных формул — это теорема 1 и следующая теорема:

ТЕОРЕМА 2. Если $f(x_1, \dots, x_s) \in E_s^\alpha(C)$, то для погрешности квадратурной формулы справедлива оценка

$$|R_N[f]| \leq C \left| \frac{1}{N} S_{M, \vec{\rho}}(\vec{0}) - 1 \right| + \frac{C}{N} \sum_{m_1, \dots, m_s = -\infty}^{\infty'} \frac{|S_{M, \vec{\rho}}(\vec{m})|}{(\bar{m}_1 \dots \bar{m}_s)^\alpha} = C \left| S_{M, \vec{\rho}}^*(\vec{0}) - 1 \right| + C \cdot \zeta(\alpha|M, \vec{\rho}), \quad (7)$$

где сумма $S_{M, \vec{\rho}}(\vec{m})$ определена равенством (3). На классе $E_s^\alpha(C)$ эту оценку нельзя улучшить.

Другими словами теорему 2 можно сформулировать так:

Для нормы $\|R_N[f]\|_{E_s^\alpha}$ линейного функционала погрешности приближенного интегрирования по квадратурной формуле (2) справедливо равенство

$$\|R_N[f]\|_{E_s^\alpha} = \left| \frac{1}{N} S_{M, \vec{\rho}}(\vec{0}) - 1 \right| + \frac{1}{N} \sum_{m_1, \dots, m_s = -\infty}^{\infty'} \frac{|S_{M, \vec{\rho}}(\vec{m})|}{(\bar{m}_1 \dots \bar{m}_s)^\alpha} = \left| S_{M, \vec{\rho}}^*(\vec{0}) - 1 \right| + \zeta(\alpha|M, \vec{\rho}). \quad (8)$$

Следуя К. И. Бабенко [1] и О. В. Локуциевскому [22], в работе [13] дано следующее определение ненасыщаемого алгоритма приближенного интегрирования на классе $E_s = \bigcup_{\alpha > 1} E_s^\alpha$.

ОПРЕДЕЛЕНИЕ 3. Будем говорить, что периодическая функция $f(\vec{x})$ из класса $E_s = \bigcup_{\alpha > 1} E_s^\alpha$ принадлежит конечному показателю $\alpha = \alpha(f(\vec{x}))$, если $f(\vec{x}) \in E_s^\alpha$ и $f(\vec{x}) \notin E_s^\beta$ для любого $\beta > \alpha$. В противном случае будем говорить, что периодическая функция из класса E_s принадлежит бесконечному показателю.

Ясно, что бесконечному показателю принадлежит любой конечный тригонометрический полином. Если периодическая функция $f(\vec{x}) \in E_s$ не является конечным тригонометрическим полиномом и принадлежит бесконечному показателю, то она будет бесконечно дифференцируемой функцией.

ОПРЕДЕЛЕНИЕ 4. Будем говорить, что алгоритм приближенного интегрирования $\langle M(j), \vec{\rho}(j), \Delta \rangle$ ($j = 1, 2, \dots$) периодических функций из класса $E_s = \bigcup_{\alpha > 1} E_s^\alpha$ ненасыщаемый типа (γ, λ) , если для любой периодической функции $f(\vec{x})$ конечного показателя $\alpha = \alpha(f(\vec{x}))$ и погрешности приближенного интегрирования выполняется равенство

$$R_{N_j}[f(\vec{x})] = O\left(\frac{\ln^\gamma N_j}{N_j^{\lambda \cdot \alpha}}\right). \quad (9)$$

Как известно (см. [21]), методом оптимальных коэффициентов Коробова можно построить ненасыщаемые алгоритмы типа $((s-1)\alpha, 1)$, а модифицированным методом Фролова — $((s-1), 1)$. Для случая равномерных сеток имеем тип $(0, \frac{1}{s})$.

Из теоремы 2 сразу следует, что если алгоритм приближенного интегрирования

$$\langle M(j), \vec{\rho}(j), \Delta \rangle \quad (j = 1, 2, \dots)$$

периодических функций из класса $E_s = \bigcup_{\alpha > 1} E_s^\alpha$ ненасыщаемый типа (γ, λ) , то

$$S_{M, \vec{\rho}}^*(\vec{0}) = 1, \quad \zeta(\alpha | M(j), \vec{\rho}(j)) = O\left(\frac{\ln^\gamma N_j}{N_j^{\lambda \cdot \alpha}}\right) \quad (j = 1, 2, \dots).$$

Из предыдущего видно, что ряды Дирихле, порождённые решетками, естественно возникают в теоретико-числовом методе в приближенном анализе и играют в его развитии существенную роль.

Целью данной работы является изучение функционального пространства над полем комплексных чисел всевозможных рядов Дирихле, порожденных заданной решёткой.

2. Пространство рядов Дирихле для многомерных решёток

Пусть Λ — произвольная s -мерная решётка в $\mathbb{R}^s$. Рядом Дирихле $f(\alpha | \Lambda)$ для решётки Λ будем называть произвольную функцию, заданную равенством

$$f(\alpha | \Lambda) = \sum_{\vec{x} \in \Lambda} \frac{a(\vec{x})}{(\bar{x}_1 \cdot \dots \cdot \bar{x}_s)^\alpha} = \sum_{k=1}^{\infty} A(\lambda_k) \lambda_k^{-\alpha} \quad \alpha = \sigma + it, \quad \sigma > \sigma_f \geq \sigma_f^*,$$

где σ_f — абсцисса абсолютной сходимости и σ_f^* — абсцисса сходимости, а λ_k — точки усечённого норменного спектра $Q_{sp}(\Lambda)$, который определяется равенством

$$Q_{sp}(\Lambda) = \{\lambda \mid \lambda = q(\vec{x}), \vec{x} \in \Lambda \setminus \{\vec{0}\}\}, \quad q(\vec{x}) = \bar{x}_1 \cdot \dots \cdot \bar{x}_s$$

и

$$A(\lambda_k) = \sum_{\bar{x}_1 \cdot \dots \cdot \bar{x}_s = \lambda_k} a(\vec{x}).$$

Как хорошо известно [23, 24], для любых рядов Дирихле справедливо неравенство $\sigma_f \leq \sigma_f^* + 1$.

По теореме Абеля (см. [23], стр. 106)

$$f(\alpha | \Lambda) = \alpha \int_{\lambda_1}^{\infty} \frac{A^*(t)}{t^{\alpha+1}} dt, \quad A^*(t) = \sum_{q(\vec{x}) \leq t} a(\vec{x}).$$

Множество всех рядов Дирихле, порожденных заданной решёткой Λ , обозначим через $\mathbb{D}(\Lambda)$.

Далее мы будем следовать работе [19], подчёркивая отличия случая решётки от случая моноида.

Пусть $\mathbb{K}$ — произвольное числовое поле. Таким образом, $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$. Если все коэффициенты $a(\vec{x}) \in \mathbb{K}$, то множество всех таких рядов Дирихле будем обозначать через $\mathbb{D}(\Lambda)_{\mathbb{K}}$ и оно является бесконечномерным линейным функциональным пространством над полем $\mathbb{K}$.

Выделим подпространство $\mathbb{D}^\infty(\Lambda)_{\mathbb{K}}$ условием $\sup_{\vec{x} \in \Lambda} |a(\vec{x})| < \infty$. На $\mathbb{D}^\infty(\Lambda)_{\mathbb{K}}$ зададим норму

$$\|f(\alpha | \Lambda)\| = \sup_{\vec{x} \in \Lambda} |a(\vec{x})|.$$

Относительно заданной нормы $\mathbb{D}^\infty(\Lambda)_\mathbb{K}$ является несепарабельным пространством. Оно будет банаховым, если поле $\mathbb{K}$ — банахово пространство над полем $\mathbb{Q}$ относительно нормы, заданной абсолютной величиной числа из поля $\mathbb{K}$. Так как отсюда следует, что либо $\mathbb{K} = \mathbb{R}$, либо $\mathbb{K} = \mathbb{C}$, то $\mathbb{D}^\infty(\Lambda)_\mathbb{K}$ — банахово пространство, только для $\mathbb{K} = \mathbb{R}$, либо $\mathbb{K} = \mathbb{C}$.

Нетрудно понять, что пространство $\mathbb{D}^\infty(\Lambda)_\mathbb{K}$ над полем $\mathbb{K}$ не является алгеброй, так как нет замкнутости относительно произведения рядов Дирихле.

Более того, для произвольной решётки Λ произведение двух рядов Дирихле $f(\alpha|\Lambda)$ и $g(\alpha|\Lambda)$, вообще говоря, не является рядом Дирихле $h(\alpha|\Lambda)$, так как для произвольной решётки Λ покоординатное произведение двух точек $\vec{x}$ и $\vec{y}$ из Λ не является точкой решётки Λ .

Принципиальное отличие пространства $\mathbb{D}(\Lambda)_\mathbb{K}$ от случая пространства $\mathbb{D}(M)_\mathbb{K}$, когда M — произвольный моноид натуральных чисел, в том, что усечённый норменный спектр $Q_{sp}(\Lambda)$ не является мультипликативным моноидом. Положение можно исправить, если рассмотреть мультипликативный моноид вещественных чисел $M(Q_{sp}(\Lambda))$, порожденный усечённым норменным спектром $Q_{sp}(\Lambda)$. Таким образом,

$$M(Q_{sp}(\Lambda)) = \{\lambda = q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_n) \mid \vec{x}_1, \dots, \vec{x}_n \in \Lambda, n \geq 1\}.$$

Ясно, что $Q_{sp}(\Lambda) \subseteq M(Q_{sp}(\Lambda))$ и мультипликативный моноид $M(Q_{sp}(\Lambda))$ — дискретное множество. Действительно, для любого $\lambda \in M(Q_{sp}(\Lambda))$ имеем:

$$\lambda \geq 1, \quad \lambda = q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_n), \quad 1 \leq \bar{x}_{1,j}, \dots, \bar{x}_{s,j} \leq \lambda.$$

Отсюда следует, что $\vec{x}_n \in [-\lambda; \lambda]^s$. Так как любому s -мерному кубу принадлежит конечное число точек решётки Λ в силу её дискретности, то дискретность мультипликативного моноида $M(Q_{sp}(\Lambda))$ доказана.

Порядком точки λ усечённого норменного спектра называется количество точек $\vec{x}$ решётки Λ , для которых $q(\vec{x}) = \lambda$. Порядок точки λ обозначается через $q(\lambda)$. Нетрудно понять, что величина

$$D(T|\Lambda) = \sum_{\lambda \in Q_{sp}(\Lambda), \lambda \leq T} q(\lambda)$$

— количество точек решётки Λ в гиперболическом кресте $K_s(T) = \{\vec{x} \mid q(\vec{x}) \leq T\}$.

В работе [16] доказана асимптотическая формула

$$D(T|\Lambda) = \frac{2^s T \ln^{s-1} T}{(s-1)! \det \Lambda} + O\left(\frac{T \ln^{s-2} T}{\det \Lambda}\right).$$

Прежде чем идти дальше, сделаем принципиальное замечание. Вся теория, построенная в работе [19], относится к случаю мультипликативного моноида натуральных чисел, а введённый выше мультипликативный моноид $M(Q_{sp}(\Lambda))$ является, вообще говоря, мультипликативным моноидом вещественных чисел. Этот случай ближе к тематике работ Б. М. Бредихина [2]–[10], но они посвящены другим вопросам, которых мы в данной работе не касаемся.

Поэтому далее мы будем утверждения, аналогичные утверждениям из работы [19], приводить, как правило, без доказательств, кроме тех случаев, когда надо проводить дополнительные рассуждения, связанные со спецификой мультипликативного моноида вещественных чисел.

Рассмотрим произведение двух рядов Дирихле из $\mathbb{D}(\Lambda)_\mathbb{K}$:

$$f(\alpha|\Lambda) = \sum_{n \in Q_{sp}(\Lambda)} \frac{A(n)}{n^\alpha}, \quad g(\alpha|\Lambda) = \sum_{n \in Q_{sp}(\Lambda)} \frac{B(n)}{n^\alpha} \quad A(n), B(n) \in \mathbb{K},$$

имеем:

$$f(\alpha|\Lambda)g(\alpha|\Lambda) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{C(n)}{n^\alpha},$$

где

$$C(n) = \sum_{m|n, m, \frac{n}{m} \in Q_{sp}(\Lambda)} A(m)B\left(\frac{n}{m}\right) \in \mathbb{K} \quad n \in M(Q_{sp}(\Lambda)).$$

Следовательно $f(\alpha|\Lambda)g(\alpha|\Lambda) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$.

Для произведения двух произвольных рядов Дирихле из $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ имеем аналогичные формулы, но с некоторыми отличиями:

$$\begin{aligned} f(\alpha) &= \sum_{n \in M(Q_{sp}(\Lambda))} \frac{a(n)}{n^\alpha}, \quad g(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{b(n)}{n^\alpha} \quad a(n), b(n) \in \mathbb{K}, \\ f(\alpha)g(\alpha) &= \sum_{n \in M(Q_{sp}(\Lambda))} \frac{c(n)}{n^\alpha}, \\ c(n) &= \sum_{m|n, m, \frac{n}{m} \in M(Q_{sp}(\Lambda))} a(m)b\left(\frac{n}{m}\right) \in \mathbb{K} \quad n \in M(Q_{sp}(\Lambda)) \end{aligned}$$

и $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ является коммутативной алгеброй над полем $\mathbb{K}$.

Хотя мультипликативный моноид $M(Q_{sp}(\Lambda))$, вообще говоря, не является мультипликативным моноидом натуральных чисел, но многие утверждения из [19] справедливы и в этом более общем случае. В частности, доказываемая ассоциативность алгебры $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ над полем $\mathbb{K}$.

Если ряд Дирихле $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ имеет коэффициент $a(1) \neq 0$, то существует обратный ряд Дирихле $f^{-1}(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$, то есть такой ряд Дирихле

$$f^{-1}(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{b(n)}{n^\alpha}, \quad \text{что} \quad f(\alpha)f^{-1}(\alpha) = 1.$$

Нетрудно видеть, что коэффициенты $b(n)$ удовлетворяют соотношениям:

$$b(1) = \frac{1}{a(1)}, \quad b(n) = -\frac{1}{a(1)} \sum_{m|n, m, \frac{n}{m} \in M(Q_{sp}(\Lambda)), m > 1} a(m)b\left(\frac{n}{m}\right) \quad n \in M(Q_{sp}(\Lambda)), n > 1.$$

Множество всех обратимых рядов Дирихле из алгебры $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ обозначим через $\mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$. Ясно, что это мультипликативный моноид, но справедливо более сильное утверждение.

ТЕОРЕМА 3. *Множество $\mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ всех обратимых рядов Дирихле из алгебры $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ является бесконечной абелевой группой, состоящей из рядов, у которых первый коэффициент отличен от нуля.*

ДОКАЗАТЕЛЬСТВО. Доказательство дословно повторяет доказательство аналогичной теоремы из [19]. $\square$

Обозначим через A_f область аналитичности ряда Дирихле $f(\alpha)$, то есть максимальную область, куда ряд Дирихле $f(\alpha)$ аналитически продолжается. Через P_f — множество полюсов его аналитического продолжения, а через Z_f — множество его нулей. Очевидно, что для $f(\alpha) \in \mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ выполняются соотношения

$$A_{f^{-1}} = (A_f \setminus Z_f) \cup P_f.$$

3. Алгебра целых рядов Дирихле

Рассмотрим кольцо целых алгебраических чисел $\mathbb{Z}_{\mathbb{K}}$ алгебраического поля $\mathbb{K}$. Ряд Дирихле

$$f(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{a(n)}{n^\alpha} \quad a(n) \in \mathbb{Z}_{\mathbb{K}}, n \in M(Q_{sp}(\Lambda))$$

будем называть целым рядом Дирихле над алгебраическим полем $\mathbb{K}$ для моноида $M(Q_{sp}(\Lambda))$. Множество всех таких рядов Дирихле будем обозначать через $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$. Ясно, что $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}} \subset \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$.

Нетрудно видеть, что множество целых рядов Дирихле, с одной стороны, является $\mathbb{Z}_{\mathbb{K}}$ -модулем, а с другой стороны, — алгеброй над целым алгебраическим кольцом $\mathbb{Z}_{\mathbb{K}}$.

Обозначим через $\mathbb{U}_{\mathbb{K}}$ группу алгебраических единиц кольца целых алгебраических чисел $\mathbb{Z}_{\mathbb{K}}$ алгебраического поля $\mathbb{K}$. Через $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}}$ обозначим подмножество целых рядов Дирихле из алгебры $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$, у которых $a(1) \in \mathbb{U}_{\mathbb{K}}$.

ТЕОРЕМА 4. *Множество $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}}$ целых рядов Дирихле является мультипликативной группой.*

ДОКАЗАТЕЛЬСТВО. Во-первых, покажем, что множество $\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}}$ замкнуто относительно операции умножения рядов Дирихле. Действительно, если

$$f(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{a(n)}{n^\alpha}, \quad g(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{b(n)}{n^\alpha} \quad a(n), b(n) \in \mathbb{Z}_{\mathbb{K}}, \quad a(1), b(1) \in \mathbb{U}_{\mathbb{K}},$$

то

$$f(\alpha)g(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{c(n)}{n^\alpha}, \quad c(n) = \sum_{m|n, m, \frac{n}{m} \in M(Q_{sp}(\Lambda))} a(m)b\left(\frac{n}{m}\right) \in \mathbb{Z}_{\mathbb{K}} \quad n \in M(Q_{sp}(\Lambda)),$$

$$c(1) = a(1)b(1) \in \mathbb{U}_{\mathbb{K}}$$

и замкнутость установлена.

Во-вторых, единичным элементом является ряд Дирихле $f(\alpha) \equiv 1$.

Наконец, для любого $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}}$ имеем:

$$f^{-1}(\alpha) = \sum_{n \in M(Q_{sp}(\Lambda))} \frac{b(n)}{n^\alpha}, \quad b(1) = \frac{1}{a(1)}, \quad b(n) = -\frac{1}{a(1)} \sum_{m|n, m, \frac{n}{m} \in M(Q_{sp}(\Lambda)), m>1} a(m)b\left(\frac{n}{m}\right)$$

$$n \in M(Q_{sp}(\Lambda)), n > 1.$$

Ясно, что $b(1) \in \mathbb{U}_{\mathbb{K}}$. Далее индукцией⁵ по n мы получаем, что для всех $n \in M(Q_{sp}(\Lambda))$, $n > 1$ имеем $b(n) \in \mathbb{Z}_{\mathbb{K}}$, что доказывает $f^{-1}(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}}$. Тем самым теорема полностью доказана. $\square$

Если определить множество $\mathbb{D}(M(Q_{sp}(\Lambda)))_{1_{\mathbb{K}}}$ целых рядов Дирихле с $a(1) = 1$, то нетрудно видеть, что это будет подгруппа: $\mathbb{D}(M(Q_{sp}(\Lambda)))_{1_{\mathbb{K}}} \subset \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}} \subset \mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$.

⁵Индукция возможна, так как мультипликативный моноид $M(Q_{sp}(\Lambda))$ — дискретное множество.

4. Алгебра необратимых рядов Дирихле

Для произвольного ряда Дирихле $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ определим его необратимую часть $f^*(\alpha)$ равенством $f^*(\alpha) = f(\alpha) - a(1)$. Ясно, что $f^*(\alpha) = f(\alpha)$ только для необратимых рядов Дирихле. Обозначим множество всех необратимых рядов Дирихле через $\mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$, а множество всех необратимых целых рядов Дирихле обозначим через $\mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$. Очевидно, что $\mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ — алгебра над полем $\mathbb{K}$, а $\mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$ — алгебра над кольцом $\mathbb{Z}_{\mathbb{K}}$.

Ясно, что справедливы следующие разложения в прямые суммы:

$$\mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}} = \mathbb{K} \bigoplus \mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{K}}, \quad \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}} = \mathbb{Z}_{\mathbb{K}} \bigoplus \mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}.$$

Кроме этого, справедливы равенства:

$$\begin{aligned} \mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{K}} &= \mathbb{K}^* + \mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{K}}, & \mathbb{D}^*(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}} &= \mathbb{Z}_{\mathbb{K}}^* + \mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}, \\ \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{U}_{\mathbb{K}}} &= \mathbb{U}_{\mathbb{K}} + \mathbb{D}^0(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}, \end{aligned}$$

где $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ и $\mathbb{Z}_{\mathbb{K}}^* = \mathbb{Z}_{\mathbb{K}} \setminus \{0\}$.

Для произвольного ряда Дирихле $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ определим его дополнительную часть $f^{**}(\alpha)$ равенством $f^{**}(\alpha) = (1 + f^*(\alpha))^{-1} - 1$.

Если дан произвольный ряд Дирихле $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$, то его приведенным рядом Дирихле назовём ряд $f^{(p)}(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$, заданный равенством $f^{(p)}(\alpha) = 1 + f^*(\alpha)$. Очевидно, что для $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{1_{\mathbb{K}}}$ будет $f^{(p)}(\alpha) = f(\alpha)$.

ТЕОРЕМА 5. Для любого $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{K}}$ справедливо равенство

$$f(\alpha) = f^{(p)}(\alpha)(a(1) + f^*(\alpha) + f(\alpha)f^{**}(\alpha)).$$

ДОКАЗАТЕЛЬСТВО. Дословно повторяет доказательство аналогичной теоремы из [19]. $\square$

СЛЕДСТВИЕ 1. Для любого $f(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$ справедливо равенство

$$f(\alpha) = f^{(p)}(\alpha)(a(1) + f^*(\alpha) + f(\alpha)f^{**}(\alpha)),$$

где $f^{(p)}(\alpha), a(1) + f^*(\alpha) + f(\alpha)f^{**}(\alpha) \in \mathbb{D}(M(Q_{sp}(\Lambda)))_{\mathbb{Z}_{\mathbb{K}}}$.

ДОКАЗАТЕЛЬСТВО. Дословно повторяет доказательство аналогичного следствия из [19]. $\square$

5. Алгебра рядов Дирихле решёток, повторяющихся умножением

Как было отмечено выше (см. стр. 239), усечённый норменный спектр $Q_{sp}(\Lambda)$ не является мультипликативным моноидом. Поэтому было введено понятие мультипликативного моноида вещественных чисел $M(Q_{sp}(\Lambda))$, порожденного усечённым норменным спектром $Q_{sp}(\Lambda)$.

Сама решётка Λ может быть замкнута относительно умножения, если это случай решётки, повторяющейся умножением (см. [12]). Но даже в этом случае отображение $q(\vec{x}) : \Lambda \rightarrow \mathbb{R}$ не является гомоморфизмом. Поясним сказанное на двух примерах.

Если F — чисто вещественное алгебраическое расширение степени s поля рациональных чисел $\mathbb{Q}$ и $\mathbb{Z}_F$ — кольцо целых алгебраических чисел поля F , то s -мерной решёткой является множество $\Lambda(F)$, следующим способом образованное с помощью $\mathbb{Z}_F$:

$$\Lambda(F) = \{(\Theta^{(1)}, \dots, \Theta^{(s)}) \mid \Theta^{(1)} \in \mathbb{Z}_F\}, \quad (10)$$

где $\Theta^{(1)}, \dots, \Theta^{(s)}$ — система алгебраически сопряженных чисел, и если d — дискриминант поля F , то $\det \Lambda(F) = \sqrt{d}$.

Легко видеть, что $q(\vec{x}) = 1$ для $\vec{x} \in \Lambda(F)$ только для $\vec{x} = (1, \dots, 1)$. С другой стороны, если $\varepsilon \in \mathbb{Z}_F$, то $q(\vec{\varepsilon}) > 1$, где $\vec{\varepsilon} = (\varepsilon^{(1)}, \dots, \varepsilon^{(s)})$, ε — алгебраическая единица поля F . Далее имеем: $\varepsilon_1 = \varepsilon^{-1}$ — алгебраическая единица поля F , $\vec{\varepsilon}_1 = ((\varepsilon^{(1)})^{-1}, \dots, (\varepsilon^{(s)})^{-1})$, $q(\vec{\varepsilon}\vec{\varepsilon}_1) = q(\vec{1}) = 1 < q(\vec{\varepsilon})q(\vec{\varepsilon}_1)$.

Второй пример связан с приводимой решёткой, повторяющейся умножением, $\Lambda(\vec{m}) = m_1\mathbb{Z} \times \dots \times m_s\mathbb{Z}$, где $m_1, \dots, m_s$ — натуральные числа. Если $\vec{x} \in \Lambda$, то $\vec{x} = (m_1n_1, \dots, m_sn_s)$, $\vec{n} = (n_1, \dots, n_s) \in \mathbb{Z}^s$. Ясно, что для $q(\vec{x})$ справедливо равенство

$$q(\vec{x}) = \prod_{n_\nu \neq 0} m_\nu |n_\nu|.$$

Если $\vec{x}\vec{y} = (x_1y_1, \dots, x_sy_s) = \vec{0}$, $\vec{x} \neq \vec{0}$, $\vec{y} \neq \vec{0}$, то $q(\vec{x}\vec{y}) = 1 < q(\vec{x})q(\vec{y})$, если $q(\vec{x}) > 1$, $q(\vec{y}) > 1$.

ТЕОРЕМА 6. *Для любого $\vec{m} \in \mathbb{N}^s$ справедливо равенство*

$$M(Q_{sp}(\Lambda(\vec{m}))) = Q_{sp}(\Lambda(\vec{m})).$$

ДОКАЗАТЕЛЬСТВО. Чтобы доказать требуемое равенство, достаточно показать, что для любых $\vec{x}_1, \dots, \vec{x}_k \in \Lambda(\vec{m})$, отличных от $\vec{0}$, найдётся $\vec{x} \in \Lambda(\vec{m})$ такой, что $q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_k) = q(\vec{x})$.

Пусть ν_0 — наименьшее ν такое, что $x_{j,\nu} \neq 0$, тогда $m_{\nu_0} |q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_k)|$. Определим $\vec{x} = (x_1, \dots, x_s)$ с помощью равенств

$$x_\nu = \begin{cases} 0, & \text{при } \nu \neq \nu_0, \\ q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_k), & \text{при } \nu = \nu_0, \end{cases}$$

тогда $\vec{x} \in \Lambda(\vec{m})$ и $q(\vec{x}) = q(\vec{x}_1) \cdot \dots \cdot q(\vec{x}_k)$, что доказывает утверждение теоремы. $\square$

Из доказанной теоремы следует, что в случае приводимой решёткой, повторяющейся умножением, $\Lambda(\vec{m})$ пространство $\mathbb{D}(\Lambda(\vec{m}))_{\mathbb{K}}$ является коммутативной, ассоциативной алгеброй над полем $\mathbb{K}$.

6. Заключение

В данной статье заложены основы теории пространств и алгебр рядов Дирихле, порожденных s -мерными решётками. Показано, что пространство таких рядов Дирихле вкладывается в алгебру рядов Дирихле моноида вещественных чисел. Таким образом возникает более общий случай, чем в работе [19]. Этот более общий случай близок по объекту исследования с тем, что рассматривался в работах Б. М. Бредихина. Один из интересных вопросов связан с выделением в спектре $Q_{sp}(\Lambda)$ тех элементов, которые будут простыми элементами в мультипликативном моноиде вещественных чисел $M(Q_{sp}(\Lambda))$. Здесь возникают непростые вопросы о подходящем понятии плотности для моноида $M(Q_{sp}(\Lambda))$ и вида асимптотического закона распределения простых элементов в зависимости от решётки Λ . Мы предполагаем рассмотреть такие вопросы в дальнейших исследованиях.

Выражаю свою благодарность научному руководителю профессору Н. М. Добровольскому за постановку задачи и доценту Н. Н. Добровольскому за постоянное внимание к работе и полезные обсуждения.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бабенко К. И. Основы численного анализа. М.: Наука, 1986.
2. Б. М. Бредихин, “Остаточный член в асимптотической формуле для функции $\nu_G(x)$ ”, Изв. вузов. Матем., 1960, 6, 40–49.
3. Б. М. Бредихин, “Элементарное решение обратных задач о базисах свободных полугрупп”, Матем. сб., 50(92):2 (1960), 221–232.
4. Б. М. Бредихин, “Свободные числовые полугруппы со степенными плотностями”, Докл. АН СССР, 118:5 (1958), 855–857.
5. Б. М. Бредихин, “О степенных плотностях некоторых подмножеств свободных полугрупп”, Изв. вузов. Матем., 1958, 3, 24–30.
6. Б. М. Бредихин, “Свободные числовые полугруппы со степенными плотностями”, Матем. сб., 46(88):2 (1958), 143–158.
7. Б. М. Бредихин, “Пример конечного гомоморфизма с ограниченной сумматорной функцией”, УМН, 11:4(70) (1956), 119–122.
8. Б. М. Бредихин, Некоторые вопросы теории характеров коммутативных полу групп, Труды 3-го Всесоюзн. матем. съезда, т. I, Москва, Изд. АН СССР (1956), 3.
9. Б. М. Бредихин, О сумматорных функциях характеров числовых полугрупп, ДАН 94 (1954), 609 — 612.
10. Б. М. Бредихин, О характерах числовых полугрупп с достаточно редкой базой, ДАН 90 (1953), 707 — 710.
11. Гурвиц А., Курант Р. Теория функций. — М.: Наука, 1968. — 618 с.
12. Б. Н. Делоне, Д. К. Фаддеев Теория иррациональностей третьей степени // Тр. Матем. ин-та им. В. А. Стеклова, 1940. Т. 11. С. 3–340.
13. Добровольская Л. П., Добровольский Н. М., Симонов А. С. О погрешности приближенного интегрирования по модифицированным сеткам // Чебышевский сборник, 2008 Т. 9. Вып. 1(25). Тула, Из-во ТГПУ им. Л. Н. Толстого. С. 185–223.
14. Добровольский Н. М., Манохин Е. В. Банаховы пространства периодических функций // Изв. ТулГУ. Сер. Механика. Математика. Информатика. Т. 4, вып. 3. Тула, 1998. С. 56–67.
15. Добровольский Н. М., Манохин Е. В., Реброва И. Ю., Рощеня А. Л. О непрерывности дзета-функции сетки с весами // Известия ТулГУ. Сер. Математика. Механика. Информатика. Т. 7, вып. 1. — Тула, 2001. С. 82–86.
16. Н. М. Добровольский, А. Л. Рощеня, “О числе точек решетки в гиперболическом кресте”, Матем. заметки, 63:3 (1998). С. 363–369.
17. Добровольский Н. Н. Одна модельная дзета-функция моноида натуральных чисел // Чебышевский сборник. 2019. — Т. 20, вып. 1, С. 148–163.
18. Добровольский Н. Н., Добровольский М. Н., Добровольский Н. М., Балаба И. Н., Реброва И. Ю. Гипотеза о “заградительном ряде” для дзета-функций моноидов с экспоненциальной последовательностью простых // Чебышевский сб. 2018. — Т. 19, вып. 1. — С. 106–123.

19. Н. Н. Добровольский, М. Н. Добровольский, Н. М. Добровольский, И. Н. Балаба, И. Ю. Реброва. Алгебра рядов Дирихле моноида натуральных чисел // Чебышевский сборник. 2019. Т. 20, вып. 1, С. 180–196.
20. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. М.: Физматгиз, 1963.
21. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. (второе издание) М.: МЦНМО, 2004. 288 с.
22. О. В. Локуциевский, М. Б. Гавриков Начала численного анализа / М.: ТОО "Янус" 1995
23. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974. — 188 с.
24. Чудаков Н. Г. Введение в теорию L -функций Дирихле. — М. – Л.: ОГИЗ, 1947. — 204 с.

REFERENCES

1. Babenko, K.I. 1986, *Osnovy chislennogo analiza* [Fundamentals of numerical analysis], Nauka, Moscow, Russia.
2. Bredikhin, B.M., 1960, "The remainder term in the asymptotic formula for the function $\nu_G(x)$ ", *Izvestiya vuzov Matematika*, no. 6, pp. 40–49.
3. Bredikhin, B.M., 1960, "An elementary solution of inverse problems on bases of free semigroups", *matematicheskiiy sbornik*, 50(92):2, pp. 221–232.
4. Bredikhin, B.M., 1958, "Free numerical semigroups with power densities", *Doklady Akademii nauk SSSR*, 118:5, pp. 855–857.
5. Bredikhin, B.M., 1958, "On power densities of some subsets of free semigroups", *Izvestiya vuzov Matematika*, no. 3, pp. 24–30.
6. Bredikhin, B.M., 1958, "Free numerical semigroups with power densities", *matematicheskiiy sbornik*, 46(88):2, pp. 143–158.
7. Bredikhin, B.M., 1956, "An example of a finite homomorphism with a bounded adder function", *UMN*, 11:4(70), pp. 119–122.
8. Bredikhin, B.M., 1956, "Some questions of the theory of characters of commutative semigroups", *Trudy 3-go Vsesoyuznogo matematicheskogo s'yezda*, vol. 1, Moskva, izdatel'stvo akademii nauk SSSR, no. 3.
9. Bredikhin, B.M., 1954, "On adder functions of characters of numerical semigroups", *DAN* 94, pp. 609 – 612.
10. Bredikhin, B.M., 1953, "On the characters of numerical semigroups with a rather rare base", *DAN* 90, pp. 707–710.
11. Gurvic A., Kurant R., 1968, *Teoriya funkciy*, Izd-vo Nauka, Moskva, 618 p.
12. Delone B.N., Faddeev D.K., 1940, "Theory of Irrationalities of the Third Degree", *trudy matematicheskogo instituta imeni Steklova V.A.*, vol. 11., pp. 3–340.
13. Dobrovol'skaya, L. P., Dobrovol'skii, N. M. & Simonov, A.S. 2008, "On the error of approximate integration over modified grids", *Chebyshevskiy sbornik*, vol. 9, no. 1(25), pp. 185–223.

14. Dobrovol'skii, N. M. & Manokhin, E.V. 1998, "Banach spaces of periodic functions", *Izvestiya TulGU. Seriya Matematika. Mekhanika. Informatika*, vol. 4, no. 3, pp. 56–67.
15. Dobrovol'skii N.M., Manokhin E.V., Rebrova I. Yu., Roshchenya A.L., 2001, "On the continuity of the zeta function of a grid with weights", *Izvestiya TulGU. Seriya Matematika. Mekhanika. Informatika*, vol. 7, no. 1, pp. 82–86.
16. N. M. Dobrovol'skii, A. L. Roshchenya, "Number of lattice points in the hyperbolic cross", *Math. Notes*, 63:3 (1998), 319–324.
17. N. N. Dobrovol'skii, 2019, "One model Zeta function of the monoid of natural numbers", *Chebyshevskii sbornik*, vol. 20, no. 1, pp. 148–163.
18. N. N. Dobrovol'skii, M. N. Dobrovol'skii, N. M. Dobrovol'skii, I. N. Balaba, I. Yu. Rebrova, 2018, "About «zagrobelna the series» for the zeta function of monoids with exponential sequence of simple", *Chebyshevskii sbornik*, vol. 19, no. 1, pp. 106–123.
19. N. N. Dobrovol'skii, M. N. Dobrovol'skii, N. M. Dobrovol'skii, I. N. Balaba, I. Yu. Rebrova, 2019, "Dirichlet series algebra of a monoid of natural numbers", *Chebyshevskii sbornik*, vol. 20, no. 1, pp. 180–196.
20. Korobov, N.M. 1963, *Teoretiko-chislovye metody v priblizhenom analize* [Number-theoretic methods in approximate analysis], Fizmat-giz, Moscow, Russia.
21. Korobov, N.M. 2004, *Teoretiko-chislovye metody v priblizhenom analize* [Number-theoretic methods in approximate analysis], 2nd ed, MTSNMO, Moscow, Russia.
22. Lokutsievskij, O. V. & Gavrikov, M. B. 1995, *Nachala chislennogo analiza* [The beginning of numerical analysis], TOO "Yanus", Moscow, Russia.
23. Chandrasekharan K., 1974, *Vvedenie v analiticheskuyu teoriju chisel*, Izd-vo Mir, Moskva, 188 p.
24. Chudakov N. G., 1947, *Introduction to the theory of L-Dirichlet functions* — M.-L.: OGIZ, — 204 p.

Получено 11.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 517.5

DOI 10.22405/2226-8383-2020-21-1-247-258

Константа Никольского для тригонометрических полиномов
с периодическим весом Гегенбауэра¹

И. А. Мартьянов

Мартьянов Иван Анатольевич — аспирант кафедры прикладной математики и информатики, Тульский государственный университет (г. Тула).

e-mail: martyanov.ivan@yandex.ru

Аннотация

В работе изучается константа Никольского (или константа Джексона–Никольского) для комплексных тригонометрических полиномов в пространстве $L^p_\alpha(\mathbb{T})$ при $p \geq 1$ с периодическим весом Гегенбауэра $|\sin x|^{2\alpha+1}$:

$$C_{p,\alpha}(n) = \sup_{T \in \mathcal{T}_n \setminus \{0\}} \frac{\|T\|_\infty}{\|T\|_p},$$

где $\|\cdot\|_p = \|\cdot\|_{L^p_\alpha(\mathbb{T})}$. Д. Джексон (1933) доказал, что $C_{p,-1/2}(n) \leq c_p n^{1/p}$ для всех $n \geq 1$. Задача нахождения $C_{p,-1/2}(n)$ имеет долгую историю. Однако точные значения известны только при $p = 2$. При $p = 1$ задача имеет интересные приложения, например, в теории чисел. Отметим результаты Я. Л. Геронимуса, Л. В. Тайкова, Д. В. Горбачева, И. Е. Симонова, П. Ю. Глазыриной. Для $p > 0$ отметим результаты И. И. Ибрагимова, В. И. Иванова, Е. Левина, Д. С. Любинского, М. И. Ганзбурга, С. Ю. Тихонова, в весовом случае — В. В. Арестова, А. Г. Бабенко, М. В. Дейкаловой, А. Хорват.

Доказывается, что супремум здесь достигается на действительном четном тригонометрическом полиноме с максимумом модуля в нуле. Как следствие, установлена связь с алгебраической константой Никольского с весом $(1 - x^2)^\alpha$, исследованная В. В. Арестовым и М. В. Дейкаловой (2015). Доказательство следует их методу и базируется на положительном операторе обобщенного сдвига в пространстве $L^p_\alpha(\mathbb{T})$ с периодическим весом Гегенбауэра. Этот оператор был построен и изучен Д. В. Чертовой (2009). Как приложение, предлагается подход к вычислению $C_{p,\alpha}(n)$ на основе соотношений двойственности Арестова–Дейкаловой.

Ключевые слова: тригонометрический полином, алгебраический полином, константа Никольского, вес Гегенбауэра.

Библиография: 23 названий.

Для цитирования:

И. А. Мартьянов. Константа Никольского для тригонометрических полиномов с периодическим весом Гегенбауэра // Чебышевский сборник, 2020, т. 21, вып. 1, с. 247–258.

¹Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-31-90152.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 517.5

DOI 10.22405/2226-8383-2020-21-1-247-258

Nikolskii constant for trigonometric polynomials with periodic Gegenbauer weight²

I. A. Martyanov

Martyanov Ivan Anatol'evich — graduate student, Department of Applied Mathematics and Computer Science, Tula State University (Tula).

e-mail: martyanov.ivan@yandex.ru

Abstract

We study the Nikolskii constant (or the Jackson–Nikolskii constant) for complex trigonometric polynomials in the space $L_\alpha^p(\mathbb{T})$ for $p \geq 1$ with the periodic Gegenbauer weight $|\sin x|^{2\alpha+1}$:

$$\mathcal{C}_{p,\alpha}(n) = \sup_{T \in \mathcal{T}_n \setminus \{0\}} \frac{\|T\|_\infty}{\|T\|_p},$$

where $\|\cdot\|_p = \|\cdot\|_{L_\alpha^p(\mathbb{T})}$. D. Jackson (1933) proved that $\mathcal{C}_{p,-1/2}(n) \leq c_p n^{1/p}$ for all $n \geq 1$. The problem of finding $\mathcal{C}_{p,-1/2}(n)$ has a long history. However, sharp constants are known only for $p = 2$. For $p = 1$, the problem has interesting applications, e.g., in number theory. We note the results of Ja. L. Geronimus, L. V. Taikov, D. V. Gorbachev, I. E. Simonov, P. Yu. Glazyrina. For $p > 0$, we note the results of I. I. Ibragimov, V. I. Ivanov, E. Levin, D. S. Lubinsky, M. I. Ganzburg, S. Yu. Tikhonov, in the weight case — V. V. Arestov, A. G. Babenko, M. V. Deikalova, Á. Horváth.

It is proved that the supremum here is achieved on a real even trigonometric polynomial with a maximum modulus at zero. As a result, a connection is established with the Nikolskii algebraic constant with weight $(1-x^2)^\alpha$, investigated by V. V. Arestov and M. V. Deikalova (2015). The proof follows their method and is based on the positive generalized translation operator in the space $L_\alpha^p(\mathbb{T})$ with the periodic Gegenbauer weight. This operator was constructed and studied by D. V. Chertova (2009). As an application, we propose an approach to computing $\mathcal{C}_{p,\alpha}(n)$ based on the Arestov–Deikalova duality relations.

Keywords: trigonometric polynomial, algebraic polynomial, the Nikolskii constant, the Gegenbauer weight.

Bibliography: 23 titles.

For citation:

I. A. Martyanov, 2020, "Nikolskii constant for trigonometric polynomials with periodic Gegenbauer weight", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 247–258.

1. Введение

Пусть $I \subset \mathbb{R}$, $v: I \rightarrow \mathbb{R}_+$ — некоторая весовая функция, $p \geq 1$, $L^p(I; v)$ — пространство Лебега функций $f: I \rightarrow \mathbb{C}$ с конечной относительно веса v нормой

$$\|f\|_{L^p(I;v)} = \left(\int_I |f(x)|^p v(x) dx \right)^{1/p}, \quad \|f\|_{L^\infty(I;v)} = \operatorname{ess\,sup}_{x \in I} |f(x)|.$$

²The reported study was funded by RFBR, project number 19-31-90152.

Будем использовать сокращение $\|\cdot\|_p = \|\cdot\|_{L^p(I;v)}$, если это не вызывает недоразумений.

Пусть $\mathbb{T} = (-\pi, \pi]$ — одномерный тор, $\alpha \geq -1/2$, $v_\alpha(x) = |\sin x|^{2\alpha+1}$ — периодический вес Гегенбауэра (см., например, [11]), $L_\alpha^p(\mathbb{T}) = L^p(\mathbb{T}; v_\alpha)$, $n \in \mathbb{Z}_+$, $\mathcal{T}_n$ — множество тригонометрических полиномов

$$T(x) = \sum_{k=0}^n (a_k \cos kx + b_k \sin kx), \quad b_0 = 0,$$

порядка не выше n с комплексными коэффициентами a_k, b_k .

В работе изучается точная константа Никольского разных метрик для периодического веса Гегенбауэра, определяемая равенством

$$\mathcal{C}_{p,\alpha}(n) = \sup_{T \in \mathcal{T}_n \setminus \{0\}} \frac{\|T\|_\infty}{\|T\|_p}, \quad \|\cdot\|_p = \|\cdot\|_{L_\alpha^p(\mathbb{T})}. \quad (1)$$

Часто она называется константой Джексона–Никольского в честь работы Д. Джексона [20].

Также введем константу Никольского для алгебраических полиномов $P(x) = \sum_{k=0}^n c_k x^k$ степени не выше $n \in \mathbb{Z}_+$ с комплексными коэффициентами c_k , множество которых обозначим через $\mathcal{P}_n$. Пусть $\mathbb{I} = [-1, 1]$, $L_\alpha^p(\mathbb{I}) = L^p(\mathbb{I}; (1-x^2)^\alpha)$ — пространство Лебега с алгебраическим весом Гегенбауэра, $\alpha \geq -1/2$. Тогда

$$\mathcal{M}_{p,\alpha}(n) = \sup_{P \in \mathcal{P}_n \setminus \{0\}} \frac{\|P\|_\infty}{\|P\|_p}, \quad \|\cdot\|_p = \|\cdot\|_{L_\alpha^p(\mathbb{I})}.$$

Константа $\mathcal{M}_{p,\alpha}(n)$ изучена в работе [12]. В ней доказано, что существует действительный экстремальный полином $P_*(x)$ степени n , такой что $\|P_*\|_p = 1$, $P_*(1) = \mathcal{M}_{p,\alpha}(n)$. Этот полином единственный при $1 \leq p < \infty$, $\alpha > -1/2$ и с точностью до константы совпадает с полиномом, имеющим единичный старший коэффициент и наименее уклоняющимся от нуля в пространстве $L^p(\mathbb{I}; (1-x)^{\alpha+1}(1+x)^\alpha)$. Все нули P_* простые и находятся на $(-1, 1)$ (см. раздел 6). В работе [13] данные результаты обобщены на случай веса Якоби.

2. Исторический обзор

Задача нахождения $\mathcal{C}_{p,\alpha}(n)$ имеет долгую историю, особенно в безвесовом случае $\alpha = -1/2$. Однако даже в нем она вычислена только при $p = 2$. Для $\alpha = -1/2$, $p = 1$ отметим результаты Я. Л. Геронимуса [2] (где задача сведена к решению нелинейного уравнения), Л. В. Тайкова [9, 10] и Д. В. Горбачева [3] (где даны двусторонние оценки), оценки сверху при $p \geq 1$ получены в работах Д. Джексона [20], И. И. Ибрагимова [7]. Отметим работы Е. Levin и D. S. Lubinsky [21], М. И. Ганзбурга и С. Ю. Тихонова [18], работу [6], где изучается предельное равенство между константами для тригонометрических полиномов и целых функций экспоненциального типа. См. в данных работах более подробный обзор проблемы.

Алгебраическая весовая константа $\mathcal{M}_{p,\alpha}(n)$ активно изучалась в работах В. В. Арестова и М. В. Дейкаловой [12, 13] (где в том числе даны двойственные соотношения), И. Е. Сиимонова и П. Ю. Глазыриной [22] (обобщение результатов Геронимуса) и других математиков из школы В. В. Арестова. Также см. работы [16, 17] о многомерной константе Никольского для сферических полиномов, где отмечается связь с алгебраическим случаем. В работе [6] дана связь тригонометрической и алгебраической констант в безвесовом случае $\alpha = -1/2$. Этот факт позволяет приближенно находить константы, используя соотношения двойственности Арестова–Дейкаловой и решение нелинейных систем уравнений. Здесь эти результаты обобщаются на случай $\alpha > -1/2$.

Для доказательства основного утверждения работы используется положительный оператор обобщенного сдвига в пространстве $L_\alpha^p(\mathbb{T})$, построенный и изученный Д. В. Чертовой [11].

Она использовала его для доказательства точных неравенств Джексона в $L^p_\alpha(\mathbb{T})$ при $1 \leq p \leq 2$. Эти результаты обобщают классические неравенства Н. И. Черных и других уральских математиков (см. библиографию в [11, 5]). В этом направлении стоит отметить работы М. Ш. Шабозова и его соавторов (см., например, [23]), а также результаты школы В. И. Иванова (см., например, обзор результатов в [5]), к которой принадлежит Д. В. Чертова. Неравенства разных метрик играют большую роль в теории приближений. Здесь необходимо отметить неоценимый вклад С. М. Никольского и его последовательной.

Константы Никольского в пространстве и родственные экстремальные задачи о минимальной L^1 -норме находят приложения в теории чисел. Например, Е. Carneiro, М. В. Milinovich и К. Soundararajan применили такие задачи в теории распределения простых чисел и дзета-функции Римана [15]. Можно упомянуть более ранний результат В. В. Арестов и В. П. Кондратьев [1], которые получили наилучшие оценки в задаче Валле-Пуссена–Ландау, связанной с нулями дзета-функции Римана и остаточным членом в асимптотической формуле для распределения простых чисел. Интересно сравнить этот подход, например, с классическими результатами школы А. А. Карацубы (см., например, [8]). Отметим в этом направлении проблему Берлинга–Сельберга, которая связана с односторонним приближением в L^1 целыми функциями экспоненциального типа.

3. Основной результат

Докажем следующее утверждение, аналогичное результатам работ [12, 13, 14, 4].

ТЕОРЕМА 1. Пусть $1 \leq p < \infty$, $\alpha \geq -1/2$. Тогда

$$C_{p,\alpha}(n) = T_*(0),$$

где T_* — экстремальный действительный четный полином порядка n , такой что $\|T_*\|_{p,\alpha} = 1$. При $1 < p < \infty$ и $p = 1$, $\alpha > -1/2$ он единственный.

Кроме того,

$$C_{p,\alpha}(n) = 2^{-1/p} \mathcal{M}_{p,\alpha}(n)$$

и $T_*(x) = 2^{-1/p} P_*(\cos x)$.

Отметим, что в безвесовом случае $\alpha = -1/2$ теорема легко следует из инвариантности нормы $L^p_{-1/2}(\mathbb{T})$ и класса $\mathcal{T}_n$ относительно операции сдвига $f(\cdot) \mapsto f(\cdot + t)$. При $\alpha > -1/2$ требуется использовать оператор обобщенного сдвига; см., например, работы [12, 13, 14, 4].

Было бы интересно узнать, является полином T_* единственным (с точностью до сдвигов аргумента) при $p = 1$, $\alpha = -1/2$. В статье [12] отмечается этот вопрос.

4. Оператор обобщенного сдвига

Пусть далее $x, t \in \mathbb{T}$. Для периодического веса Гегенбауэра нужный нам линейный положительный оператор обобщенного сдвига $T^t = T^t_\alpha$ в пространстве $L^p_\alpha(\mathbb{T})$ был построен и изучен в работе [11]. Дадим его в интегральной форме. В [11] он вначале введен как мультипликатор в $L^2_\alpha(\mathbb{T})$.

При $\alpha = -1/2$ имеем

$$T^t f(x) = \frac{f(x+t) + f(x-t)}{2},$$

а при $\alpha > -1/2$

$$T^t f(x) = \frac{c_\alpha}{2} \int_0^\pi (f(\psi)(1+B) + f(-\psi)(1-B)) \sin^{2\alpha} \theta d\theta, \quad (2)$$

где

$$\psi = \psi_{x,t}(\theta) = \arccos(\cos x \cos t + \sin x \sin t \cos \theta) \in [0, \pi], \quad (3)$$

$$B = B_{x,t}(t) = \frac{\sin x \cos t - \cos x \sin t \cos \theta}{\sin \psi} \in [-1, 1], \quad 1 - B^2 \geq \frac{\sin^2 t \sin^2 \theta}{\sin^2 \psi}, \quad (4)$$

$$c_\alpha = \frac{\Gamma(\alpha + 1)}{\Gamma(1/2)\Gamma(\alpha + 1/2)}, \quad T^t 1 = 1.$$

Таким образом, T^t определен на всех интегрируемых функциях $f \in L_\alpha^1(\mathbb{T})$. Выражение (2) можно также записать в виде

$$T^t f(x) = c_\alpha \int_0^\pi (f_e(\psi) + f_o(\psi)B) \sin^{2\alpha} \theta d\theta, \quad (5)$$

где

$$f_e(x) = \frac{f(x) + f(-x)}{2}, \quad f_o(x) = \frac{f(x) - f(-x)}{2}$$

обозначают соответственно четную и нечетную компоненты функции f . Отсюда следует, что при $\alpha > -1/2$ на четных функциях f оператор T^t совпадает со сдвигом Гегенбауэра

$$f \mapsto c_\alpha \int_0^\pi f(\psi) \sin^{2\alpha} \theta d\theta \quad (6)$$

(при $\alpha = 0$ он также называется сдвигом Лежандра).

Следуя [11] введем в пространстве $L_\alpha^2(\mathbb{T})$ ортогональный базис, состоящий из следующих полиномов $\varphi_m = \varphi_{m,\alpha}$:

$$\varphi_0(x) = 1, \quad \varphi_{2k}(x) = R_k^{(\alpha)}(\cos x), \quad \varphi_{2k-1}(x) = R_{k-1}^{(\alpha+1)}(\cos x) \sin x, \quad k \in \mathbb{N},$$

где $R_k^{(\alpha)}(t) = \frac{P_k^{(\alpha,\alpha)}(t)}{P_k^{(\alpha,\alpha)}(1)}$ — полиномы Гегенбауэра (Якоби). Тогда функция $f \in L_\alpha^2(\mathbb{T})$ раскладывается в периодический ряд Фурье–Гегенбауэра

$$f(x) = \sum_{m=0}^{\infty} f_m \varphi_m(x), \quad f_m = \frac{(f, \varphi_m)_\alpha}{(\varphi_m, \varphi_m)_\alpha}, \quad (f, g)_\alpha = \int_{\mathbb{T}} f(x) \overline{g(x)} v_\alpha(x) dx,$$

где, напомним, $v_\alpha(x) = |\sin x|^{2\alpha+1}$. Полиномы φ_{2k} и φ_{2k-1} — соответственно четные и нечетные действительные тригонометрические полиномы порядка k и система $\{\varphi_m\}_{m=0}^{2n}$ образует ортогональный базис в подпространстве $\mathcal{T}_n$.

ПРЕДЛОЖЕНИЕ 9 ([11]). Пусть $\alpha \geq -1/2$, $f \in L_\alpha^1(\mathbb{T})$, $x, t \in \mathbb{T}$. Тогда

$$T^t \varphi_{2k}(x) = \varphi_{2k}(t) \varphi_{2k}(x), \quad T^t \varphi_{2k-1}(x) = \varphi_{2k}(t) \varphi_{2k-1}(x),$$

$$T^{-t} = T^t, \quad T^0 f(x) = f(x), \quad T^t f \geq 0 \text{ для } f \geq 0,$$

$$(T^t f, 1)_\alpha = (f, 1)_\alpha, \quad \|T^t\|_{p \rightarrow p} = 1 \text{ для } 1 \leq p \leq \infty,$$

$$T^t f(x) = T^x f(t) \text{ для четной } f.$$

В отличие от обобщенного сдвига Гегенбауэра (6) оператор $(x, t) \mapsto T^t f(x)$ при $\alpha > -1/2$ не является симметричным от x, t на всех f . Введем положительный оператор $(t, x) \mapsto S^x f(t)$ равенством

$$S^x f(t) = T^t f(x).$$

При $\alpha = -1/2$ и на четных функциях эти операторы совпадают. Покажем, что норма S^x в $L_\alpha^p(\mathbb{T})$ также не превосходит единицы. Подобный факт известен, например, для положительного оператора обобщенного сдвига Данкля [19].

ЛЕММА 1. (i) Пусть $1 \leq p \leq \infty$, $\alpha \geq -1/2$, $x \in \mathbb{T}$. Тогда

$$\|S^x\|_{p \rightarrow p} = 1.$$

(2) Если $p = 1$, $\alpha > -1/2$, $x \in \mathbb{T}$, f — непрерывна и $\|S^x f\|_1 = \|f\|_1$, то $\pm f \geq 0$ на $\mathbb{T}$.

ДОКАЗАТЕЛЬСТВО. (i) Достаточно рассмотреть случай $\alpha > -1/2$. Вначале покажем, что

$$(S^x f, 1)_\alpha = (f, 1)_\alpha, \quad f \in L^1_\alpha(\mathbb{T}). \quad (7)$$

Это равенство легко доказать для тригонометрических полиномов, представленных в виде

$$f(x) = \sum_{k \geq 0} (f_{2k-1} \varphi_{2k-1}(x) + f_{2k} \varphi_{2k}(x)),$$

(здесь и далее слагаемое с индексом -1 опускается), поскольку

$$S^x f(t) = T^t f(x) = \sum_{k \geq 0} \varphi_{2k}(t) (f_{2k-1} \varphi_{2k-1}(x) + f_{2k} \varphi_{2k}(x)) \quad (8)$$

и в силу ортогональности

$$(S^x f, 1)_\alpha = \sum_{k \geq 0} (\varphi_{2k}, 1)_\alpha (f_{2k-1} \varphi_{2k-1}(x) + f_{2k} \varphi_{2k}(x)) = (1, 1)_\alpha f_0 = (f, 1)_\alpha.$$

Теперь, чтобы расширить (7) на все интегрируемые функции, в силу плотности множества тригонометрических полиномов достаточно показать, что оператор $S^x f$ ограничен в $L^1_\alpha(\mathbb{T})$. Это так, поскольку по (5), (4) и предложению 9

$$|S^x f(t)| \leq c_\alpha \int_0^\pi (|f_e(\psi)| + |f_o(\psi)|) \sin^{2\alpha} \theta d\theta \leq 2c_\alpha \int_0^\pi |f|_e(\psi) \sin^{2\alpha} \theta d\theta = 2T^x |f|_e(t)$$

и

$$\|S^x f\|_1 \leq 2\|T^x |f|_e\|_1 \leq 2\||f|_e\|_1 \leq 2\|f\|_1.$$

Равенство (7) установлено. Из него и положительности оператора S^x следует, что

$$\|S^x f\|_1 \leq \|S^x |f|\|_1 = (S^x |f|, 1)_\alpha = (|f|, 1)_\alpha = \|f\|_1. \quad (9)$$

Также имеем

$$|S^x f(t)| = |T^t f(x)| \leq \|f\|_\infty T^t 1 = \|f\|_\infty,$$

откуда получаем $\|S^x f\|_\infty \leq \|f\|_\infty$. Теперь по интерполяционной теореме Рисса–Торина заключаем, что $\|S^x f\|_p \leq \|f\|_p$ для любого $p \geq 1$. При этом легко видеть, что на константах имеет место равенство. Поэтому $\|S^x\|_{p \rightarrow p} = 1$.

(ii) Доказательство аналогично [12, лемма 3]. Пусть $\|S^x f\|_1 = \|f\|_1$. Тогда из (9) следует, что для $t \in \mathbb{T}$

$$\begin{aligned} \left| \frac{c_\alpha}{2} \int_0^\pi (f(\psi)(1+B) + f(-\psi)(1-B)) \sin^{2\alpha} \theta d\theta \right| &= \\ &= \frac{c_\alpha}{2} \int_0^\pi (|f(\psi)|(1+B) + |f(-\psi)|(1-B)) \sin^{2\alpha} \theta d\theta. \end{aligned}$$

В силу (4) почти всюду имеем $|B| < 1$, поэтому почти всюду при $\theta \in [0, \pi]$

$$f(\psi)(1+B) + f(-\psi)(1-B) = \pm(|f(\psi)|(1+B) + |f(-\psi)|(1-B)).$$

Отсюда вытекает, что $f(\psi)$ и $f(-\psi)$ не могут менять знак при изменении θ и t . При этом из (3) следует, что ψ покрывает $[0, \pi]$. Поэтому заключаем, что f не может менять знак на $\mathbb{T}$.

Лемма доказана. $\square$

Также нам потребуется

ЛЕММА 2. Пусть $T \in \mathcal{T}_n$, $x \in \mathbb{T}$, $\tilde{T}(t) = S^x T(t)$. Тогда $\tilde{T} \in \mathcal{T}_n$ и $\tilde{T}(0) = T(x)$.

Эта лемма сразу следует из формулы (8).

5. Доказательство теоремы 1

Вначале покажем, что экстремум в (1) достигается на действительном четном тригонометрическом полиноме с максимумом модуля в нуле.

Подпространство тригонометрических полиномов $\mathcal{T}_n \subset L_\alpha^p(\mathbb{T})$ имеет конечную размерность $2n + 1$, поэтому оно является множеством существования. Пусть $T \in \mathcal{T}_n$ — экстремальный полином, такой что

$$\frac{\|T\|_\infty}{\|T\|_p} = C_{p,\alpha}(n).$$

Имеем $\|T\|_\infty = \varepsilon T(x_0)$ для некоторой точки $x_0 \in \mathbb{T}$, $\varepsilon = \pm 1$. Как в лемме 2 положим $\tilde{T}(t) = \varepsilon S^{x_0} T(t)$. Тогда $\tilde{T} \in \mathcal{T}_n$ — четный полином, для которого

$$\tilde{T}(0) = \varepsilon T(x_0) = \|T\|_\infty$$

и по лемме 1 (i)

$$\|\tilde{T}\|_p = \|S^{x_0} T\|_p \leq \|T\|_p.$$

Отсюда

$$C_{p,\alpha}(n) \leq \frac{\|\tilde{T}\|_\infty}{\|\tilde{T}\|_p}.$$

Следовательно, здесь равенство и $T_* = \tilde{T}$ — экстремальный полином.

Если полином $\tilde{T}$ комплекснозначный, то его можно представить в виде $\tilde{T} = \tilde{T}_1 + i\tilde{T}_2$, где $\tilde{T}_1, \tilde{T}_2 \in \mathcal{T}_n$ — четные действительные полиномы и $\tilde{T}(0) = \tilde{T}_1(0)$. Теперь можно взять полином $\tilde{T}_1$, для которого, очевидно, $|\tilde{T}_1| \leq |\tilde{T}|$ на $\mathbb{T}$, и, следовательно, $\|\tilde{T}_1\|_p \leq \|\tilde{T}\|_p$. Поэтому $\tilde{T}_1$ экстремальный.

Полином $T_* = \tilde{T}_1$ можно нормировать условием $\|T_*\|_{p,\alpha} = 1$. Тогда $T_*(0) = C_{p,\alpha}(n)$. Его единственность при $1 < p < \infty$ вытекает из строгой нормированности пространства $L_\alpha^p(\mathbb{T})$.

Для доказательства единственности T_* при $p = 1$, $\alpha > -1/2$ вначале установим равенство $C_{p,\alpha}(n) = 2^{-1/p} M_{p,\alpha}(n)$ и связь экстремальных полиномов $T_*(x) = 2^{-1/p} P_*(\cos x)$. Это легко следует из четности тригонометрического полинома T_* , которая позволяет представить его в виде $T_*(x) = P(\cos x)$, $P \in \mathcal{P}_n$. Осталось воспользоваться интегральной формулой

$$\int_{-\pi}^{\pi} |P(\cos x)|^p |\sin x|^{2\alpha+1} dx = 2 \int_{-1}^1 |P(x)|^p (1-x^2)^\alpha dx.$$

Как было сказано при постановке задачи, P_* — единственный при $p = 1$, $\alpha > -1/2$ и он меняет знак на $(-1, 1)$. Поэтому четный тригонометрический полином также будет единственным и меняющим знак. Если же найдется экстремальный полином T_* , не являющийся четным, то как и выше рассмотрим четный экстремальный полином $\tilde{T}_*(t) = \varepsilon S^{x_0} T_*(t)$. Для него $\|S^{x_0} T_*\|_1 = \|T_*\|_1$. Отсюда по лемме 1 (ii) находим, что T_* , а, следовательно, и $\tilde{T}_*$ не меняют знак на $\mathbb{T}$. Получили противоречие.

Теорема доказана.

6. Применение соотношений двойственности

Арестова–Дейкаловой

Укажем в качестве приложения теоремы 1 как можно приближенно вычислять константу $M_{p,\alpha}(n)$, а, значит, и $C_{p,\alpha}(n)$. Это можно сделать на основе соотношения двойственности из работы [12] (см. (10)). Для случая $\alpha = -1/2$ предлагаемый метод был применен в работе [6].

Пусть $1 \leq p < \infty$, $\alpha \geq -1/2$, $h_\alpha(x) = (1-x^2)^\alpha$ и $H_\alpha(x) = (1-x)h_\alpha(x)$ — весовые функции. Тогда [12]

$$\mathcal{M}_{p,\alpha}(n) = \frac{\|\rho_n\|_{L^p(\mathbb{I}; h_\alpha)}^{p-1}}{I(n, p)},$$

где

$$I(n, p) = \int_{-1}^1 |\rho_n(x)|^{p-1} \operatorname{sign} \rho_n(x) h_\alpha(x) dx > 0$$

и ρ_n — полином, наименее уклоняющийся от нуля в пространстве $L^p(\mathbb{I}; H_\alpha)$:

$$\rho_n = \operatorname{argmin} \{ \|\rho\|_{L^p(\mathbb{I}; H_\alpha)} : \rho(x) = x^n + Q(x), Q \in \mathcal{P}_{n-1} \}.$$

Он единственный в этой проблеме, имеет вид

$$\rho_n(x) = \prod_{i=1}^n (x - x_{ni}), \quad -1 < x_{n1} < \dots < x_{nn} < 1,$$

и характеризуется соотношением ортогональности

$$\int_{-1}^1 Q(x) |\rho_n(x)|^{p-1} \operatorname{sign} \rho_n(x) H_\alpha(x) dx = 0, \quad \forall Q \in \mathcal{P}_{n-1}. \quad (10)$$

Кроме того, экстремальный полином $P_* \in \mathcal{P}_n$, такой что $\|P_*\|_p = 1$ и $P_*(1) = \mathcal{M}_{p,\alpha}(n)$, равен

$$P_* = \frac{\rho_n}{\|\rho_n\|_p}.$$

Из приведенных выше соотношений следует, что константа $\mathcal{M}_{p,\alpha}(n)$ определяется корнями x_{ni} полинома ρ_n . Для их вычисления запишем соотношение ортогональности (10) на базисных в подпространстве $\mathcal{P}_{n-1}$ функциях. Можно взять ортогональный базис в $L^2(\mathbb{I}; H_\alpha)$, который образуют полиномы Якоби

$$\psi_k(x) = \frac{P_k^{(\alpha+1, \alpha)}(x)}{P_k^{(\alpha+1, \alpha)}(1)}, \quad k \in \mathbb{Z}_+.$$

Тогда, полагая $x_{n0} = -1$, $x_{n,n+1} = 1$, получаем

$$\sum_{i=0}^n (-1)^{n-i} \int_{x_{ni}}^{x_{n,i+1}} \psi_j(x) \rho_n^{p-1}(x) H_\alpha(x) dx = 0, \quad j = 0, 1, \dots, n-1.$$

Для произвольного p решение данных нелинейных n уравнений относительно n неизвестных $x_{ni} \in (-1, 1)$, $i = 1, \dots, n$, является непростой задачей. Формулы значительно упрощаются в важном случае $p = 1$. Тогда имеем

$$\sum_{i=0}^n (-1)^{n-i} \int_{x_{ni}}^{x_{n,i+1}} \psi_j(x) H_\alpha(x) dx = 0.$$

Как известно, первообразные $\Psi_j(x) = \int_{-1}^x \psi_j(t) H_\alpha(t) dt$ могут быть выражены через полиномы Якоби. Поэтому в этом случае получаем систему нелинейных уравнений

$$\sum_{i=0}^n (-1)^{n-i} (\Psi_j(x_{n,i+1}) - \Psi_j(x_{ni})) = 0$$

или

$$\sum_{i=1}^n (-1)^{n-i} \Psi_j(x_{ni}) = 2^{-1} \Psi_j(1),$$

где $\Psi_j(1) = 0$ при $j \geq 1$ в силу ортогональности ψ_j . Приближенно эту систему можно эффективно решить методом Ньютона. Вычисления ускоряет эмпирический факт, что нули последовательных экстремальных полиномов перемежаются. Решение системы единственное, поскольку полином ρ_n единственный.

7. Заключение

В работе доказано, что экстремум в задаче о весовой константе Никольского с весом Гегенбауэра достигается на действительном четном тригонометрическом полиноме с максимумом модуля в нуле. Это позволило установить связь с алгебраической константой Никольского с ультрасферическим весом, которая была исследована В. В. Арестовым и М. В. Дейкаловой. Доказательство следует их методу и базируется на положительном операторе обобщенного сдвига, построенным и изученным Д. В. Чертовой. Как приложение, предложен подход к вычислению весовой константы Никольского на основе соотношений двойственности Арестова–Дейкаловой. Детали реализации и развитие данного подхода к приближенному вычислению констант Никольского планируется привести в последующих работах.

Автор благодарит Д. В. Горбачева за помощь при подготовке работы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Арестов В. В., Кондратьев В. П. Об одной экстремальной задаче для неотрицательных тригонометрических полиномов // Матем. заметки. 1990. Том 47, № 1. С. 15–28.
2. Геронимус Я. Л. Об одной экстремальной задаче Чебышева // Изв. АН СССР. Сер. матем. 1938. Том 2, вып. 4. С. 445–456.
3. Горбачев Д. В. Интегральная задача Конягина и (C, L) -константы Никольского // Труды ИММ УрО РАН. 2005. Том 11, № 2. С. 72–91.
4. Горбачев Д. В., Добровольский Н. Н. Константы Никольского в пространствах $L^p(\mathbb{R}, |x|^{2\alpha+1} dx)$ // Чебышевский сборник. 2018. Том 19, № 2. С. 67–79.
5. Горбачев Д. В., Иванов В. И. Точное неравенство Джексона в $L_p(\mathbb{R}^d)$ с весом Данкля // Матем. заметки. 2019. Том 105, № 5. С. 666–684.
6. Горбачев Д. В., Мартянов И. А. О взаимосвязи констант Никольского для тригонометрических полиномов и целых функций экспоненциального типа // Чебышевский сборник. 2018. Том 19, № 2. С. 80–89.
7. Ибрагимов И. И. Экстремальные задачи в классе тригонометрических полиномов // Докл. АН СССР. 1958. Том 121, № 3. С. 415–417.
8. Рахмонов З. Х. Оценка плотности нулей дзета-функции Римана // УМН. 1994. Том 49, № 2(296). С. 161–162.
9. Тайков Л. В. Один круг экстремальных задач для тригонометрических полиномов // УМН. 1965. Том 20, № 3. С. 205–211.

10. Тайков Л. В. О наилучшем приближении ядер Дирихле // Матем. заметки. 1993. Том 53, № 6. С. 116–121.
11. Чертова Д. В. Теоремы Джексона в пространствах L_p , $1 \leq p < 2$, с периодическим весом Якоби // Изв. ТулГУ. Естественные науки. 2009. Вып. 1. С. 5–27.
12. Arestov V., Deikalova M. Nikol'skii inequality between the uniform norm and L_q -norm with ultraspherical weight of algebraic polynomials on an interval // Comput. Methods Funct. Theory. 2015. Vol. 15, no. 4. P. 689–708.
13. Arestov V., Deikalova M. Nikol'skii inequality between the uniform norm and L_q -norm with Jacobi weight of algebraic polynomials on an interval // Analysis Math. 2016. Vol. 42, no. 2. P. 91–120.
14. Arestov V., Babenko A., Deikalova M., Horváth Á. Nikol'skii inequality between the uniform norm and integral norm with Bessel weight for entire functions of exponential type on the half-line // Anal. Math. 2018. Vol. 44, no. 1. P. 21–42.
15. Carneiro E., Milinovich M. B., Soundararajan K. Fourier optimization and prime gaps // Comment. Math. Helv. 2019. Vol. 94. P. 533–568.
16. Dai F., Gorbachev D., Tikhonov S. Nikolskii constants for polynomials on the unit sphere // J. d'Analyse Math. 2019 (to appear); arXiv:1708.09837. 2017. 21 p.
17. Dai F., Gorbachev D., Tikhonov S. Estimates of the asymptotic Nikolskii constants for spherical polynomials // arXiv:1907.03832. 2019. 27 p.
18. Ganzburg M. I., Tikhonov S. Yu. On sharp constants in Bernstein–Nikolskii inequalities // Constr. Approx. 2017. Vol. 45, no. 3. P. 449–466.
19. Gorbachev D. V., Ivanov V. I., Tikhonov S. Yu. Positive L^p -bounded Dunkl-type generalized translation operator and its applications // Constr. Approx. 2019. Vol. 49, no. 3. P. 555–605.
20. Jackson D. Certain problems of closest approximation // Bull. Am. Math. Soc. 1933. Vol. 39. P. 889–906.
21. Levin E., Lubinsky D. Asymptotic behavior of Nikolskii constants for polynomials on the unit circle // Comput. Methods Funct. Theory. 2015. Vol. 15, no. 3. P. 459–468.
22. Simonov I. E., Glazyrina P. Y. Sharp Markov–Nikolskii inequality with respect to the uniform norm and the integral norm with Chebyshev weight // J. Approx. Theory. 2015. Vol. 192. P. 69–81.
23. Шабозов М. Ш., Фарозова А. Д. Точное неравенство Джексона–Стечкина с неклассическим модулем непрерывности // Тр. ИММ УрО РАН. 2016. Том 22, № 4. С. 311–319.

REFERENCES

1. Arestov, V., Babenko, A., Deikalova, M. & Horváth, Á. 2018. “Nikol'skii inequality between the uniform norm and integral norm with Bessel weight for entire functions of exponential type on the half-line”, *Anal. Math.*, vol. 44, no. 1, pp. 21–42.
2. Arestov, V. & Deikalova, M. 2015. “Nikol'skii inequality between the uniform norm and L_q -norm with ultraspherical weight of algebraic polynomials on an interval”, *Comput. Methods Funct. Theory*, vol. 15, no. 4, pp. 689–708.

3. Arestov, V. & Deikalova, M. 2016. "Nicol'skii inequality between the uniform norm and L_q -norm with Jacobi weight of algebraic polynomials on an interval", *Analysis Math.*, vol. 42, no. 2, pp. 91–120.
4. Arestov, V. V. & Kondrat'ev, V. P. 1990. "Certain extremal problem for nonnegative trigonometric polynomials", *Math. Notes*, vol. 47, no. 1, pp. 10–20.
5. Carneiro, E., Milinovich, M. B. & Soundararajan, K. 2019. "Fourier optimization and prime gaps", *Comment. Math. Helv.*, vol. 94, pp. 533–568.
6. Chertova, D. V. 2009. "Jackson theorems in L_p -spaces, $1 \leq p \leq 2$, with periodic Jacobi weight", *Izv. Tul. Gos. Univ. Estestv. Nauki*, no. 1, pp. 5–27. (in Russian)
7. Dai, F., Gorbachev, D. & Tikhonov, S. 2017. "Nikolskii constants for polynomials on the unit sphere", *arXiv:1708.09837*, 21 p.
8. Dai, F., Gorbachev, D. & Tikhonov, S. 2019. "Estimates of the asymptotic Nikolskii constants for spherical polynomials", *arXiv:1907.03832*, 27 p.
9. Ganzburg, M. I. & Tikhonov S. Yu. 2017. "On sharp constants in Bernstein–Nikolskii inequalities", *Constr. Approx.*, vol. 45, no. 3, pp. 449–466.
10. Geronimus, J. 1938. "Sur un problème extrémal de Tchebycheff", *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 2, no. 4, pp. 445–456. (in Russian)
11. Gorbachev, D. V., Ivanov, V. I. & Tikhonov, S. Yu. 2019. "Positive L^p -bounded Dunkl-type generalized translation operator and its applications", *Constr. Approx.*, vol. 49, no. 3, pp. 555–605.
12. Gorbachev, D. V. 2005. "An integral problem of Konyagin and the (C, L) -constants of Nikol'skii", *Proc. Steklov Inst. Math. Suppl.*, vol. 2, pp. S117–S138.
13. Gorbachev, D. V. & Dobrovolskii, N. N. 2018. "Nikolskii constants in $L^p(\mathbb{R}, |x|^{2\alpha+1} dx)$ spaces", *Chebyshevskii Sbornik*, vol. 19, no. 2, pp. 67–79. (in Russian)
14. Gorbachev, D. V. & Ivanov, V. I. 2019. "A sharp Jackson inequality in $L_p(\mathbb{R}^d)$ with Dunkl weight", *Math. Notes*, vol. 105, no. 5, pp. 657–673.
15. Gorbachev, D. V. & Martyanov, I. A. 2018. "On interrelation of Nikolskii constants for trigonometric polynomials and entire functions of exponential type", *Chebyshevskii Sbornik*, vol. 19, no. 2, pp. 80–89. (in Russian)
16. Ibragimov, I. I. 1958. "Extremum problems in the class of trigonometric polynomials", *Dokl. Akad. Nauk SSSR*, vol. 121, no. 3, pp. 415–417. (in Russian)
17. Jackson, D. 1933. "Certain problems of closest approximation", *Bull. Am. Math. Soc.*, vol. 39, pp. 889–906.
18. Levin, E. & Lubinsky, D. 2015. "Asymptotic behavior of Nikolskii constants for polynomials on the unit circle", *Comput. Methods Funct. Theory*, vol. 15, no. 3, pp. 459–468.
19. Rakhmonov, Z. Kh. 1994. "Estimate of the density of the zeros of the Riemann zeta function", *Uspekhi Mat. Nauk. Russian Math. Surveys*, vol. 49, no. 2, pp. 168–169.

20. Simonov, I. E. & Glazyrina, P. Y. 2015. “Sharp Markov–Nikolskii inequality with respect to the uniform norm and the integral norm with Chebyshev weight”, *J. Approx. Theory*, vol. 192, pp. 69–81.
21. Taikov, L. V. 1965. “A group of extremal problems for trigonometric polynomials”, *Uspekhi Mat. Nauk*, vol. 20, no. 3(123), 205–211. (in Russian)
22. Taikov, L. V. 1993. “On the best approximation of Dirichlet kernels”, *Math. Notes*, vol. 53, no. 6, pp. 640–643.
23. Shabozov, M. Sh. & Farozova, A. D. 2016. “The Jackson–Stechkin inequality with nonclassical modulus of continuity”, *Trudy Inst. Mat. i Mekh. UrO RAN*, vol. 22, no. 4, pp. 311–319.

Получено 25.11.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512.643.5:512.643.8:511.331.1

DOI 10.22405/2226-8383-2020-21-1-259-272

**Асимптотическая структура
собственных чисел и собственных векторов
некоторых треугольных ганкелевых матриц**

Ю. В. Матиясевич

Матиясевич Юрий Владимирович — доктор физико-математических наук, профессор, академик Российской академии наук, советник РАН Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН, президент Санкт-Петербургского математического общества (г. Санкт-Петербург).

e-mail: yumat@pdmi.ras.ru

Аннотация

Ганкелевы матрицы, рассматриваемые в статье, возникли при одной переформулировке гипотезы Римана, предложенной ранее автором. Компьютерные вычисления показали, что в случае дзета-функции Римана собственные числа и собственные вектора таких матриц обладают интересной структурой.

В статье изучается модельная ситуация, когда вместо дзета-функции взята функция, имеющая единственный нуль. Для этого случая указаны первые члены асимптотических разложений наименьшего и наибольших (по абсолютной величине) собственных чисел и соответствующих им собственных векторов.

Ключевые слова: Дзета-функция Римана, гипотеза Римана, ганкелевы матрицы, собственные числа, собственные вектора.

Библиография: 12 названий.

Для цитирования:

Ю. В. Матиясевич. Асимптотическая структура собственных чисел и собственных векторов некоторых треугольных ганкелевых матриц // Чебышевский сборник, 2020, т. 21, вып. 1, с. 259–272.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512.643.5:512.643.8:511.331.1

DOI 10.22405/2226-8383-2020-21-1-259-272

**Asymptotic structure of eigenvalues and eigenvectors
of certain triangular Hankel matrices**

Yu. V. Matiyasevich

Matiyasevich Yuri Vladimirovich — doctor of physical and mathematical sciences, professor, full member of Russian Academy of Sciences, RAS Counselor of St. Petersburg department of Steklov Mathematical Institute of Russian Academy of Sciences, president of the St. Petersburg Mathematical society (St. Petersburg).

e-mail: yumat@pdmi.ras.ru

Abstract

The Hankel matrices considered in the article arose at one reformulation of the Riemann hypothesis proposed earlier by the author.

Computer calculations showed that in the case of the Riemann zeta function the eigenvalues and the eigenvectors of such matrices have an interesting structure.

The article studies a model situation when instead of the zeta function function one takes a function having a single zero. For this case we indicate the first terms of the asymptotic expansions of the smallest and largest (in absolute value) eigenvalues and the corresponding eigenvectors.

Keywords: Riemann zeta function, Riemann Hypothesis, Hankel matrices, eigenvalues, eigenvectors.

Bibliography: 12 titles.

For citation:

Yu. V. Matiyasevich, 2020, “Asymptotic structure of eigenvalues and eigenvectors of certain triangular Hankel matrices”, *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 259–272.

1. Введение

Изучение предельного распределения собственных чисел ганкелевых матриц растущего размера является классической тематикой. При этом следует различать две постановки задачи.

При первой рассматривается растущая последовательность матриц

$$(c_0), \begin{pmatrix} c_0 & c_1 \\ c_1 & c_2 \end{pmatrix}, \begin{pmatrix} c_0 & c_1 & c_2 \\ c_1 & c_2 & c_3 \\ c_2 & c_3 & c_4 \end{pmatrix}, \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_4 \\ c_2 & c_3 & c_4 & c_5 \\ c_3 & c_4 & c_5 & c_6 \end{pmatrix}, \dots \quad (1)$$

где

$$c_0, c_1, \dots, c_k, \dots \quad (2)$$

— некоторая фиксированная последовательность чисел.

При второй постановке задачи матрицы растут в направлении другой диагонали, например, так:

$$(c_1), \quad \begin{pmatrix} c_2 & c_1 \\ c_1 & c_0 \end{pmatrix}, \quad \begin{pmatrix} c_3 & c_2 & c_1 \\ c_2 & c_1 & c_0 \\ c_1 & c_0 & 0 \end{pmatrix}, \quad \begin{pmatrix} c_4 & c_3 & c_2 & c_1 \\ c_3 & c_2 & c_1 & c_0 \\ c_2 & c_1 & c_0 & 0 \\ c_1 & c_0 & 0 & 0 \end{pmatrix}, \quad \dots \quad (3)$$

Иными словами, в первом случае фиксируются главные диагонали (как начальные отрезки последовательности (2)), а во втором — побочные диагонали (для всех матриц все элементы этих диагоналей равны одному и тому же элементу c_k последовательности (2)).

Во втором случае матрицы являются почти треугольными — количество ненулевых поддиагоналей под побочной диагональю останется постоянным.

Поведение собственных чисел матриц последовательностей (1) и (3) является весьма различным. Первая постановка задачи является более традиционной, но в настоящей работе будут рассматриваться последовательности матриц вида (3). Интерес к этому возник у автора при изучении одной переформулировки гипотезы Римана про дзета-функцию (см. [4, 5, 6, 8]). Появляющиеся при этом ганкелевы матрицы описаны ниже в параграфе 2, причём в общей постановке, а не только для дзета-функции. Компьютерные вычисления собственных чисел этих матриц именно для дзета-функции выявили ряд интересных закономерностей и позволили автору сформулировать новые гипотезы про неё; частично эти наблюдения воспроизведены ниже в параграфе 3.

Теоретическое исследование матриц, возникающих в случае дзета-функции, представляется трудным, поскольку их элементы определяются через тейлоровские коэффициенты этой функции, которые ведут себя довольно нерегулярным образом. Для того, чтобы понять, какие из наблюдаемых закономерностей присущи именно дзета-функции, а какие являются общими для матриц рассматриваемого типа, в настоящей работе рассматривается простейшая модельная ситуация — случай, когда матрицы являются треугольными, а их элементы порождаются функцией с единственным нулём вместо дзета-функции. Для таких матриц в параграфах 4 и 5 будут указаны первые члены асимптотических разложений, соответственно, наименьшего и наибольших (по абсолютной величине) собственных чисел и отвечающих им собственных векторов, а затем проведено сравнение с численными данными, полученными для случая дзета-функции Римана.

2. Связь определителей специальных ганкелевых матриц с нулями целой функции

Пусть $f(w)$ — мероморфная функция,

$$f(0) = 1, \quad (4)$$

числа

$$w_1, w_2, \dots, w_n \quad (5)$$

являются нулями этой функции, причём каждый из них встречается в (5) в соответствии со своей кратностью,

$$|w_1| \leq |w_2| \leq \dots \leq |w_{n-1}| \leq |w_n|, \quad (6)$$

и в круге

$$|w| \leq |w_n| \quad (7)$$

нет нулей, отличных от (5).

Рассмотрим *аппроксимацию Паде* типа (n, m) к $f(w)$: пусть $P_{n,m}(w)$ и $Q_{n,m}(w)$ — многочлены степеней n и m соответственно, такие что

$$f(w) \approx \frac{P_{n,m}(w)}{Q_{n,m}(w)} = \frac{1 + p_{n,m,1}w + \dots + p_{n,m,n}w^n}{1 + q_{n,m,1}w + \dots + q_{n,m,m}w^m} \quad (8)$$

$$= f(w) + O(w^k), \quad (9)$$

где k имеет максимально возможное значение (поскольку в (8) в нашем распоряжении имеются $n + m$ коэффициентов

$$p_{n,m,1}, \dots, p_{n,m,n}, q_{n,m,1}, \dots, q_{n,m,m}, \quad (10)$$

то в общем случае $k = n + m + 1$).

Теорема Монтессу де Болора [9] (см. также [1, 11]) говорит, что при сделанных предположениях относительно нулей (5) именно к ним с ростом m стремятся нули многочлена $P_{n,m}(w)$:

$$P_{n,m}(w) \rightarrow \prod_{k=1}^n \left(1 - \frac{w}{w_n}\right), \quad (11)$$

в частности,

$$|p_{n,m,n}| \rightarrow W_n, \quad (12)$$

где

$$W_n = \prod_{k=1}^n \frac{1}{|w_n|}. \quad (13)$$

Нетрудно понять, что коэффициенты (10) выражаются через коэффициенты разложения

$$f(w) = 1 + \phi_1 w + \dots + \phi_k w^k + \dots \quad (14)$$

Для упрощения последующих формул положим $\phi_0 = 1$ и $\phi_k = 0$ при $k < 0$. К. Якоби ([3], см. также [1, теорема 1.1.2]) дал явные выражения для $p_{n,m,n}$ через определители ганкелевых матриц

$$M_{n,m} = (-1)^{n+m} \begin{pmatrix} \phi_{n+m-1} & \phi_{n+m-2} & \dots & \phi_n \\ \phi_{n+m-2} & \phi_{n+m-3} & \dots & \phi_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_n & \phi_{n-1} & \dots & \phi_{n-m+1} \end{pmatrix}, \quad (15)$$

а именно,

$$p_{n,m,n} = (-1)^{n+m+1} \frac{\det(M_{n,m+1})}{\det(M_{n,m})} \quad (16)$$

при условии, что $\det(M_{n,m}) \neq 0$.

Отсюда и из (12) следует, что если n фиксировано, а m стремится к бесконечности, то

$$|\det(M_{n,m})|^{\frac{1}{m}} \rightarrow W_n. \quad (17)$$

3. Приложения к гипотезе Римана

Дзета-функция Римана $\zeta(z)$ при $\operatorname{Re}(z) > 1$ задаётся рядом Дирихле

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}. \quad (18)$$

Эта функция может быть аналитически доопределена на всю комплексную плоскость за исключением точки $z = 1$, которая является единственным и простым полюсом $\zeta(z)$.

Уже Л. Эйлер знал, что отрицательные чётные числа,

$$z_1 = -2, z_2 = -4, \dots, z_k = -2k, \dots, \quad (19)$$

являются нулями дзета-функции; ныне эти нули называют *тривиальными*. Б. Риман доказал, что все остальные, *нетривиальные*, нули этой функции лежат в *критической полосе*

$$0 \leq \operatorname{Re}(z) \leq 1, \quad (20)$$

и высказал свою знаменитую гипотезу о том, что они лежат на *критической прямой*

$$\operatorname{Re}(z) = \frac{1}{2}. \quad (21)$$

Благодаря установленному Риманом *функциональному уравнению* для доказательства этой гипотезы достаточно показать, что тривиальные нули (19) являются единственными нулями дзета-функции, лежащими в полуплоскости

$$\operatorname{Re}(z) < \frac{1}{2}. \quad (22)$$

Мы избавимся от полюса дзета-функции, введя в рассмотрение целую функцию

$$\zeta^*(z) = 2(z-1)\zeta(z); \quad (23)$$

множитель 2 добавлен ради дальнейшего получения нормировки (4).

При замене переменной

$$z = \frac{w}{w+1}, \quad w = \frac{z}{1-z} \quad (24)$$

полуплоскость (22) переходит в круг

$$|w| < 1, \quad (25)$$

а тривиальные нули (19) переходят в числа

$$w_1 = \frac{z_1}{1-z_1} = -\frac{2}{3}, \dots, w_k = \frac{z_k}{1-z_k} = -\frac{2k}{2k+1}, \dots, \quad (26)$$

являющимися нулями функции

$$\tilde{\zeta}(w) = \zeta^*\left(\frac{w}{w+1}\right). \quad (27)$$

В терминах этой функции гипотеза Римана состоит в том, что в круге (25) нет нулей, отличных от (26).

До конца этого параграфа мы будем полагать, что функция $\tilde{\zeta}(w)$ взята на роль функции $f(w)$ из предыдущего параграфа.

Из гипотезы Римана следует, что для любого n начальные нули (5) (значения которых указаны в (26)) удовлетворяют условиям, предполагавшимся в предыдущем параграфе. Определяя матрицы (15) через тейлоровские коэффициенты функции $\tilde{\zeta}(w)$, мы, согласно (17), получаем, что

$$|\det(M_{n,m})|^{\frac{1}{m}} \rightarrow W_n = \prod_{k=1}^n \frac{2k+1}{2k}. \quad (28)$$

Нетрудно понять, что справедливо и обратное — если условия (28) выполнены для всех n , то гипотеза Римана верна. Действительно, предположим, что это не так, и пусть $\check{w}$ — это нуль функции $\tilde{\zeta}(w)$, лежащий в круге (25), но отличный от нулей (26). Возьмём в качестве n количество нулей функции $\tilde{\zeta}(w)$, лежащих в круге $|w| \leq |\check{w}|$. Пусть это будут нули $\check{w}_1, \dots, \check{w}_n$, занумерованные так, что $|\check{w}_1| \leq \dots \leq |\check{w}_n|$. Согласно (17)

$$|\det(M_{n,m})|^{\frac{1}{m}} \rightarrow \prod_{k=1}^n \frac{1}{|\check{w}_n|}. \quad (29)$$

Легко видеть, что $|\check{w}_1| \leq |w_1|, \dots, |\check{w}_{n-1}| \leq |w_{n-1}|$ и $|\check{w}_n| < |w_n|$. Следовательно,

$$\prod_{k=1}^n \frac{1}{|\check{w}_n|} > \prod_{k=1}^n \frac{1}{|w_n|} = \prod_{k=1}^n \frac{2k+1}{2k}, \quad (30)$$

что даёт требуемое противоречие вместе с (29) и (28).

Приведённая переформулировка гипотезы Римана мотивирует изучение матриц вида (15), в частности, их собственных чисел и собственных векторов. Компьютерные вычисления показали, что в случае дзета-функции эти числа и вектора имеют богатую структуру, частично описанную ниже.

Пусть

$$\mu_{n,m,1}, \mu_{n,m,2}, \dots, \mu_{n,m,m} \quad (31)$$

— собственные числа матрицы $M_{n,m}$; они вещественны, поскольку матрица ганкелева, и её элементы — вещественные числа. Мы будем считать, что нумерация такова, что

$$|\mu_{n,m,1}| \leq \dots \leq |\mu_{n,m,k}| \leq |\mu_{n,m,k+1}| \leq \dots \leq |\mu_{n,m,m}|. \quad (32)$$

На рис. 1 собственные числа (31) для $n = 1$ изображены следующим образом: число $\mu_{1,m,k}$ представлено точкой с координатами $(\ln(|\mu_{1,m,k}|), m)$, причём точка имеет белый цвет, если $\mu_{1,m,k} < 0$, и чёрный в противоположном случае (изображения собственных чисел $\mu_{n,m,k}$ для $n > 1$, можно найти в [5, 6, 7, 8]; в [7] приведены также изображения соответствующих собственных векторов).

На рис. 1 видно, что наименьшие (по абсолютной величине) собственные числа расположены вдоль почти прямолинейных “траекторий”. Автор высказал следующую гипотезу про их параметры.

Предположение А [6, 7, 8] . Для всех n и k существует рациональное число $A_{n,k}$ такое, что при $m \rightarrow \infty$

$$\mu_{n,m,k} = (-1)^{n+k} (Y_{n,k} + o(1)) (-w_{n+k})^m, \quad (33)$$

где

$$Y_{n,k} = A_{n,k} \left. \frac{d}{dw} \tilde{\zeta}(w) \right|_{w=w_{n+k}}. \quad (34)$$

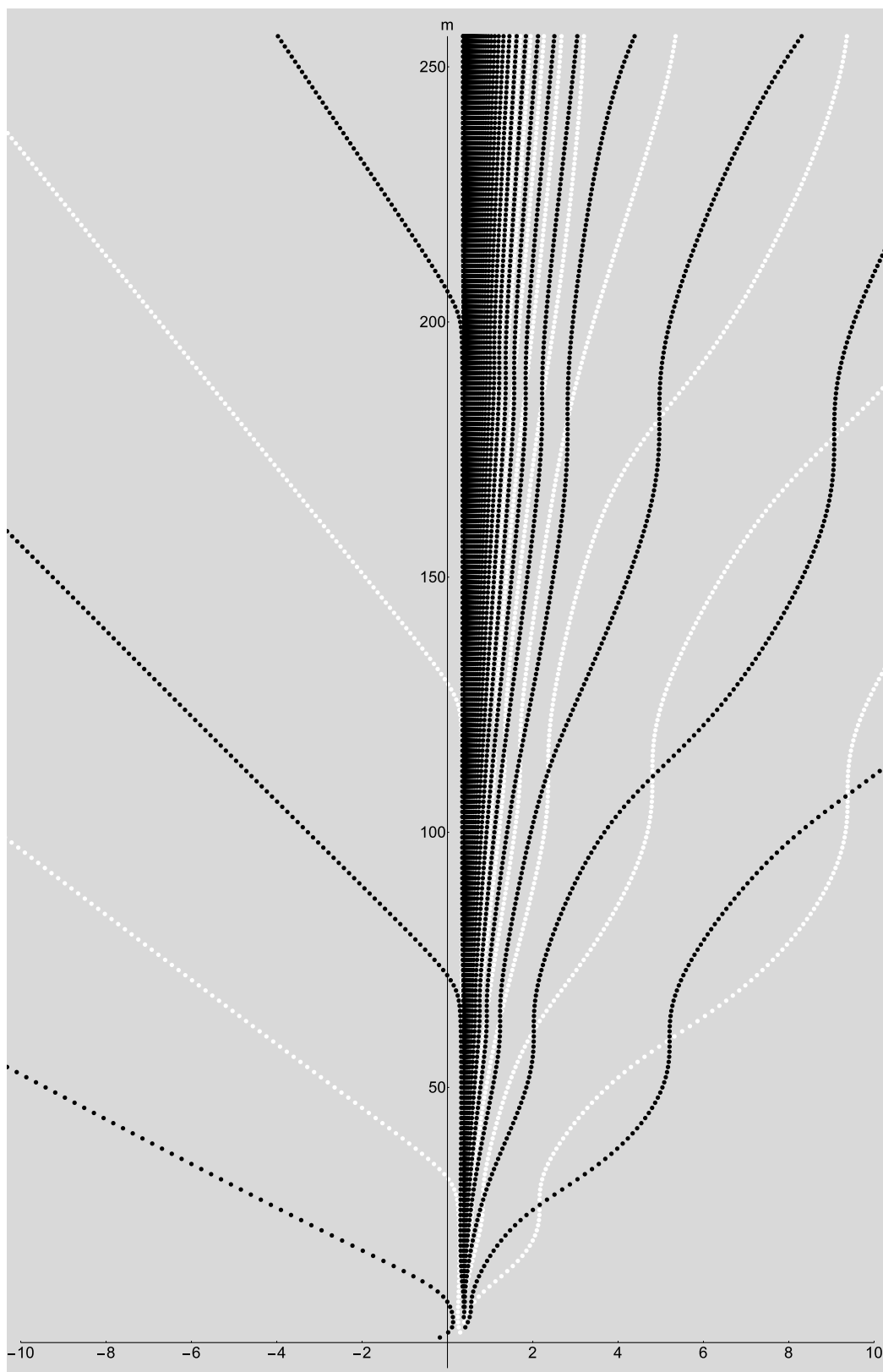
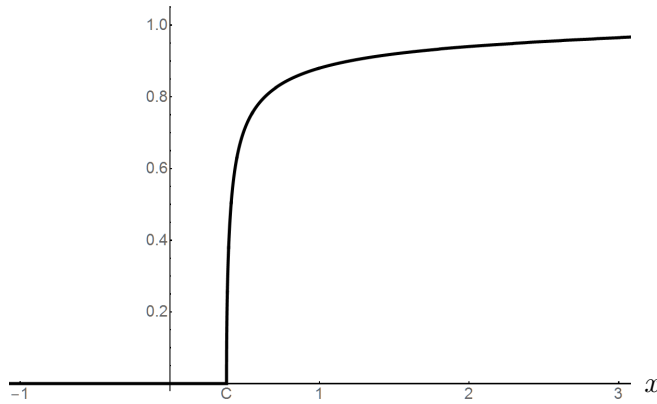


Рис. 1: Логарифмы модулей собственных чисел матриц (15) при $m = 1, \dots, 256$, $k = 1, \dots, m$.

Рис. 2: Ожидаемый график $F(x)$

Для $n = 0$ ожидается, что

$$A_{0,k} = (w_k^2 - 1) \prod_{j=1}^{k-1} \frac{w_j w_k - 1}{(w_j - w_k)^2}. \quad (35)$$

При $n > 0$ предполагаемую величину $A_{n,k}$ удалось указать лишь для отдельных значений n и k (см. [8, 7]).

На рис. 1 также видно, что собственные числа имеют точку сгущения при $\ln(|\mu_{1,m,k}|) \approx 0.4$. По-другому это можно увидеть следующим образом.

Условие (28) можно переписать в логарифмическом виде:

$$\frac{1}{m} \ln(|\det(M_{n,m})|) = \frac{1}{m} \sum_{k=1}^m \ln(|\mu_{n,m,k}|) \rightarrow \ln(W_n). \quad (36)$$

Положим, что каждое собственное число $\mu_{n,m,k}$ имеет вес $1/m$ и рассмотрим соответствующую функцию распределения:

$$F_{n,m}(x) = \sum_{\ln(|\mu_{n,m,k}|) \leq x} \frac{1}{m}. \quad (37)$$

Графики распределений $F_{n,m}$ для небольших значений n и m можно найти в [5, 7].

Используя $F_{n,m}$ условие (28) можно записать следующим образом:

$$\frac{1}{m} \ln(|\det(M_{n,m})|) = \int_{-\infty}^{+\infty} x dF_{n,m}(x) \rightarrow \ln(W_n). \quad (38)$$

Вычисления позволили автору высказать гипотезу о наличии предельного распределения.

Предположение С [8]. Существует непрерывная функция $F(x)$ такая, что для каждого n и каждого x при $m \rightarrow \infty$

$$F_{n,m}(x) \rightarrow F(x), \quad (39)$$

причём $F(x) = 0$ при $x < C_0$ и $F(x) > 0$ при $x > C_0$, где

$$C_0 = \ln(f(1)) = \ln(-\zeta(1/2)) = 0.378679220... \quad (40)$$

Ожидаемый вид $F(x)$ показан на рис. 2. Удивительным представляется то обстоятельство, что $F(x)$ не зависит от n , хотя предельные значения интегралов в (38) от этого параметра зависят.

4. Наименьшее собственное число

В этом и в следующем параграфах мы рассмотрим модельный случай функции, имеющей лишь один нуль,

$$g(z) = 1 - \frac{z}{z_1}. \quad (41)$$

На роль функции $f(w)$ мы возьмём функцию, получающуюся из $g(z)$ применением замены переменной (24):

$$f(w) = g\left(\frac{w}{1+w}\right) = 1 - \frac{w}{z_1(1+w)}; \quad (42)$$

эта функция имеет единственный нуль

$$w_1 = \frac{z_1}{1 - z_1}.$$

Так определённая функция $f(w)$ имеет разложение

$$f(w) = 1 - \frac{1}{z_1}w + \frac{1}{z_1}w^2 - \frac{1}{z_1}w^3 + \dots, \quad (43)$$

и, соответственно, ганкелевы матрицы (15) при $n = 0$ имеют вид

$$M_{0,m} = \begin{pmatrix} \frac{-1}{z_1} & \frac{1}{z_1} & \dots & \frac{(-1)^{m-1}}{z_1} & (-1)^m \\ \frac{1}{z_1} & \dots & \dots & (-1)^m & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \frac{(-1)^{m-1}}{z_1} & (-1)^m & \dots & \dots & 0 \\ (-1)^m & 0 & \dots & 0 & 0 \end{pmatrix}. \quad (44)$$

На рис. 3 изображены собственные числа матриц (44) для $z_1 = -100$. Видно, что первые (наименьшие по абсолютной величине) собственные числа расположены вдоль почти прямолинейной траектории аналогично рис. 1. Для них можно указать первые три члена асимптотики (считая, что w_1 мало):

$$\begin{aligned} \mu_{0,m,1} = & (w_1 - 1)(-w_1)^{m-1} + \\ & + (-m + w_1 + mw_1 - w_1^2 + mw_1^2 - mw_1^3)(-w_1)^{3m-2} + \\ & + \frac{1}{2}(m - 5m^2 + 5mw_1 + 5m^2w_1 - 2w_1^2 - 6mw_1^2 + 10m^2w_1^2 + 2w_1^3 - 6mw_1^3 - \\ & - 10m^2w_1^3 + 5mw_1^4 - 5m^2w_1^4 + mw_1^5 + 5m^2w_1^5)(-w_1)^{5m-3} + \\ & + O(w_1^{7m}). \end{aligned} \quad (45)$$

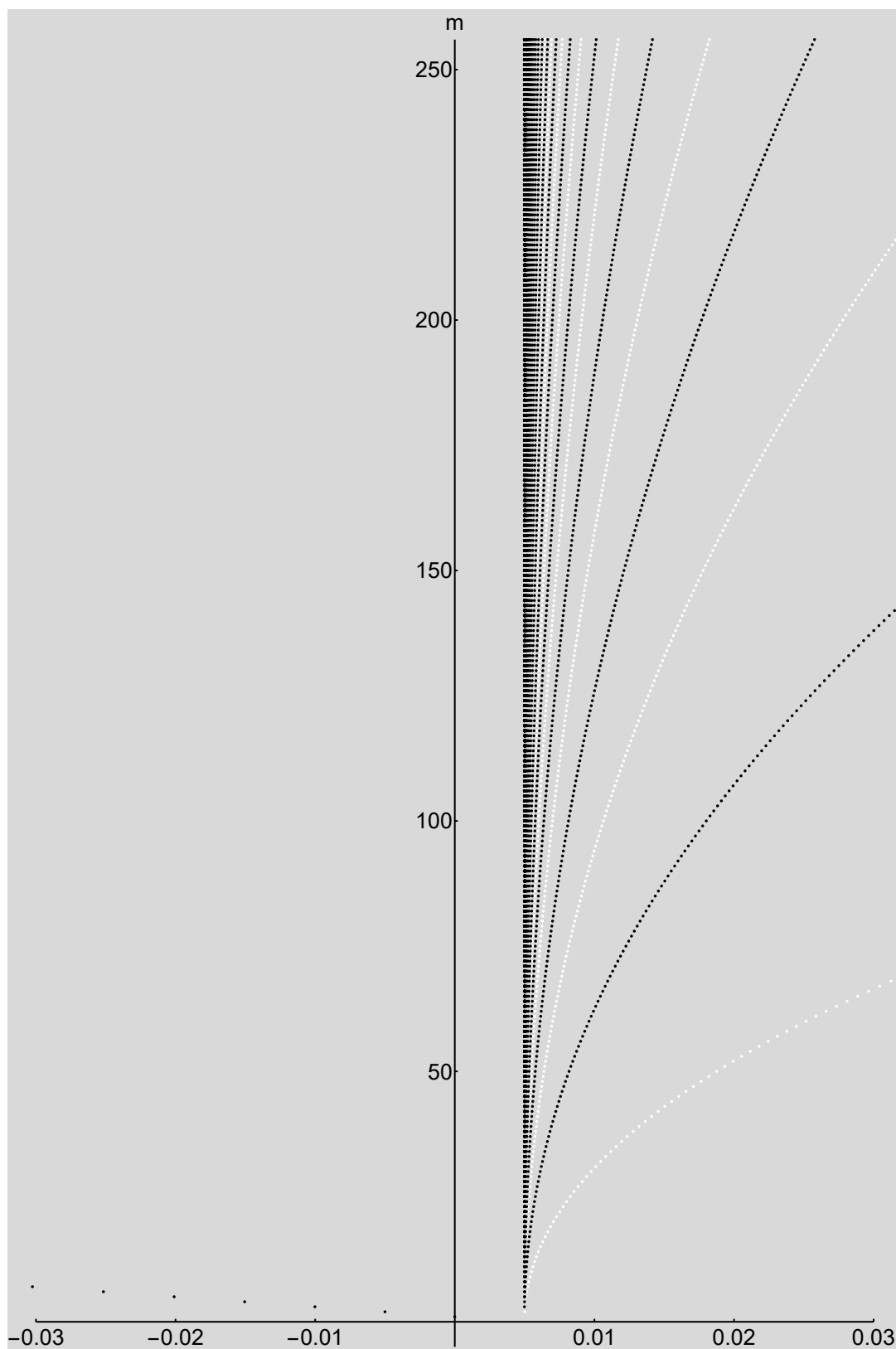


Рис. 3: Логарифмы модулей собственных чисел матриц (44) при $z_1 = -100$, $m = 1, \dots, 256$ и $k = 1, \dots, m$.

Асимптотика для j -го элемента собственного вектора, соответствующего первому собственному числу, имеет вид

$$\begin{aligned}
& \left(2w_1^{j+2} - 2w_1^{3-j}\right)w_1^m + \\
& \left((-2j(w_1^2 - 1)w_1^2 - 2w_1^2(2m(w_1^2 - 1) + 1))w_1^{-j} + \right. \\
& \quad \left.(2w_1(2m(w_1^2 - 1) + w_1^2) - 2jw_1(w_1^2 - 1)w_1^j)\right)w_1^{3m} + \\
& + \left((jw_1(w_1^2 - 1)^2 - j^2w_1(w_1^2 - 1)^2)\right)w_1^{-j} + \\
& \quad \left.+(j^2(w_1^2 - 1)^2 - j(w_1^2 - 1)^2)w_1^j\right)w_1^{5m} + O(w_1^{7m}). \tag{46}
\end{aligned}$$

Главный член разложения в (45), а именно, $(w_1 - 1)(-w_1)^{m-1}$, согласуется с (35) для $n = 0$, $k = 1$: в этом случае (35) и (34) дают значения

$$A_{0,1} = w_1^2 - 1 \quad \text{и} \quad Y_{0,1} = A_{0,1} \left. \frac{d}{dw} f(w) \right|_{w=w_1} = 1 - \frac{1}{w_1} \tag{47}$$

соответственно.

Асимптотические разложения (45) и (46) первоначально были найдены на основе анализа численных данных для матриц (44) с разными значениями z_1 и m . Формальное доказательство затем было получено посредством символьных вычислений в системе МАТНЕМАТИСА.

5. Точка сгущения и предельная функция распределения

В этом параграфе мы рассмотрим асимптотическое поведение собственных чисел матриц (44), отличных от самых маленьких (рассматривавшихся в предыдущем параграфе); при этом мы будем считать, что z_1 велико (по абсолютной величине). В этих условиях при $k \geq 1$

$$(-1)^k \mu_{0,m,k+1} = 1 - \frac{1}{2}z_1^{-1} + \frac{\tau_k}{8}z_1^{-2} + \tag{48}$$

$$+ \left(\frac{\tau_k}{16} + \frac{-\frac{\tau_k}{16} - \frac{\tau_k^2}{16}}{m} \right) z_1^{-3} +$$

$$+ \left(\frac{\tau_k}{32} - \frac{\tau_k^2}{128} + \frac{-\frac{\tau_k}{16} - \frac{\tau_k^2}{16}}{m} + \frac{\frac{3\tau_k}{128} + \frac{\tau_k^2}{16} + \frac{5\tau_k^3}{128}}{m^2} \right) z_1^{-4} +$$

$$+ \left(\frac{\tau_k}{64} - \frac{3\tau_k^2}{256} + \frac{-\frac{3\tau_k}{64} - \frac{13\tau_k^2}{384} + \frac{5\tau_k^3}{384}}{m} + \frac{\frac{9\tau_k}{256} + \frac{3\tau_k^2}{32} + \frac{15\tau_k^3}{256}}{m^2} + \frac{-\frac{\tau_k}{128} - \frac{31\tau_k^2}{768} - \frac{23\tau_k^3}{384} - \frac{7\tau_k^4}{256}}{m^3} \right) z_1^{-5} +$$

$$+ O(z_1^{-6}), \tag{49}$$

где

$$\tau_k = \operatorname{tg}^2 \left(\frac{\pi k}{2m} \right) = \frac{\pi^2 k^2}{4m^2} + O(m^{-6}). \tag{50}$$

У собственного вектора, соответствующего этому собственному числу, j -ый элемент асимптотически равен

$$\sin\left(\frac{\pi k}{m}(j-1/2)\right) + \quad (51)$$

$$\begin{aligned} &+ \left(1/4 \left((-1)^k + \sec^2\left(\frac{\pi k}{2m}\right)\right) \sin\left(\frac{\pi k}{m}(j-1/2)\right) + \right. \\ &+ \frac{1}{8m} \left((7 + (-1)^k) \sec\left(\frac{\pi k}{2m}\right) - 6\right) \sin\left(\frac{\pi k}{m}(j-1/2)\right) + \\ &\left. + 2(j-1/2) \operatorname{tg}\left(\frac{\pi k}{m}\right) \cos\left(\frac{\pi k}{m}(j-1/2)\right)\right) z_1^{-1} + O(z_1^{-2}). \end{aligned} \quad (52)$$

Приведённые асимптотические выражения хорошо согласуются с численными данными, полученными для дзета-функции. А именно, если ограничиться первыми тремя членами (48), то видно, что значение

$$C_1 = \ln(f(1)) = \ln\left(1 - \frac{1}{2z_1}\right) \quad (53)$$

является точкой сгущения логарифмов модулей собственных чисел, что аналогично (40). При этом, согласно определению (37), функция распределения $F_{0,m}(x)$ имеет вид

$$F_{0,m}(x) = \begin{cases} 0, & \text{если } x < C_1, \\ \frac{1}{m} \left\lfloor \frac{m}{\pi} \arctan(\sqrt{2(x-C_1)}) \right\rfloor, & \text{в противоположном случае,} \end{cases} \quad (54)$$

так что при возрастании m

$$F_{0,m}(x) \rightarrow F_0(x) = \begin{cases} 0, & \text{если } x < C_1, \\ \frac{1}{\pi} \arctan(\sqrt{2(x-C_1)}), & \text{в противоположном случае.} \end{cases} \quad (55)$$

График $F_0(x)$ очень похож на представленный на рис. 1 график ожидаемого предельного распределения для дзета-функции.

В разложении (52) его основной член, а именно, (51), зависит от j синусоидально, что визуально хорошо согласуется (при небольших значениях k) с численными данными, полученными для случая дзета-функции Римана (см. [7]).

Аналогично (45) и (46), асимптотические разложения (49) и (52) первоначально были найдены на основе анализа численных данных для матриц (44), а затем формальное доказательство было получено в системе МАТНЕМАТИСА.

6. Заключение

Приведённые асимптотические выражения для собственных чисел и собственных векторов матриц (44) показывают, что уже для простейшей функции, имеющей лишь один нуль, проявляются качественные и количественные свойства, численно обнаруженные ранее для дзета-функции Римана.

Интересным направлением дальнейших исследований представляется нахождение собственных чисел и векторов матриц (15), порожденных другими функциями с конечным количеством нулей. Шаги в этом направлении уже были сделаны в работах [2, 12]. А именно, там указаны собственные числа и собственные вектора матриц (3) для специальных случаев антиленточных ганкедовых матриц; в наших обозначениях это соответствует тому, что все, кроме конечного количества, элементы последовательности (2) равны нулю, то есть случаю, когда $f(w)$ — это многочлен.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бейкер Дж., Грейвс-Моррис П. *Аппроксимации Паде*. М., Мир, 1986.
2. Fonseca C. The eigenvalues of some anti-tridiagonal Hankel matrices // Kuwait J. Sci., Vol. 45:1, pp 1–6, 2018.
3. Jacobi, C. G. J. Über die Darstellung einer Reihe Gegebner Werthe durch eine Gebrochne Rationale Function. // J. Reine Angew. Math., Bd 30, S. 127–156, 1846.
4. Matiyasevich, Yu. *Hidden Life of Riemann's Zeta Function 2. Electrons and Trains*. <http://arxiv.org/abs/0709.0028>, 2007.
5. Matiyasevich, Yu. Riemann's zeta function: Some computations and conjectures. // In Proceedings of Conference on Algorithmic Number Theory (Turku, 2007), A.-M. Ernvall-Hytönen, M. Jutila, J. Karhumäki and A. Lepsitö, Eds., TUCS General Publication Series 46, pp. 87–112, Turku, 2007, 978-952-12-2014-2.
http://logic.pdmi.ras.ru/~yumat/personaljournal/zetahiddenlife/talks/turku2007/Matiyasevich_2007.pdf,
<http://tucs.fi/publications/attachment.php?fname=G46.pdf> (весь том).
6. Matiyasevich, Yu. V. The Riemann hypothesis and eigenvalues of related Hankel matrices. I. // Preprint POMI 14-03, 2014. <http://www.pdmi.ras.ru/preprint/2014/14-03.html>
7. Matiyasevich, Yu. V. *Structure of eigenvalues and eigenvectors of certain almost triangular Hankel matrices*. // Выступление на 7-ой Петербургской конференции по спектральной теории, 4 июля 2015г. http://logic.pdmi.ras.ru/~yumat/talks/birman_2015
8. Ю. В. Матиясевич. Гипотеза Римана в терминах собственных чисел специальных ганкелевых матриц // Совр. пробл. матем., Том 23, С. 871–101, 2016. DOI: 10.4213/spm64.
9. de Montessus de Ballore, R. Sur le fraction continues algébriques. // Bull. Soc. Math. France, Vol.30, 28–36, 1902.
10. Riemann, B. Über die Anzhal der Primzahlen unter einer gegebenen Grösse. // Monatsberichte der Berliner Akademie, November, 1859. Included into: Riemann, B. *Gesammelte Werke*. Teubner, Leipzig, 1892; reprinted by Dover Books, New York, 1953,
http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/zeta.pdf.
 English translation:
<http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf>.
11. Saff E. B. An extension of Montessus de Ballore's theorem on the convergence of interpolating rational functions // J. Approximation Theory, vol. 6:1, pp. 63–67, 1972.
12. Lita da Silva J. *Spectral properties of anti-heptadiagonal persymmetric Hankel matrices*. <http://arxiv.org/abs/1907.00260>

REFERENCES

1. Baker G. A., Jr., Graves-Morris P. R., *Padé Approximations, Vols. 1 and 2*, Encyclopedia of mathematics and its applications, Vols. 13 and 14, Addison Wesley, Reading, Mass., 1981.
2. Fonseca C. The eigenvalues of some anti-tridiagonal Hankel matrices // Kuwait J. Sci., 45:1, pp 1–6, 2018.

3. Jacobi, C. G. J. Über die Darstellung einer Reihe Gegebner Werthe durch eine Gebrochne Rationale Function. // J. Reine Angew. Math., Bd 30, 127–156, 1846.
4. Matiyasevich, Yu. *Hidden Life of Riemann's Zeta Function 2. Electrons and Trains*.
<http://arxiv.org/abs/0709.0028>, 2007.
5. Matiyasevich, Yu. Riemann's zeta function: Some computations and conjectures. // In Proceedings of Conference on Algorithmic Number Theory (Turku, 2007), A.-M. Ernvall-Hytönen, M. Jutila, J. Karhumäki and A. Lepsitö, Eds., TUCS General Publication Series 46, pp. 87–112, Turku, 2007, 978-952-12-2014-2.
http://logic.pdmi.ras.ru/~yumat/personaljournal/zetahiddenlife/talks/turku2007/Matiyasevich_2007.pdf,
<http://tucs.fi/publications/attachment.php?fname=G46.pdf> (whole volume).
6. Matiyasevich, Yu. V. The Riemann hypothesis and eigenvalues of related Hankel matrices. I. Preprint POMI 14-03, 2014. <http://www.pdmi.ras.ru/preprint/2014/14-03.html>
7. Matiyasevich, Yu. V. *Structure of eigenvalues and eigenvectors of certain almost triangular Hankel matrices*. // Talk given at 7th St.Petersburg Conference in Spectral Theory on July 4, 2015. http://logic.pdmi.ras.ru/~yumat/talks/birman_2015
8. Yu. V. Matiyasevich. Riemann's hypothesis in terms of the eigenvalues of special Hankel matrices // Proc. Steklov Inst. Math., 296, suppl. 2, (2017), 78–91, 2017. DOI: 10.1134/S0081543817030099.
9. de Montessus de Ballore, R. Sur le fraction continues algébriques. // Bull. Soc. Math. France, Vol. 30, 28–36, 1902.
10. Riemann, B. Über die Anzhal der Primzahlen unter einer gegebenen Grösse. // Monatsberichte der Berliner Akademie, November, 1859. Included into: Riemann, B. *Gesammelte Werke*. Teubner, Leipzig, 1892; reprinted by Dover Books, New York, 1953,
http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/zeta.pdf.
 English translation:
<http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf>.
11. Saff E. B., An extension of Montessus de Ballore's theorem on the convergence of interpolating rational functions // J. Approximation Theory, Vol. 6:1, pp. 63–67, 1972.
12. Lita da Silva J. *Spectral properties of anti-heptadiagonal persymmetric Hankel matrices*. <http://arxiv.org/abs/1907.00260>.

Получено 18.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.6

DOI 10.22405/2226-8383-2020-21-1-273-296

Периодические элементы $\sqrt{f}$ в эллиптических полях
с полем констант нулевой характеристики

В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников

Платонов Владимир Петрович — академик РАН, доктор физико-математических наук, профессор, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН»; Математический институт им. В. А. Стеклова РАН (г. Москва).

e-mail: platonov@mi-ras.ru

Петрунин Максим Максимович — кандидат физико-математических наук, научный сотрудник, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН» (г. Москва).

e-mail: petrulin@niisi.ras.ru

Штейников Юрий Николаевич — кандидат физико-математических наук, научный сотрудник, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН» (г. Москва).

e-mail: yuriisht@gmail.com

Аннотация

Исследование проблемы периодичности функциональных непрерывных дробей элементов эллиптических и гиперэллиптических полей было начато около 200 лет назад в классических работах Н. Абеля и П. Л. Чебышева. В 2014 году В. П. Платоновым был предложен общий концептуальный метод, базирующийся на глубокой связи трех классических проблем: проблема существования и построения фундаментальных S -единиц в гиперэллиптических полях, проблема кручения в якобианах гиперэллиптических кривых и проблема периодичности непрерывных дробей элементов в гиперэллиптических полях. В 2015-2019 годах в работах В. П. Платонова с соавторами был достигнут большой прогресс в исследовании проблемы периодичности элементов в гиперэллиптических полях, в особенности в эффективной классификации таких периодических элементов. Так, например, в указанных работах В. П. Платонова с соавторами были найдены все эллиптические поля $\mathbb{Q}(x)(\sqrt{f})$ такие, что $\sqrt{f}$ разлагается в периодическую непрерывную дробь в $\mathbb{Q}((x))$, а также были получены дальнейшие продвижения в обобщении указанного результата, как на другие числовые поля констант, так и на гиперэллиптические кривые рода 2 и выше. В настоящей статье мы приводим полное доказательство анонсированного нами в 2019 году результата о конечности числа эллиптических полей $k(x)(\sqrt{f})$ над произвольным числовым полем k с периодическим разложением $\sqrt{f}$, для которых соответствующая эллиптическая кривая содержит k -точку четного порядка не превосходящего 18 или k -точку нечетного порядка не превосходящего 11. Для произвольного поля k являющегося квадратичным расширением $\mathbb{Q}$ найдены все такие эллиптические поля, а для поля $k = \mathbb{Q}$ было получено новое доказательство конечности числа периодических $\sqrt{f}$, не использующее параметризацию эллиптических кривых и точек конечного порядка на них.

Ключевые слова: эллиптическое поле, гиперэллиптическое поле, периодичность, непрерывные дроби, длина периода, фундаментальные единицы, S -единицы, результат, базис Грёбнера, квадратичная иррациональность

Библиография: 22 названия.

Для цитирования:

В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников. Периодические элементы $\sqrt{f}$ в эллиптических полях с полем констант нулевой характеристики // Чебышевский сборник, 2020, т. 21, вып. 1, с. 273–296.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.6

DOI 10.22405/2226-8383-2020-21-1-273-296

Periodic elements $\sqrt{f}$ in elliptic fields with a field of constants of zero characteristic

V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov

Platonov Vladimir Petrovich — Academician, Chief researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences; Steklov Mathematical Institute of Russian Academy of Sciences (Moscow).

e-mail: platonov@mi-ras.ru

Petrinin Maxim Maximovich — phd, scientific researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences (Moscow).

e-mail: petrinin@niisi.ras.ru

Shteinikov Yurii Nikolaevich — phd, scientific researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences (Moscow).

e-mail: yuriisht@gmail.com

Abstract

A study of the periodicity problem of functional continued fractions of elements of elliptic and hyperelliptic fields was begun about 200 years ago in the classical papers of N. Abel and P. L. Chebyshev. In 2014 V. P. Platonov proposed a general conceptual method based on the deep connection between three classical problems: the problem of the existence and construction of fundamental S -units in hyperelliptic fields, the torsion problem in Jacobians of hyperelliptic curves, and the periodicity problem of continued fractions of elements of hyperelliptic fields. In 2015–2019, in the papers of V. P. Platonov et al. was made great progress in studying the problem of periodicity of elements in hyperelliptic fields, especially in the effective classification of such periodic elements. In the papers of V. P. Platonov et al, all elliptic fields $\mathbb{Q}(x)(\sqrt{f})$ were found such that $\sqrt{f}$ decomposes into a periodic continued fraction in $\mathbb{Q}((x))$, and also further progress was obtained in generalizing the indicated result, as to other fields of constants, and to hyperelliptic curves of genus 2 and higher. In this article, we provide a complete proof of the result announced by us in 2019 about the finiteness of the number of elliptic fields $k(x)(\sqrt{f})$ over an arbitrary number field k with periodic decomposition of $\sqrt{f}$, for which the corresponding elliptic curve contains a k -point of even order not exceeding 18 or a k -point of odd order not exceeding 11. For an arbitrary field k being quadratic extension of $\mathbb{Q}$ all such elliptic fields are found, and for the field $k = \mathbb{Q}$ we obtained new proof about of the finiteness of the number of periodic $\sqrt{f}$, not using the parameterization of elliptic curves and points of finite order on them.

Keywords: elliptical field, hyperelliptic field, periodicity, continued fractions, period length, fundamental units, S -units, resultant, Gröbner basis, quadratic irrationality

Bibliography: 22 titles.

For citation:

V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov, 2020, "Periodic elements $\sqrt{f}$ in elliptic fields with a field of constants of zero characteristic", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 273–296.

1. Введение

Пусть k — поле характеристики 0, и $f \in k[x]$ — многочлен свободный от квадратов. В работах [1, 2, 3, 4, 5] были получены основополагающие результаты, связанные с проблемой периодичности разложения элементов поля $k(x)(\sqrt{f})$ в непрерывную дробь в поле формальных степенных рядов $k((1/x))$. В частности, было показано, что с точки зрения изучения вопросов, связанных с периодичностью элементов поля $L = k(x)(\sqrt{f})$ ключевым является элемент $\sqrt{f}$. Этот элемент периодичен в $k((1/x))$ в случае, когда поле L содержит периодические элементы. Однако в случае непрерывных дробей в поле формальных степенных рядов $k((x))$ даже наличие в поле L периодических элементов не гарантирует периодичность разложения элемента $\sqrt{f}$ в функциональную непрерывную дробь. Более того, периодичность $\sqrt{f}$ — сравнительно редкое явление.

В работах [6, 7, 8, 18] было доказано, что квазипериодический $\sqrt{f} \in k((x))$ с необходимостью является периодическим, и были построены первые примеры периодических $\sqrt{f}$. А в работах [9, 10] с точностью до естественного отношения эквивалентности была доказана конечность числа таких нетривиальных (то есть, не попадающих в серию $cx^3 + 1$, $c \in \mathbb{Q}$) многочленов f степени $\deg f = 3$ с рациональными коэффициентами, а также был поставлен вопрос в более общем случае: для каких свободных от квадратов многочленов $f \in \mathbb{Q}[x]$ непрерывная дробь $\sqrt{f} \in \mathbb{Q}((x))$ является периодической.

В работе [11] для гиперэллиптических полей, содержащих фундаментальные S -единицы малых степеней, с помощью метода, основанного на решении норменного уравнения, были получены рекуррентные соотношения на коэффициенты решения норменного уравнения для полей, обладающих S -единицами малых степеней. С помощью этих соотношений были найдены новые примеры периодических элементов $\sqrt{f}$ для $f \in \mathbb{Q}[x]$.

Однако уже в случае, когда многочлен имеет степень 3, для полей, содержащих фундаментальные S -единицы нечётной степени начиная с 9, соотношения на коэффициенты кардинально усложняются, и указанный метод становится неприменим. В работе [12] был предложен новый эффективный метод для решения норменного уравнения, основанный на применении базисов Грёбнера. В работе [12] было доказано, что для любого поля k характеристики 0 с точностью до естественной эквивалентности существует лишь конечное число бесквадратных многочленов над k нечётной степени, отличной от 11, таких, что элемент $\sqrt{f}$ периодичен, а соответствующее гиперэллиптическое поле $k(x)(\sqrt{f})$ содержит S -единицу степени 11. Кроме того, было доказано, что в случае $k = \mathbb{Q}$ многочленов с указанными свойствами нечётной степени отличной от 9 и 11, не существует.

Остаётся открытым естественный вопрос о периодичности $\sqrt{f}$ для эллиптических полей, рассматриваемых над числовым полем. Полного решения нет даже для $\deg f = 3$ и квадратичных расширений поля $\mathbb{Q}$. В работе [13] было сделано продвижение в этом направлении, и было дано описание кубических многочленов $f(x)$ с коэффициентами в квадратичных числовых полях $\mathbb{Q}(\sqrt{5})$ и $\mathbb{Q}(\sqrt{-15})$, для которых разложение в непрерывную дробь иррациональности $f(x)$ над этими полями периодично. Вышеупомянутые квадратичные числовые поля обладают новым кручением, а значит и фундаментальными S -единицами степеней, не встречающихся в эллиптических полях с полем констант $\mathbb{Q}$.

В работе [19] нами был предложен новый метод доказательства конечности таких многочленов, основанный на комбинации последовательного вычисления результатов, применения базисов Грёбнера и нетривиальных вычислениях в системах компьютерной алгебры MAGMA [20] и Sage [21]. Применение более слабого условия конечности позволяет доказать, что существует не более конечного числа неизоморфных эллиптических полей $k(x)(\sqrt{f})$, $\deg f = 3$, содержащих точку четного порядка не превосходящего 18 или точку нечётного порядка 5, 7, 11, таких, что элемент $\sqrt{f}$ периодичен. Более того, для поля k — квадратичного расширения $\mathbb{Q}$ — удаётся получить полную классификацию многочленов с указанными

свойствами. А для случая $k = \mathbb{Q}$ в качестве следствия было получено новое доказательство конечности числа периодических $\sqrt{f}$, не использующее параметризацию эллиптических кривых и точек конечного порядка на них. Теорема для случая квадратичного поля в качестве поля констант в сочетании с известными к настоящему моменту результатами, связанными с описанием кручения в эллиптических кривых над квадратичными полями, даёт основания предполагать, что количество нетривиальных неэквивалентных многочленов f с коэффициентами из квадратичных расширений $\mathbb{Q}$ с периодическим разложением $\sqrt{f}$ — конечно. В настоящей статье приводится полное доказательство анонсированных в [19] результатов.

Напомним некоторые факты, которые потребуется нам в дальнейшем. Для неприводимого над k многочлена h определим дискретное нормирование ν_h элемента поля $k(x)$ равенством $\nu_h\left(h^m \frac{p}{q}\right) = m$, где взаимно простые многочлены p, q не делятся на h . Бесконечное нормирование ν_∞ , в свою очередь, определим равенством $\nu_\infty\left(\frac{p}{q}\right) = \deg q - \deg p$.

Далее считаем, что $\deg h = 1$, и без ограничения общности положим $h = x$. Пусть нормирование ν_x поля $k(x)$ имеет два продолжения ν_x^+ и ν_x^- на поле $L = k(x)(\sqrt{f})$. Если $\deg f = 2g + 1$ для $g \in \mathbb{N}$, то бесконечное нормирование ν_∞ поля $k(x)$ имеет единственное продолжение на L , обозначим его также ν_∞ , и положим $S = \{\nu_x^+, \nu_\infty\}$. Группа обратимых элементов кольца S -целых элементов поля L называется группой S -единиц. Если существует хотя бы одна нетривиальная S -единица (то есть отличная от константы поля k), то в описанном нами случае группа S -единиц является прямым произведением $k \setminus \{0\}$ и бесконечной циклической группы. Образующие этой циклической группы называются фундаментальными S -единицами. Степенью S -единицы $\lambda_1 + \lambda_2 \sqrt{f} \in L$, где $\lambda_1, \lambda_2 \in k(x)$, называется показатель m в норменном выражении $\lambda_1^2 - \lambda_2^2 f = bh^m$, $b \in k \setminus \{0\}$, $m \in \mathbb{Z}$. Для эллиптического поля существование фундаментальной S -единицы степени m равносильно существованию k -точки порядка m соответствующей эллиптической кривой. Вложив поле L в поле формальных степенных рядов $k((x))$ можно разложить элемент поля L в функциональную непрерывную дробь. Необходимым условием для того, чтобы в поле L существовали элементы, разлагающиеся в периодическую непрерывную дробь в $k((x))$ (периодические элементы), является наличие нетривиальной S -единицы в поле L . Более подробные сведения о нормированиях, функциональных непрерывных дробях и S -единицах содержатся в работах [14, 18].

2. Формулировка основных результатов

Поскольку периодичность разложения в непрерывную дробь $\sqrt{f(x)}$ равносильна периодичности $\sqrt{a^2 f(bx)}$ для произвольных $a, b \in k \setminus \{0\}$, мы будем рассматривать многочлены с точностью до указанной эквивалентности. Сформулируем основные результаты.

ТЕОРЕМА 1. Пусть k — произвольное поле нулевой характеристики. Тогда существует универсальная константа C , не зависящая от поля k , такая, что существует не более C попарно неэквивалентных над k многочленов f , $\deg f = 3$, для которых выполнены следующие условия:

1. $\sqrt{f}$ — периодичен в $k((x))$;
2. поле $L = k(x)(\sqrt{f})$ содержит фундаментальную S -единицу четной степени не превосходящей 18 или нечётной степени 5, 7, 9 или 11 для $S = \{\nu_\infty, \nu_x^+\}$.

Нетривиальным многочленом f будем называть многочлен неэквивалентный многочлену $cx^3 + 1$, где $c \in k \setminus \{0\}$.

ТЕОРЕМА 2. *Если в условиях теоремы 1 поле k — расширение $\mathbb{Q}$ степени не более 2 и $k \neq \mathbb{Q}(\sqrt{21})$, то многочлен f может быть равен только одному из следующих представителей:*

$$\begin{aligned} f &= \frac{3}{16}x^3 - \frac{1}{2}x^2 + x + 1, \\ f &= \frac{12}{8}x^3 - \frac{5}{4}x^2 + x + 1, \\ f &= -\frac{120}{8}x^3 + \frac{25}{4}x^2 + x + 1. \end{aligned}$$

В случае когда $k = \mathbb{Q}(\sqrt{21})$, множество таких многочленов f исчерпывается тремя указанными выше и дополнительно многочленом

$$f = \frac{3}{32} \left(9\sqrt{21} - 41 \right) x^3 - \frac{1}{4} \left(3\sqrt{21} - 13 \right) x^2 + x + 1.$$

Других нетривиальных многочленов с указанными свойствами с точности до вышеуказанного отношения эквивалентности многочленов f и инволюции поля $\mathbb{Q}(\sqrt{21})$ меняющей знак у $\sqrt{21}$, не существует.

Отметим, что нетривиальный пример кубического многочлена $f \in \mathbb{Q}(\sqrt{21})[x] \setminus \mathbb{Q}[x]$ с периодическим разложением $\sqrt{f} \in \mathbb{Q}(\sqrt{21})((x))$ был впервые получен в [13].

В качестве следствия из теоремы 2 мы получаем альтернативное доказательство конечности числа различных нетривиальных эллиптических полей L с периодичным $\sqrt{f}$ для случая поля констант $k = \mathbb{Q}$, доказанного в [9, 10] с использованием параметризации эллиптических кривых и точек конечного порядка на них.

СЛЕДСТВИЕ 1. *Множество нетривиальных неэквивалентных свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 3$, имеющих периодическое разложение $\sqrt{f}$ в непрерывную дробь, исчерпывается тремя нетривиальными многочленами:*

$$\begin{aligned} f &= \frac{3}{16}x^3 - \frac{1}{2}x^2 + x + 1, \\ f &= \frac{12}{8}x^3 - \frac{5}{4}x^2 + x + 1, \\ f &= -\frac{120}{8}x^3 + \frac{25}{4}x^2 + x + 1, \end{aligned}$$

и серией многочленов $cx^3 + 1$, где $c \in \mathbb{Q} \setminus \{0\}$.

ДОКАЗАТЕЛЬСТВО. В [18] показано, что если эллиптическое поле над полем констант k содержит периодические элементы, то оно содержит фундаментальную S -единицу, а также было показано, что степень фундаментальной S -единицы равна порядку некоторой k -точки кручения. Таким образом, из результата Б. Мазира [22] следует, что степень фундаментальной S -единицы в произвольном эллиптическом поле с полем рациональных чисел в качестве поля констант не превосходит 12, и не может быть равна 11. Откуда многочлен $f \in \mathbb{Q}[x]$ степени 3 такой, что элемент $\sqrt{f}$ разлагается в периодическую непрерывную дробь, всегда удовлетворяет условиям теоремы 2, за исключением случая, когда поле $L = \mathbb{Q}(x)(\sqrt{f})$ содержит фундаментальную S -единицу степени 3. Поэтому искомое множество нетривиальных многочленов, для которых степень соответствующей фундаментальной S -единицы не равна 3, есть множество из трех многочленов, указанное в теореме 2. В случае же когда степень S -единицы равна трем, множество искомых многочленов исчерпывается тривиальной серией $cx^3 + 1$ (см. например [18, 10]). Следствие доказано. $\square$

3. Периодический корень

В работах [6], [18] был доказан критерий периодичности элемента вида $\frac{\sqrt{f}}{x^s}$, а также доказаны факты, полезные в настоящей статье. Приведём здесь критерий в необходимой нам общности.

ТЕОРЕМА 3. Пусть $\deg f = 2g + 1$. Элемент $\sqrt{f}$ периодичен тогда и только тогда, когда существует решение $Y, Z \in k[x^{-1}]$, $Y \neq 0$, уравнения $Y^2 - Z^2 \frac{f}{x^{2g+2}} = b$, для которого $Z = Z'x^{-g}$, $Z' \in k[x^{-1}]$. Более того, если это условие выполнено для некоторого решения, то оно выполнено для всех таких решений.

Из теоремы следует, что достаточно рассматривать только фундаментальное решение указанного уравнения, т.е. решение с максимальным значением $\nu_x(Y) < 0$. Такое решение соответствует фундаментальной S -единице чётной степени или квадрату фундаментальной S -единицы нечётной степени поля $k(x)(\sqrt{f})$ (см. [18]). Переформулируем утверждение теоремы 3 на языке многочленов из $k[x]$ (см. также [10]).

ТЕОРЕМА 4. Пусть многочлен f свободен от квадратов, а $\deg f = 2g + 1$. Элемент $\sqrt{f}$ квазипериодичен тогда и только тогда, когда некоторого $m \in \mathbb{N}$, существует решение $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $b \in k \setminus \{0\}$, $f = d_1 d_2$, уравнения

$$\mu_1^2 d_1 - \mu_2^2 d_2 = bx^m, \quad (1)$$

и решение для наименьшего такого m удовлетворяет условиям

1. $\deg \mu_2 = \frac{m - \deg d_2}{2}$,
2. $\deg \mu_1 \leq \frac{m + \deg d_2}{2} - (2g + 1)$.

ДОКАЗАТЕЛЬСТВО. По теореме 3 элемент $\sqrt{f}$ периодичен тогда и только тогда, когда пара Y, Z , где $Z = Z'x^{-g}$ и $Y, Z' \in k[x^{-1}]$, является фундаментальным решением уравнения $Y^2 - Z^2 \frac{f}{x^{2g+2}} = b'$. Пусть $v_x(Y) = -m$, тогда

$$\lambda_1^2 - \lambda_2^2 f = b'x^{2m}, \quad (2)$$

где $\lambda_1 = x^m Y$, $\lambda_2 = x^{m-(2g+1)} Z'$. В силу нечётности степени f получаем $\deg \lambda_1 = m$, $\deg \lambda_2 \leq m - (2g + 1)$, а $b' = b^2$ для некоторого $b \in k \setminus \{0\}$. Кроме того ясно, что λ_1, λ_2 взаимно просты как многочлены.

Воспользуемся формулой разности квадратов:

$$(\lambda_1 - bx^m)(\lambda_1 + bx^m) = \lambda_2^2 f.$$

Обе скобки в левой части взаимно просты, иначе $x \mid \lambda_1$, откуда $x \mid \lambda_2$, что противоречит взаимной простоте λ_1, λ_2 .

В этом случае, получаем

$$\begin{aligned} \lambda_1 - bx^m &= \mu_1^2 d_1, \\ \lambda_1 + bx^m &= \mu_2^2 d_2, \\ \mu_1 \mu_2 &= \lambda_2. \end{aligned} \quad (3)$$

Откуда $2\lambda_1 = \mu_1^2 d_1 + \mu_2^2 d_2$, и

$$2bx^m = \mu_2^2 d_2 - \mu_1^2 d_1.$$

В силу того, что f свободен от квадратов, мы можем утверждать, что с точностью до умножения на константу такое разложение на d_1, d_2 и μ_1, μ_2 единственное.

Так как степени d_1 и d_2 имеют разную чётность, выполнено или $\deg(\mu_1^2 d_1) = t$ или $\deg(\mu_2^2 d_2) = t$. Без ограничения общности будем считать, что $\deg(\mu_2^2 d_2) = t$ (в противном случае, заменим b на $-b$, и поменяем местами индексы в обозначениях 1 и 2). Откуда в силу (3) и неравенства $\deg \lambda_2 \leq t - (2g + 1)$ получаем $\deg \mu_1 \leq \frac{m + \deg d_2}{2} - (2g + 1)$.

Обратно, если находится такое решение, то по формулам выше легко получить решение, удовлетворяющее условию критерия периодичности $\sqrt{f}$. $\square$

ЗАМЕЧАНИЕ 1. Если в результате процедуры из доказательства теоремы 3 мы получим $\deg d_1 = 0$, то t обязано быть нечётным числом, в противном случае мы получим решение уравнения (2) с показателем $t < 2t$ чего не может быть в силу условия минимальности.

3.1. Результат

Рассмотрим многочлены $f = \sum_i a_i x^{n-i}, g = \sum_i b_i x^{m-i}$, где $a_0, b_0 \neq 0$. Пусть x_i — корни многочлена f , а y_i — корни многочлена g . Напомним, что величина

$$R(f, g) = a_0^m b_0^n \prod (x_i - y_j)$$

называется результатом пары f, g . Следующая лемма хорошо известна, мы приводим ее без дополнительных пояснений.

- ЛЕММА 1.**
1. Результат многочленов f и g равен определителю матрицы Сильвестра.
 2. $R(f, g)$ является однородным многочленом степени t по переменным a_i и степени n по переменным b_j с коэффициентами из $\mathbb{Z}$.
 3. $R(f, g) = 0$ только в том случае, когда f и g имеют общий корень в алгебраическом замыкании.

Результат, как общеизвестно, позволяет также сводить решение системы алгебраических уравнений к нахождению корней многочленов. В более общей форме, он позволяет исключать переменные из системы алгебраических уравнений. В самом деле, пусть полиномиальная система

$$f_1(x_1, \dots, x_n) = 0, \dots, f_n(x_1, \dots, x_n) = 0;$$

где $f_i \in \mathbb{Q}[x_1, \dots, x_n]$ имеет решение при каком-то x_n . Тогда представляя каждый f_i как полином от x_n над кольцом $\mathbb{Q}[x_1, \dots, x_{n-1}]$ вычисляя $n - 1$ результат пар f_1, f_i мы получаем новую полиномиальную систему с $n - 1$ уравнением и $n - 1$ переменной вида

$$g_i(x_1, \dots, x_{n-1}) = 0, g_i(x_1, \dots, x_{n-1}) \in \mathbb{Q}[x_1, \dots, x_{n-1}].$$

В наших вычислениях и алгоритмах мы несколько модифицируем эту схему. А именно, на каждом шаге предварительно вычисляются попарные наибольшие общие делители многочленов f_i : $\gcd(f_i, f_j)$. Если множество корней первоначальной системы не обнуляет многочлен $\gcd(f_i, f_j)$, то процедура сокращения на многочлен $\gcd(f_i, f_j)$ корректна. Последовательное применение вышеприведённой процедуры позволяет получить в рассматриваемых нами случаях либо константный многочлен, либо многочлен, зависящий только от одной переменной. С помощью переупорядочивания многочленов на каждом шаге, мы можем добиться того, чтобы на последнем шаге был многочлен от заданной переменной. Построение системы из n таких многочленов, полученных для каждой из переменных исходной системы, позволяет найти все корни исходной системы. Для краткости будем называть эту итеративную процедуру R -преобразованием системы или просто R -процедурой.

4. Нетривиальные решения

Пусть $t \in k[x]$, $s = \deg t$, $t = t_0 + t_1x + t_2x^2 + \dots + t_sx^s \in k[x]$. Обозначим через $lc(t) = t_s$, через $plc(t) = t_{s-1}$, а через $fc(t) = t_0$ коэффициент при нулевой степени x .

ОПРЕДЕЛЕНИЕ 1. Пусть заданы $g, m \in \mathbb{N}$. Будем называть набор $(\mu_1, \mu_2, d_1, d_2, b)$, где $b \in k \setminus \{0\}$, $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $d_1 \neq 0$, $d_2 \neq 0$, $fc(\mu_1) \neq 0$, $\deg d_1 + \deg d_2 = 2g + 1$, а произведение $f = d_1d_2$ свободно от квадратов, **решением обобщённого норменного уравнения над k** , если выполнено соотношение (1).

Мы будем писать **нетривиальное решение норменного уравнения**, если $d_1 = 1$, в этом случае мы будем писать (μ_1, μ_2, f, b) вместо $(\mu_1, \mu_2, 1, d_2, b)$. Мы будем писать просто **нетривиальное решение**, если из контекста ясно, что речь идёт о нетривиальном решении норменного или обобщённого норменного уравнения.

Пусть задано нетривиальное решение обобщённого норменного уравнения. Определим коэффициенты a_i, b_j, h_k, f_k из следующих равенств:

$$\mu_1 = \sum_i a_i x^i; \quad \mu_2 = \sum_i b_i x^i; \quad d_1 = \sum_i h_i x^i; \quad d_2 = \sum_i f_i x^i.$$

ОПРЕДЕЛЕНИЕ 2. Назовем системой обобщенного норменного уравнения систему уравнений относительно неизвестных a_i, b_j, h_k, f_k к которой сводится обобщенное норменное уравнение (1).

ЗАМЕЧАНИЕ 2. Если $(\mu_1, \mu_2, d_1, d_2, b)$ — нетривиальное решение норменного уравнения. Тогда $f_0 h_0 = a^2$ и $\frac{f_0}{h_0} = a'^2$, для некоторых $a, a' \in k \setminus \{0\}$, в частности, $f_0 = a^2$, если $d_1 = 1$.

ОПРЕДЕЛЕНИЕ 3. Будем называть **допустимыми преобразованиями** нетривиального решения обобщённого норменного уравнения над полем k , если оно переводит набор $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ в один из следующих наборов:

- $\Gamma_{1,\gamma}(\Omega) = (\mu_1(\gamma x), \mu_2(\gamma x), d_1(\gamma x), d_2(\gamma x), \gamma^m b)$.
- $\Gamma_{2,\gamma}(\Omega) = (\gamma \mu_1, \gamma \mu_2, d_1, d_2, \gamma^2 b)$,
- $\Gamma_{3,\gamma}(\Omega) = (\gamma \mu_1, \mu_2, d_1, \gamma^2 d_2, \gamma^2 b)$,
- $\Gamma_{4,\gamma}(\Omega) = (\mu_1, \mu_2, \gamma d_1, \gamma d_2, \gamma b)$,

для некоторого $\gamma \in k \setminus \{0\}$, или преобразования, полученные путём последовательного применения вышеперечисленных преобразований.

В дальнейшем нам потребуются ещё несколько допустимых преобразований:

- $\Gamma_{5,\gamma}(\Omega) = \Gamma_{2,\frac{1}{\gamma}} \circ \Gamma_{3,\gamma}(\Omega) = (\mu_1, \gamma \mu_2, d_1, \frac{1}{\gamma^2} d_2, b)$,
- $\Gamma_{6,\gamma}(\Omega) = \Gamma_{4,\frac{1}{\gamma^2}} \circ \Gamma_{3,\gamma}(\Omega) = (\gamma \mu_1, \mu_2, \frac{1}{\gamma^2} d_1, d_2, b)$,
- $\Gamma_{7,\gamma}(\Omega) = \Gamma_{4,\gamma^2} \circ \Gamma_{5,\gamma}(\Omega) = (\mu_1, \gamma \mu_2, \gamma^2 d_1, d_2, \gamma^2 b)$,
- $\Gamma_{8,\gamma}(\Omega) = \Gamma_{4,\gamma} \circ \Gamma_{5,\gamma}(\Omega) = (\mu_1, \gamma \mu_2, \gamma d_1, \frac{1}{\gamma} d_2, \gamma b)$,

Нетрудно видеть, что допустимые преобразования, применённые к нетривиальному решению для g, t , снова дают нетривиальное решение для g, t и тем самым, в силу обратимости они задают отношение эквивалентности на нетривиальных решениях, что с учётом соотношения $f = d_1 d_2$ некоторым образом обобщает отношение эквивалентности из §2 и работы [12]. Заметим, что допустимые преобразования меняют коэффициенты многочленов μ_1, μ_2, d_1, d_2 и константу b .

Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение обобщённого норменного уравнения над k , тогда для этого нетривиального решения выполнено $\deg d_2 > 0$. Действительно, из доказательства теоремы 4 следует, что выполнено одно из двух: или m — нечётное число, или $\deg d_1 > 0$ и $\deg d_2 > 0$. Если m — нечётное число, то $\deg d_2$ обязано быть нечётным числом, и, следовательно, $\deg d_2 > 0$.

ЛЕММА 2. Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение обобщённого норменного уравнения над k , тогда для данного m

- существует нетривиальное решение над k с $h_0 = f_0 = 1 = lc(\mu_1)$ и $f_1 = 0$ или $f_1 = 1$.
- существует нетривиальное решение над k с $h_0 = f_0 = 1 = lc(\mu_2)$ и $f_1 = 0$ или $f_1 = 1$.

ДОКАЗАТЕЛЬСТВО. Пусть $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ — нетривиальное решение. У решения $\Omega_1 = \Gamma_{8, f_0}(\Omega)$ коэффициент $f_0(\Omega_1) = 1$.

Поскольку младший коэффициент нового $d_1(\Omega_1)$ — полный квадрат в k , для

$$\Omega_2 = \Gamma_{7, \frac{1}{\gamma_2}}(\Omega_1) = \left(\mu_1, \frac{\gamma_1}{\gamma_2} \mu_2, \frac{\gamma_1}{\gamma_2^2} d_1, \frac{1}{\gamma_1} d_2, \frac{\gamma_1}{\gamma_2^2} b \right)$$

выполнено $h_0(\Omega_2) = f_0(\Omega_2) = 1$, где $\gamma_2 = \sqrt{fc(d_1)\gamma_1} = \sqrt{fc(d_1)fc(d_2)}$.

Положим $\gamma_3 = 1$ если $f_1 = 0$ и $\frac{\gamma_2^2}{\gamma_1 f_1}$ иначе.

Тогда для

$$\Omega_3 = \Gamma_{1, \gamma_3}(\Omega_2) = \left(\mu_1(\gamma_3 x), \frac{\gamma_1}{\gamma_2} \mu_2(\gamma_3 x), \frac{\gamma_1}{\gamma_2^2} d_1(\gamma_3 x), \frac{1}{\gamma_1} d_2(\gamma_3 x), \frac{\gamma_1 \gamma_3^m}{\gamma_2^2} b \right),$$

$f_1(\Omega_3) = 0$ или $f_1(\Omega_3) = 1$.

Наконец, положив $\gamma_4 = lc(\mu_1(\gamma_3 x)) = lc(\mu_1) \gamma_3^{\deg \mu_1}$, получаем, что

$$\begin{aligned} \Omega_4 &= \Gamma_{2, \frac{1}{\gamma_4}}(\Omega_3) = \Gamma_{2, \frac{1}{\gamma_4}} \circ \Gamma_{1, \gamma_3} \circ \Gamma_{7, \frac{1}{\gamma_2}} \circ \Gamma_{8, \gamma_1}(\Omega) = \\ &= \left(\frac{1}{\gamma_4} \mu_1(\gamma_3 x), \frac{\gamma_1}{\gamma_2 \gamma_4} \mu_2(\gamma_3 x), \frac{\gamma_1}{\gamma_2^2} d_1(\gamma_3 x), \frac{1}{\gamma_1} d_2(\gamma_3 x), \frac{\gamma_1 \gamma_3^m}{\gamma_2^2 \gamma_4} b \right), \end{aligned}$$

удовлетворяет условию леммы. Второй случай рассматривается аналогично. Лемма доказана. $\square$

Аналогично предыдущей лемме выводится следующее утверждение.

ЛЕММА 3. Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение Ω обобщённого норменного уравнения над k , тогда для данного m существует решение с набором из 4 коэффициентов, указанных ниже, равных 1 при условии, что в Ω указанные коэффициенты не обращаются в 0, причём указанное решение может быть получено из Ω помощью допустимых преобразований над k . Возможны следующие наборы из 4 коэффициентов.

1. a_i, a_t, b_j, h_k ;

2. $a_i, a_t, b_j, f_k;$

3. $b_i, b_t, a_j, h_k;$

4. $b_i, b_t, a_j, f_k;$

5. $f_i, f_t, b_j, a_k;$

6. $h_i, h_t, b_j, a_k;$

ДОКАЗАТЕЛЬСТВО. Доказательство этой леммы проводится по аналогии с доказательством леммы 2 и рассуждениям из работы [12]. $\square$

5. Доказательство основных результатов

ДОКАЗАТЕЛЬСТВО. По Теореме 4 для того, чтобы $\sqrt{f}$ был периодичен необходимо и достаточно найти решение уравнения (1) для наименьшего m , удовлетворяющего условиям теоремы 1 и теоремы 2. Из доказательства теоремы 4 нетрудно видеть, что если степень фундаментальной S -единицы — чётная, то она равна $2m$, а $\deg d_i > 0$ для $i = 1, 2$. При этом, если степень S -единицы нечётная, то без ограничения общности $\deg d_1 = 0$.

Таким образом, по теореме 4 необходимо и достаточно исследовать конечность числа решений уравнения (1). Что эквивалентно исследованию системы алгебраических уравнений на коэффициенты μ_1, μ_2, d_1, d_2 , построенных по (1), для следующих значений $\deg d_1$ и m :

$$\deg d_1 = 0, m = 5, 7, 9, 11; \deg d_1 = 1, m = 4, 6, 8; \deg d_1 = 2, m = 5, 7, 9. \quad (4)$$

Отметим, что конечность числа решений для $m = 11, \deg d_1 = 0$ была получена в [12] с использованием базисов Грёбнера, а случаи $m \leq 3$, т.е. случай нечетной степени фундаментальной S -единицы ≤ 3 или четной ≤ 6 , не могут давать нужных нам решений за исключением тривиального случая $m = 3, \deg d_1 = 0$, описанного, например, в [18].

Пусть $d_2 = f_0^2 + f_1x + f_2x^2 + f_3x^3$, где f_2, f_3 быть может, принимают нулевые значения. Ясно, что $f_0 \neq 0$, поскольку многочлен f должен иметь ненулевое свободное слагаемое. Далее отмечаем, что $h_0 \neq 0$, так как в противном случае согласно соотношению (1) мы легко приходим к тому, что степень соответствующей S -единицы строго меньше $2m$.

Аналогичным образом мы показываем, что в уравнении (2) для каждого из случаев $\deg \lambda_2 = m - (2g + 1)$ или что тоже самое $lc(\lambda_2) \neq 0$. Предположим обратное, $lc(\lambda_2) = 0$. Тогда согласно Лемме 2 пункту 1, существует решение системы нормального уравнения с $h_0 = f_0 = lc(\mu_1) = f_1 = 1$ или же $h_0 = f_0 = lc(\mu_1) = 1$ и $f_1 = 0$ над полем $\bar{k}$. Однако, базис Грёбнера этих систем сводится к ненулевой константе, что эквивалентно отсутствию решений. Итак, это означает, что $lc(\mu_2) \neq 0$.

Можно показать, что не существует решений системы в случае, когда $f_1 = 0$, что позволяет нам положить $f_1 \neq 0$. Действительно, в противном случае, согласно Лемме 3 существует решение над полем $\bar{k}$ с $f_1 = 0$ системы нормального уравнения с инициализированной четверкой из пункта 3) леммы при

$$b_0 = lc(\mu_2) = a_0 = h_0 = 1. \quad (5)$$

Однако же базис Грёбнера этой системы почти для каждой пары $(\deg d_1, m)$ из перечня (4) при условии (5) состоит из единицы, что равносильно отсутствию решений. Поэтому, в каждом из этих случаев $f_1 \neq 0$. Случаи, где указанное рассуждение избыточно, или базис Грёбнера отличен от единицы, отмечены и разобраны отдельно.

Для каждой из исследуемых систем обобщённого норменного уравнения соответствующих парам из перечня (4) применим R -процедуру, описанную в параграфе §3.1 так, чтобы процедура последовательного исключения переменных для каждой из систем приводила к многочлену не более чем одной переменной в качестве результата последней пары многочленов. С помощью вычислений в системах компьютерной алгебры SageMath и Magma можно показать, что для каждой из систем всякой переменной этой системы можно сопоставить многочлен от этой переменной, полученный применением вышеуказанной R -процедуры. Это позволяет сделать вывод о конечности числа решений изначальной системы, а, как следствие, о конечности различных неэквивалентных многочленов f с периодическим разложением $\sqrt{f}$ для полей, содержащих фундаментальную S -единицу соответствующей степени.

Поле L содержит фундаментальную S -единицу степени 5

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 1, 1, 5)$. Согласно схеме предложенной выше мы делаем вывод, что $h_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Отсюда и из вида обобщенного норменного уравнения следует что и $a_0 \neq 0$. Далее, из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_1 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует, откуда без ограничения общности полагаем $f_1 \neq 0$.

Поэтому подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_1 = 1$ получаем систему из 4 уравнений с 4 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -2a_0a_1 + b_0^2 + 2b_0 = 0 \\ b_0^2f_2 - a_1^2 + 2b_0 + 1 = 0 \\ b_0^2f_3 + 2b_0f_2 + 1 = 0 \\ 2b_0f_3 + f_2 = 0 \end{cases} \quad (6)$$

После исключения a_0 из первого уравнения, заменяя a_1 на $-1/2b_0 - 1$, а также избавляясь от b_0 из второго уравнения получим систему из трех уравнений с 3 неизвестными.

$$\begin{cases} b_0f_2 - 1/4b_0 + 1 = 0 \\ b_0^2f_3 + 2b_0f_2 + 1 = 0 \\ 2b_0f_3 + f_2 = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (11) существует единственное интересующее нас решение, а именно: $f_3 = 3/16, f_2 = -1/2, f_0 = 1, a_0 = -4/3, f_1 = 1, d_0 = 4/3, d_1 = 1, a_1 = -5/3$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S -единицу степени 7

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 2, 2, 7)$.

Пусть как и раньше

$$\begin{aligned} d_1 &= 1, d_2 = f_3x^3 + f_2x^2 + f_1x + f_0^2, \\ \mu_1 &= a_2x^2 + a_1x + a_0, \mu_2 = b_2x^2 + b_1x + b_0. \end{aligned}$$

Откуда исходная система обобщенного норменного уравнения выглядит следующим образом

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2b_0 b_1 f_0^2 + b_0^2 f_1 - 2a_0 a_1 = 0 \\ b_1^2 f_0^2 + 2b_0 b_2 f_0^2 + 2b_0 b_1 f_1 + b_0^2 f_2 - a_1^2 - 2a_0 a_2 = 0 \\ 2b_1 b_2 f_0^2 + b_1^2 f_1 + 2b_0 b_2 f_1 + 2b_0 b_1 f_2 + b_0^2 f_3 - 2a_1 a_2 = 0 \\ b_2^2 f_0^2 + 2b_1 b_2 f_1 + b_1^2 f_2 + 2b_0 b_2 f_2 + 2b_0 b_1 f_3 - a_2^2 = 0 \\ b_2^2 f_1 + 2b_1 b_2 f_2 + b_1^2 f_3 + 2b_0 b_2 f_3 = 0 \\ b_2^2 f_2 + 2b_1 b_2 f_3 = 0. \end{cases}$$

Отдельно обосновываем, что не существует решений с $f_1 = 0$.

Действительно, в противном случае, согласно Лемме 3 существует решение над полем $\bar{k}$ с $f_1 = 0$ системы норменного уравнения с инициализированной четверкой из пункта 3) леммы при

$$b_0 = lc(\mu_2) = a_0 = h_0 = 1. \quad (7)$$

Однако же базис Грёбнера этой системы состоит из единицы, что равносильно отсутствию решений. Поэтому $f_1 \neq 0$. Далее применим Лемму 2 пункт , и положим $f_0 = f_1 = b_2 = 1$. Далее, мы можем выразить переменные a_0, a_1 через остальные. Подставив в систему их выражения $a_0 = -b_0, a_1 = -1/2d_0 - d_1, a_2 = -1/2b_0 f_2 + 1/8b_0 - 1/2b_1 - 1$, получаем систему из 4 уравнений и 4 неизвестных:

$$\begin{cases} -1/2b_0 f_2 + b_1 f_2 + b_0 f_3 + 1/8b_0 - 1/4b_1 + 1 = 0 \\ -1/4b_0^2 f_2^2 + 1/8b_0^2 f_2 - 1/2b_0 b_1 f_2 + b_1^2 f_2 + \\ + 2b_0 b_1 f_3 - 1/64b_0^2 + 1/8b_0 b_1 - 1/4b_1^2 + b_0 f_2 + 1/4b_0 + b_1 = 0 \\ b_1^2 f_3 + 2b_1 f_2 + 2b_0 f_3 + 1 = 0 \\ 2b_1 f_3 + f_2 = 0. \end{cases}$$

Из последнего уравнения видно, что переменную f_2 можно исключить из системы. Ее значение определяется однозначно из набора остальных переменных. Вычисляя последовательные результаты по R -процедуре из §3.1 для каждой из переменных b_0, b_1, f_3 мы получаем такое следствие:

$$\begin{cases} (3b_0 - 64)b_0^9(225b_0^2 - 816b_0 + 256)^2 = 0 \\ (3b_1 + 4)^2(3b_1 - 4)^3b_1^5(45b_1^2 - 204b_1 + 80) = 0 \\ (8f_3 - 3)^2(16f_3 - 3)^3f_3^6(256f_3^2 + 1968f_3 - 45) = 0 \end{cases} \quad (8)$$

При вычислениях результата по процедуре из параграфа 3.1, приводящих к многочленам от переменной f_2 и f_3 , мы получаем в процессе R -процедуры один нетривиальный общий множитель равный f_3^2 . Сокращение на него в обоих случаях корректно, так как в силу $\deg d_2 = 3$ мы заключаем, что $f_3 \neq 0$.

При вычислении результата, приводящему к многочлену от переменной b_0 , мы получаем в процессе два нетривиальных общих множителя равные $f_3^2, 4b_0 f_3^2 - b_0^2 f_2^2$. Сокращение второй множитель корректно, так как базис Грёбнера исходной системы дополненной этим уравнением дает помимо прочего многочлен b_0 . Он не может быть равен нулю в нашем случае для нашей задачи.

При вычислении результата, приводящему к многочленам от переменной b_1 мы не получаем в процессе нетривиальных общих множителей отличных от константы, в этом случае сокращений не возникает.

Нетрудно видеть, что система (8) имеет не более одного с точностью до инволюции поля констант интересующего нас решения над каким-либо полем k , являющимся квадратичным расширением $\mathbb{Q}$. Причём единственное решение с $b_0 \neq 0$ с точностью до инволюции поля $\mathbb{Q}(\sqrt{21})$, меняющей знак у $\sqrt{21}$, она имеет тогда и только тогда, когда $\mathbb{Q}(\sqrt{21}) \subset k$, а именно

$$f_3 = \frac{27\sqrt{21} - 123}{32}, \quad f_2 = \frac{-3\sqrt{21} + 13}{4}, \quad b_1 = \frac{6\sqrt{21} + 34}{15}, \quad b_0 = \frac{24\sqrt{21} + 136}{75}.$$

Указанное решение позволяет построить многочлен $f \in \mathbb{Q}(\sqrt{21})[x]$ с периодическим разложением $\sqrt{f} \in \mathbb{Q}(\sqrt{21})((x))$:

$$f = \frac{27\sqrt{21} - 123}{32}x^3 - \frac{3\sqrt{21} - 13}{4}x^2 + x + 1.$$

В заключение отметим, что в силу (8) каждая из исследуемых переменных b_0, b_1, f_2, f_3 может принимать не более чем конечное число значений для любого поля k . Для каждой переменной это число не превосходит степени соответствующего многочлена в системе (8).

Поле L содержит фундаментальную S -единицу степени 9

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 3, 3, 9)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 10 уравнений и 13 неизвестных.

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2b_0 b_1 f_0^2 + b_0^2 f_1 - 2a_0 a_1 = 0 \\ b_1^2 f_0^2 + 2b_0 b_2 f_0^2 + 2b_0 b_1 f_1 + b_0^2 f_2 - a_1^2 - 2a_0 a_2 = 0 \\ 2b_1 b_2 f_0^2 + 2b_0 b_3 f_0^2 + b_1^2 f_1 + 2b_0 b_2 f_1 + 2b_0 b_1 f_2 + b_0^2 f_3 - 2a_1 a_2 - 2a_0 a_3 = 0 \\ b_2^2 f_0^2 + 2b_1 b_3 f_0^2 + 2b_1 b_2 f_1 + 2b_0 b_3 f_1 + b_1^2 f_2 + 2b_0 b_2 f_2 + 2b_0 b_1 f_3 - a_2^2 - 2a_1 a_3 = 0 \\ 2b_2 b_3 f_0^2 + b_2^2 f_1 + 2b_1 b_3 f_1 + 2b_1 b_2 f_2 + 2b_0 b_3 f_2 + b_1^2 f_3 + 2b_0 b_2 f_3 - 2a_2 a_3 = 0 \\ b_3^2 f_0^2 + 2b_2 b_3 f_1 + b_2^2 f_2 + 2b_1 b_3 f_2 + 2b_1 b_2 f_3 + 2b_0 b_3 f_3 - a_3^2 = 0 \\ b_3^2 f_1 + 2b_2 b_3 f_2 + b_2^2 f_3 + 2b_1 b_3 f_3 = 0 \\ b_3^2 f_2 + 2b_2 b_3 f_3 = 0 \\ b_3^2 f_3 + c = 0 \end{cases}$$

Воспользуемся Леммой 3, подставим в систему норменного уравнения $b_3 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 9 уравнений и 9 неизвестных:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -2a_0 a_1 + b_0^2 + 2b_0 b_1 = 0 \\ b_0^2 f_2 - a_1^2 - 2a_0 a_2 + 2b_0 b_1 + b_1^2 + 2b_0 b_2 = 0 \\ 2b_0 b_1 f_2 + b_0^2 f_3 - 2a_1 a_2 - 2a_0 a_3 + b_1^2 + 2b_0 b_2 + 2b_1 b_2 + 2b_0 = 0 \\ b_1^2 f_2 + 2b_0 b_2 f_2 + 2b_0 b_1 f_3 - a_2^2 - 2a_1 a_3 + 2b_1 b_2 + b_2^2 + 2b_0 + 2b_1 = 0 \\ 2b_1 b_2 f_2 + b_1^2 f_3 + 2b_0 b_2 f_3 - 2a_2 a_3 + b_2^2 + 2b_0 f_2 + 2b_1 + 2b_2 = 0 \\ b_2^2 f_2 + 2b_1 b_2 f_3 - a_3^2 + 2b_1 f_2 + 2b_0 f_3 + 2b_2 + 1 = 0 \\ b_2^2 f_3 + 2b_2 f_2 + 2b_1 f_3 + 1 = 0 \\ 2b_2 f_3 + f_2 = 0 \end{cases}$$

Отметим, что в случае $f_1 = 0$ базис Грёбнера дает нулевую размерность данной системы. Решение построенное по этому базису дает многочлен $2x^3 + 1$, принадлежащий тривиальной серии, в нашем случае он интереса не представляет, поскольку соответствует степени S -единицы равной трем.

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражения: $a_0 = -b_0$, $a_1 = -\frac{1}{2}b_0 - b_1$, $a_2 = -\frac{1}{2}b_0f_2 + \frac{1}{8}b_0 - \frac{1}{2}b_1 - b_2$, $a_3 = \frac{1}{4}(b_0 - 2b_1)f_2 - \frac{1}{2}b_0f_3 - \frac{1}{16}b_0 + \frac{1}{8}b_1 - \frac{1}{2}b_2 - 1$, В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении

$$-\frac{1}{64}(16b_0f_2^2 - 24b_0f_2 + 32b_1f_2 - 64b_2f_2 + 32b_0f_3 - 64b_1f_3 + 5b_0 - 8b_1 + 16b_2 - 64)b_0 = 0.$$

После преобразования получается система из 5 уравнений от переменных b_2, f_3, b_1, f_2, b_0 :

$$\begin{cases} -\frac{1}{4}b_0f_2^2 + \frac{3}{8}b_0f_2 - \frac{1}{2}b_1f_2 + b_2f_2 - \frac{1}{2}b_0f_3 + b_1f_3 - \frac{5}{64}b_0 + \frac{1}{8}b_1 - \frac{1}{4}b_2 + 1 = 0 \\ \frac{1}{4}b_0^2f_2^2 - \frac{1}{2}b_0b_1f_2^2 - \frac{1}{2}b_0^2f_2f_3 - \frac{1}{8}b_0^2f_2 + \frac{1}{2}b_0b_1f_2 - \frac{1}{2}b_1^2f_2 + b_1b_2f_2 + \frac{1}{8}b_0^2f_3 - \frac{1}{2}b_0b_1f_3 + \\ + b_1^2f_3 + b_0b_2f_3 + \frac{1}{64}b_0^2 - \frac{3}{32}b_0b_1 + \frac{1}{8}b_1^2 - \frac{1}{4}b_1b_2 + b_0f_2 + \frac{1}{4}b_0 + b_1 = 0 \\ -\frac{1}{16}b_0^2f_2^2 + \frac{1}{4}b_0b_1f_2^2 - \frac{1}{4}b_1^2f_2^2 + \frac{1}{4}b_0^2f_2f_3 - \frac{1}{2}b_0b_1f_2f_3 - \frac{1}{4}b_0^2f_3^2 + \frac{1}{32}b_0^2f_2 - \\ -\frac{1}{8}b_0b_1f_2 + \frac{1}{8}b_1^2f_2 + \frac{1}{4}b_0b_2f_2 - \frac{1}{2}b_1b_2f_2 + b_2^2f_2 - \frac{1}{16}b_0^2f_3 + \frac{1}{8}b_0b_1f_3 - \frac{1}{2}b_0b_2f_3 + 2b_1b_2f_3 - \\ -\frac{1}{256}b_0^2 + \frac{1}{64}b_0b_1 - \frac{1}{64}b_1^2 - \frac{1}{16}b_0b_2 + \frac{1}{8}b_1b_2 - \frac{1}{4}b_2^2 + \frac{1}{2}b_0f_2 + b_1f_2 + b_0f_3 - \frac{1}{8}b_0 + \frac{1}{4}b_1 + b_2 = 0 \\ b_2^2f_3 + 2b_2f_2 + 2b_1f_3 + 1 = 0 \\ 2b_2f_3 + f_2 = 0 \end{cases}$$

При вычислении R-процедуры для переменной b_2 было проведено сокращение на общий множитель $b_0^2 \cdot b_2^2 \cdot (-48b_2^2 - 112b_2 + b_0 - 64)^2$.

При вычислении R-процедуры для переменной f_3 было проведено сокращение на следующие общие множители: $f_3^2, f_3^6 \cdot (4f_3^2b_0 + 8f_3 - 3)^2$.

При вычислении R-процедуры для переменной b_1 было проведено сокращение на следующие общие множители: $f_2 \cdot (4f_2 - 1), f_2, b_0^6$.

При вычислении R-процедуры для переменной f_2 было проведено сокращение на следующие общие множители: $f_2 \cdot (4f_2 - 1), f_2, b_0^3 \cdot (4f_2 - 1)^4$.

При вычислении R-процедуры для переменной b_0 было проведено сокращение на следующие общие множители: $f_2 \cdot (4f_2 - 1), f_2, b_0^3 \cdot (4f_2 - 1)^4$. В каждом из этих случаев, базис Гребнера системы дополненный каждым из этих общих множителей, сводится к ненулевой константе. Тем самым мы обосновываем корректность сокращения на общий множитель и поэтому вышеуказанные сокращения корректны. Вычисляя последовательные результаты по R-процедуре из §3.1 для каждой из переменных b_2, f_3, b_1, f_2, b_0 , мы получаем в качестве следствия систему из 5 уравнений и 5 неизвестных. В силу большой рациональной высоты коэффициентов, мы приводим данные многочлены в сокращенном виде, указывая лишь переменную и степень неприводимых сомножителей. Как и ранее мы обозначаем через $P_{x,k}$ некоторый неприводимый над $\mathbb{Q}$ многочлен от переменной x степени k .

$$\begin{cases} (3b_2 - 4)b_2(45b_2^2 - 204b_2 + 80)P_{b_2,3}P_{b_2,55} = 0 \\ (16f_3 - 3)f_3(256f_3^2 + 1968f_3 - 45)P_{f_3,3}P_{f_3,46} = 0 \\ (b_1 - 32)(3b_1 - 64)b_1(225b_1^2 - 816b_1 + 256)P_{b_1,3}P_{b_1,8}P_{b_1,10}P_{b_1,11}P_{b_1,14}P_{b_1,15}^* \\ *P_{b_1,66}P_{b_1,90}P_{b_1,92}P_{b_1,112} = 0 \\ (4f_2 - 3)f_2(2f_2 + 1)(4f_2 - 1)(4f_2^2 - 26f_2 - 5)^* \\ *P_{f_2,3}P_{f_2,11}P_{f_2,14}P_{f_2,15}P_{f_2,37}P_{f_2,48}P_{f_2,54}P_{f_2,69} = 0 \\ (b_0 - 64)b_0P_{b_0,3}P_{b_0,11}P_{b_0,14}P_{b_0,15}P_{b_0,37}P_{b_0,48}P_{b_0,54}P_{b_0,69} = 0 \end{cases} \quad (9)$$

Из полученной системы мы извлекаем отсутствие нетривиальных решений над произвольным полем k у которого степень расширения над $\mathbb{Q}$ не более 2. Этот случай мы тоже разобрали.

В заключение отметим, что в силу (9) каждая из исследуемых переменных f_2, d_0, f_3, d_2, d_1 может принимать не более чем конечное число значений для любого поля k ,

Поле L содержит фундаментальную S -единицу степени 11

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 4, 4, 11)$. Как отмечалось выше этот случай был разобран в [12] с использованием базисов Грёбнера. При вычислении базиса Грёбнера соответствующей системы, нетрудно видеть, что для поля k , являющегося конечным расширением поля $\mathbb{Q}$ степени не более 2, интересующих нас решений не существует.

Поле L содержит фундаментальную S -единицу степени 8

В данном случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 0, 1, 4)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_1 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует.

Поэтому подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_1 = 1$ получаем систему из 4 уравнений с 4 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 + b_0^2 + 2b_0 = 0 \\ b_0^2 f_2 + 2b_0 + 1 = 0 \\ 2b_0 f_2 + 1 = 0 \end{cases} \quad (10)$$

После исключения a_0 из первого уравнения получим систему из трех уравнений с 3 неизвестными.

$$\begin{cases} -b_0 h_1 + b_0 + 2 = 0 \\ b_0^2 f_2 + 2b_0 + 1 = 0 \\ 2b_0 f_2 + 1 = 0 \end{cases}$$

После упрощения мы получаем такую систему.

$$\begin{cases} f_2(4f_2 - 3) = 0 \\ h_1 + 2 = 0 \\ b_0(3b_0 + 2) = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (10) существует единственное интересующее нас решение, а именно: $f_2 = 3/4, a_0 = 2/3, b_0 = -2/3, h_1 = -2$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S -единицу степени 10

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 0, 2, 5)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 6 уравнений и

9 неизвестных.

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2b_0 b_1 f_0^2 + b_0^2 f_1 - a_0^2 h_1 = 0 \\ b_1^2 f_0^2 + 2b_0 b_2 f_0^2 + 2b_0 b_1 f_1 - a_0^2 h_2 = 0 \\ 2b_1 b_2 f_0^2 + b_1^2 f_1 + 2b_0 b_2 f_1 = 0 \\ b_2^2 f_0^2 + 2b_1 b_2 f_1 = 0 \\ b_2^2 f_1 + c = 0 \end{cases} \quad (11)$$

Воспользуемся Леммой 2, подставим в систему норменного уравнения $b_2 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 5 уравнений и 5 неизвестных:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 + b_0^2 + 2b_0 b_1 = 0 \\ -a_0^2 h_2 + 2b_0 b_1 + b_1^2 + 2b_0 = 0 \\ b_1^2 + 2b_0 + 2b_1 = 0 \\ 2b_1 + 1 = 0 \end{cases}$$

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражение $a_0 = -b_0$. В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении $-(b_0 h_1 - b_0 - 2b_1)b_0 = 0$

После преобразования получается система из 4 уравнений от переменных h_2, h_1, b_1, b_0 :

$$\begin{cases} -b_0 h_1 + b_0 + 2b_1 = 0 \\ -b_0^2 h_2 + 2b_0 b_1 + b_1^2 + 2b_0 = 0 \\ b_1^2 + 2b_0 + 2b_1 = 0 \\ 2b_1 + 1 = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (11) существует единственное решение: $h_2 = 40/9, f_0 = 1, a_0 = -3/8, f_1 = 1, b_1 = -1/2, b_0 = 3/8, h_1 = -5/3, b_2 = 1$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S -единицу степени 12

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 1, 2, 6)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_2 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует, откуда без ограничения общности полагаем $f_1 \neq 0$.

Подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_2 = 1$ получаем систему из 6 уравнений с 6 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 - 2a_0 a_1 + b_0^2 + 2b_0 b_1 = 0 \\ b_0^2 f_2 - 2a_0 a_1 h_1 - a_1^2 + 2b_0 b_1 + b_1^2 + 2b_0 = 0 \\ 2b_0 b_1 f_2 - a_1^2 h_1 + b_1^2 + 2b_0 + 2b_1 = 0 \\ b_1^2 f_2 + 2b_0 f_2 + 2b_1 + 1 = 0 \\ 2b_1 f_2 + 1 = 0. \end{cases} \quad (12)$$

Заметим, что можно избавиться от переменных a_0 и b_1 из первого и пятого уравнения. Исключая их после упрощения мы получаем систему из 4 неизвестных.

$$\begin{cases} 3/4b_0h_1^2 + b_0f_2 - 1/2b_0h_1 - b_1h_1 - 1/4b_0 + b_1 + 2 = 0 \\ -1/4b_0^2h_1^3 + 1/2b_0^2h_1^2 + b_0b_1h_1^2 + 2b_0b_1f_2 - 1/4b_0^2h_1 - b_0b_1h_1 - b_1^2h_1 + b_1^2 + 2b_0 + 2b_1 = 0 \\ b_1^2f_2 + 2b_0f_2 + 2b_1 + 1 = 0 \\ 2b_1f_2 + 1 = 0. \end{cases} \quad (13)$$

Вычисляя последовательные результаты по R -процедуре для каждой из текущих переменных b_0, b_1, f_2, h_1 мы получаем такое следствие:

$$\begin{cases} (3b_1 + 2)b_1(5b_1^3 + 6b_1^2 + 12b_1 + 8) = 0 \\ h_1^2(h_1 + 2)(h_1 - 1)(h_1^3 + 6h_1^2 + 6h_1 + 2) = 0 \\ (25b_0^3 + 156b_0^2 + 240b_0 - 32) = 0 \\ (4f_2 - 3)f_2(64f_2^3 - 48f_2^2 + 12f_2 - 5) = 0. \end{cases} \quad (14)$$

При вычислениях результата в ходе R -преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на нетривиальные общий множитель f_2 или его степени. Сокращение в каждом из случаев корректно, так как $f_2 \neq 0$. Это обосновывает корректность сокращения в ходе R -процедуры. Отметим, что в силу (14) каждая из исследуемых переменных b_0, b_1, h_1, f_2 может принимать не более чем конечное число значений для любого поля k , а для случая поля квадратичного поля k или поля $k = \mathbb{Q}$ нетрудно видеть, что система (14) не имеет решений.

Поле L содержит фундаментальную S -единицу степени 14

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 1, 3, 7)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_2 \neq 0$. В силу того, что $\deg d_2 = 1$, заключаем, что $f_1 \neq 0$.

Поэтому подставляя согласно Лемме 2 значения $h_0 = f_1 = 1, f_0 = 1, b_2 = 1$ получаем систему из 7 уравнений с 7 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2h_1 - 2a_0a_1 + b_0^2 + 2b_0b_1 = 0 \\ -2a_0a_1h_1 - a_0^2h_2 - a_1^2 + 2b_0b_1 + b_1^2 + 2b_0b_2 = 0 \\ -a_1^2h_1 - 2a_0a_1h_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ -a_1^2h_2 + 2b_1b_2 + b_2^2 + 2b_0 + 2b_1 = 0 \\ b_2^2 + 2b_1 + 2b_2 = 0 \\ 2b_2 + 1 = 0 \end{cases} \quad (15)$$

Заменяя a_0 на b_0 и заменяя a_1 на $1/2b_0h_1 - 1/2b_0 - b_1$ и после упрощения мы получаем систему от 5 неизвестных.

$$\begin{cases} 3/4b_0h_1^2 - 1/2b_0h_1 - b_1h_1 - b_0h_2 - 1/4b_0 + b_1 + 2b_2 = 0 \\ -1/4b_0^2h_1^3 + 1/2b_0^2h_1^2 + b_0b_1h_1^2 + b_0^2h_1h_2 - \\ -1/4b_0^2h_1 - b_0b_1h_1 - b_1^2h_1 - b_0^2h_2 - 2b_0b_1h_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ -1/4b_0^2h_1^2h_2 + 1/2b_0^2h_1h_2 + b_0b_1h_1h_2 - 1/4b_0^2h_2 - b_0b_1h_2 - b_1^2h_2 + 2b_1b_2 + d_2^2 + 2b_0 + 2d_1 = 0 \\ b_2^2 + 2b_1 + 2b_2 = 0 \\ 2b_2 + 1 = 0. \end{cases} \quad (16)$$

Переменные b_2, b_1 явно вычисляются. Вычисляя последовательные результаты по R -процедуре для каждой из текущих переменных мы получаем такое следствие:

$$\begin{cases} (h_2 - 40)h_2(9h_2 - 40)(2025h_2^3 - 39816h_2^2 + 210112h_2 - 75264) \cdot \\ \cdot (1866240000h_2^9 - 55205712000h_2^8 + 606471399225h_2^7 - 3130271733456h_2^6 + \\ + 8727283377792h_2^5 - 18049927509504h_2^4 + 34435309195264h_2^3 - \\ - 34230846619648h_2^2 - 178494898176h_2 + 1040449536000) = 0 \\ (h_1 - 1)(3h_1 + 5)(45h_1^3 + 273h_1^2 + 791h_1 + 427) = 0 \\ (13824b_0^3 - 92096b_0^2 - 7416b_0 - 405) = 0 \end{cases} \quad (17)$$

При вычислениях результата в ходе R -преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на многочлены, которые не обнуляются на множестве решений системы, что обосновывает корректность сокращения в ходе R -процедуры. Для случая квадратичного поля k или случая $k = \mathbb{Q}$ нетрудно видеть, что последняя система не имеет нетривиальных решений.

Поле L содержит фундаментальную S -единицу степени 16

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 2, 3, 8)$

Ясно, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$, иначе сокращая на x в (1) заключаем, что степень единицы должна быть строго меньше 16. Из сравнения степеней левой и правой частей (1) и теоремы 4 нетрудно видеть, что $lc(\mu_2) = b_3 \neq 0$. Как отмечалось выше, в условиях теоремы 1 и тем более теоремы 2 не существует решений системы с $f_1 = 0$, откуда без ограничения общности полагаем $f_1 \neq 0$.

Воспользуемся Леммой 2, подставим в систему норменного уравнения $f_1 = 1, f_0 = 1, b_3 = 1, h_0 = 1$ и получим следующие уравнения:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2h_1 - 2a_0a_1 + b_0^2 + 2b_0b_1 = 0 \\ b_0^2f_2 - 2a_0a_1h_1 - a_1^2 - 2a_0a_2 + 2b_0b_1 + b_1^2 + 2b_0b_2 = 0 \\ 2b_0b_1f_2 - a_1^2h_1 - 2a_0a_2h_1 - 2a_1a_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ b_1^2f_2 + 2b_0b_2f_2 - 2a_1a_2h_1 - a_2^2 + 2b_1b_2 + b_2^2 + 2b_0 + 2b_1 = 0 \\ 2b_1b_2f_2 - a_2^2h_1 + b_2^2 + 2b_0f_2 + 2b_1 + 2b_2 = 0 \\ b_2^2f_2 + 2b_1f_2 + 2b_2 + 1 = 0 \\ 2b_2f_2 + 1 = 0. \end{cases} \quad (18)$$

Из этой системы мы можем исключить переменные a_0, a_1, a_2 . Замены у нас получаются следующими: $a_0 = -b_0, a_1 = 1/2b_0h_1 - 1/2b_0 - b_1, a_2 = -3/8b_0h_1^2 - 1/2b_0f_2 + 1/4(b_0 + 2b_1)h_1 + 1/8b_0 -$

$-1/2b_1 - b_2$. После простого упрощения системы мы получаем эквивалентную систему от переменных b_0, b_1, b_2, h_1, f_2 .

$$\left\{ \begin{array}{l} -\frac{5}{8}b_0h_1^3 - \frac{1}{2}b_0f_2h_1 + \frac{3}{8}b_0h_1^2 + \frac{3}{4}b_1h_1^2 - \\ -\frac{1}{2}b_0f_2 + b_1f_2 + \frac{1}{8}b_0h_1 - \frac{1}{2}b_1h_1 - b_2h_1 + \frac{1}{8}b_0 - \frac{1}{4}b_1 + b_2 + 2 = 0 \\ \frac{15}{64}b_0^2h_1^4 + \frac{1}{8}b_0^2f_2h_1^2 - \frac{7}{16}b_0^2h_1^3 - \frac{7}{8}b_0b_1h_1^3 - \frac{1}{4}b_0^2f_2^2 - \frac{1}{4}b_0^2f_2h_1 - \frac{1}{2}b_0b_1f_2h_1 + \\ + \frac{5}{32}b_0^2h_1^2 + \frac{7}{8}b_0b_1h_1^2 + \frac{3}{4}b_1^2h_1^2 + \frac{1}{4}b_0b_2h_1^2 + \frac{1}{8}b_0^2f_2 - \frac{1}{2}b_0b_1f_2 + b_1^2f_2 + b_0b_2f_2 + \\ + \frac{1}{16}b_0^2h_1 - \frac{1}{8}b_0b_1h_1 - \frac{1}{2}b_1^2h_1 - \frac{1}{2}b_0b_2h_1 - b_1b_2h_1 - \frac{1}{64}b_0^2 + \frac{1}{8}b_0b_1 - \frac{1}{4}b_1^2 + \\ + \frac{1}{4}b_0b_2 + b_1b_2 + 2b_0 + 2b_1 = 0 \\ -\frac{9}{64}b_0^2h_1^5 - \frac{3}{8}b_0^2f_2h_1^3 + \frac{3}{16}b_0^2h_1^4 + \frac{3}{8}b_0b_1h_1^4 - \frac{1}{4}b_0^2f_2^2h_1 + \frac{1}{4}b_0^2f_2h_1^2 + \frac{1}{2}b_0b_1f_2h_1^2 + \frac{1}{32}b_0^2h_1^3 - \\ -\frac{5}{8}b_0b_1h_1^3 - \frac{1}{4}b_1^2h_1^3 - \frac{3}{4}b_0b_2h_1^3 + \frac{1}{8}b_0^2f_2h_1 - \\ -\frac{1}{2}b_0b_1f_2h_1 - b_0b_2f_2h_1 - \frac{1}{16}b_0^2h_1^2 + \frac{1}{8}b_0b_1h_1^2 + \frac{1}{2}b_1^2h_1^2 + \frac{1}{2}b_0b_2h_1^2 + b_1b_2h_1^2 + 2b_1b_2f_2 - \\ -\frac{1}{64}b_0^2h_1 + \frac{1}{8}b_0b_1h_1 - \frac{1}{4}b_1^2h_1 + \frac{1}{4}b_0b_2h_1 - b_1b_2h_1 - b_2^2h_1 + b_2^2 + 2b_0f_2 + 2b_1 + 2b_2 = 0 \\ b_2^2f_2 + 2b_1f_2 + 2b_2 + 1 = 0 \\ 2b_2f_2 + 1 = 0 \end{array} \right. \quad (19)$$

Применим R -преобразование системы. В каждом из случаев получается ненулевой многочлен от каждой из переменных, что завершает доказательств нашей теоремы. Выпишем уравнения, которые получились у нас в результате R -преобразования системы, причём вместо каждого многочлена мы выпишем лишь его радикал. Полученная система является следствием над $\overline{\mathbb{Q}}$ исходной системы. Обозначим через $P_{x,k}$ — некоторый многочлен от переменной x степени k .

$$\left\{ \begin{array}{l} b_0P_{b_0,6}P_{b_0,55}P_{b_0,107} = 0 \\ (h_1 + 2)h_1(h_1 - 1)P_{h_1,2}P_{h_1,3}P_{h_1,6}P_{h_1,20}P_{h_1,48} = 0 \\ (4f_2 - 3)(4f_2 - 1)f_2P_{f_2,2}P_{f_2,3}P_{f_2,6} = 0 \\ (b_2 + 2)(3b_2 + 2)b_2P_{b_2,2}P_{b_2,3}P_{b_2,6} = 0 \\ b_1(b_1 - 4)P_{b_1,2}P_{b_1,3}P_{b_1,6}P_{b_1,20}P_{b_1,48} = 0 \end{array} \right. \quad (20)$$

В силу ограничений объёма, мы не имеем возможности привести полный вид всех многочленов, входящих в систему (20). Приведём для примера несколько многочленов:

$$\begin{aligned} P_{b_0,6} &= 35162859375b_0^6 + 964070910000b_0^5 + 6924423153600b_0^4 - 5147602126848b_0^3 - \\ &- 48716872445952b_0^2 + 63203662036992b_0 + 674064760832; \\ P_{f_2,6} &= 76877824f_2^6 - 162641920f_2^5 + 102620928f_2^4 - 33014016f_2^3 + 8659440f_2^2 - 502200f_2 + 212625; \\ P_{b_2,6} &= 212625b_2^6 + 251100b_2^5 + 2164860b_2^4 + 4126752b_2^3 + 6413808b_2^2 + 5082560b_2 + 1201216; \\ P_{b_1,20} &= 8255648563200b_1^{20} - 182292029964288b_1^{19} + \\ &+ 3700176823118016b_1^{18} - 41672730322305792b_1^{17} + 220048281041334912b_1^{16} - \\ &- 274861679147380224b_1^{15} - 2622240588850487424b_1^{14} + 13231629527936646384b_1^{13} - \\ &- 17982425793551807808b_1^{12} - 35374972142113715184b_1^{11} + \\ &+ 167662143348451723824b_1^{10} - 267859272743637980872b_1^9 + 220469209547236109547b_1^8 - \\ &- 85941395765711763492b_1^7 - 150095028152499744b_1^6 + \\ &+ 11146097842624151552b_1^5 + 1592601206869000192b_1^4 + 44728120934137856b_1^3 - \\ &- 1174039007592448b_1^2 + 32358283608064b_1 - 549755813888. \end{aligned}$$

При вычислениях результата в ходе R -преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на нетривиальные общие множители: f_2, b_2, b_0 или произведения их степеней. Сокращение в каждом из случаев корректно, так как $b_0 \neq 0$ или базис Гребнера исходной системы, дополненный каждым из уравнений: $b_2 = 0$ и $f_2 = 0$, сводится к ненулевой константе. Это обосновывает корректность сокращения в ходе R -процедуры.

Также возникает сокращение на множитель b_1^2 . Вычисляя Базис Гребнера исходной системы дополненной каждым из этих уравнений, мы находим явно все решения. Эти решения не удовлетворяют условию $b_0 \neq 0$ и, следовательно, нам не подходят.

В заключение отметим, что в силу (20) каждая из исследуемых переменных b_0, b_1, b_2, h_1, f_2 может принимать не более чем конечное число значений для любого поля k , а для случая квадратичного поля k нетрудно видеть, что система (20) не имеет решений.

Поле L содержит фундаментальную S -единицу степени 18

В данном случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 2, 4, 9)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 10 уравнений и 13 неизвестных. Выпишем ее в явном виде.

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2b_0 b_1 f_0^2 + b_0^2 f_1 - a_0^2 h_1 - 2a_0 a_1 = 0 \\ b_1^2 f_0^2 + 2b_0 b_2 f_0^2 + 2b_0 b_1 f_1 - 2a_0 a_1 h_1 - a_0^2 h_2 - a_1^2 - 2a_0 a_2 = 0 \\ 2b_1 b_2 f_0^2 + 2b_0 b_3 f_0^2 + b_1^2 f_1 + 2b_0 b_2 f_1 - a_1^2 h_1 - 2a_0 a_2 h_1 - 2a_0 a_1 h_2 - 2a_1 a_2 = 0 \\ b_2^2 f_0^2 + 2b_1 b_3 f_0^2 + 2b_0 b_4 f_0^2 + 2b_1 b_2 f_1 + 2b_0 b_3 f_1 - 2a_1 a_2 h_1 - a_1^2 h_2 - 2a_0 a_2 h_2 - a_2^2 = 0 \\ 2b_2 b_3 f_0^2 + 2b_1 b_4 f_0^2 + b_2^2 f_1 + 2b_1 b_3 f_1 + 2b_0 b_4 f_1 - a_2^2 h_1 - 2a_1 a_2 h_2 = 0 \\ b_3^2 f_0^2 + 2b_2 b_4 f_0^2 + 2b_2 b_3 f_1 + 2b_1 b_4 f_1 - a_2^2 h_2 = 0 \\ 2b_3 b_4 f_0^2 + b_3^2 f_1 + 2b_2 b_4 f_1 = 0 \\ b_4^2 f_0^2 + 2b_3 b_4 f_1 = 0 \\ b_4^2 f_1 + c = 0 \end{cases}$$

Поскольку $\deg d_2 = 1$, то отсюда следует, что $f_1 \neq 0$. Поэтому можем воспользоваться Леммой 3, подставим в систему норменного уравнения $b_4 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 9 уравнений и 9 неизвестных:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 - 2a_0 a_1 + b_0^2 + 2b_0 b_1 = 0 \\ -2a_0 a_1 h_1 - a_0^2 h_2 - a_1^2 - 2a_0 a_2 + 2b_0 b_1 + b_1^2 + 2b_0 b_2 = 0 \\ -a_1^2 h_1 - 2a_0 a_2 h_1 - 2a_0 a_1 h_2 - 2a_1 a_2 + b_1^2 + 2b_0 b_2 + 2b_1 b_2 + 2b_0 b_3 = 0 \\ -2a_1 a_2 h_1 - a_1^2 h_2 - 2a_0 a_2 h_2 - a_2^2 + 2b_1 b_2 + b_2^2 + 2b_0 b_3 + 2b_1 b_3 + 2b_0 = 0 \\ -a_2^2 h_1 - 2a_1 a_2 h_2 + b_2^2 + 2b_1 b_3 + 2b_2 b_3 + 2b_0 + 2b_1 = 0 \\ -a_2^2 h_2 + 2b_2 b_3 + b_3^2 + 2b_1 + 2b_2 = 0 \\ b_3^2 + 2b_2 + 2b_3 = 0 \\ 2b_3 + 1 = 0 \end{cases}$$

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражения: $a_0 = -b_0, a_1 = \frac{1}{2} b_0 h_1 - \frac{1}{2} b_0 - b_1, a_2 = -\frac{3}{8} b_0 h_1^2 + \frac{1}{4} (b_0 + 2b_1) h_1 + \frac{1}{2} b_0 h_2 + \frac{1}{8} b_0 - \frac{1}{2} b_1 - b_2$. В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении $-\frac{1}{8} (5b_0 h_1^3 - 3b_0 h_1^2 - 6b_1 h_1^2 - 12b_0 h_1 h_2 - b_0 h_1 + 4b_1 h_1 + 8b_2 h_1 + 4b_0 h_2 + 8b_1 h_2 - b_0 + 2b_1 - 8b_2 - 16b_3) b_0 = 0$.

После преобразования получается система из 6 уравнений от переменных $h_2, b_0, h_1, b_3, b_2, b_1$:

$$\left\{ \begin{array}{l}
 -\frac{5}{8}b_0h_1^3 + \frac{3}{8}b_0h_1^2 + \frac{3}{4}b_1h_1^2 + \frac{3}{2}b_0h_1h_2 + \frac{1}{8}b_0h_1 - \frac{1}{2}b_1h_1 - b_2h_1 - \\
 -\frac{1}{2}b_0h_2 - b_1h_2 + \frac{1}{8}b_0 - \frac{1}{4}b_1 + b_2 + 2b_3 = 0 \\
 \frac{15}{64}b_0^2h_1^4 - \frac{7}{16}b_0^2h_1^3 - \frac{7}{8}b_0b_1h_1^3 - \frac{9}{8}b_0^2h_1^2h_2 + \frac{5}{32}b_0^2h_1^2 + \frac{7}{8}b_0b_1h_1^2 + \frac{3}{4}b_1^2h_1^2 + \frac{1}{4}b_0b_2h_1^2 + \\
 + \frac{5}{4}b_0^2h_1h_2 + \frac{5}{2}b_0b_1h_1h_2 + \frac{3}{4}b_0^2h_2^2 + \frac{1}{16}b_0^2h_1 - \frac{1}{8}b_0b_1h_1 - \frac{1}{2}b_1^2h_1 - \frac{1}{2}b_0b_2h_1 - b_1b_2h_1 - \frac{1}{8}b_0^2h_2 - \\
 - \frac{3}{2}b_0b_1h_2 - b_1^2h_2 - b_0b_2h_2 - \frac{1}{64}b_0^2 + \frac{1}{8}b_0b_1 - \frac{1}{4}b_1^2 + \frac{1}{4}b_0b_2 + b_1b_2 + 2b_0b_3 + 2b_1b_3 + 2b_0 = 0 \\
 -\frac{9}{64}b_0^2h_1^5 + \frac{3}{16}b_0^2h_1^4 + \frac{3}{8}b_0b_1h_1^4 + \frac{3}{4}b_0^2h_1^3h_2 + \frac{1}{32}b_0^2h_1^3 - \frac{5}{8}b_0b_1h_1^3 - \\
 -\frac{1}{4}b_1^2h_1^3 - \frac{3}{4}b_0b_2h_1^3 - \frac{7}{8}b_0^2h_1^2h_2 - \frac{7}{4}b_0b_1h_1^2h_2 - \frac{3}{4}b_0^2h_1h_2^2 - \frac{1}{16}b_0^2h_1^2 + \frac{1}{8}b_0b_1h_1^2 + \frac{1}{2}b_1^2h_1^2 + \\
 + \frac{1}{2}b_0b_2h_1^2 + b_1b_2h_1^2 + 2b_0b_1h_1h_2 + b_1^2h_1h_2 + 2b_0b_2h_1h_2 + \frac{1}{2}b_0^2h_2^2 + b_0b_1h_2^2 - \\
 -\frac{1}{64}b_0^2h_1 + \frac{1}{8}b_0b_1h_1 - \\
 -\frac{1}{4}b_1^2h_1 + \frac{1}{4}b_0b_2h_1 - b_1b_2h_1 - b_2^2h_1 + \frac{1}{8}b_0^2h_2 - \frac{1}{4}b_0b_1h_2 - b_1^2h_2 - b_0b_2h_2 - 2b_1b_2h_2 + b_2^2 + \\
 + 2b_1b_3 + 2b_2b_3 + 2b_0 + 2b_1 = 0 \\
 -\frac{9}{64}b_0^2h_1^4h_2 + \frac{3}{16}b_0^2h_1^3h_2 + \frac{3}{8}b_0b_1h_1^3h_2 + \frac{3}{8}b_0^2h_1^2h_2^2 + \\
 + \frac{1}{32}b_0^2h_1^2h_2 - \frac{5}{8}b_0b_1h_1^2h_2 - \frac{1}{4}b_1^2h_1^2h_2 - \frac{3}{4}b_0b_2h_1^2h_2 - \frac{1}{4}b_0^2h_1h_2^2 - \frac{1}{2}b_0b_1h_1h_2^2 - \frac{1}{4}b_0^2h_2^3 - \\
 -\frac{1}{16}b_0^2h_1h_2 + \frac{1}{8}b_0b_1h_1h_2 + \frac{1}{2}b_1^2h_1h_2 + \frac{1}{2}b_0b_2h_1h_2 + b_1b_2h_1h_2 - \frac{1}{8}b_0^2h_2^2 + \frac{1}{2}b_0b_1h_2^2 + b_0b_2h_2^2 - \\
 -\frac{1}{64}b_0^2h_2 + \frac{1}{8}b_0b_1h_2 - \frac{1}{4}b_1^2h_2 + \frac{1}{4}b_0b_2h_2 - b_1b_2h_2 - b_2^2h_2 + 2b_2b_3 + b_3^2 + 2b_1 + 2b_2 = 0 \\
 b_3^2 + 2b_2 + 2b_3 = 0 \\
 2b_3 + 1 = 0
 \end{array} \right. \quad (21)$$

Вычисление базиса Гребнера данной системы показывает нулевую размерность данной системы, что равносильно конечности числа решений в переменных $h_1, b_1, b_2, h_2, b_0, b_3$. Более того, у всех решений $b_0 = 0$, а следовательно, они нам не подходят. Кроме того, вычисление базиса Грёбнера показывает отсутствие нетривиальных решений над полем $\mathbb{Q}$ и над произвольным квадратичным расширением поля $\mathbb{Q}$. Доказательство теорем завершено.

6. Заключение

В работах [15, 16, 17] доказана ограниченность кручения в эллиптических кривых над квадратичными полями и дано описание возможных групп кручения. Из результатов работ, в частности следует, что в эллиптических полях над квадратичными полями реализуются все степени фундаментальных S -единиц до 18 включительно за исключением 17 и только они. С учётом теоремы 2, чтобы завершить доказательство конечности числа нетривиальных неэквивалентных периодических $\sqrt{f}$ над квадратичными полями в качестве поля констант, остаётся доказать конечность с точностью до отношения эквивалентности таких полей, обладающих фундаментальной S -единицей степени 13 и 15. Последнее, наряду с результатами компьютерных вычислений позволяет выдвинуть следующую гипотезу.

Гипотеза. Пусть k — квадратичное расширение поля $\mathbb{Q}$. Тогда существует универсальная константа C , не зависящая от поля k , такая, что существует не более C попарно неэквивалентных над k нетривиальных многочленов f , $\deg f = 3$, для которых $\sqrt{f}$ периодичен в $k((x))$.

□

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Abel N. H. Ueber die integration der differential-formel $\rho dx/\sqrt{R}$ wenn r und ρ ganze functionen sind. *Journal für die reine und angewandte Mathematik*, Vol. 1, P. 185–221, 1826.
2. Tchebicheff P. Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré' // *Journal des math. pures et appl.* 1857. Vol. 2. P. 168–192.
3. Платонов В. П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // *Успехи математических наук.* 2014. Т. 69:1, № 415. С. 3–38.
4. Schmidt W. M. On continued fractions and Diophantine approximation in power series fields // *Acta arithmetica.* 2000. Vol. 95, № 2. P. 139–166.
5. Adams W. W., Razar M. J. Multiples of points on elliptic curves and continued fractions // *Proceedings of the London Mathematical Society.* – 1980. – Vol. 41 – P. 481–498.
6. Платонов В. П., Петрунин М. М. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // *ДАН.* 2016. Т. 470, № 3. С. 260–265.
7. Платонов В. П., Петрунин М. М. S-единицы и периодичность в квадратичных функциональных полях // *УМН.* 2016. Т. 71, № 5. С. 181–182.
8. Петрунин М. М. S-единицы и периодичность квадратного корня в гиперэллиптических полях. 2017. // *Доклады Академии наук.* 2018. Т. 474, № 2. С. 155–158.
9. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в эллиптических полях // *Доклады Академии наук.* 2017. Т. 475, № 2. С. 133–136.
10. Платонов В. П., Федоров Г. В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях // *Математический сборник.* 2018. Т. 4, № 209. С. 54–94.
11. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях // *Доклады Академии наук.* 2017. Т. 474, № 5. С. 540–544.
12. Платонов В. П., Жгун В. С., Петрунин М. М., Штейников Ю.Н. О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // *Доклады Академии наук.* 2018. Т. 483, № 6. С. 603–608.
13. Платонов В. П., Жгун В. С., Федоров Г.В. О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант. // *Доклады Академии наук.* 2018. Т. 482, № 2. С. 137–141.
14. Беляш-Кривец В. В., Платонов В. П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // *Математический сборник.* 2009. Т. 200, № 11. С. 15–44.
15. Kenku M. A., Momose F. Torsion points on elliptic curves defined over quadratic fields // *Nagoya Mathematical Journal.* 1988. Vol. 109. P. 125–149.
16. Kamienny Sheldon. Torsion points on elliptic curves and q-coefficients of modular forms // *Inventiones mathematicae.* 1992. Vol. 109, № 1. P. 221–229.

17. Kamienny S., Najman F. Torsion groups of elliptic curves over quadratic fields // *Acta Arithmetica*. 2012. Vol. 3, № 152. P. 291–305.
18. Платонов В. П., Петрунин М.М. Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // *Труды МИАН*. 2018, Т. 302, С. 354–376.
19. Платонов В. П., Петрунин М. М., Штейников Ю. Н. О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // *Докл. РАН*. 2019, Т. 488, №3, С. 237–242.
20. Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, 24 (1997), 235–265.
21. SageMath, the Sage Mathematics Software System (Version 9.0), The Sage Developers, 2020, <https://www.sagemath.org>.
22. Mazur B. Rational isogenies of prime degree // *Inventiones Mathematicae*. 1978. № 2 (44). P. 129–162.

REFERENCES

1. Abel N. H. 1826, “Ueber die integration der differential-formel $\rho dx/\sqrt{R}$ wenn r und ρ ganze functionen sind”, *Journal für die reine und angewandte Mathematik*, vol. 1, pp. 185–221.
2. Tchebicheff P. 1857, “Sur l’intégration des différentielles qui contiennent une racine carrée d’un polynome du troisieme ou du quatrieme degré”, *Journal des math. pures et appl.*, vol. 2. pp. 168–192.
3. Platonov V. P. 2014, “Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field”, *Russian Math. Surveys*, vol. 69, no. 1. pp. 1–34.
4. Schmidt W. M. 2000, “On continued fractions and Diophantine approximation in power series fields”, *Acta arithmetica*, vol. 95, no. 2. pp. 139–166.
5. Adams, W.W., Razar, M.J., 1980. “Multiples of Points on Elliptic Curves and Continued Fractions”, *Proceedings of the London Mathematical Society*, vol. 41, pp. 481–498.
6. Platonov V. P., Petrunin M. M. 2016 “S-units in hyperelliptic fields and periodicity of continued fractions”, *Dokl. Math.*, vol. 94, no. 2. pp. 532–537.
7. Platonov V. P., Petrunin M. M. 2016. S-Units and periodicity in quadratic function fields *Russian Math. Surveys*, vol. 71, no. 5. стр. 973–975.
8. Petrunin M. M. 2017 “S-units and periodicity of square root in hyperelliptic fields”, *Dokl. Math.*, vol. 95, no. 3. pp. 222–225.
9. Platonov V. P., Fedorov G. V. 2017. “On the periodicity of continued fractions in elliptic fields”, *Dokl. Math.*, vol 96, no. 1. pp. 332–335.
10. Platonov V.P., Fedorov G.V. 2018, “On the problem of periodicity of continued fractions in hyperelliptic fields”, *Sb.Math.*, vol. 209, no. 4, pp. 519–559.
11. Platonov V. P., Fedorov G. V. 2017, “On the periodicity of continued fractions in hyperelliptic fields”, *Dokl. Math.*, vol. 95, no. 3. pp. 254–258.

12. Platonov V. P., Zhgoon V. S., Petrunin M. M., Shteinikov Yu. N. 2018, “On the finiteness of hyperelliptic fields with special properties and periodic expansion of $\sqrt{f}$ ”, *Dokl. Math.*, vol 98, pp. 603–608.
13. Platonov V.P., Zhgoon V.S., Fedorov G.V. 2018, “Continued rational fractions in hyperelliptic fields and the Mumford representation”, *Dokl. Math.*, vol. 482, no. 2. pp. 137–141.
14. Benyash-Krivets V.V., Platonov V.P. 2009, “Groups of S-units in hyperelliptic fields and continued fractions”, *Sb.Math.*, vol. 200, no.11, pp.1587–1615.
15. Kenku M. A., Momose F. 1988, “Torsion points on elliptic curves defined over quadratic fields”, *Nagoya Mathematical Journal*, vol. 109. pp. 125–149.
16. Kamienny S. 1992, “Torsion points on elliptic curves and q-coefficients of modular forms”, *Inventiones mathematicae*, vol. 109, no. 1. pp. 221–229.
17. Kamienny S., Najman F. 2012, “Torsion groups of elliptic curves over quadratic fields”, *Acta Arithmetica*, vol. 3, no. 152. pp. 291–305.
18. Platonov V. P., Petrunin M.M. 2018, “Groups of S-units and the problem of periodicity of continued fractions in hyperelliptic fields” *Proc. Steklov Inst. math.*, vol. 302, pp. 336–357.
19. Platonov V. P., Petrunin M. M., Shteinikov Yu. N. 2019, “On the finiteness of the number of elliptic fields with given degrees of S-units and periodic expansion of $\sqrt{f}$ ”, *Dokl. Math.*, vol. 100, no. 2, pp. 1–5.
20. Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, 24 (1997), 235–265.
21. SageMath, the Sage Mathematics Software System (Version 9.0), The Sage Developers, 2020, <https://www.sagemath.org>.
22. Mazur B. 1978, “Rational isogenies of prime degree (with appendix by Goldfeld D.)”, *Inventiones mathematicae*, vol. 44, no. 2, pp. 129–162.

Получено 27.01.2018 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 514.172.45

DOI 10.22405/2226-8383-2020-21-1-297-309

О полноте списка выпуклых RR -многогранников

В. И. Субботин

Субботин Владимир Иванович — кандидат физико-математических наук, доцент, Донской государственный аграрный университет (г. Новочеркасск).

e-mail: geometry@mail.ru

Аннотация

В статье дано доказательство полноты перечня одного класса выпуклых симметричных многогранников в трёхмерном евклидовом пространстве. Этот класс принадлежит классу так называемых RR -многогранников. RR -многогранники характеризуются следующими условиями симметрии: у каждого многогранника класса RR существуют симметричные ромбические вершины и существуют грани, не принадлежащие ни одной звезде этих вершин; причём каждая грань, не входящая в звезду ромбической вершины, является правильной. Ромбичность вершины здесь означает, что звезда вершины составлена из n равных, одинаково расположенных ромбов. Симметричность вершины означает, что через неё проходит ось вращения порядка n её звезды. Ранее автором были найдены все многогранники с ромбическими или дельтоидными вершинами и локально симметричными гранями. При этом локально симметричные грани не принадлежат ни одной из ромбических или дельтоидных звёзд. Класс RR -многогранников получается из рассмотренных ранее заменой условия локальной симметрии неромбических граней условием их правильности.

Таким образом, рассматриваемый класс RR связан с известным результатом Н. Джонсона и В. Залгаллера о перечислении всех выпуклых многогранников с условием правильности граней. Но, как показано в настоящей статье, RR -многогранники не могут быть просто получены из класса правильных, а требуют специального метода. Настоящая статья посвящена доказательству полноты класса RR -многогранников с двумя изолированными симметричными ромбическими вершинами V , W . При этом ромбы сходятся в вершинах V , W не обязательно своими острыми углами и V , W не обязательно разделены только одним поясом правильных граней.

Ключевые слова: симметричная ромбическая вершина, звезда вершины, пояс правильных граней, RR -многогранник.

Библиография: 26 названий.

Для цитирования:

В. И. Субботин. О полноте списка выпуклых RR -многогранников // Чебышевский сборник, 2020, т. 21, вып. 1, с. 297–309.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 514.172.45

DOI 10.22405/2226-8383-2020-21-1-297-309

On the completeness of the list of convex RR -polyhedra

V. I. Subbotin

Subbotin Vladimir Ivanovich — Candidate of Physical and Mathematical Sciences, Associate Professor, Don State Agrarian University (Novocherkassk).

e-mail: geometry@mail.ru

Abstract

The article gives proof of the completeness of the list of one class of convex symmetric polyhedra in three-dimensional Euclidean space. This class belongs to the class of so-called RR -polyhedra. The RR -polyhedra are characterized by the following symmetry conditions: each polyhedron of the class RR has symmetric rhombic vertices and there are faces that do not belong to any star of these vertices; and each face that does not belong to the star of the rhombic vertex is regular. The vertex rhombicity here means that the vertex star is composed of n equal, equally spaced rhombuses. The symmetry of the vertex means that the rotation axis of the order n of its star passes through it. Previously, the author found all polyhedra with rhombic or deltoid vertices and locally symmetric faces. Moreover, locally symmetric faces do not belong to any of the rhombic or deltoid stars. The class of RR -polyhedra is obtained from the previously considered replacement of the local symmetry condition of the non-rhombic faces by the condition of their regularity.

Thus, the considered class RR is connected with the well-known result of D. Johnson and V. Zalgaller on the enumeration of all convex polyhedra with the condition of the regularity of the faces. But as shown in this article, RR -polyhedra cannot simply be obtained from the class of regular-faced, but require a special method. The proof of completeness of the class of RR -polyhedra with two isolated symmetric rhombic vertices V , W is given in this article. Wherein, the rhombuses converge at the vertices of V , W not necessarily at its acute angles, and V , W are not necessarily separated by only one belt of regular faces.

Keywords: symmetric rhombic vertex, the star of the vertex, the belt of regular faces, RR -polyhedron.

Bibliography: 26 titles.

For citation:

V. I. Subbotin, 2020, "On the completeness of the list of convex RR -polyhedra", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 297–309.

1. Введение

Целью настоящей статьи является доказательство полноты списка одного класса замкнутых выпуклых симметричных многогранников в E^3 , принадлежащих классу так называемых RR -многогранников. Последний класс характеризуется условиями симметрии на элементы многогранника, а именно: многогранник M называется в работе RR -многогранником (от слов "rhombic" и "regular"), если у него существуют симметричные ромбические вершины и существуют грани, не принадлежащие звёздам этих вершин и являющиеся правильными многоугольниками одного типа. Здесь звезда вершины V многогранника, обозначаемая далее $Star(V)$ — это совокупность всех граней, имеющих одну общую вершину, совпадающую с V . Если звезда

$Star(V)$ состоит из n равных и одинаково расположенных, т.е. сходящихся в вершине V либо своими острыми, либо тупыми углами ромбов, то вершину V будем называть ромбической. Если звёзды $Star(V)$ и $Star(W)$ не имеют общих вершин, то будем говорить, что эти звёзды *отделены* друг от друга, а вершины V и W будем называть *изолированными*.

Если V расположена на оси вращения порядка n множества $Star(V)$, то V называется симметричной n -ромбической вершиной.

Естественность понятия класса RR -многогранников очевидна из следующих соображений.

Существует класс правильных (платоновых) многогранников в E^3 ; существует класс многогранников Джонсона–Залгаллера только с одним условием симметрии на грани: все грани являются правильными многоугольниками не обязательно одного типа. Известны также различные обобщения этих классов ([1–10], [22], [24–26]). Существуют также два многогранника, каждая вершина которых является симметричной ромбической — ромбододекаэдр и ромботриаконтаэдр. Известен также многогранник с двумя изолированными симметричными ромбическими вершинами и правильными гранями, в котором ромбические звёзды отделены одним поясом правильных граней (шестиугольниками) — удлинённый ромбододекаэдр. Заметим, что поясом граней здесь и в дальнейшем называется связное множество граней $F_1, F_2, \dots, F_n$ такое, что любые две грани F_i, F_{i+1} и также F_1, F_n имеют только одно общее ребро, а любые две другие грани этого множества не имеют общих рёбер.

В связи с этим возникает вопрос, каковы все те многогранники, у которых существуют симметричные ромбические вершины, а остальные грани являются правильными?

В работе автора [19] дано конструктивное доказательство существования двух RR -многогранников с двадцатью и двадцатью четырьмя гранями. Оба этих многогранника имеют зеркальные оси симметрии. Кроме того, в [20] анонсирована теорема, в которой доказывается полнота списка RR -многогранников с *одним* поясом правильных граней и изолированными *остроугольными* симметричными ромбическими вершинами. Под остроугольной ромбической вершиной понимается ромбическая вершина V , которая является вершиной острых углов ромбов звезды $Star(V)$.

В настоящей работе будут найдены все RR -многогранники с двумя симметричными, изолированными — как остроугольными так и тупоугольными — ромбическими вершинами, звёзды которых зеркально расположены. При этом условие наличия только одного пояса правильных граней не обязательно.

Заметим, что некоторые другие взаимосвязи геометрии многогранников с симметрией его элементов можно найти, например, в [11–18], [21], [23].

2. Основная теорема

Напомним определение зеркально расположенных звёзд вершин.

ОПРЕДЕЛЕНИЕ 1. *Две равные симметричные n -ромбические звёзды $Star(V)$ и $Star(W)$, расположенные друг к другу своими вогнутыми сторонами, будем называть зеркально расположенными, если вершины V и W расположены либо на оси вращения порядка n фигуры $Star(V) \cup Star(W)$, либо $Star(V)$ и $Star(W)$ могут быть совмещены при помощи зеркального поворота вокруг оси порядка $2n$, проходящей через их вершины.*

Под зеркальным поворотом вокруг оси L понимается композиция поворота вокруг оси L и отражения в плоскости, перпендикулярной этой оси.

Здесь докажем основную теорему.

ТЕОРЕМА 1. *Множество всех RR -многогранников с двумя зеркально расположенными ромбическими звёздами $Star(V)$ и $Star(W)$, отделёнными друг от друга правильными гранями одного типа, исчерпывается следующими девятью многогранниками:*

- 1) шесть многогранников с n -ромбическими вершинами, $6 \leq n < 12$, и правильными треугольными гранями;
- 2) 24-гранник с 4-ромбическими вершинами и правильными треугольными гранями;
- 3) 20-гранник с 5-ромбическими вершинами и квадратными гранями;
- 4) Удлиненный ромбический додекаэдр.

ДОКАЗАТЕЛЬСТВО. Доказательство разобьём на несколько частей.

1. В этой части будут найдены все RR -многогранники с треугольными гранями.

Граница каждой ромбической звезды $Star(V)$ представляет собой пространственную ломаную линию $MRNSPTQ \dots$. Звенья этой ломаной являются сторонами ромбов звезды $Star(V)$, а вершины являются вершинами острых и тупых углов ромбов. Границу ромбической звезды $Star(V)$ обозначим $L(V)$, острые углы ромбов — α . Обозначим β углы с вершинами на $L(V)$, образованные сторонами двух смежных ромбов (Рис.1,а)). Углы β в дальнейшем будем называть свободными.

Сначала проверим возможность RR -многогранников с остроугольными ромбическими вершинами.

Рассмотрим случай n -ромбической вершины V при $n = 3$. В этом случае, помещая в свободные углы равносторонние треугольные грани T_i , мы не сможем получить вторую ромбическую звезду, отделённую правильными треугольными гранями от звезды $Star(V)$. Действительно, для каждой грани T_i найдётся параллельная ромбическая грань звезды $Star(V)$ (Рис.1,б)). Но в силу равносторонности граней T_i каждая ромбическая грань составлена из двух правильных треугольников. Поэтому, приставляя к граням T_i новые треугольные грани, мы получим только ромбоэдр, гранями которого являются шесть равных ромбов с острыми углами $\frac{\pi}{3}$.

Рассмотрим случай n -ромбической вершины V при $n = 4$. Покажем, что и в этом случае не существует многогранника с двумя ромбическими вершинами, разделёнными правильными треугольными гранями.

В этом случае для каждой из четырёх треугольных граней T_i , помещённой в свободный угол β_i , существует равная и параллельная ей треугольная грань T_j , причём обе грани T_i и T_j параллельны оси вращения звезды $Star(V)$. Если приставить треугольные грани F_1 и F_2 соответственно к двум соседним граням T_1 и T_2 , то угол γ с вершиной S , общей с вершинами граней F_1 и F_2 , будет меньше $\frac{\pi}{3}$, так как две другие стороны граней F_1 и F_2 , имеющие общую вершину, перпендикулярны друг другу (Рис.1,с)).

Рассмотрим случай n -ромбической вершины V при $n = 5$. Если предположить существование RR -многогранника с двумя ромбическими вершинами, разделёнными правильными треугольными гранями в этом случае, то грани $RNSK$ и $SPTL$ будут являться ромбами, а не разделёнными рёбрами на две треугольные грани каждая, Рис.1,а). Действительно, если предположить, что KS не параллельна RN , а SL не параллельна PT , то переходя по параллельным рёбрам $RN \parallel MV$, $PT \parallel VQ$ и т.д., на завершающем шаге получим два ребра, являющимися соседними сторонами правильной треугольной грани. Значит, угол KSL не равен $\frac{\pi}{3}$ и в этот угол нельзя будет поместить треугольную грань.

Если $6 \leq n < 12$, то RR -многогранники с двумя ромбическими вершинами, разделёнными правильными треугольными гранями, могут быть построены. На Рис.1,д) — фрагмент одного из многогранников, на Рис.2,а) — один из шести многогранников в целом.

Действительно, найдём связь величины угла α со свободными углами β .

Для этого рассмотрим трёхгранный угол с вершиной P на Рис.1,а). Обозначая δ двугранный угол с ребром VP , получим:

$$\cos \beta = \cos^2 \alpha + \sin^2 \alpha \cos \delta, \quad \sin \frac{\delta}{2} = \frac{\sin \frac{\beta}{2}}{\sin \alpha}.$$

С другой стороны, рассматривая правильную n -угольную пирамиду $MNPQ \dots V$ получим для двугранного угла δ выражение:

$$\sin \frac{\delta}{2} = \frac{\sin \frac{\pi(n-2)}{2n}}{\cos \frac{\alpha}{2}};$$

следовательно,

$$\sin \frac{\alpha}{2} = \frac{\sin \frac{\beta}{2}}{2 \sin \frac{\pi(n-2)}{2n}}. \quad (1)$$

Из последней формулы по заданным n и β мы можем найти острый угол α .

При $n = 11$ получаем многогранник с максимальным числом граней – 66. Заметим, что при $n > 11$, очевидно, симметричную ромбическую звезду построить нельзя, так как должно выполняться неравенство $n\alpha < 2\pi$, т.е. начиная с $n = 12$ угол $\alpha < \frac{\pi}{6}$. Но при выполнении последнего неравенства сумма плоских углов при вершине P будет $> 2\pi$.

Проверим теперь, для каких n возможно поместить в свободные углы по две равносторонних треугольных грани, так как по три таких грани поместить нельзя: сумма плоских углов при вершине P (Рис.1,a)) будет $\geq 2\pi$.

Случай $n = 3$ очевиден, так как в этом случае помещается только один треугольник, что следует из изложенного в начале этого пункта.

При $n = 4$ мы получим 24-гранный RR -многогранник с зеркально-поворотной осью 8-го порядка (Рис.2,b), существование и единственность которого доказана автором в [19].

Докажем невозможность многогранника с двумя треугольными гранями в свободных углах при $n = 5$. На Рис.1,e) угол между рёбрами m и n не равен углу между рёбрами p и q . Переходя к паре рёбер r , s соответственно параллельных рёбрам p и q и далее, на завершающем шаге получим угол, эквивалентный углу 2. Но угол 2 равен углу 3. Следовательно, угол 1 не равен углу 3. Поэтому, если в угол 1 поместить два треугольника, то двугранный угол между ними не будет равен двугранному углу, который образуют треугольные грани с общей вершиной P . Пусть возможно поместить в угол 5 и во все углы, ему эквивалентные относительно вращения звезды $Star(V)$, две треугольные грани. Тогда сторона BC , лежащая против угла 5, и все стороны, ей эквивалентные, образуют плоский правильный 5-угольник $ABC \dots$ с осью вращения, проходящей через вершину V (Рис.1,e)). Следовательно, в этом случае вторая ромбическая вершина не будет существовать.

Две треугольных грани нельзя поместить и в случае $n \geq 6$, так как тупые углы ромбов в этом случае будут $> \frac{2\pi}{3}$, и сумма плоских углов в вершине P и ей эквивалентных будет $> 2\pi$.

Теперь рассмотрим возможность существования RR -многогранников с треугольными гранями и двумя тупоугольными симметричными ромбическими вершинами.

Очевидно, что в случае тупоугольной вершины V тупые углы ромбов звезды $Star(V)$ должны быть $< \frac{2\pi}{3}$.

Пусть тупоугольной вершине S ромбов звезды $Star(V)$, принадлежащей граничной ломаной $L(V)$, инцидентны вершины четырёх треугольных граней. Если в вершине T ломаной $L(V)$, в которой сходятся ромбы своими острыми углами, сходятся только две треугольных грани, то получим "ромбическую 6-угольную призму" с зеркальной осью симметрии 6-го порядка. Её боковые грани представляют собой ромбы с острыми углами $\frac{\pi}{3}$ и условными рёбрами. На Рис.1,f) изображена развёртка многогранника без тупоугольных ромбических звёзд:

рёбра p и q отождествляются, а верхняя и нижняя ломаные являются граничной ломаной соответственно для двух ромбических звёзд. Этот многогранник, как легко видеть, не является RR -многогранником, так как пары треугольных граней с общей вершиной в вершинах острых углов ромбов звезды $Star(V)$ вырождаются в одну ромбическую грань с условным ребром.

Пусть в вершинах ломаной $L(V)$, в которых должны сходиться ромбы звезды $Star(V)$ своими острыми углами (одна из таких вершин — T , Рис.1,g)), сходятся по три треугольных грани, а в вершинах ломаной $L(V)$, инцидентных тупым углам ромбов звезды $Star(V)$ (одна из таких вершин — S) — по-прежнему по четыре треугольных грани. Тогда предполагаемый многогранник M с двумя ромбическими вершинами должен будет иметь 30 граней, из которых 24 — треугольные, обычную ось вращения 3-го порядка и плоскость симметрии, перпендикулярную этой оси. Однако такой многогранник M не будет выпуклым.

Это легко видеть, рассмотрев отсечение по боковым рёбрам (через одно) правильной треугольной призмы с последующим отсечением новых рёбер верхнего и нижнего оснований призмы. Отсечения можно выбрать так, чтобы получить 11-гранник M' с осью вращения 3-го порядка и плоскостью симметрии, перпендикулярной этой оси. Гранями M' будут являться шесть равных равнобедренных трапеций Π'_i , меньшие основания которых примем равными 1, три ромба R_i , разбиваемых на два правильных треугольника со стороной 1, и два больших параллельных правильных треугольника Δ , со стороной, равной большому основанию трапеций Π'_i .

Чтобы построить многогранник M , заменим трапеции Π'_i пространственными трапециями Π_i , составленными из трёх правильных треугольников и с теми же самыми меньшими основаниями. Очевидно, для того, чтобы три большие основания пространственных трапеций Π_i являлись граничной ломаной $L(V)$ нужно, чтобы три равных расстояния d_i между вершинами этой ломаной, эквивалентных вершине T , равнялось трём равным расстояниям ρ_i между вершинами, эквивалентными S , Рис.1,g). То же верно и для второй ромбической вершины многогранника. Проводя вычисления, видим, что длины больших сторон трапеций Π'_i , равные $\frac{\sqrt{3}}{2} + 1$, будут больше больших диагоналей ромбов R_i , равных $\sqrt{3}$. Но большие диагонали ромбов R_i больше расстояний d_i . Таким образом, верно неравенство $d_i < \rho_i$, то есть мы не получаем ромбических звёзд. Мы не сможем получить равенство $\rho_i = d_i$, так как при увеличении d_i (при уменьшении ρ_i) одновременно в двух ромбических звёздах происходит "перелом" ромбов по меньшим их диагоналям, так как углы граничных ломаных ромбических звёзд в вершине S и ей эквивалентных, будут увеличиваться и выпуклость многогранника M будет нарушена.

Для наглядности на Рис.1,g) изображена часть предполагаемого многогранника M : восемь треугольных граней, две из трёх переломанных ромбических граней и одна из предполагаемых ромбических звёзд $Star(V)$. Рёбра, по которым происходит перелом ромбов на два треугольника показаны пунктиром.

Рассмотрим следующий возможный случай, когда в вершине S и ей эквивалентных сходятся по три треугольных грани, а в вершине T и ей эквивалентных — две. В этом случае получаем многогранник с одной ромбической тупоугольной вершиной. На Рис.1,h) изображена его развёртка без возможно ромбической звезды и без одной треугольной грани. Последняя получается после отождествления рёбер p и q путём отождествления вершин этих ребер, помеченных одинаковыми цифрами. В результате получается правильная треугольная грань rst . Цифрой 2 помечены вершины, в которых ромбические вершины возможной звезды $Star(V)$ сходятся своими острыми углами. Таким образом, в этом случае RR -многогранник невозможен.

2. В этой части доказательства теоремы будут найдены все RR -многогранники с квадратными гранями. Как и в части 1, сначала проверим возможность RR -многогранников с остроугольными ромбическими вершинами.

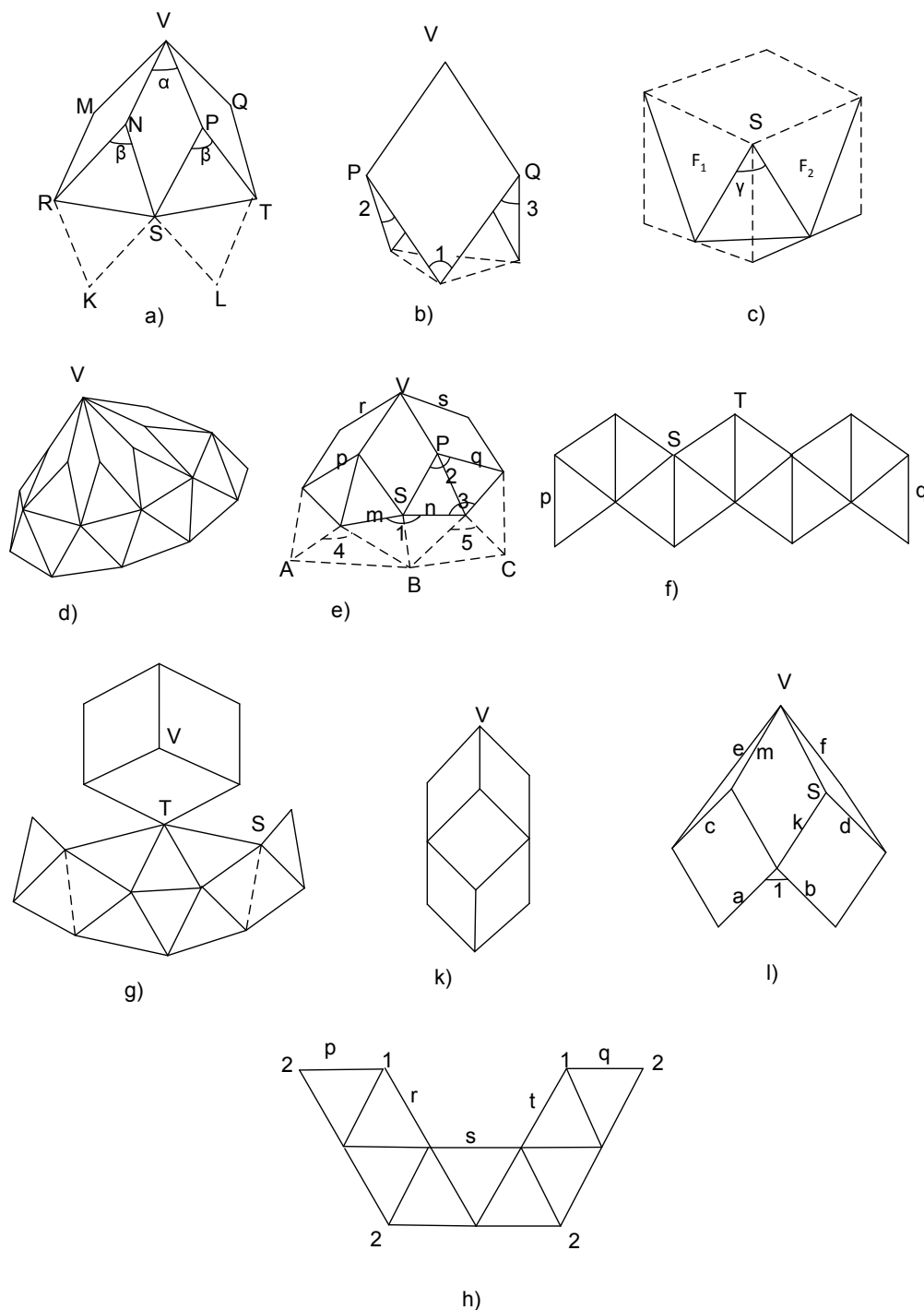
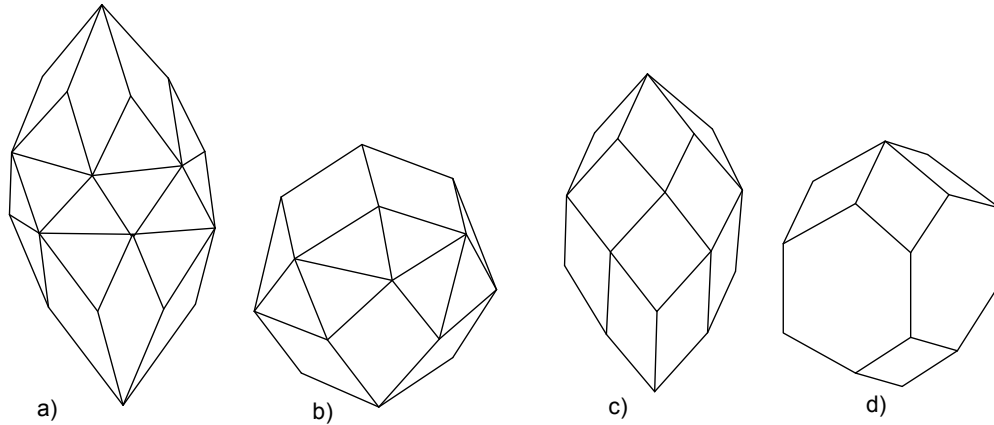


Рис. 1: К доказательству теоремы 1

Рассмотрим случай 3-ромбической вершины V . В этом случае в свободные углы нельзя поместить квадраты, так как свободные углы равны острым углам ромбов.

В случае 4-ромбической вершины V , выбрав острые углы ромбов равными $\frac{\pi}{3}$, квадратные грани в свободных углах β возможны, и очевидно, возможен многогранник с двумя симметричными ромбическими вершинами и квадратными гранями, но у него ромбические звёзды имеют общие вершины. Таким образом, нарушается условие делимости ромбических звёзд. (Рис.1,k)). Добавлять новые квадратные грани нельзя, так как угол 1 на Рис.1,l) не может

Рис. 2: RR -многогранники

быть равен $\frac{\pi}{2}$. Действительно, в противном случае, переходя по параллельным рёбрам $a \parallel c$, $b \parallel d$, и т.д., получим, что острый угол ромбов вершины V равен $\frac{\pi}{2}$.

Если V — 5-ромбическая вершина, то RR -многогранник возможен. Получим 20-гранник с зеркальной осью симметрии 10-го порядка (Рис.2,с)). Доказательство его существования и единственности приведено в работе автора [19].

Аналогично получаем доказательство невозможности RR -многогранников с квадратными гранями в случае 6- и 7-ромбических вершин. Только в этом случае переход по парам параллельных рёбер следует начинать с рёбер k и d на Рис.1,1).

Для n -ромбических вершин в случае $n > 7$ доказательство невозможности RR -многогранников следует из того, что тупые углы ромбов будут в этом случае $> \frac{3\pi}{4}$ и в вершине S сумма плоских углов будет $> 2\pi$.

Рассмотрим возможность существования RR -многогранников с квадратными гранями и двумя *тупоугольными* симметричными ромбическими вершинами.

Очевидно, в этом случае ромбические вершины могут быть только трёхгранными. В вершинах граничной кривой $L(V)$ могут сходиться только по два квадрата; в противном случае в вершинах ломаной $L(V)$ сумма плоских углов будет $> 2\pi$, и мы получаем призматическую поверхность — замкнутый пояс из шести квадратов. Граничная ломаная этого пояса является плоской и не может быть совмещена с пространственной ломаной LV .

3. Рассмотрим возможность RR -многогранников с 5-угольными правильными гранями.

Рассмотрим сначала случай остроугольных ромбических вершин.

Для 3-гранных ромбических вершин невозможность доказывается так же, как в случае треугольных граней. Для 4-гранных вершин невозможность RR -многогранника следует из невозможности пояса из 5-угольников с двумя парами параллельных граней.

В случае 5-гранных вершин вычисление по вышеприведённой формуле (1) для острого угла ромба даёт: $\alpha = \frac{\pi}{3}$. Поэтому три пятиугольника не могут сходиться в вершинах S_i ломаной $L(V)$, которым инцидентны острые вершины ромбов звезды $Star(V)$.

Покажем, что в вершинах S_i не могут сходиться и по два пятиугольника. Действительно, мы получили бы в этом случае пояс додекаэдра из пяти 5-угольников. Но у такого пояса для двух соседних 5-угольников угол между их сторонами с общей вершиной равен $\frac{3\pi}{5}$, что больше острых углов ромбов. Поэтому граничная ломаная $L(V)$ не может быть совмещена с пространственной границей пояса.

При $n = 6$ в вершинах S_i ломаной $L(V)$, которым инцидентны острые вершины ромбов,

для двух соседних 5-угольников угол между их сторонами в вершинах S_i только увеличится по сравнению с только-что рассмотренным случаем $n = 5$, а острый угол ромбов уменьшится. Поэтому и здесь граничная ломаная $L(V)$ не может быть совмещена с пространственной границей пояса.

При $n > 6$ сумма плоских углов в вершинах ломаной $L(V)$, в которых сходятся ромбы своими тупыми углами и 5-угольники, будет больше 2π . Это можно проверить, вычисляя острые углы ромбов по формуле (1).

Рассмотрим случай тупоугольных ромбических вершин и правильных 5-угольных граней.

Как и раньше, в каждой вершине ломаной $L(V)$ может сходить только по две 5-угольных грани. Рассмотрим пояс Π из шести 5-угольников с граничной ломаной L . Если граничная ломаная L пояса Π была бы одновременно и граничной ломаной звезды, то для соседних пятиугольников пояса Π углы между сторонами, имеющими общую вершину, должны были быть равными через один. Но это невозможно, так как тупые углы ромбов звезды $Star(V)$ должны быть $< \frac{2\pi}{3}$, а три угла ломаной L будут $> \frac{2\pi}{3}$. Поэтому не существует ромбических тупоугольных звёзд, граничная ломаная которых была бы и граничной ломаной пояса Π .

4. Здесь рассмотрим случай k -угольных граней при $k \geq 6$. Пусть сначала ромбические вершины являются остроугольными.

Случай 3-ромбических вершин, как и ранее, не даёт новых многогранников при $k \geq 6$.

Пусть ромбические вершины 4-гранные, а правильные грани — 6-угольные. Как известно, в этом случае существует 12-гранник, удовлетворяющий определению RR -многогранника — удлинённый ромбододекаэдр (Рис.2,d)).

Помещая в свободные углы звезды $Star(V)$ правильные k -угольники при $k > 6$, для 4-гранных вершин должен получиться пояс, четыре грани которого попарно параллельны. Однако, это при нечётных k , $k > 6$ невозможно. При чётных k , $k > 6$ такой пояс возможен, но в этом случае, очевидно, звезда $Star(V)$ не является ромбической. Поэтому и в этих случаях RR -многогранник невозможен.

Если ромбические вершины 5-гранные, а правильные грани — k -угольные, $k \geq 6$, то сумма плоских углов в вершинах ломаной $L(V)$, в которых сходятся ромбы своими острыми углами и k -угольники, будет больше 2π , что проверяется непосредственно по формуле (1).

При $n > 5$ для остроугольных n -ромбических вершин и правильных k -угольных граней, $k \geq 6$, очевидно, рассматриваемые RR -многогранники не существуют. Действительно, в этом случае сумма плоских углов в вершинах ломаной $L(V)$, в которых сходятся ромбы своими тупыми углами и k -угольники, будет больше 2π .

В случае тупоугольных ромбических вершин RR -многогранников с k -угольными гранями не существует при любом $k \geq 6$.

Действительно, так как тупые углы ромбов тупоугольной звезды должны быть меньше $\frac{2\pi}{3}$, то в вершинах ломаной $L(V)$, в которых сходятся ромбы своими острыми углами, не может сходить два k -угольника для всех $k \geq 6$. $\square$

Теорема доказана.

ЗАМЕЧАНИЕ 1. Из доказательства следует, что в условии теоремы 1 можно не требовать заранее условия зеркальной расположенности двух ромбических звёзд.

3. Заключение

Доказанная теорема даёт полный список всех девяти RR -многогранников с двумя изолированными симметричными ромбическими вершинами и правильными гранями одного типа. На Рис.2, а) представлен один из шести RR -многогранников с правильными треугольными гранями и n -ромбическими вершинами при $6 \leq n < 12$; на Рис.2, б), в), г) — три остальных.

Очевидно, каждый из найденных многогранников имеет ось вращения, обычную или зеркально-поворотную. Наибольшее число граней — 66 — имеет RR -многогранник с правильными треугольными гранями и с 11-гранными ромбическими вершинами.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Coxeter H. S. Regular polytopes. London-NY. 1963.
2. Деза М., Гришухин В. П., Штогрин М. И. Изометрические полиэдральные подграфы в гиперкубах и кубических решетках. М.: МЦНМО, 2007.
3. Емеличев В. А., Ковалёв М. М., Кравцов М. К. Многогранники. Графы. Оптимизация. М.: Наука, 1981.
4. Cromwell P. R. Polyhedra. Cambridge Univ. Press, Cambridge, 1997.
5. Grunbaum B. Convex Polytopes. John Wiley & Sons, New York, 1967.
6. Johnson N. W. Convex polyhedra with regular faces // Can. J. Math. 1966. Vol. 18, № 1. P. 169—200.
7. Jurij Kovic. Centrally symmetric convex polyhedra with regular polygonal faces // Math. Commun. 2013. Vol. 18. P. 429—440.
8. Залгаллер В. А. Выпуклые многогранники с правильными гранями // Зап. научн. сем. ЛОМИ. 1967. Т. 2. С. 1-220.
9. Тимофеев А. В. О выпуклых многогранниках с равноугольными и паркетными гранями // Чебышевский сборник. 2011. Т. 12, № 2. С. 118—126.
10. Гурин А. М. К истории изучения выпуклых многогранников с правильными гранями // Сиб. электрон. матем. изв. 2010. Т. 7, № 2. С. А5—А23.
11. Субботин В. И. О выпуклых RR -многогранниках с нетреугольными гранями // “Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории”. Материалы XVI Международной конференции, посвящённой 80-летию со дня рождения профессора Мишеля Деза. Тула: ТГПУ им. Л.Н.Толстого, 2019. С. 277-278.
12. Субботин В. И. Об одном классе сильно симметричных многогранников // Чебышевский сборник. 2016. Т. 17, № 4. С. 132-140.
13. Субботин В. И. О некоторых обобщениях сильно симметричных многогранников // Чебышевский сборник. 2015. Т. 16, № 2. С. 222-230.
14. Субботин В. И. О вполне симметричных многогранниках // Материалы Международной конференции по дискретной геометрии и её приложениям, посвящённой 70-летию проф. С. С. Рышкова. М.: МГУ. 2001. С. 88-89.
15. Субботин В. И. Выпуклые многогранники с дельтоидными вершинами // Чебышевский сборник. 2018. Т. 19, № 2. С. 489-498.
16. Subbotin V. I. Characterization of polyhedral partitioning a space. // Voronoy conference on analytic number theory and spatial tessellations. Kiev: September, 22-28, 2003. P. 46.

17. Субботин В. И. Многогранники с максимальным числом несимметричных граней // Метрическая геометрия поверхностей и многогранников. Материалы Международной конф., посвящ. 100-летию Н.В.Ефимова. М.: Макс-Пресс, 2010. С. 60-61.
18. Субботин В. И. О симметричных многогранниках с несимметричными гранями // Материалы Международного семинара “Дискретная математика и её приложения”, посвящ. 80-летию акад. О. Б. Лупанова. М.: МГУ. 2012. С. 398-400.
19. Субботин В. И. О двух классах многогранников с ромбическими вершинами // Зап. научн. семин. ПОМИ. 2018. Т.476. С.153–164.
20. Субботин В. И. О многогранниках с симметричными ромбическими вершинами и правильными гранями // Материалы Международной конференции, посвящ. 100-летию со дня рождения В.Т.Базылева. М.: МПГУ. 2019. С. 139-140.
21. Farris S. L. Completely classifying all vertex-transitive and edge-transitive polyhedra. // *Geometriae Dedicata*. 1988. Vol. 26, № 1. P. 111-124.
22. Grunbaum B. Regular polyhedra — old and new.// *Aequationes mathematicae*. 1977. Vol. 16, № 1-2. P. 1-20.
23. Wills J. M. On polyhedra with transitivity properties // *Discrete and Computational Geometry*. 1986. Vol. 1, № 3. P. 195-199.
24. Berman M. Regular-faced Convex Polyhedra, // *Journal of The Franklin Institute*. 1971. Vol. 291, № 5. P. 329-352.
25. Coxeter H. S. Regular and semi-regular polytopes. II, // *Mathematische Zeitschrift*. 1985. Vol. 188, № 4. P. 559–591.
26. Coxeter H. S. Regular and semi-regular polytopes. III, // *Mathematische Zeitschrift*. 1988. Vol. 200, № 1. P. 3–45.

REFERENCES

1. Coxeter H. S. 1963, *Regular polytopes*, London-NY.
2. Deza M, Grishukhin V. P. , Shtogrin M. I. 2008, *Isometricheskie poliedralnye podgrafy v gipercubach i kubicheskikh reshetkach [Scale-Isometric Polytopal Graphs in Hypercubes and Cubic Lattices]*, MCNMO, Moscow.
3. Emelichev V. A., Kovalev M. M., Kravzov M. K. 1981, *Mnogogranniki. Grafi. Optimizacija. [Polyhedra. Graph. Optimization]*, Nauka, Moscow.
4. Cromwell P. R. 1997, *Polyhedra*, Cambridge University Press, Cambridge.
5. Grunbaum B. 1967, *Convex Polytopes*, John Wiley & Sons, New York.
6. Johnson N. W. 1966, “Convex polyhedra with regular faces“, *Can. J. Math.*, vol. 18, № 1, pp. 169–200.
7. Jurij Kovic. 2013, “Centrally symmetric convex polyhedra with regular polygonal faces“, *Math. Commun.*, vol. 18, pp. 429–440.
8. Zalgaller V. A. 1967, “Convex polyhedra with regular faces“, *Zapiski nauchnykh seminarov LOMI*, vol. 2, pp. 1-220.

9. Timofeenko A. V. 2011, "On convex polyhedra with equiangular and parquet faces", *Chebyshevskiy sbornik*, vol. 12, no. 2, pp. 118-126.
10. Gurin A. M. 2010, "On the history of studying convex polyhedra with regular faces ", *Sib. electron. math. izv.*, vol. 7, pp. A5-A23.
11. Subbotin V.I. 2019, "On convex RR -polyhedrons with non-triangular faces", *Materialy XVI megdunarodnoj konferencii "Algebra, teoriya chisel i diskretnaja geometrija: sovremennye problemy, prilozheniya i problemy istorii", posvyashchyonnoj 80-letiyu professora Mishelja Deza (Proc. Int. Conf. "Algebra, number theory and discrete geometry: modern problems, applications and problems of history")*, Tula, pp. 277-278.
12. Субботин В. И. 2016, "On a class of strongly symmetric polytopes", *Chebyshevskiy sbornik*, vol. 17, no. 4, pp. 132-140.
13. Subbotin V.I. 2015, "Some generalizations strongly symmetric polyhedra", *Chebyshevskiy sbornik*, vol. 16, no. 2, pp. 222-230.
14. Subbotin V. I. 2001, "On Completely symmetrical polyhedra", *Materialy Megdunarudnoy konferencii po diskretnoy geometrii i eyo prilozheniyam, posvyashchyonnoj 70-letiyu prof. S.S.Ryshkova (Proc. Int. Conf. on discrete geometry and its applications)*, Moscow, pp. 88-89.
15. Subbotin V. I. 2018, "Convex polyhedra with delthoidal vertices", *Chebyshevskiy sbornik*, vol. 19, no. 2, pp. 489-498.
16. Subbotin V. I. 2003, "Characterization of polyhedral partitioning a space", *Voronoy conference on analytic number theory and spatial tessellations*, Kiev, p. 46.
17. Subbotin V. I. 2010, "Polyhedra with the maximum number of asymmetrical faces", *Materialy megdunarodnoy konferencii "Metriceskaja geometriya poverchnostey i mnogogrannikov", posvyashchyonnoj 100-letiyu N.V.Efimova (Proc. Int. Conf. "Metric geometry of surfaces and polyhedra")*, Moscow, pp. 60-61.
18. Subbotin V. I. 2012, "On symmetric polyhedra with asymmetrical faces", *Trudy megdunarodnogo seminar "Diskretnaja matematika i eyo prilozheniya", posvyashchyonnogo 80-letiyu O. B. Lupanova (Proc. Int. Seminar "Discrete Mathematics and Its Applications")*, Moscow, pp. 398-400.
19. Subbotin V. I. 2018, "On two classes of polyhedra with rhombic vertices", *Zapiski nauchnykh seminarov POMI*, vol. 476, pp. 153-164.
20. Subbotin V. I. 2019, "On polyhedra with symmetric rhombic vertices and regular faces", *Trudy megdunarodnogo seminar "Klassicheskaja i sovremennaja geometrija", posvyashchyonnogo 80-letiyu V.T.Bazyleva (Proc. Int. Conf. "Classical and modern geometry")*, Moscow, pp. 139-140.
21. Farris, S. L. 1988, "Classifying all vertex-transitive and edge-transitive polyhedra", *Geometriae Dedicata*, vol. 26, no. 1, pp. 111-124.
22. Grünbaum, B. 1977, "Regular polyhedra — old and new", *Aequationes mathematicae*, vol. 16, no. 1-2, pp. 1-20.
23. Wills J. M. 1986, "On polyhedra with transitivity properties", *Discrete and Computational Geometry*, vol. 1, no. 3, pp. 195-199.
24. Berman M. 1971, "Regular-faced Convex Polyhedra", *Journal of The Franklin Institute*, vol. 291, no. 5, pp. 329-352.

-
25. Coxeter H.S. 1985, “Regular and semi-regular polytopes. II“, *Mathematische Zeitschrift*, vol. 188, no. 4, pp. 559–591.
26. Coxeter H.S. 1988, “Regular and semi-regular polytopes. III“, *Mathematische Zeitschrift*, vol. 200, no. 1, pp. 3–45.

Получено 3.06.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 539.3:534.26

DOI 10.22405/2226-8383-2020-21-1-310-321

Определение поля смещений в неоднородном покрытии упругой пластины при прохождении через неё плоской звуковой волны¹

Л. А. Толоконников, Т. Ш. Нгуен

Толоконников Лев Алексеевич — доктор физико-математических наук, профессор кафедры прикладной математики и информатики, Тульский государственный университет (г. Тула).
e-mail: tolokonnikovla@mail.ru

Нгуен Тхи Шанг — аспирант кафедры прикладной математики и информатики, Тульский государственный университет (г. Тула).
e-mail: nguyensangnb@gmail.com

Аннотация

В статье рассматривается краевая задача для системы линейных обыкновенных дифференциальных уравнений второго порядка, построенная для определения поля смещений в непрерывно-неоднородном упругом покрытии пластины при прохождении через неё плоской звуковой волны.

Полагается, что однородная изотропная упругая пластина с неоднородным по толщине упругим покрытием граничит с идеальными жидкостями.

Методом степенных рядов получено приближенное аналитическое решение краевой задачи. Краевая задача сведена к задачам с начальными условиями. Решение краевой задачи представлено в виде линейной комбинации фундаментальных решений. Найденное аналитическое решение краевой задачи справедливо для широкого класса законов неоднородности материала покрытия.

Проведены численные расчеты зависимостей компонентов вектора смещения на границах покрытия от угла падения плоской волны.

Ключевые слова: краевая задача, поле смещений, отражение и прохождение звуковых волн, однородная упругая пластина, непрерывно-неоднородное покрытие.

Библиография: 15 названий.

Для цитирования:

Л. А. Толоконников, Т. Ш. Нгуен. Определение поля смещений в неоднородном покрытии упругой пластины при прохождении через неё плоской звуковой волны // Чебышевский сборник, 2020, т. 21, вып. 1, с. 310–321.

¹Исследование выполнено за счет гранта Российского научного фонда (проект 18-11-00199).

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 539.3:534.26

DOI 10.22405/2226-8383-2020-21-1-310-321

**Determination of the displacement field
in an inhomogeneous coating of an elastic plate
when passing through her plane sound wave**

L. A. Tolokonnikov, T. S. Nguyen

Tolokonnikov Lev Alexeevich — doctor of physical and mathematical Sciences, Professor of the Department of Applied Mathematics and Computer Science, Tula State University (Tula).
e-mail: tolokonnikovla@mail.ru

Nguyen Thi Sang — undergraduate department of of the Department of Applied Mathematics and Computer Science, Tula State University (Tula).
e-mail: nguyensangnb@gmail.com

Abstract

The article considers a boundary value problem for a system of linear second-order ordinary differential equations constructed for determining the displacement field in a continuously inhomogeneous elastic coating of the plate when a plane sound wave passes through.

It is believed that a homogeneous isotropic elastic plate with inhomogeneous in thickness elastic coating borders on ideal liquids.

An approximate analytical solution of the boundary value problem by the power series method is obtained. The boundary-value problem is reduced to problems with initial conditions. The solution of the boundary value problem is presented in the form of a linear combination of fundamental decisions. Found analytical solution boundary value problem is valid for a wide class of heterogeneity laws of the coating material.

The numerical calculations of the dependences of the components of the displacement vector at the boundaries of the coating from the angle of incidence of the plane wave are presented.

Keywords: boundary-value problem, displacement field, reflection and transmission of sound waves, homogeneous elastic plate, continuously inhomogeneous coating.

Bibliography: 15 titles.

For citation:

L. A. Tolokonnikov, T. S. Nguyen, 2020, "Determination of the displacement field in an inhomogeneous coating of an elastic plate when passing through her plane sound wave", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 310–321.

1. Введение

Отражение и прохождение плоской звуковой волны через плоский неоднородный упругий слой исследовано в [1–9]. Задачи о прохождении плоской звуковой волны через однородную изотропную упругую пластину с непрерывно-неоднородным упругим покрытием решены в [10–14]. В этих работах для определения поля смещений в неоднородном покрытии построена краевая задача для системы линейных обыкновенных дифференциальных уравнений второго порядка, которая решается численными методами. Однако всегда желательно иметь аналитическое решение задачи. Его использование позволяет существенно сократить вычислительные затраты.

В настоящей работе получено приближенное аналитическое решение краевой задачи, описывающее поле смещений в неоднородном по толщине упругом покрытии пластины и справедливое для широкого класса законов неоднородности материала покрытия.

2. Постановка задачи

Рассмотрим однородную изотропную упругую пластину толщиной H , материал которой характеризуется плотностью ρ_0 и упругими постоянными λ_0 и μ_0 . Пластина имеет покрытие в виде неоднородного по толщине изотропного упругого слоя толщиной h , материал которого имеет плотность $\rho = \rho(z)$ и модули упругости $\lambda = \lambda(z)$, $\mu = \mu(z)$. При этом декартова система прямоугольных координат x, y, z выбрана таким образом, что ось x лежит в плоскости, разделяющей однородный слой и неоднородное покрытие, а ось z направлена вниз по нормали к поверхности пластины (рис.1). Пластина с покрытием помещена между двумя полупространствами, заполненными идеальными однородными жидкостями, которые имеют плотности ρ_1, ρ_2 и скорости звука c_1, c_2 соответственно.

Из полупространства $z < -h$ на пластину с покрытием падает под произвольным углом плоская гармоническая звуковая волна, волновой вектор $\mathbf{k}_1$ которой лежит в плоскости x, z . Потенциал скорости падающей волны записывается в виде

$$\psi_0 = A_0 \exp\{i[k_{1x}x + k_{1z}(z + h) - \omega t]\},$$

где A_0 — амплитуда волны; $k_{1x} = k_1 \sin \theta_0$, $k_{1z} = k_1 \cos \theta_0$ — проекции волнового вектора k_1 на оси координат x и z соответственно; $k_1 = \omega/c_1$ — волновое число в полупространстве $z < -h$; θ_0 — угол падения плоской волны, составляемый нормалью к фронту волны с осью z ; ω — круговая частота; t — время. В дальнейшем временной множитель $e^{-i\omega t}$ будем опускать.

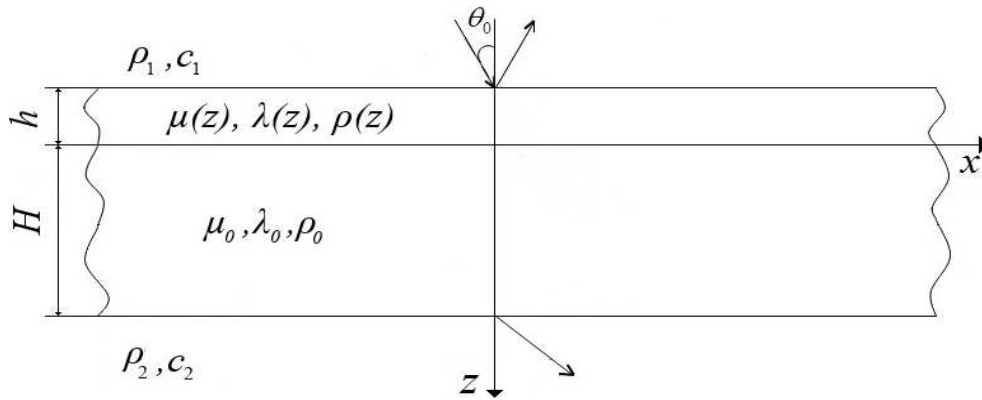


Рис. 1: Геометрия задачи

Задача об отражении и прохождении плоской звуковой волны через упругую пластину с неоднородным покрытием, граничащую с идеальными жидкостями, решена в [10]. При этом для аналитического описания волновых полей в полупространствах $z < -h$ и $z > H$, в однородной пластине и неоднородном покрытии необходимо знание значений компонентов вектора смещения $\mathbf{u}$ в неоднородном покрытии на его границах ($z = -h$ и $z = 0$).

Компоненты вектора смещения в неоднородном покрытии выражаются формулами

$$u_x = U_1(z) \exp(ik_{1x}x), u_z = U_2(z) \exp(ik_{1x}x),$$

а функции $U_n(z)$ ($n = 1, 2$) являются решением краевой задачи для системы линейных обыкновенных дифференциальных уравнений второго порядка

$$\mathbf{A}\mathbf{U}'' + \mathbf{B}\mathbf{U}' + \mathbf{C}\mathbf{U} = 0, \quad (1)$$

$$\begin{aligned}(\mathbf{A}\mathbf{U}' + \mathbf{E}\mathbf{U})_{z=-h} &= \mathbf{D}, \\ (\mathbf{A}\mathbf{U}' + \mathbf{F}\mathbf{U})_{z=0} &= 0,\end{aligned}\tag{2}$$

где $\mathbf{U} = (U_1, U_2)^T$;

$$\mathbf{A} = \begin{pmatrix} \mu & 0 \\ 0 & \lambda + 2\mu \end{pmatrix}; \quad \mathbf{B} = \begin{pmatrix} \mu' & ik_{1x}(\lambda + \mu) \\ ik_{1x}(\lambda + \mu) & \lambda' + 2\mu' \end{pmatrix};$$

$$\mathbf{C} = \begin{pmatrix} -k_{1x}^2(\lambda + 2\mu) + \omega^2\rho & ik_{1x}\mu' \\ ik_{1x}\lambda' & -k_{1x}^2\mu + \omega^2\rho \end{pmatrix};$$

$$\mathbf{E} = \begin{pmatrix} 0 & ik_{1x}\mu \\ ik_{1x}\lambda & i\omega^2\rho_1/k_{1z} \end{pmatrix}; \quad \mathbf{F} = \begin{pmatrix} f_{11} & ik_{1x}\mu + f_{12} \\ ik_{1x}\lambda + f_{21} & f_{22} \end{pmatrix};$$

$$\mathbf{D} = (0; -2i\rho_1\omega A_0)^T;$$

$$f_{1j} = \mu_0 \left[2k_{1x} \sqrt{k_l^2 - k_{1x}^2} (\beta_{j1} - \beta_{j2}) + s_3 (\gamma_{j1} + \gamma_{j2}) \right];$$

$$f_{2j} = s_1 (\beta_{j1} + \beta_{j2}) + s_2 (\gamma_{j1} - \gamma_{j2}) \quad (j = 1, 2);$$

$$\beta_{11} = k_{1x} t_2 w_1; \quad \beta_{21} = \sqrt{k_\tau^2 - k_{1x}^2} r_2 w_1; \quad \beta_{12} = k_{1x} t_1 w_1; \quad \beta_{22} = -\sqrt{k_\tau^2 - k_{1x}^2} r_1 w_1;$$

$$\gamma_{11} = -\sqrt{k_l^2 - k_{1x}^2} q_2 w_2; \quad \gamma_{21} = k_{1x} g_2 w_2; \quad \gamma_{12} = \sqrt{k_l^2 - k_{1x}^2} q_1 w_2; \quad \gamma_{22} = -k_{1x} g_1 w_2;$$

$$w_1 = \frac{-4i\mu_0 s_3}{r_1 t_2 + r_2 t_1}; \quad w_2 = \frac{4is_1}{g_1 q_2 - g_2 q_1};$$

$$g_j = (-1)^j 4s_1 \sqrt{k_l^2 - k_{1x}^2} \sqrt{k_\tau^2 - k_{1x}^2} - (s_{7-j} e_{1l} + s_{9-j} e_{2l}) e_{j\tau};$$

$$q_j = 4s_1 k_{1x}^2 + (s_{7-j} e_{1l} - s_{9-j} e_{2l}) e_{j\tau};$$

$$t_j = 4\mu_0 s_3 \sqrt{k_l^2 - k_{1x}^2} \sqrt{k_\tau^2 - k_{1x}^2} + (s_{6+(-1)^j} e_{2\tau} - s_{7+(-1)^j} e_{1\tau}) e_{jl};$$

$$r_j = 4\mu_0 k_{1x}^2 s_3 + (-1)^j (s_{6+(-1)^j} e_{2\tau} + s_{7+(-1)^j} e_{1\tau}) e_{jl};$$

$$s_1 = (\lambda_0 + 2\mu_0) k_l^2 - 2\mu_0 k_{1x}^2; \quad s_2 = 2\mu_0 k_{1x} \sqrt{k_\tau^2 - k_{1x}^2}; \quad s_3 = 2k_{1x}^2 - k_\tau^2; \quad s_4 = \frac{\omega_2 \rho_2}{\sqrt{k_\tau^2 - k_{1x}^2}};$$

$$s_{4+j} = s_3 (s_4 \sqrt{k_l^2 - k_{1x}^2} - s_1) - 2k_{1x} \sqrt{k_l^2 - k_{1x}^2} (s_4 k_{1x} - (-1)^j s_2);$$

$$s_{6+j} = s_3 (s_4 \sqrt{k_l^2 - k_{1x}^2} + s_1) - 2k_{1x} \sqrt{k_l^2 - k_{1x}^2} (s_4 k_{1x} - (-1)^j s_2) \quad (j = 1, 2);$$

$$e_{1l} = e^{i\sqrt{k_l^2 - k_{1x}^2} H}; \quad e_{2l} = e^{-i\sqrt{k_l^2 - k_{1x}^2} H}; \quad e_{1\tau} = e^{i\sqrt{k_\tau^2 - k_{1x}^2} H}; \quad e_{2\tau} = e^{-i\sqrt{k_\tau^2 - k_{1x}^2} H};$$

$k_2 = \omega/c_2$ — волновое число в полупространстве $z > H$; $k_l = \omega/c_l$ и $k_\tau = \omega/c_\tau$ — волновые числа продольных и поперечных упругих волн в однородной пластине; $c_l = \sqrt{(\lambda_0 + \mu_0)/\rho_0}$ и $c_\tau = \sqrt{\mu_0/\rho_0}$ — скорости продольных и поперечных волн соответственно.

Найдем аналитическое решение краевой задачи (1), (2).

3. Аналитическое решение задачи

Для решения краевой задачи (1), (2) воспользуемся методом степенных рядов [15].

Решение системы (1) будем искать в виде

$$U_n(z) = \sum_{s=0}^{\infty} U_n^{(s)}(z-a)^s \quad (n = 1, 2), \quad (3)$$

где a — некоторая точка отрезка $[-h, 0]$.

Если на отрезке $[-h, 0]$ функция $\rho(z)$ является дифференцируемой, а функции $\lambda(z)$ и $\mu(z)$ имеют непрерывные производные до второго порядка включительно, то все коэффициенты системы (1) будут представлять собой функции, непрерывные вместе со своими первыми производными на $[-h, 0]$. Тогда ряды (3) будут сходящимися на $[-h, 0]$ [15].

Предположим, что функции ρ , λ и μ имеют вид многочленов относительно переменной z (или аппроксимированы такими многочленами):

$$\rho(z) = \sum_{k=0}^R \rho^{(k)}(z-a)^k, \quad \lambda(z) = \sum_{k=0}^R \lambda^{(k)}(z-a)^k, \quad \mu(z) = \sum_{k=0}^R \mu^{(k)}(z-a)^k, \quad (4)$$

где R — степень многочленов.

Обозначим элементы матриц **A**, **B**, **C** через A_{mn} , B_{mn} , C_{mn} соответственно. Запишем систему (1) в координатной форме

$$\sum_{n=1}^2 (A_{mn}U_n'' + B_{mn}U_n' + C_{mn}U_n) = 0, \quad m = 1, 2. \quad (5)$$

Так как элементы матриц **A**, **B**, **C** выражаются через модули упругости и плотность материала покрытия, то с учетом (4) получаем

$$A_{mn} = \sum_{k=0}^R A_{mn}^{(k)}(z-a)^k, \quad B_{mn} = \sum_{k=0}^R B_{mn}^{(k)}(z-a)^k, \quad C_{mn} = \sum_{k=0}^R C_{mn}^{(k)}(z-a)^k. \quad (6)$$

Коэффициенты $A_{mn}^{(k)}$, $B_{mn}^{(k)}$, $C_{mn}^{(k)}$ имеют вид

$$\begin{aligned} A_{11}^{(k)} &= \mu^{(k)}, \quad A_{12}^{(k)} = A_{21}^{(k)} = 0, \quad A_{22}^{(k)} = \lambda^{(k)} + 2\mu^{(k)}, \\ B_{11}^{(k)} &= (k+1)\mu^{(k+1)}, \quad B_{12}^{(k)} = B_{21}^{(k)} = ik_{1x}(\lambda^{(k)} + \mu^{(k)}), \quad B_{22}^{(k)} = (k+1)(\lambda^{(k+1)} + 2\mu^{(k+1)}), \\ C_{11}^{(k)} &= -k_{1x}^2(\lambda^{(k)} + 2\mu^{(k)}) + \omega^2\rho^{(k)}, \quad C_{12}^{(k)} = ik_{1x}(k+1)\mu^{(k+1)}, \\ C_{21}^{(k)} &= ik_{1x}(k+1)\lambda^{(k+1)}, \quad C_{22}^{(k)} = -k_{1x}^2\mu^{(k)} + \omega^2\rho^{(k)}. \end{aligned}$$

Производные U_n' и U_n'' согласно (3) запишем в виде

$$U_n' = \sum_{s=0}^{\infty} (s+1)U_n^{(s+1)}(z-a)^s, \quad U_n'' = \sum_{s=0}^{\infty} (s+1)(s+2)U_n^{(s+2)}(z-a)^s. \quad (7)$$

С учетом разложений (3), (6), и (7) будем иметь

$$A_{mn}U_n'' = \sum_{s=0}^{\infty} \left(\sum_{k=0}^{R_1} (s+1-k)(s+2-k)A_{mn}^{(k)}U_n^{(s+2-k)} \right) (z-a)^s,$$

$$B_{mn}U'_n = \sum_{s=0}^{\infty} \left(\sum_{k=0}^{R_1} (s+1-k) B_{mn}^{(k)} U_n^{(s+1-k)} \right) (z-a)^s,$$

$$C_{mn}U_n = \sum_{s=0}^{\infty} \left(\sum_{k=0}^{R_1} C_{mn}^{(k)} U_n^{(s-k)} \right) (z-a)^s,$$

где $R_1 = \min(R, s)$.

Подставляя последние выражения в уравнения (5) и приравнявая нулю коэффициенты при каждой степени $(z-a)$, получаем уравнения для определения коэффициентов $U_n^{(s)}$ ($n = 1, 2$)

$$\sum_{n=1}^2 \sum_{k=0}^{R_1} [(s+1-k)(s+2-k)A_{mn}^{(k)} U_n^{(s+2-k)} + (s+1-k)B_{mn}^{(k)} U_2^{(s+1-k)} + C_{mn}^{(k)} U_n^{(s-k)}] = 0,$$

$$s = 0, 1, 2, \dots; \quad m = 1, 2.$$

Выделяя из первой суммы последнего равенства член с индексом $k = 0$, будем иметь

$$\sum_{n=1}^2 (s+1)(s+2)A_{mn}^{(0)} U_n^{(s+2)} = - \sum_{n=1}^2 \sum_{k=0}^{R_1} \{ (s+1-k)[(s-k)A_{mn}^{(k+1)} + B_{mn}^{(k)}] U_n^{(s+1-k)} + C_{mn}^{(k)} U_n^{(s-k)} \} \quad (m = 1, 2). \quad (8)$$

Составим из (8) систему двух уравнений относительно неизвестных $U_1^{(s+2)}$ и $U_2^{(s+2)}$

$$a_{m1}^{(s)} U_1^{(s+2)} + a_{m2}^{(s)} U_2^{(s+2)} = b_m^{(s)}, \quad m = 1, 2, \quad (9)$$

где

$$a_{mn}^{(s)} = (s+1)(s+2)A_{mn}^{(0)} \quad (m, n = 1, 2);$$

$$b_m^{(s)} = - \sum_{n=1}^2 \sum_{k=0}^{R_1} \{ (s+1-k)[(s-k)A_{mn}^{(k+1)} + B_{mn}^{(k)}] U_n^{(s+1-k)} + C_{mn}^{(k)} U_n^{(s-k)} \}.$$

Так как $A_{12}^{(0)} = A_{21}^{(0)} = 0$, то $a_{12}^{(s)} = a_{21}^{(s)} = 0$. Поэтому из (9) находим

$$U_n^{(s+2)} = b_n^{(s)} / a_{nn}^{(s)} \quad (n = 1, 2; \quad s = 0, 1, \dots). \quad (10)$$

Рекуррентные соотношения (10) позволяют вычислить все коэффициенты разложений (3) за исключением $U_n^{(0)}$ и $U_n^{(1)}$ ($n = 1, 2$).

Для нахождения этих коэффициентов сведем краевую задачу (1), (2) к задачам с начальными условиями в точке $z = a$. Найдем четыре линейно независимых решения системы дифференциальных уравнений (1). В качестве фундаментальных решений можно выбрать четыре решения задачи Коши $\mathbf{U}^l(z) = (U_1^l, U_2^l)^T$ ($l = 1, 2, 3, 4$) системы (1) с начальными условиями, являющимися линейно независимыми.

Возьмем следующие начальные условия:

$$\mathbf{U}^l|_{z=a} = (\delta_{1l}, \delta_{2l})^T, \quad \mathbf{U}^{l'}|_{z=a} = (\delta_{3l}, \delta_{4l}) \quad (l = 1, 2, 3, 4), \quad (11)$$

где δ_{ij} — символ Кронекера; l — порядковый номер задачи Коши.

Однородность системы (1) позволяет представить решение краевой задачи (1), (2) в виде линейной комбинации фундаментальных решений

$$\mathbf{U} = \sum_{l=1}^4 C_l \mathbf{U}^l, \quad (12)$$

где C_l – постоянные.

Каждую составляющую вектора $\mathbf{U}^l$ будем искать в виде (3)

$$U_n^l = \sum_{s=0}^{\infty} U_n^{l(s)} (z-a)^s \quad (n = 1, 2). \quad (13)$$

Все коэффициенты разложений (13) за исключением $U_n^{l(0)}$ и $U_n^{l(1)}$ ($n = 1, 2$) вычисляются по формуле (10)

$$U_n^{l(s+2)} = c_n^{l(s)} \quad (n = 1, 2; \quad l = 1, 2, 3, 4; \quad s = 0, 1, \dots), \quad (14)$$

где

$$c_n^{l(s)} = -[(s+1)(s+2)A_{nn}^{(0)}]^{-1} \sum_{q=1}^2 \sum_{k=0}^{R_1} \{(s+1-k)[(s-k)A_{mq}^{(k+1)} + B_{mq}^{(k)}]U_q^{l(s+1-k)} + C_{mq}^{(k)}U_q^{l(s-k)}\}.$$

Учитывая, что $U_n^{l'}|_{z=a} = U_n^{l(1)}$, из начальных условий (11), получаем

$$U_1^{l(0)} = \delta_{1l}; \quad U_2^{l(0)} = \delta_{2l}; \quad U_1^{l(1)} = \delta_{3l}; \quad U_2^{l(1)} = \delta_{4l} \quad (l = 1, 2, 3, 4).$$

Подставляя (12) в краевые условия (2), получим систему четырех линейных алгебраических уравнений относительно неизвестных C_l ($l = 1, 2, 3, 4$)

$$\sum_{l=1}^4 C_l (\mathbf{A}\mathbf{U}^{l'} + \mathbf{E}\mathbf{U}^l)_{z=-h} = \mathbf{D},$$

$$\sum_{l=1}^4 C_l (\mathbf{A}\mathbf{U}^{l'} + \mathbf{F}\mathbf{U}^l)_{z=0} = 0.$$

Определив из этой системы коэффициенты C_l , согласно (12) и (13) находим приближенное аналитическое решение краевой задачи (1),(2)

$$U_n(z) = \sum_{l=1}^4 C_l \sum_{s=0}^{\infty} U_n^{l(s)} (z-a)^s \quad (n = 1, 2). \quad (15)$$

В качестве точки $z = a$ можно взять любую точку отрезка $[-h, 0]$. Выберем $a = -h/2$, то есть середину отрезка $[-h, 0]$.

На основе полученного аналитического решения краевой задачи были проведены численные расчеты зависимостей модулей компонентов вектора смещения в неоднородном покрытии $|u_x| = |U_1(z)|$, $|u_z| = |U_2(z)|$ на границах покрытия (при $z = -h$ и $z = 0$) от угла падения плоской волны. Исследовался случай, когда жидкости по обе стороны тела являются одинаковыми ($k_1 = k_2$, $\rho_1 = \rho_2$). Полагалось, что амплитуда падающей волны $A_0 = 1$, а отношение толщины покрытия h к толщине однородной пластины H , равно 0,2. Рассматривалась алюминиевая пластина толщиной $H = 0,1$ м ($\rho_0 = 2,7 \cdot 10^3$ кг/м³, $\lambda_0 = 5,3 \cdot 10^{10}$ Н/м², $\mu_0 = 2,6 \cdot 10^{10}$ Н/м²) с покрытием на основе поливинилбутирала, находящаяся в воде ($\rho_1 = \rho_2 = 10^3$ кг/м³, $c_1 = c_2 = 1485$ м/с). Волновой размер пластины полагался равным $k_1 H = 5$. Расчеты проводились как для однородного покрытия с плотностью $\tilde{\rho} = 1,07 \cdot 10^3$ кг/м³ и модулями упругости $\tilde{\lambda} = 3,9 \cdot 10^9$ Н/м², $\tilde{\mu} = 9,8 \cdot 10^8$ Н/м², так и для неоднородных покрытий, механические характеристики которых менялись по толщине слоя по закону

$$\rho = \tilde{\rho} f(z), \quad \lambda = \tilde{\lambda} f(z), \quad \mu = \tilde{\mu} f(z).$$

Рассматривались следующие линейный и квадратичный законы неоднородности:

$$f_1(z) = a_1 \left(-\frac{z}{h} + 0,5 \right) \quad (a_1 = 1), \quad f_2(z) = a_2 \left[\left(\frac{z}{h} \right)^2 + 0,5 \right] \quad (a_2 = 6/5).$$

Множитель a_j ($j = 1, 2$) выбран так, чтобы среднее значение функции $f_j(z)$ по толщине слоя было равно единице.

Согласно (4) для линейного закона неоднородности материала покрытия ($R = 1$) имеем

$$\rho(z) = \tilde{\rho}[\rho^{(0)} + \rho^{(1)}(z + h/2)], \quad \lambda(z) = \tilde{\lambda}[\lambda^{(0)} + \lambda^{(1)}(z + h/2)], \quad \mu(z) = \tilde{\mu}[\mu^{(0)} + \mu^{(1)}(z + h/2)],$$

где

$$\rho^{(0)} = \tilde{\rho}, \quad \rho^{(1)} = -\tilde{\rho}/h, \quad \lambda^{(0)} = \tilde{\lambda}, \quad \lambda^{(1)} = -\tilde{\lambda}/h, \quad \mu^{(0)} = \tilde{\mu}, \quad \mu^{(1)} = -\tilde{\mu}/h,$$

$$\rho^{(k)} = \lambda^{(k)} = \mu^{(k)} = 0 \quad (k = 2, 3, \dots),$$

а для квадратичного ($R = 2$) —

$$\rho(z) = \rho^{(0)} + \rho^{(1)}(z + h/2) + \rho^{(2)}(z + h/2)^2, \quad \lambda(z) = \lambda^{(0)} + \lambda^{(1)}(z + h/2) + \lambda^{(2)}(z + h/2)^2,$$

$$\mu(z) = \mu^{(0)} + \mu^{(1)}(z + h/2) + \mu^{(2)}(z + h/2)^2,$$

где

$$\rho^{(0)} = 0,9\tilde{\rho}, \quad \rho^{(1)} = -1,2\tilde{\rho}/h, \quad \rho^{(2)} = 1,2\tilde{\rho}/h^2, \quad \lambda^{(0)} = 0,9\tilde{\lambda}, \quad \lambda^{(1)} = -1,2\tilde{\lambda}/h, \\ \lambda^{(2)} = 1,2\tilde{\lambda}/h^2, \quad \mu^{(0)} = 0,9\tilde{\mu}, \quad \mu^{(1)} = -1,2\tilde{\mu}/h, \quad \mu^{(2)} = 1,2\tilde{\mu}/h^2, \\ \rho^{(k)} = \lambda^{(k)} = \mu^{(k)} = 0 \quad (k = 3, 4, \dots).$$

Зависимости $|U_j(z)/A_0|$ ($j = 1, 2$) от θ_0 при $z = -h$ представлены на рис. 2 и рис. 3, а при $z = 0$ — на рис. 4 и рис. 5. Сплошные линии соответствуют однородному покрытию, пунктирные и штриховые — покрытиям с линейным и квадратичным законами неоднородности соответственно. Сравнение приведенных зависимостей показывает существенное влияние неоднородности материала покрытия на поле смещений.

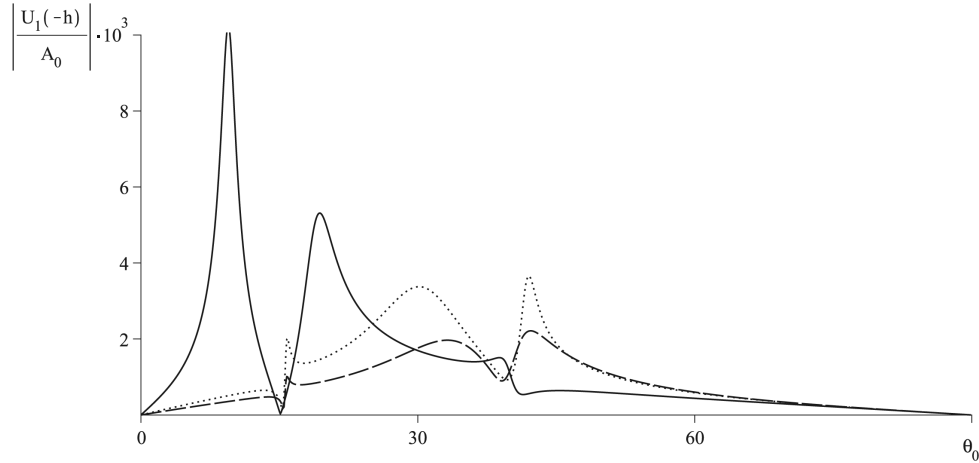
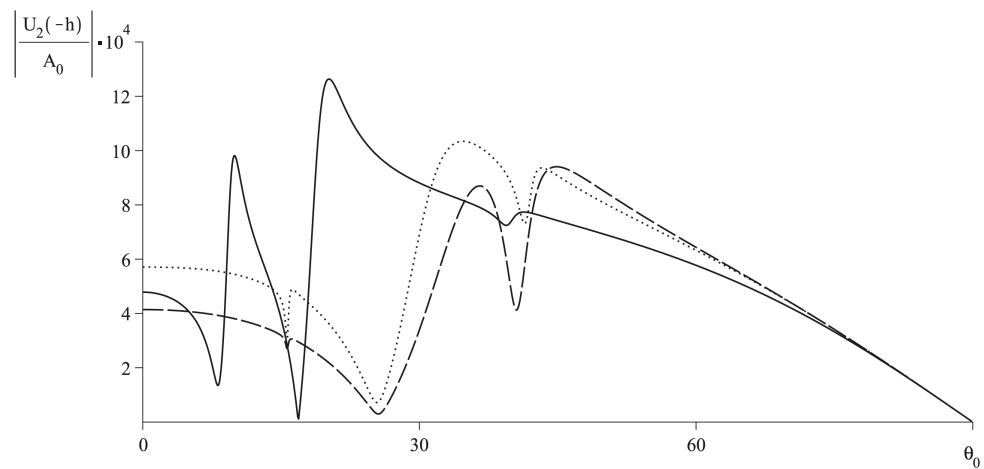
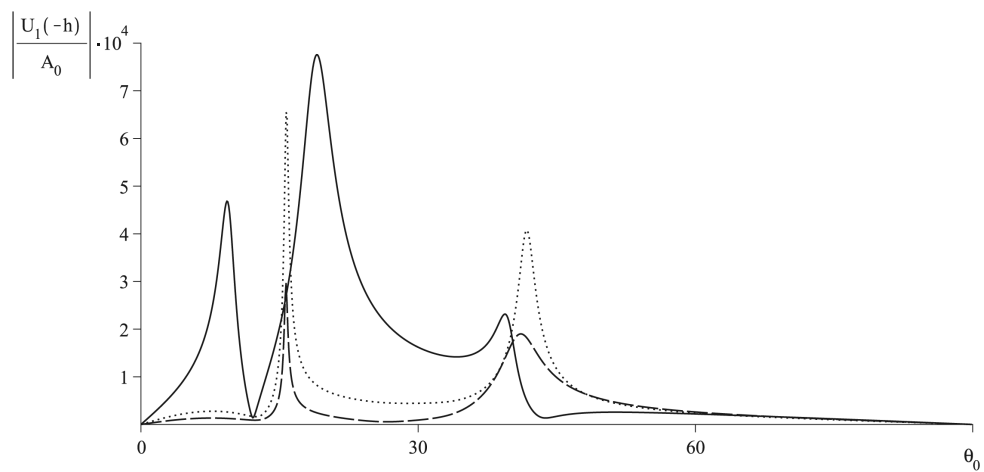
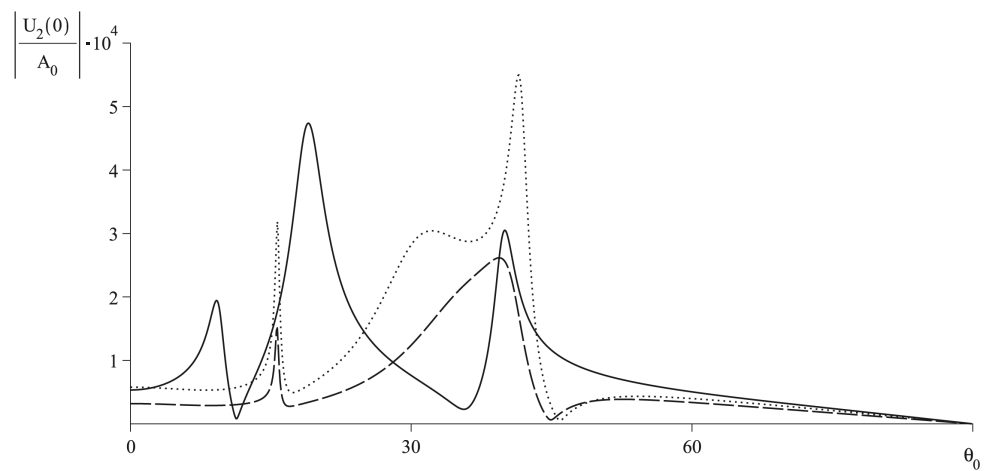


Рис. 2: Зависимость $|U_1(-h)/A_0|$ от θ_0

Рис. 3: Зависимость $|U_2(-h)/A_0|$ от θ_0 Рис. 4: Зависимость $|U_1(0)/A_0|$ от θ_0 Рис. 5: Зависимость $|U_2(0)/A_0|$ от θ_0

4. Заключение

Полученное аналитическое решение рассматриваемой краевой задачи для системы линейных обыкновенных дифференциальных уравнений второго порядка позволяет эффективно исследовать поле смещений в упругом неоднородном по толщине покрытии пластины при прохождении плоской звуковой волны, а также существенно сократить вычислительные затраты при численном анализе отраженного и прошедшего через пластину с покрытием акустических полей.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Приходько В. Ю., Тюткин В. В. Расчет коэффициента отражения звуковых волн от твердых слоисто-неоднородных сред // Акустический журн. 1986. Т. 32. Вып. 2. С. 212-218.
2. Скобельцын С. А., Толоконников Л. А. Прохождение звуковых волн через трансверсально-изотропный неоднородный плоский слой // Акустический журн. 1990. Т. 36. Вып. 4. С. 740-744.
3. Ринкевич А. Б., Смирнов А. Н. Распространение упругих волн в неоднородной трансверсально-изотропной пластине // Дефектоскопия. 2000. № 8. С. 78-83.
4. Толоконников Л. А. Отражение и преломление плоской звуковой волны анизотропным неоднородным слоем // Прикладная механика и техническая физика. 1999. Т. 40. № 5. С. 179-184.
5. Толоконников Л. А. Прохождение звука через неоднородный анизотропный слой, граничащий с вязкими жидкостями // Прикладная математика и механика. 1998. Т. 62. Вып. 6. С. 1029-1035.
6. Ларин Н. В., Толоконников Л. А. Прохождение плоской звуковой волны через неоднородный термоупругий слой // Прикладная математика и механика. 2006. Т. 70. Вып. 4. С. 650-659.
7. Толоконников Л. А., Ларин Н. В. Прохождение звука через термоупругий дискретно-неоднородный плоский слой, граничащий с теплопроводными жидкостями // Прикладная механика и техническая физика. 2017. Т. 58. № 1. С. 108-116.
8. Ларин Н. В., Скобельцын С. А., Толоконников Л. А. Определение законов неоднородности плоского упругого слоя с заданными звукоотражающими свойствами // Акустический журн. 2015. Т. 61. № 5. С. 552-558.
9. Скобельцын С. А. Определение параметров неоднородности анизотропного упругого слоя по прохождению звука // Известия Тульского гос. ун-та. Технические науки. 2016. Вып. 7. Ч. 2. С. 246-257.
10. Толоконников Л. А., Юдачев В. В. Отражение и преломление плоской звуковой волны упругим плоским слоем с неоднородным покрытием // Известия Тульского гос. ун-та. Естественные науки. 2015. Вып. 3. С. 219-226.
11. Толоконников Л. А., Нгуен Т. Ш. О влиянии неоднородного покрытия упругой пластины на отражение и прохождение звука // Известия Тульского гос. ун-та. Технические науки. 2018. Вып. 6. С. 362-372.

12. Толоконников Л. А., Нгуен Т. Ш. Прохождение звука через упругую пластину с неоднородным покрытием, граничащую с вязкими жидкостями // Чебышевский сборник. 2019. Т. 20 Вып. 2. С. 311-324.
13. Ларин И. В., Скобельцын С. А., Толоконников Л. А. Моделирование неоднородного покрытия упругой пластины с оптимальными звукоотражающими свойствами // Прикладная математика и механика. 2016. Т. 80. Вып. 4. С. 480-488.
14. Ларин Н. В. Определение законов неоднородности покрытия термоупругой пластины, обеспечивающих наименьшее звукоотражение // Известия Тульского гос. ун-та. Технические науки. 2016. Вып. 11. Ч. 2. С. 216-234.
15. Смирнов В. И. Курс высшей математики. Т. 3. Ч. 2. М.: Наука, 1969. 672 с.

REFERENCES

1. Prikhod'ko, V. Yu. & Tyutekin, V. V. 1986, "Calculation of reflection coefficient of sound waves from solid layered media", *Akust. Zhurnal*, vol. 32, no 2, pp. 212-218, [in Russian].
2. Skobel'tsyn, S. A. & Tolokonnikov, L. A. 1990, "Transmission of sound waves through a transversely isotropic inhomogeneous plane layer", *Akust. Zhurnal*, vol. 36, no 4, pp. 740-744, [in Russian].
3. Rinkevich, A. B. & Smirnov, A. N. 2000, "Propagation of elastic waves in a non-uniform transversely isotropic plate", *Defektoskopiya*, no 8, pp. 78-83, [in Russian].
4. Tolokonnikov, L. A. 1999, "Reflection and refraction of a planar acoustic waves in an anisotropic inhomogeneous layer", *J. Appl. Mech. and Techn. Physics*, vol. 40, no 5, pp. 936-941.
5. Tolokonnikov, L. A. 1998, "The transmission of sound through an inhomogeneous anisotropic layer adjoining viscous liquids", *J. Appl. Math. Mech.*, vol. 62, no 6, pp. 953-958.
6. Larin, N. V. & Tolokonnikov, L. A. 2006, "The transmission of a plane acoustic wave through a non-uniform thermoelastic layer", *J. Appl. Math. Mech.*, vol. 70, no 4, pp. 590-598.
7. Tolokonnikov, L. A. & Larin, N. V. 2017, "Sound propagation through a discretely inhomogeneous thermoelastic plane layer adjacent to heat-conducting liquids", *J. Appl. Mech. and Techn. Physics*, vol. 58, no 1, pp. 95-102.
8. Larin, N. V., Skobel'tsyn, S. A. & Tolokonnikov, L. A. 2015, "Determination of the Inhomogeneity Laws for an Elastic Layer with Preset Sound-Reflecting Properties", *Acoustical Physics*, vol. 61, no 5, pp. 504-510.
9. Skobel'tsyn, S. A. 2016, "Determining of the heterogeneity parameters of an anisotropic elastic layer on the sound transmission", *Izv. Tul. Gos. Univ., Ser. Tekh. Nauki*, no 7-2, pp. 246-257, [in Russian].
10. Tolokonnikov, L. A. & Yudachev, V. V. 2015, "Reflection and refraction of a planar acoustic waves in an elastic planar layer with a non-uniform covering", *Izv. Tul. Gos. Univ., Ser. Estestv. Nauki*, no 3, pp. 219-226, [in Russian].
11. Tolokonnikov, L. A. & Nguyen, T. S. 2018, "About the influence of an non-uniform covering of the elastic plate on sound reflection and transmission", *Izv. Tul. Gos. Univ., Ser. Tekh. Nauki*, no 6, pp. 362-372, [in Russian].

12. Tolokonnikov, L. A. & Nguyen, T. S. 2019, "The transmission of sound through an elastic plate with an inhomogeneous coating adjoining viscous liquids", *Chebyshevskii sbornik*, vol. 20, no 2, pp. 311-324, [in Russian].
13. Larin, N. V., Skobel'tsyn, S. A. & Tolokonnikov, L. A. 2016, "Modelling the inhomogeneous coating of an elastic plate with optimum sound-reflecting properties", *J. Appl. Math. Mech.*, vol. 80, no 4, pp. 339-344.
14. Larin, N. V. 2016, "Determination of the inhomogeneity laws for coating of the thermoelastic plate to obtain minimum sound reflection", *Izv. Tul. Gos. Univ., Ser. Tekh. Nauki*, no 11-2, pp. 216-234, [in Russian].
15. Smirnov, V. I. 1969, "Higher Mathematics Course, vol. 3-2", Nauka, Moscow, 672 p., [in Russian].

Получено 19.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.6

DOI 10.22405/2226-8383-2020-21-1-322-340

О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков¹

Г. В. Федоров

*Посвящается 80-летию
академика РАН В. П. Платонова*

Федоров Глеб Владимирович — кандидат физико-математических наук, механико-математический факультет, Московский государственный университет имени М. В. Ломоносова (г. Москва).

e-mail: fedorov@mech.math.msu.su

Аннотация

Одной из актуальных современных проблем алгебры и теории чисел является проблема существования и поиска фундаментальных S -единиц в гиперэллиптических полях. Проблема существования и поиска S -единиц в гиперэллиптических полях эквивалентна разрешимости норменного уравнения — функционального уравнения Пелля — с некоторыми дополнительными условиями на вид этого уравнения и его решения. Существует глубокая связь между точками конечного порядка в якобиевом многообразии (якобиане) гиперэллиптической кривой и нетривиальными S -единицами соответствующего гиперэллиптического поля. Эта связь легла в основу предложенного В. П. Платоновым алгебраического подхода к известной фундаментальной проблеме об ограниченности кручения в якобиевых многообразиях гиперэллиптических кривых. Для эллиптических кривых над полем рациональных чисел проблема кручения была решена Мазуром в 1970-ых годах. Для кривых рода 2 и выше над полем рациональных чисел проблема кручения оказалась значительно сложнее, и пока далека от своего полного решения. Основные результаты, полученные к настоящему времени в этом направлении, относятся к описанию подгрупп кручения якобиевых многообразий конкретных гиперэллиптических кривых, а также к описанию некоторых семейств гиперэллиптических кривых рода $g \geq 2$.

В данной статье нами найден новый метод исследования разрешимости функциональных норменных уравнений, дающий полное описание гиперэллиптических кривых над полем рациональных чисел, якобиевы многообразия которых обладают точками кручения данных порядков. Наш метод основан на аналитическом изучении представителей дивизоров конечного порядка в группе классов дивизоров степени ноль и их представлений Мамфорда. В качестве иллюстрации работы нашего метода в данной статье непосредственно найдены все параметрические семейства гиперэллиптических кривых рода два над полем рациональных чисел, якобиевы многообразия которых обладают рациональными точками кручения порядков не превосходящих пяти. Более того, наш метод позволяет определить, какому найденному параметрическому семейству принадлежит данная кривая, якобиан которой обладает точкой кручения порядка, не превосходящего пяти.

Ключевые слова: непрерывные дроби, фундаментальные единицы, S -единицы, кручение в якобианах, гиперэллиптические поля, дивизоры, группа классов дивизоров.

Библиография: 30 названий.

¹Работа выполнена при поддержке РНФ (грант №19-71-00029).

Для цитирования:

Г. В. Федоров. О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков // Чебышевский сборник, 2020, т. 21, вып. 1, с. 322–340.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.6

DOI 10.22405/2226-8383-2020-21-1-322-340

On families of hyperelliptic curves over the field of rational numbers, whose jacobian contains torsion points of given orders ²

G. V. Fedorov (Moscow)

*Dedicated to the 80-year anniversary
of academician RAS V. P. Platonov*

Fedorov Gleb Vladimirovich — candidate of physical and mathematical Sciences, faculty of mechanics and mathematics, Lomonosov Moscow state University (Moscow).

e-mail: fedorov@mech.math.msu.su

Abstract

One of the pressing contemporary problems of algebra and number theory is the problem of the existence and searching for fundamental S -units in hyperelliptic fields. The problem of the existence and searching of S -units in hyperelliptic fields is equivalent the solvability of the norm equation — the functional Pell equation — with some additional conditions on the form of this equation and its solution. There is a deep connection between points of finite order in Jacobian variety (Jacobian) of hyperelliptic curve and nontrivial S -units of hyperelliptic field. This connection formed the basis of the algebraic approach proposed by V.P. Platonov to the well-known fundamental problem of boundedness of torsion in Jacobian varieties of hyperelliptic curves. For elliptic curves over a field of rational numbers, the torsion problem was solved by Mazur in the 1970s. For curves of genus 2 and higher over the field of rational numbers, the torsion problem turned out to be much more complicated, and it is far from its complete solution. The main results obtained in this direction include to the description of torsion subgroups of Jacobian varieties of specific hyperelliptic curves, and also to the description of some families of hyperelliptic curves of the genus $g \geq 2$.

In this article, we have found a new method for studying solvability. functional norm equations giving a full description hyperelliptic curves over the field of rational numbers, whose Jacobian varieties possess torsion points of given orders. Our method is based on an analytical study of representatives finite order divisors in a divisor class group of degree zero and their Mumford representations. As an illustration of the operation of our method in this article, we directly found all parametric families of hyperelliptic curves of genus two over the field of rational numbers, whose Jacobian varieties have rational torsion points of orders not exceeding five. Moreover, our method allows us to determine which parametric family found this curve belongs, whose Jacobian has a torsion point of order not exceeding five.

Keywords: continued fractions, fundamental units, S -units, torsion in the Jacobians, hyperelliptic fields, divisors, divisor class group.

Bibliography: 30 titles.

For citation:

G. V. Fedorov, 2020, "On families of hyperelliptic curves over the field of rational numbers whose Jacobian contains torsion points of given orders", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 322–340.

²The work was supported by RSF (grant №19-71-00029).

1. Введение

Путь A — абелево многообразие размерности g над числовым полем K . По теореме Мордела-Вейля множество $A(K)$ K -точек многообразия A является конечно порожденной абелевой группой изоморфной $\mathbb{Z}^r \oplus A(K)_{tors}$, где $A(K)_{tors}$ — группа кручения K -точек многообразия A . Естественным образом возникают две проблемы: проблема полного описания конечных групп, реализуемых как группа кручения многообразия A над числовыми полями, и проблема полного перечисления многообразий A над числовым полем K , реализующих данную группу кручения. Для случая $g = 1$ эллиптических кривых над полем $\mathbb{Q}$ рациональных чисел первая проблема была решена Б. Мазуром в 1977 году [1]. С учетом результата Б. Мазура, в статьях Д. Куберта [2] и [3] была дана полная параметризация кубических эллиптических кривых для каждой из возможных групп точек конечного порядка, тем самым была решена вторая проблема для кубических эллиптических кривых над полем рациональных чисел. Для эллиптических кривых четвертой степени над полем рациональных чисел первая проблема эквивалентна кубическому случаю (см., например, [4]), а вторая проблема была решена в [5] с помощью формул [4], устанавливающих бирациональную эквивалентность кривых третьей и четвертой степени. Более подробно эллиптический случай над полем рациональных чисел с помощью теории функциональных непрерывных дробей исследован в [6], [7] для кривых третьей степени и в [8], [9] для кривых четвертой степени.

Для случая $g = 1$ эллиптических кривых над квадратичным полем констант проблема описания групп точек конечного порядка была решена в 1986 году С. Каменни [10]. Проблема описания эллиптических кривых над квадратичным полем констант реализующих данную группу кручения была решена в 1988 году М. Кенку и Ф. Момозем [11]. Исследование элементов кубических эллиптических полей над квадратичным полем констант, имеющих периодическое разложение в функциональную дробь, и связь с проблемой перечисления эллиптических кривых над квадратичным полем констант имеющих точку кручения заданного порядка проведены в статьях [12], [13] и [14].

В 1996 году Л. Мерел [15] доказал для каждого $d \geq 1$ существование постоянной $B(d)$, зависящей только от d , такой, что для любой эллиптической кривой E , определенной над числовым полем K степени d , справедливо неравенство $|E(K)_{tors}| \leq B(d)$. В случае $g \geq 2$ проблема ограниченности порядка подгруппы кручения даже для гиперэллиптических кривых над полем $\mathbb{Q}$ остается открытой. Тем более не решены проблема описания возможных групп кручения над числовыми полями и проблема перечисления гиперэллиптических кривых рода g над числовым полем K , реализующих данную группу кручения. Основные результаты, полученные к настоящему времени в этом направлении, относятся к описанию подгрупп кручения якобиевых многообразий определенного вида гиперэллиптических кривых рода $g \geq 2$, а также к описанию некоторых семейств гиперэллиптических кривых рода $g \geq 2$, якобианы которых обладают точками кручения определенного порядка (подробнее см. [16]). На основе нового подхода, предложенного В.П. Платоновым, доказана гипотеза о существовании $\mathbb{Q}$ -точек любого порядка, не превосходящего 30, в якобианах гиперэллиптических кривых рода 2 над полем рациональных чисел (см. [17]). В статье [18] приведено доказательство существования рациональных точек кручения некоторых порядков больших 30 в соответствующих якобианах гиперэллиптических кривых над полем рациональных чисел. С помощью метода Флина-Лепровоста В.П. Платонов и автор [19] построили бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28.

Глубокие идеи, высказанные В.П. Платоновым, позволили установить связь среди четырех самостоятельных фундаментальных проблем: проблемы существования в гиперэллиптическом поле L нетривиальных S -единиц специального вида, где $S = \{v_x^-, v_x^+\}$, проблемы квазипериодичности непрерывной дроби квадратичной иррациональности $\alpha \in L$, проблемы существова-

ния решения определенного вида у норменного уравнения (функционального уравнения типа Пелля) и проблемы кручения у класса дивизора $v_x^- - v_x^+$ в группе классов дивизоров $\Delta^\circ(L)$. Последняя проблема эквивалентна наличию точки конечного порядка в якобиевом многообразии гиперэллиптической кривой, соответствующей гиперэллиптическому полю L . Более подробно об указанных связях и развитии идей В.П. Платонова читатель может ознакомиться в статьях [21]-[25]. Фундаментальные наблюдения В.П. Платонова оказали важное и существенное влияние на современное развитие описанных проблем, являясь основой для многих настоящих и будущих исследований.

В данной статье нами найден новый метод исследования разрешимости функциональных норменных уравнений (функционального уравнения типа Пелля), дающий полную параметризацию гиперэллиптических кривых над полем рациональных чисел, якобиевы многообразия которых обладают точками кручения данных порядков. Наш метод основан на аналитическом изучении представителей дивизоров конечного порядка в группе классов дивизоров степени ноль и их представлений Мамфорда, и частично опирается на результаты статей [26]-[29]. Отметим, что в статье [30] путем изучения функциональных непрерывных дробей с малыми длинами периодов найдены необходимые условия на вид гиперэллиптических полей, но не даны исчерпывающие описания соответствующих кривых, якобиевы многообразия которых обладают рациональными точками кручения малых порядков. В качестве иллюстрации работы нашего метода в данной статье непосредственно найдены все параметрические семейства гиперэллиптических кривых рода два над полем рациональных чисел, якобиевы многообразия которых обладают рациональными точками кручения порядков не превосходящих 5. Более того, наш метод позволяет определить, какому найденному параметрическому семейству принадлежит данная кривая, якобиан которой обладает точкой кручения порядка, не превосходящего 5.

2. Вспомогательные сведения

Пусть K — поле характеристики отличной от 2, $h \in K[x]$ — неприводимый многочлен, многочлен $f \in K[x]$ свободен от квадратов, $\deg f \geq 3$, нормирование v_h поля $K(x)$ имеет два продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Положим $S_h = \{v_h^-, v_h^+\}$. Мультипликативная группа S_h -целых элементов поля L называется *группой S_h -единиц*. Если группа S_h -единиц U_h нетривиальна, то для данного S_h она является прямым произведением K^* и бесконечной циклической группы. Образующая бесконечной циклической группы называется *фундаментальной S_h -единицей*. Любая нетривиальная S_h -единица $u \in U_h$ поля L имеет вид

$$u_h = \frac{\mu_1 + \mu_2 \sqrt{f}}{h^m}, \quad v_h(\mu_2) = 0, \quad \max(\deg(\mu_1^2), \deg(\mu_2^2 f)) = 2m \deg h, \quad (1)$$

где $\mu_1, \mu_2 \in K[x]$ и $m \in \mathbb{N}$ (см. лемму 2.2 [7]). Степенью нетривиальной S_h -единицы $u_h \in U_h$, записанной в виде (1), называется число $\deg u_h = m \in \mathbb{N}$.

Предложение 1. *Следующие утверждения эквивалентны*

1. m — минимальное натуральное число такое, что уравнение

$$\omega_1^2 - \omega_2^2 f = bh^{2m}, \quad \max(2 \deg \omega_1, 2 \deg \omega_2 + \deg f) = 2m \deg h \quad (2)$$

имеет решение $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$, для некоторого $b \in K^*$;

2. в поле $L = K(x)(\sqrt{f})$ существует фундаментальная S_h -единица $u_h = (\omega_1 + \omega_2 \sqrt{f})/h^m$ степени m ;

3. m — минимальное натуральное число, для которого существует функция $\beta \in L$ такая, что ее главный дивизор имеет вид $(\beta) = m((h)^- - (h)^+)$.

ДОКАЗАТЕЛЬСТВО. Доказательство легко получается по аналогии с предложением 3.1 [20], или леммой 2.3 [7], или теореме 3 [25]. $\square$

Если выполнены эквивалентные условия предложения 1, то с точностью до постоянного множителя элемент β совпадает с u_h или $bu_h^{-1} = (\omega_1 - \omega_2\sqrt{f})/h^m$. При этом в случае, когда m нечетно и существует такое $\gamma \in K^*$, что $b = \gamma^2$ и $f \mid \omega_1 - \gamma h^m$, выполняется тождество $\mu_1^2 - \mu_2^2 f = \gamma h^m$ для некоторых $\mu_1, \mu_2 \in K[x]$. Таким образом, для нечетного m показатель $2m$ степени h в норменном уравнении (2) может оказаться не минимальным.

Пусть $g \in \mathbb{N}$, $f, h \in \mathbb{Q}[x]$, причем многочлен f свободен от квадратов, $2g+1 \leq \deg f \leq 2g+2$, $(f, h) \in \mathbb{Q}^*$, $\deg h \leq g$. Бесконечное нормирование поля $\mathbb{Q}(x)$ может иметь два неэквивалентных продолжения v_∞^- и v_∞^+ или два эквивалентных продолжения $v_\infty = v_\infty^- = v_\infty^+$ на поле $L = \mathbb{Q}(x)(\sqrt{f})$.

ПРЕДЛОЖЕНИЕ 2. Для описания с точностью до изоморфизма всех гиперэллиптических кривых $C : y^2 = f(x)$ рода два над полем рациональных чисел, якобиевы многообразия которых обладают точкой с кручением заданного порядка m достаточно решить уравнение вида

$$\omega_1^2 - \omega_2^2 f = \gamma h^m, \quad \max(2 \deg \omega_1, 2 \deg \omega_2 + \deg f) = m \cdot \deg h, \quad (3)$$

где $h, f, \omega_1, \omega_2 \in \mathbb{Q}[x]$, $1 \leq \deg h \leq 2$, $(h, \omega_1) \in \mathbb{Q}^*$, $\text{lc}(h) = \text{lc}(\omega_2) = 1$, многочлен f свободен от квадратов, $5 \leq \deg f \leq 6$, $\gamma \in \mathbb{Q}^*$.

ДОКАЗАТЕЛЬСТВО. В группе классов дивизоров степени ноль $\Delta^\circ(L)$ гиперэллиптического поля L , соответствующего гиперэллиптической кривой C рода два, достаточно рассмотреть канонические представители вида $D - (\infty^- + \infty^+)$, где D — некоторый эффeктивный дивизор степени два, определенный над полем $\mathbb{Q}$. Пусть класс дивизора $D - (\infty^- + \infty^+) = P_1 + P_2 - (\infty^- + \infty^+)$ имеет порядок m в группе классов дивизоров $\Delta^\circ(L)$. Если $P_1 + P_2 \neq 2\infty^-$ и $P_1 + P_2 \neq 2\infty^+$, то существует функция $\omega_1 + \omega_2\sqrt{f} \in \mathbb{Q}[x][\sqrt{f}]$, дивизор которой имеет вид

$$(\omega_1 + \omega_2\sqrt{f}) = m(P_1 + P_2 - (\infty^- + \infty^+)),$$

а также существует многочлен $h \in \mathbb{Q}[x]$, $1 \leq \deg h \leq 2$, дивизор которого имеет вид

$$(h) = (P_1 + P_2) + \iota(P_1 + P_2) - 2(\infty^- + \infty^+).$$

Это означает, что

$$(\omega_1 + \omega_2\sqrt{f}) = m((h)^- - (\infty^- + \infty^+)).$$

Последнее соотношение эквивалентно разрешимости уравнения (3).

Если $P_1 + P_2 = 2\infty^-$, то можно рассмотреть изоморфную кривую $C_1 : Y^2 = F(X)$, где $X = 1/x$, $Y = yX^{g+1}$, $F = X^{2g+2}f(1/X)$. В группе классов дивизоров для этой кривой класс дивизора $v_X^- - v_X^+$ имеет порядок m . Тогда существует функция $\omega_1 + \omega_2\sqrt{F} \in \mathbb{Q}[X][\sqrt{F}]$, дивизор которой имеет вид

$$(\omega_1 + \omega_2\sqrt{F}) = m(2(X)^- - (\infty^- + \infty^+)). \quad (4)$$

Если положить $h = X^2$, то равенство (4) равносильно разрешимости уравнения вида (3). $\square$

3. Основные результаты

Нашей целью является явное параметрическое описание всех свободных от квадратов многочленов f , удовлетворяющих (3) для некоторых $h, f, \omega_1, \omega_2 \in \mathbb{Q}[x]$, $\gamma \in \mathbb{Q}^*$, и приведенным выше условиям. Из уравнения (3) видно, что в зависимости от четности $\deg f$ и $\deg h^m$ число γ может принимать одно из трех значений $\text{lc}(\omega_1)^2$, $-\text{lc}(f)$, $\text{lc}(\omega_1)^2 - \text{lc}(f)$. Более точная связь степеней многочленов ω_1, ω_2, h, f и значений для числа γ представлена в таблице 1 для различных значений $m, n, k \in \mathbb{N}$. Таким образом, в любом случае значение γ в (3) однозначно восстанавливается по данным многочленам f и ω_1 .

Далее штрихом будем обозначать производную по переменной x , например, $h' = dh/dx$.

Таблица 1: возможные значения параметра γ

$\deg h$	m	$\deg \omega_1$	$\deg f$	γ
$2n-1$	$2k$	$k(2n-1)$	$< 2k(2n-1) - 2 \deg \omega_2$	$\text{lc}(\omega_1)^2$
$2n-1$	$2k$	$k(2n-1)$	$2k(2n-1) - 2 \deg \omega_2$	$\text{lc}(\omega_1)^2 - \text{lc}(f)$
$2n-1$	$2k$	$< k(2n-1)$	$2k(2n-1) - 2 \deg \omega_2$	$-\text{lc}(f)$
$2n-1$	$2k-1$	$\leq 2nk - n - k$	$(2k-1)(2n-1) - 2 \deg \omega_2$	$-\text{lc}(f)$
$2n$	m	mn	$< 2mn - 2 \deg \omega_2$	$\text{lc}(\omega_1)^2$
$2n$	m	mn	$2mn - 2 \deg \omega_2$	$\text{lc}(\omega_1)^2 - \text{lc}(f)$
$2n$	m	$< mn$	$2mn - 2 \deg \omega_2$	$-\text{lc}(f)$

3.1. Общий подход

ТЕОРЕМА 1. Пусть даны некоторые многочлены $h, \omega_2 \in \mathbb{Q}[x]$, причем $\text{lc}(h) = \text{lc}(\omega_2) = 1$ и ω_2 свободен от квадратов. Уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ таких, что $(\omega_1, h) \in \mathbb{Q}^*$, тогда и только тогда, когда разрешима система сравнений

$$\begin{cases} q_0^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2h(q_1 \omega_2' + q_0') \equiv m q_0 h' \pmod{\omega_2} \end{cases} \quad (5)$$

в многочленах $q_0, q_1 \in \mathbb{Q}[x]$ таких, что $\deg q_0, \deg q_1 < \deg \omega_2$, $(q_0, h) \in \mathbb{Q}^*$, $2(\deg q_1 + \deg \omega_2) \leq m \deg h$.

ДОКАЗАТЕЛЬСТВО. Предположим, что уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ таких, что $(\omega_1, h) \in \mathbb{Q}^*$. Запишем $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2 , и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2 . Тогда $(q_0, h) \in \mathbb{Q}^*$, так как $(\omega_1, h) \in \mathbb{Q}^*$. Кроме того, $\deg q_0, \deg q_1 < \deg \omega_2$, и $2(\deg q_1 + \deg \omega_2) \leq 2 \deg \omega_1 \leq m \deg h$. Из (3) следует, что $\omega_2^2 \mid \omega_1^2 - \gamma h^m$. Так как многочлен ω_2 свободен от квадратов, то последнее условие равносильно системе сравнений

$$\begin{cases} \omega_1^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2\omega_1' \omega_1 \equiv \gamma m h^{m-1} h' \pmod{\omega_2}. \end{cases} \quad (6)$$

Из $(\omega_1, h) \in \mathbb{Q}^*$ следует $(\omega_2, h) \in \mathbb{Q}^*$, поэтому домножим второе сравнение на h и воспользуемся первым сравнением. Тогда рассматриваемая система сравнений будет равносильна

$$\begin{cases} \omega_1^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2\omega_1' h \equiv m \omega_1 h' \pmod{\omega_2}. \end{cases} \quad (7)$$

Подставляя выражение для ω_1 , получаем искомую систему (5).

Пусть теперь система сравнений (5) разрешима в многочленах $q_0, q_1 \in \mathbb{Q}[x]$ таких, что $\deg q_0, \deg q_1 < \deg \omega_2$, $(q_0, h) \in \mathbb{Q}^*$, $2(\deg q_1 + \deg \omega_2) \leq m \deg h$. Положим $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, где $q_2 \in \mathbb{Q}[x]$ — произвольный многочлен такой, что $\deg \omega_1 \leq [\deg h \cdot m/2]$. Так как $2(\deg q_1 + \deg \omega_2) \leq m \deg h$, то действительно такой многочлен q_2 можно подобрать (возможно нулевой). Таким образом, справедлива система (7), причем ввиду $(q_0, h) \in \mathbb{Q}^*$ имеем $(q_0, \omega_2) \in \mathbb{Q}^*$ и $(\omega_1, \omega_2) \in \mathbb{Q}^*$, а также $(\omega_1, h) \in \mathbb{Q}^*$. Домножая второе уравнение (7) на ω_1 и подставляя первое уравнение (7), приходим к системе (6), из которой следует условие $\omega_2^2 \mid \omega_1^2 - \gamma h^m$, поскольку многочлен ω_2 свободен от квадратов. Отсюда получаем многочлен f , для которого выполнено (3). $\square$

ТЕОРЕМА 2. Пусть дано $m \in \mathbb{N}$ и многочлены $\omega_2, h \in \mathbb{Q}[x]$ такие, что $4 \deg \omega_2 \leq m \deg h + 2$, $(\omega_2, h) \in \mathbb{Q}^*$ и ω_2 свободен от квадратов. Уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ тогда и только тогда, когда γh^m является квадратичным вычетом по модулю ω_2 , то есть найдется многочлен $q_0 \in \mathbb{Q}[x]$, $\deg q_0 \leq \deg \omega_2$, такой, что $q_0^2 \equiv \gamma h^m \pmod{\omega_2}$.

ДОКАЗАТЕЛЬСТВО. По предложению 1 из разрешимости уравнения (3) следует разрешимость системы сравнений (5). Остается показать только, что сравнение $2h(q_1 \omega_2' + q_0') \equiv m q_0 h' \pmod{\omega_2}$ всегда разрешимо относительно многочлена $q_1 \in \mathbb{Q}[x]$. Так как многочлен ω_2 свободен от квадратов, то $(\omega_2', \omega_2) \in \mathbb{Q}^*$, следовательно, ω_2' обратим по модулю ω_2 . Кроме того, $(h, \omega_2) \in \mathbb{Q}^*$, значит многочлен h также обратим по модулю ω_2 . Значит, $q_1 \equiv (m q_0 h' h^{-1}/2 - q_0')(\omega_2')^{-1} \pmod{\omega_2}$, причем $\deg q_1 < \deg \omega_2$.

Заметим, что, если для некоторого q_0 выполнено сравнение $q_0^2 \equiv \gamma h^m \pmod{\omega_2}$, то можно положить q_1 равным остатку от деления $(m q_0 h' h^{-1}/2 - q_0')(\omega_2')^{-1}$ на ω_2 . Из условия $4 \deg \omega_2 \leq m \deg h + 2$ следует, что можно положить $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, для некоторого (возможно нулевого) многочлена $q_2 \in \mathbb{Q}[x]$, причем $\deg \omega_1 \leq [\deg h \cdot m/2]$. Далее доказательство в точности как у теоремы 1. $\square$

В некоторых частных случаях для описанного выше общего подхода к решению уравнения (3) можно увеличить продуктивность. Например, предположим, что в (3) порядок $m = 2k$ и число $\gamma = \tau^2$ является полным квадратом в $\mathbb{Q}^*$. Тогда $\omega_2^2 f = (\omega_1 - \tau h^k)(\omega_1 + \tau h^k)$. Так как множители в правой части последнего равенства взаимнопросты, то можно представить $\omega_2 = \omega_3 \cdot \omega_4$ так, что разрешимость (3) равносильна системе условий

$$\begin{cases} \omega_3^2 \mid \omega_1 - \tau h^k, \\ \omega_4^2 \mid \omega_1 + \tau h^k. \end{cases} \quad (8)$$

Следовательно, $\omega_1 = f_1 \omega_3^2 + \tau h^k = f_2 \omega_4^2 - \tau h^k$, где $f = f_1 \cdot f_2$, причем $\deg f_1, \deg f_2 \geq 1$, поскольку иначе порядок будет равен k , а не $2k$, как мы желаем. Если дополнительно предположить, что многочлен ω_2 свободен от квадратов, то система (8) равносильна системе сравнений

$$\begin{cases} f_2 \omega_4^2 \equiv 2h^k \pmod{\omega_3}, \\ \frac{f_2'}{f_2} + 2 \frac{\omega_4'}{\omega_4} \equiv k \frac{h'}{h} \pmod{\omega_3}, \\ f_1 \omega_3^2 \equiv -2h^k \pmod{\omega_4}, \\ \frac{f_1'}{f_1} + 2 \frac{\omega_3'}{\omega_3} \equiv k \frac{h'}{h} \pmod{\omega_4}. \end{cases} \quad (9)$$

Чтобы найти решение задачи (3) в рассматриваемом частном случае можно, положить $\omega_1 = f_1 \omega_3^2 + \tau h^k$ и найти многочлены $\omega_3, \omega_4, f_1, f_2$ с неопределенными коэффициентами, удовлетворяющими последним двум условиям системы (9).

Далее для каждого значения $0 \leq \deg \omega_2 \leq 2$ рассмотрим решение задачи (3) согласно подходу, описанному в теоремах 1 и 2.

3.2. Случай $\deg \omega_2 = 0$

В этом случае решить задачу (3) не составляет труда:

$$F = \omega_1^2 - \gamma h^m,$$

где $h, \omega_1 \in \mathbb{Q}[x]$ — произвольные многочлены такие, что $\deg h \geq 1$, $\text{lc}(\omega_1) = \text{lc}(h) = 1$, $(h, \omega_1) \in \mathbb{Q}^*$, $m \in \mathbb{N}$ такое, что $2 \deg \omega_1 \leq m \deg h$, $\gamma \in \mathbb{Q}^*$ — любое. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов. Возможные значения $\deg F \leq 6$, $\deg h \leq 2$, m , $\deg \omega_1$ и γ приведены в таблице 2.

Таблица 2: значения параметров для случая $\deg \omega_2 = 0$

$\deg F$	$\deg h$	m	$\deg \omega_1$	γ
3	1	3	≤ 1	$-\text{lc}(f)$
3	1	4	2	$\text{lc}(\omega_1)^2$
4	1	4	≤ 2	$\text{lc}(\omega_1)^2 - \text{lc}(f)$
5	1	5	≤ 2	$-\text{lc}(f)$
5	1	6	3	$\text{lc}(\omega_1)^2$
5	2	3	3	$\text{lc}(\omega_1)^2$
6	1	6	≤ 3	$\text{lc}(\omega_1)^2 - \text{lc}(f)$
6	2	3	≤ 3	$\text{lc}(\omega_1)^2 - \text{lc}(f)$

3.3. Случай $\deg \omega_2 = 1$

Воспользуемся теоремой 1. Для этого случая $q_0, q_1 \in \mathbb{Q}$ и $\omega_2 = x - a$ для некоторого $a \in \mathbb{Q}$. Система (5) имеет решение

$$q_0 = \sqrt{\gamma h^m(a)}, \quad q_1 = \frac{mh'(a) \cdot q_0}{2h(a)}$$

для любых $a \in \mathbb{Q}$, $h \in \mathbb{Q}[x]$, $\deg h \geq 1$, $\text{lc}(h) = 1$, $h(a) \neq 0$, $\gamma \in \mathbb{Q}^*$, $m \in \mathbb{N}$, $m \geq 2$. Тогда имеем

$$\omega_1 = q_2(x - a)^2 + q_1(x - a) + q_0, \quad F = \frac{\omega_1^2 - \gamma h^m}{(x - a)^2},$$

где q_2 — произвольный многочлен, $2 \deg q_2 \leq m \deg h - 4$, такой, что $(\omega_1, h) \in \mathbb{Q}^*$. При $m \deg h < 4$ имеем $q_2 = 0$. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов. Возможные значения $\deg F \leq 6$, $\deg h \leq 2$, m , $\deg \omega_1$ и γ приведены в таблице 3.

3.4. Случай $\deg \omega_2 = 2$

Воспользуемся теоремой 2. Для этого случая $\deg q_0 = \deg q_1 = 1$ и с помощью сдвига можно считать, что $\omega_2 = x^2 + b$ для некоторого $b \in \mathbb{Q}$. Кроме того, с помощью растяжения можно считать, что $h = q\omega_2 + c$ или $h = q\omega_2 + x + c$, где $q \in \mathbb{Q}[x]$, $\text{lc}(q) = 1$. Остается найти значения параметров, при которых сравнение $q_0^2 \equiv \gamma h^m \pmod{x^2 + b}$ разрешимо.

Пусть $h = q\omega_2 + c$ для некоторого многочлена $q \in \mathbb{Q}[x]$, $\text{lc}(q) = 1$. Тогда необходимо решить сравнение $q_0^2 \equiv \gamma c^m \pmod{x^2 + b}$. Положим $q_0 = a_0 + a_1x$, тогда получаем систему

$$\begin{cases} 2a_0a_1 = 0, \\ a_0^2 - ba_1^2 = \gamma c^m. \end{cases} \quad (10)$$

Таблица 3: значения параметров для случая $\deg \omega_2 = 1$

$\deg F$	$\deg h$	m	$\deg \omega_1$	γ
3	1	5	≤ 2	$-\operatorname{lc}(f)$
3	1	6	3	$\operatorname{lc}(\omega_1)^2$
4	1	6	≤ 3	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
5	1	7	≤ 3	$-\operatorname{lc}(f)$
5	1	8	4	$\operatorname{lc}(\omega_1)^2$
5	2	4	4	$\operatorname{lc}(\omega_1)^2$
6	1	8	≤ 4	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
6	2	4	≤ 4	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$

Если $a_0 = 0$, то $b = -\gamma c^m / a_1^2$ для любых $a_1, c \in \mathbb{Q}^*$. Если $a_1 = 0$ и $2 \deg \omega_1 \leq 2 \deg \omega_2 + \deg f$, то $\gamma = a_0^2 / c^m$ для любых $a_0, b, c \in \mathbb{Q}^*$. Если $a_1 = 0$ и $2 \deg \omega_1 > 2 \deg \omega_2 + \deg f$, то $\gamma = 1$, $a_0 = t^m$, $c = t^2$ для любых $b, t \in \mathbb{Q}^*$. Как отмечалось в теореме 2, многочлен q_1 восстанавливается из сравнения $2h(q_1\omega_2' + q_0') \equiv mq_0h' \pmod{\omega_2}$. Тогда имеем

$$\omega_1 = q_2(x^2 + b)^2 + q_1(x^2 + b) + q_0, \quad F = \frac{\omega_1^2 - \gamma h^m}{\omega_2^2},$$

где q_2 — произвольный многочлен подходящей степени, $\operatorname{lc}(q_2) = 1$. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов.

Таблица 4: значения параметров для случая $\deg \omega_2 = 2$

$\deg F$	$\deg h$	m	$\deg \omega_1$	γ
3	1	8	4	$\operatorname{lc}(\omega_1)^2$
4	1	8	≤ 4	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
5	1	9	≤ 4	$-\operatorname{lc}(f)$
5	1	10	5	$\operatorname{lc}(\omega_1)^2$
5	2	5	5	$\operatorname{lc}(\omega_1)^2$
6	1	10	≤ 5	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
6	2	5	≤ 5	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$

Пусть $h = q\omega_2 + x + c$ для некоторого многочлена $q \in \mathbb{Q}[x]$, $\operatorname{lc}(q) = 1$. Тогда необходимо решить сравнение $q_0^2 \equiv \gamma(x + c)^m \pmod{x^2 + b}$. Положим $\gamma(x + c)^m \equiv Cx + B \pmod{x^2 + b}$ и $q_0 = a_0 + a_1x$, тогда получаем систему

$$\begin{cases} 2a_0a_1 = C, \\ a_0^2 - ba_1^2 = B, \end{cases} \quad (11)$$

причем $B = B(\gamma, b, c)$ и $C = C(\gamma, b, c)$. Из первого уравнения при условии, что $C \neq 0$, имеем $a_1 = C/2a_0$, тогда из второго получаем

$$a_0^2 = \frac{B \pm \sqrt{B^2 + bC^2}}{2}. \quad (12)$$

Если представить $(x + c)^m = (x^2 + b)Q(x) + Cx + B$ для некоторого $Q(x) \in \mathbb{Q}[x]$, то

$$\begin{aligned} B^2 + bC^2 &= (B + \sqrt{-b}C)(B - \sqrt{-b}C) = \prod_{x=\pm\sqrt{-b}} ((x^2 + b)Q(x) + Cx + B) = \\ &= (\sqrt{-b} + c)^m(-\sqrt{-b} + c)^m = (b + c^2)^m. \end{aligned}$$

Остается подобрать значения параметров γ, b, c так, чтобы $(b + c^2)^m$ и выражение в правой части равенства (12) являлись полными квадратами над $\mathbb{Q}$.

Случай $C = 0$ необходимо рассматривать отдельно.

Далее многочлены q_1 и f восстанавливаются также, как было указано выше. Возможные значения $\deg F \leq 6$, $\deg h \leq 2$, m , $\deg \omega_1$ и γ приведены в таблице 4.

4. Параметрические семейства кривых рода два

В качестве иллюстрации приведенных методов приведем параметризацию для гиперэллиптических кривых рода два над полем $\mathbb{Q}$, имеющих рациональную точку. Такие кривые могут быть заданы уравнением $C : y^2 = f(x)$, где $f(x) \in [x]$ — свободный от квадратов многочлен, $5 \leq \deg f \leq 6$.

Напомним, что в любом классе дивизоров степени ноль содержится единственный представитель вида $D - (\infty^- + \infty^+)$, где D — эффeктивный дивизор степени 2, не содержащий самосопряженных точек с кратностью 2. Такой представитель будем называть *каноническим*. Мы будем использовать буквами $P, P_1, P_2, \dots$ для обозначения некоторых плейсов степени один. Путем домножения многочлена f на $\text{lc}(\omega_2)^2$, можно без ограничения общности считать, что $\text{lc}(\omega_2) = 1$. Также без ограничения общности в норменном уравнении мы можем делать линейные замены вида $X = ax + b$, поскольку “сдвиг” и “растяжение” по координате x соответствует изоморфизму гиперэллиптических кривых. Например, с помощью “сдвига” и “растяжения” без ограничения общности можно считать, что многочлен ω степени $k \geq 2$ имеет вид $\omega = a_k x^k + a_{k-2} x^{k-2} + \dots + a_2 x^2 + x + a_0$ или $\omega = a_k x^k + a_{k-2} x^{k-2} + \dots + a_2 x^2 + a_0$. В различных ситуациях с помощью “сдвига” и “растяжения” мы будем фиксировать разные коэффициенты многочленов ω_1 и ω_2 . Кроме того, умножая норменное уравнение на полный квадрат, можно без ограничения общности считать, что зафиксирован еще один из коэффициентов многочленов ω_1 или ω_2 . Например, таким образом можно зафиксировать старший коэффициент многочлена ω_1 , $\text{lc}(\omega_1) = 1$.

Далее рассмотрим по-очереди возможные порядки $3 \leq m \leq 5$ в якобиевых многообразиях гиперэллиптической кривой рода 2, как в предложении 2. Отметим, что случай $m = 2$ возможен только для дивизора вида $2(P - \infty) \sim 0$, который является главным дивизором для функции $x - x_P$ в поле $L = \mathbb{Q}(x)(\sqrt{f})$, где $f = (x - x_P)\omega$, $\omega \in \mathbb{Q}[x]$, $\deg \omega = 4$. Основы теории дивизоров в гиперэллиптических полях в наших обозначениях описаны в статье [26].

4.1. Порядок 3

Рассмотрим в классе дивизоров порядка 3 канонический представитель $D - (\infty^- + \infty^+)$. Если $v_\infty^+(D) > 0$, то $v_\infty^+(D) = 2$, поскольку по лемме Мамфорда (см. лемму 2.2 [26]) дивизор вида $3(P - \infty^-)$ не может быть главным в поле L . Если $v_\infty^+(D) = 2$, то соотношение $3(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega^2 - f = \gamma,$$

где $\deg \omega = 3$, $\text{lc}(\omega) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига и растяжения мы можем считать, что $\omega_1 = x^3 + x + c_0$ или $\omega_1 = x^3 + c_0$, где $c_0, \gamma \in \mathbb{Q}$. Таким

образом, искомая параметризация имеет вид

$$f = \omega_1^2 - \gamma,$$

где $\omega_1 \in \mathbb{Q}[x]$ и $\gamma \neq 0$ такие, что многочлен f свободен от квадратов.

Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то соотношение $3(D - (\infty^- + \infty^+)) \sim 0$ эквивалентно существованию многочлена $\omega \in \mathbb{Q}[x]$, $\deg \omega \leq 3$, $\text{lc}(\omega) = 1$, такого, что $\omega^2 - f = \gamma h^3$, где $\gamma \in \mathbb{Q}^*$ и $h = \text{Pol}(D) \in \mathbb{Q}[x]$ — такой многочлен, что $\text{lc}(h) = 1$, $\deg h = 2$, главный дивизор $(h) = D + \iota D - 2(\infty^- + \infty^+)$. Без ограничения общности путем сдвига мы можем считать, что $\omega_1 = x^3 + x + c_0$ или $\omega_1 = x^3 + c_0$, где $c_0, \gamma \in \mathbb{Q}$. Таким образом, искомая параметризация имеет вид

$$f = \omega^2 - \gamma h^3,$$

где $\gamma \in \mathbb{Q}^*$, $\omega, h \in \mathbb{Q}[x]$ такие, что многочлен f свободен от квадратов, $5 \leq \deg f \leq 6$.

4.2. Порядок 4

Рассмотрим в классе дивизоров порядка 4 канонический представитель $D - (\infty^- + \infty^+)$. Если $v_\infty^+(D) > 0$, то $v_\infty^+(D) = 2$, поскольку по лемме Мамфорда (см. лемму 2.2 [26]) дивизор вида $4(P - \infty^-)$ не может быть главным в поле L . Если $v_\infty^+(D) = 2$, то соотношение $4(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega_1^2 - \omega_2^2 f = \gamma, \quad (13)$$

где $\deg \omega_1 = 4$, $\deg \omega_2 = 1$, $\text{lc}(\omega_1) = \text{lc}(\omega_2) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига мы можем считать, что $\omega_2 = x$. Тогда уравнение (13) равносильно системе

$$\begin{cases} \omega_1^2(0) = \gamma, \\ 2\omega_1(0)\omega_1'(0) = 0. \end{cases}$$

Таким образом, искомая параметризация имеет вид

$$f = \frac{\omega_1^2 - \gamma}{x^2},$$

где $\gamma = \omega_1^2(0)$, $\omega_1 = x^4 + c_3 x^3 + c_2 x^2 + c_0 \in \mathbb{Q}[x]$ такой, что f — свободен от квадратов.

Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то соотношение $4(D - (\infty^- + \infty^+)) \sim 0$ эквивалентно существованию многочленов $\omega_1, \omega_2 \in \mathbb{Q}[x]$, $\deg \omega_1 \leq 4$, $\deg \omega_2 \leq 1$, таких, что

$$\omega_1^2 - \omega_2^2 f = \gamma h^4, \quad \max(2 \deg \omega_1, 2 \deg \omega_2 + \deg f) = 8, \quad 5 \leq \deg f \leq 6,$$

где $h = \text{Pol}(D)$, $\text{lc}(h) = 1$, $\deg h = 2$, $\text{lc}(\omega_2) = 1$. С помощью сдвига всегда можно считать, что $h = x^2 + b$ для некоторой постоянной $b \in \mathbb{Q}^*$.

Рассмотрим случай, когда $\deg \omega_2 = 1$. Тогда путем растяжения можно считать, что $\omega_2 = x$ или $\omega_2 = x - 1$. Как в теореме 1 запишем $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2 , и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2 .

Пусть $\omega_2 = x$, тогда $b \neq 0$, и по пункту 3.3 имеем $q_1 = 0$, $q_0 = b^2 t$, $\gamma = t^2$, где $t \in \mathbb{Q}^*$. Отсюда для произвольного $q_2 \in \mathbb{Q}[x]$, $\deg q_2 \leq 2$, $b, t \in \mathbb{Q}^*$, находим

$$f = (q_2 - t(x^2 + 2b))(q_2 x^2 + b^2 t + t(x^2 + b)^2).$$

Мы можем без ограничения общности предполагать, что $\text{lc}(q_2) = 1$, поскольку, умножая норменное уравнение на полный квадрат, можно зафиксировать один из коэффициентов многочлена ω_1 .

Пусть $\omega_2 = x - 1$, тогда по пункту 3.4 имеем $q_1 = 4t(b+1)$, $q_0 = t(b+1)^2$, $\gamma = t^2$, где $t \in \mathbb{Q}^*$. Отсюда для произвольного $q_2 \in \mathbb{Q}[x]$, $\deg q_2 \leq 2$, $\text{lc}(q_2) = 1$, $b, t \in \mathbb{Q}^*$, находим

$$f = (q_2 - t((x+1)^2 + 2(b+1))) (q_2(x-1)^2 + 4t(b+1)(x-1) + t(b+1)^2 + t(x^2 + b)^2).$$

Если $\deg \omega_2 < 1$, то $\omega_2 = 1$ и $f = \omega_1^2 - \gamma h^4$, причем $\deg \omega_1 = 4$, $\text{lc}(\omega_1) = 1$, $5 \leq \deg f \leq 6$. Значит, должно быть $\gamma = 1$ и $1 \leq \deg(\omega - h^2) \leq 2$, то есть $\omega = h^2 + a_2x^2 + a_1x + a_0$, где $a_0, a_1, a_2 \in \mathbb{Q}^*$ — произвольные числа, $a_2^2 + a_1^2 \neq 0$, откуда

$$f = (a_2x^2 + a_1x + a_0)(2h^2 + a_2x^2 + a_1x + a_0).$$

За счет растяжения и сдвига можно считать, что $h = x^2 + b$ для некоторой постоянной $b \in \mathbb{Q}^*$, и $a_1 = 1$ или $a_1 = 0$.

4.3. Порядок 5

Рассмотрим в классе дивизоров порядка 5 канонический представитель $D - (\infty^- + \infty^+)$. Необходимо рассмотреть три случая: $v_\infty^+(D) = 2$, $v_\infty^+(D) = 1$ и $v_\infty^-(D) = v_\infty^+(D) = 0$.

Если $v_\infty^+(D) = 2$, то соотношение $5(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega_1^2 - \omega_2^2 f = \gamma, \quad (14)$$

где $\deg \omega_1 = 5$, $\deg \omega_2 = 2$, $\text{lc}(\omega_1) = \text{lc}(\omega_2) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига мы можем считать, что $\omega_2 = x^2 + b$. Тогда уравнение (14) равносильно системе сравнений

$$\begin{cases} \omega_1^2 \equiv \gamma \pmod{\omega_2}, \\ 2\omega_1\omega_1' \equiv 0 \pmod{\omega_2}. \end{cases}$$

Как в теореме 1 запишем $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2 , и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2 . Тогда последняя система сравнений равносильна системе

$$\begin{cases} q_0^2 \equiv \gamma \pmod{\omega_2}, \\ q_0(\omega_2'q_1 + q_0') \equiv 0 \pmod{\omega_2}. \end{cases}$$

Без ограничения общности путем растяжения мы можем считать, что $q_0 = x + a_0$ или $q_0 = a_0$. Если $q_0 = x + a_0$, то из первого сравнения системы имеем $a_0 = 0$, $\gamma = -b \neq 0$, и второе сравнение системы имеет вид

$$x(2x(a_2x + a_1) + 1) \equiv 0 \pmod{x^2 + b}.$$

Отсюда получаем, что $a_1 = 0$, $a_2 = 1/2b$. Положим $q_2 = x + a$, тогда искомая параметризация имеет вид

$$\begin{aligned} f = & x^6 + 2ax^5 + x^4 \frac{(a^2b + 2b^2 + 1)}{b} + x^3 \frac{a(4b^2 + 1)}{b} + \\ & + x^2 \frac{(8a^2b^3 + 4b^4 + 12b^2 + 1)}{4b^2} + xa(2b^2 + 3) + \frac{a^2b^3 + 1}{b}, \end{aligned}$$

где $a, b \in \mathbb{Q}$ такие, что $b \neq 0$, многочлен f свободен от квадратов.

Если $v_\infty^+(D) = 1$, то соотношение $5(P - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega^2 - f = \gamma h^5, \quad (15)$$

где $h, \omega \in \mathbb{Q}[x]$, $\deg \omega \leq 2$, $\deg h = 1$. Без ограничения общности с помощью сдвига можно считать, что $h = x$. С помощью растяжения по x и домножения норменного уравнения на постоянную, являющуюся полным квадратом в $\mathbb{Q}^*$, можно считать, что $\omega = ax^2 + x + 1$ или $\omega = ax^2 + 1$, где $a, \gamma \in \mathbb{Q}$, $\gamma \neq 0$. Тогда при $\omega = ax^2 + x + 1$ искомая параметризация имеет вид

$$f = -\gamma x^5 + a^2 x^4 + 2ax^3 + x^2(2a + 1) + 2x + 1,$$

а при $\omega = ax^2 + 1$ искомая параметризация имеет вид

$$f = -\gamma x^5 + a^2 x^4 + 2ax^2 + 1.$$

Пусть теперь $v_\infty^-(D) = v_\infty^+(D) = 0$, $h = \text{Pol}(D)$, $\text{lc}(h) = 1$, $\deg h = 2$. Соотношение $5(D - (\infty^- + \infty^+)) \sim 0$ эквивалентно существованию многочленов $\omega_1, \omega_2 \in \mathbb{Q}[x]$, $\deg \omega_1 \leq 5$, $\deg \omega_1 \leq 2$, таких, что

$$\omega_1^2 - \omega_2^2 f = \gamma h^5, \quad \max(2 \deg \omega_1, 2 \deg \omega_2 + \deg f) = 10.$$

За счет сдвига и растяжения по x не ограничивая общности достаточно рассмотреть следующие случаи

- $\deg \omega_2 = 2$, $\deg \omega_1 \leq 5$, $\omega_2 = x^2 + b$, $h = \omega_2 + x + c$;
- $\deg \omega_2 = 2$, $\deg \omega_1 \leq 5$, $\omega_2 = x^2 + b$, $h = \omega_2 + c$;
- $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + c$, $\gamma = 1$, $\omega_2 = x$;
- $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + x + c$, $\gamma = 1$, $\omega_2 = x$;
- $\deg \omega_2 = 0$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + c$, $\gamma = 1$, $\omega_2 = 1$,

где $b, c \in \mathbb{Q}$.

Случай $\omega_2 = x^2 + b$, $h = \omega_2 + x + c$.

По пункту 3.4 имеем $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, $\deg q_0, \deg q_1, \deg q_2 \leq 1$, $q_0 = a_0 + a_1 x$, $q_1 = a_2 + a_3 x$, и $q_2 = ex + a$, $a, e \in \mathbb{Q}$. Как в 3.4 запишем

$$\gamma(x + c)^5 \equiv Cx + B \pmod{x^2 + b}, \quad B = \gamma(5b^2c - 10bc^3 + c^5), \quad C = \gamma(b^2 - 10bc^2 + 5c^4).$$

Получаем систему (11), из которой при условии, что $C \neq 0$, находим выражение (12) для a_0^2 , причем $B^2 + bC^2 = \gamma^2(b + c^2)^5$. Сделаем замену $b = s^2 - c^2$, тогда

$$a_0^2 = \frac{\gamma(c + s)}{2}(-4c^2 + 2cs + s^2)^2.$$

Сделаем замену $c = -s + 2t^2/\gamma$, тогда

$$a_0 = \frac{t(5\gamma^2 s^2 - 20\gamma s t^2 + 16t^4)}{\gamma^2}, \quad a_1 = \frac{\gamma^2 s^2 - 12\gamma s t^2 + 16t^4}{2\gamma t}. \quad (16)$$

Далее из сравнения $2h(q_1 \omega_2' + q_0') \equiv m q_0 h' \pmod{\omega_2}$ находим коэффициенты многочлена q_1 :

$$a_2 = \frac{-5\gamma^2 s - 60\gamma s t^2 + 20\gamma t^2 + 80t^4}{8\gamma t}, \quad a_3 = \frac{\gamma^2 s - 20\gamma s t^2 + 4\gamma t^2 + 80t^4}{16t^3}. \quad (17)$$

В итоге получаем параметризацию

$$\begin{aligned}
f &= f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0, \\
f_6 &= -\gamma + e^2, \quad f_5 = -5\gamma + 2ae, \\
f_4 &= e^2 \left(\frac{8st^2}{\gamma} - \frac{8t^4}{\gamma^2} \right) + e \left(-\frac{\gamma s(-\gamma + 20t^2)}{8t^3} + \frac{\gamma + 20t^2}{2t} \right) + \\
&\quad + s(5\gamma - 12t^2) + \frac{-10\gamma^2 + \gamma a^2 - 10\gamma t^2 + 12t^4}{\gamma}, \\
f_3 &= e \left(\frac{s(-5\gamma^2 - 60\gamma t^2 + 64at^3)}{4\gamma t} - \frac{t(-5\gamma^2 - 20\gamma t^2 + 16at^3)}{\gamma^2} \right) - \\
&\quad - \frac{s(-\gamma^2 a + 20\gamma at^2 - 160\gamma t^3 + 320t^5)}{8t^3} + \frac{\gamma^2 a - 20\gamma^2 t + 20\gamma at^2 - 80\gamma t^3 + 80t^5}{2\gamma t}, \\
f_2 &= e^2 \left(\frac{16s^2 t^4}{\gamma^2} - \frac{32st^6}{\gamma^3} + \frac{16t^8}{\gamma^4} \right) + \\
&\quad + e \left(-\frac{s^2(-3\gamma + 20t^2)}{2t} + \frac{st(-21\gamma + 100t^2)}{2\gamma} - \frac{2t^3(-7\gamma + 20t^2)}{\gamma^2} \right) - \\
&\quad - \frac{s^2(-\gamma^5 + 40\gamma^4 t^2 - 400\gamma^3 t^4 + 2560\gamma^2 t^6 - 10240\gamma t^8 + 12288t^{10})}{256\gamma t^6} + \\
&\quad + \frac{s(\gamma^5 - 40\gamma^3 at^3 + 560\gamma^3 t^4 - 480\gamma^2 at^5 + 256\gamma a^2 t^6 - 3840\gamma t^8 + 3072t^{10})}{32\gamma^2 t^4} - \\
&\quad - \frac{-\gamma^5 + 40\gamma^4 t^2 - 80\gamma^3 at^3 + 560\gamma^3 t^4 - 320\gamma^2 at^5 + 128\gamma a^2 t^6 - 1280\gamma t^8 + 768t^{10}}{16\gamma^3 t^2}, \\
f_1 &= e \left(\frac{s^2 t(5\gamma^2 - 60\gamma t^2 + 32at^3)}{\gamma^2} - \frac{st^3(15\gamma^2 - 140\gamma t^2 + 64at^3)}{\gamma^3} + \frac{4t^5(3\gamma^2 - 20\gamma t^2 + 8at^3)}{\gamma^4} \right) - \\
&\quad - \frac{s^2(5\gamma^4 - 40\gamma^3 t^2 - 96\gamma^2 at^3 + 720\gamma^2 t^4 + 640\gamma at^5 - 5120\gamma t^6 + 5120t^8)}{64\gamma t^4} + \\
&\quad + \frac{s(10\gamma^3 - 21\gamma^2 at + 40\gamma^2 t^2 + 100\gamma at^3 - 480\gamma t^4 + 320t^6)}{2\gamma^2} - \\
&\quad - \frac{-\gamma^4 + 40\gamma^3 t^2 - 56\gamma^2 at^3 + 80\gamma^2 t^4 + 160\gamma at^5 - 640\gamma t^6 + 320t^8}{4\gamma^3}, \\
f_0 &= -\frac{s^3(-\gamma + 4t^2)^5}{16\gamma^2 t^4} + \frac{s^2(-7\gamma^5 - 40\gamma^4 t^2 + 320\gamma^3 at^3)}{64\gamma^3 t^2} + \\
&\quad + \frac{s^2(-240\gamma^3 t^4 - 3840\gamma^2 at^5 + 12800\gamma^2 t^6 + 1024\gamma a^2 t^6 - 20480\gamma t^8 + 12288t^{10})}{64\gamma^3 t^2} - \\
&\quad - \frac{s(\gamma^5 - 80\gamma^4 t^2 + 120\gamma^3 at^3 + 240\gamma^3 t^4 - 1120\gamma^2 at^5 + 2560\gamma^2 t^6 + 256\gamma a^2 t^6 - 3200\gamma t^8 + 1536t^{10})}{8\gamma^4} + \\
&\quad + \frac{t^2(\gamma^5 - 40\gamma^4 t^2 + 48\gamma^3 at^3 + 80\gamma^3 t^4 - 320\gamma^2 at^5 + 640\gamma^2 t^6 + 64\gamma a^2 t^6 - 640\gamma t^8 + 256t^{10})}{4\gamma^5},
\end{aligned}$$

где параметры $a, e \in \mathbb{Q}$, $t, s, \gamma \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $C = 0$ возможен только, если $c = 0$, но тогда $b = 0$, чего не может быть, так как в этом случае $(\omega_2, h) = x \notin \mathbb{Q}^*$.

Также отметим, что многочлен ω_2 должен быть свободен от квадратов, поскольку иначе $b = 0$, что влечет $c = 0$, а это невозможно.

Случай $\omega_2 = x^2 + b$, $h = \omega_2 + c$.

Аналогично действуя по пункту 3.4, имеем два варианта, когда $a_0 = 0$ или $a_1 = 0$.

При $a_0 = 0$ получаем

$$q_2 = ex + a, \quad a_1 = t, \quad a_2 = 0, \quad a_3 = \frac{5c^4tv - t^3}{2c^5v}.$$

Отсюда получаем параметризацию

$$\begin{aligned} f &= (e^2 - \gamma)x^6 + 2aex^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \\ f_4 &= -\frac{2\gamma c^5 e^2}{t^2} + \frac{3\gamma^2 c^5 - 5\gamma ct^2 + a^2 t^2}{t^2} - \frac{et(-5\gamma c^4 + t^2)}{\gamma c^5}, \\ f_3 &= -\frac{4\gamma ac^5 e}{t^2} - \frac{at(-5\gamma c^4 + t^2)}{\gamma c^5}, \\ f_2 &= \frac{\gamma^2 c^{10} e^2}{t^4} + \frac{e(-5\gamma c^4 + 3t^2)}{t} + \\ &+ \frac{-12\gamma^5 c^{20} + 40\gamma^4 c^{16} t^2 - 8\gamma^3 a^2 c^{15} t^2 - 40\gamma^3 c^{12} t^4 + 25\gamma^2 c^8 t^6 - 10\gamma c^4 t^8 + t^{10}}{4\gamma^2 c^{10} t^4}, \\ f_1 &= \frac{2\gamma^2 ac^{10} e}{t^4} + \frac{a(-5\gamma c^4 + 3t^2)}{t}, \\ f_0 &= -\frac{-\gamma^5 c^{20} + 5\gamma^4 c^{16} t^2 - \gamma^3 a^2 c^{15} t^2 - 10\gamma^3 c^{12} t^4 + 10\gamma^2 c^8 t^6 - 5\gamma c^4 t^8 + t^{10}}{\gamma c^5 t^6}, \end{aligned}$$

где параметры $a, e \in \mathbb{Q}$, $c, t, \gamma \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

При $a_1 = 0$ необходимо рассмотреть два случая: $\deg f = 6$ или $\deg f = 5$. Пусть $\deg f = 6$, тогда можно положить

$$q_2 = ex + a, \quad a_0 = t, \quad a_2 = 5t/(2c), \quad a_3 = 0.$$

Отсюда получаем параметризацию

$$\begin{aligned} f &= e^2 - \frac{t^2}{c^5}x^6 + 2aex^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \\ f_4 &= 2be^2 - \frac{-a^2c^5 + 3bt^2 + 5ct^2}{c^5}, \quad f_3 = \frac{e(4abc + 5t)}{c}, \\ f_2 &= b^2e^2 - \frac{-2a^2bc^5 - 5ac^4t + 3b^2t^2 + 10bct^2 + 10c^2t^2}{c^5}, \\ f_1 &= \frac{e(2ab^2c + 5bt + 2ct)}{c}, \\ f_0 &= -\frac{-4a^2b^2c^5 - 20abc^4t - 8ac^5t + 4b^3t^2 + 20b^2ct^2 + 40bc^2t^2 + 15c^3t^2}{4c^5}, \end{aligned}$$

где параметры $a, b, c, e, t \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

В случае, когда $\deg f = 5$ имеем $\deg \omega_1 = 6$, $\text{lc}(\omega_1) = 1$, $q_2 = x + a$,

$$\gamma = 1, \quad a_0 = t^5, \quad c = t^2, \quad a_2 = \frac{5t^3}{2}, \quad a_3 = 0.$$

Отсюда получаем параметризацию

$$\begin{aligned} f &= 2ax^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \\ f_5 &= 2a, \quad f_4 = a^2 - b - 5t^2, \quad f_3 = 4ab + 5t^3, \\ f_2 &= 2a^2b + 5at^3 - 2b^2 - 10bt^2 - 10t^4, \quad f_1 = 2ab^2 + 5bt^3 + 2t^5, \\ f_0 &= -\frac{-4a^2b^2 - 20abt^3 - 8at^5 + 4b^3 + 20b^2t^2 + 40bt^4 + 15t^6}{4}, \end{aligned}$$

где параметры $a, b, t \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + c$, $\omega_2 = x$

Так как в этом случае $\deg(\omega_1^2) > \deg(\omega_2^2 f)$ и $\text{lc}(\omega_1) = 1$, то в норменном уравнении $\gamma = 1$. Таким образом, норменное уравнение (3) эквивалентно системе

$$\begin{aligned}\deg(\omega_1^2 - h^5) &\leq 8, \\ \omega_1^2 &\equiv h^5 \pmod{x^2}.\end{aligned}$$

Положим $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, тогда первое условие системе равносильно условию $a_4 = 0$, а второе условие системы равносильно условиям $a_1 = 0$ и $a_0^2 = c^5$. Значит, можно положить $a_0 = t^5$, $c = t^2$, $a_2 = e$, $a_3 = s$, откуда получается параметризация

$$f = (2s - 5t^2)x^6 + 2ex^5 + (s^2 - 10t^4)x^4 + (2es + 2t^5)x^3 + (e^2 - 10t^6)x^2 + 2st^5x + 2et^5 - 5t^8,$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + x + c$, $\omega_2 = x$

Аналогично предыдущему случаю $\gamma = 1$ и можно положить $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, где $c = t^2$, $a_0 = t^5$, $a_1 = 5c^3/2$, $a_2 = e$, $a_3 = s$, $a_4 = 5/2$. Отсюда получается параметризация

$$\begin{aligned}f = x^6 \left(2s - \frac{5(4t^2 + 3)}{4} \right) + x^5 (5s - 2(-e + 10t^2 + 5)) + \\ + x^4 (s^2 - 5(-e + 2t^4 - t^3 + 6t^2 + 1)) + x^3 \left(2es + \frac{4t^5 - 60t^4 + 25t^3 - 40t^2 - 2}{2} \right) + \\ + x^2 (e^2 + 5st^3 - 10t^6 + 5t^5 - 30t^4 - 5t^2) + \\ + x (2st^5 - 5t^3(-e + 4t^3 + 2t)) - \frac{t^5(-8e + 20t^3 + 15t)}{4},\end{aligned}$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg \omega_2 = 0$, $\deg \omega_1 = 5$, $\text{lc}(\omega_1) = 1$, $h = x^2 + c$, $\omega_2 = 1$

Если положить $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, то норменное уравнение (3) дает условие $\deg(\omega_1^2 - h^5) \leq 6$, откуда $a_0 = e$, $a_1 = s$, $a_2 = 0$, $a_3 = 5t/2$, $a_4 = 0$, $c = t$. Отсюда получается параметризация

$$f = x^6 \left(2s - \frac{15t^2}{4} \right) + 2ex^5 + x^4 (5st - 10t^3) + 5etx^3 + x^2 (s^2 - 5t^4) + 2esx + e^2 - t^5,$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

5. Заключение

Автор выражает большую благодарность академику В. П. Платонову за многолетнюю поддержку, постановку задач и активное участие в совместных математических исследованиях.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Mazur B. Rational points on modular curves // Modular Funct. one Var. V, Proc. Int. Conf., Bonn 1976. Lect. Notes Math. 1977. Vol. 601. P. 107-148.
2. Kubert D. S. Universal bounds on the torsion of elliptic curves // Proc. London Math. Soc. (3). 1976. Vol. 33, № 2. P. 193-237.
3. Kubert D. S. Universal bounds on the torsion of elliptic curves // Compositio Mathematica. 1979. Vol. 38, № 1. P. 121-128.
4. Adams W. W., Razar M. J. Multiples of points on elliptic curves and continued fractions // Proc. London Math. Soc. 1980. Vol. 41, № 3. P. 481-498.
5. Van Der Poorten A. J., Tran X. C. Periodic continued fractions in elliptic function fields // International Algorithmic Number Theory Symposium. – Springer, Berlin, Heidelberg, 2002. P. 390-404.

6. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в эллиптических полях // ДАН. 2017. Т. 475, № 2. С. 133-136.
7. Платонов В. П., Федоров Г. В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209, № 4. С. 54-94.
8. Платонов В. П., Федоров Г. В. Критерий периодичности непрерывных дробей ключевых элементов гиперэллиптических полей // Чебышевский сборник. 2019. Т. 20, № 1. С. 246-258.
9. Федоров Г. В. Об ограниченности длин периодов непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел // Чебышевский сборник. 2019. Т. 20, № 4. С. 321-334.
10. Kamienny S. Torsion points on elliptic curves over all quadratic fields // Duke Math. J. 1986. Vol. 53, № 1. P. 157-162.
11. Kenku M. A, Momose F. Torsion points on elliptic curves defined over quadratic fields // Nagoya Math. J. 1988. Vol. 109. P. 125-149.
12. Платонов В. П., Жгун В. С., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант // ДАН. 2018. Т. 482, № 2. С. 137-141.
13. Платонов В. П., Жгун В. С., Петрунин М. М., Штейников Ю. Н. О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // ДАН. 2018. Т. 483, № 6. С. 603-608.
14. Платонов В. П., Петрунин М. М., Штейников Ю. Н. О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // ДАН. 2019. Т. 488, № 3. С. 237-242.
15. Merel L. Bornes pour la torsion des courbes elliptiques sur les corps de nombres // Invent. Math. 1996. Vol. 124, № 1-3. P. 437-449.
16. Howe E. W. Genus-2 Jacobians with torsion points of large order // Bull. London Math. Soc. 2015. Vol. 47. P. 127-135.
17. Платонов В. П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. 2014. Т. 69, № 1(415). С. 3-38.
18. Петрунин М. М. Вычисление фундаментальных S-единиц в гиперэллиптических полях рода 2 и проблема кручения в якобианах гиперэллиптических кривых // Чебышевский сборник. 2015. Т. 16, № 4. С. 250-283.
19. Платонов В. П., Федоров Г. В. Бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28 // ДАН. 2018. Т. 482, № 4. С. 385-388.
20. Бенияш-Кривец В. В., Платонов В. П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Матем. сб. 2009. Т. 200, № 1. С. 15-44.
21. Платонов В. П., Федоров Г. В. S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // ДАН. 2015. Т. 465, № 5. С. 537-541.
22. Платонов В. П., Петрунин М. М. S-единицы и периодичность в квадратичных функциональных полях // УМН. 2016. Т. 71, № 5. С. 181-182.
23. Платонов В. П., Петрунин М. М. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // ДАН. 2016. Т. 470, № 3. С. 260-265.
24. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях // ДАН. 2017. Т. 474, № 5. С. 540-544.
25. Платонов В. П., Петрунин М. М. Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Тр. МИАН. 2018. Т. 302. С. 354-376.

26. Федоров Г. В. Об S-единицах для нормирований второй степени в гиперэллиптических полях // Известия РАН. 2020. Т. 84, № 2 (в печати).
27. Федоров Г. В. Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях // Чебышевский сборник. 2018. Т. 19, № 3. С. 283-298.
28. Жгун В. С. Обобщенные якобианы и непрерывные дроби в гиперэллиптических полях // Чебышевский сборник. 2017. Т. 18, № 4. С. 208-220.
29. Платонов В. П., Жгун В. С., Федоров Г. В. Непрерывные дроби в гиперэллиптических полях и многочлены Мамфорда // ДАН. 2016. Т. 471, № 6. С. 640-644.
30. Кузнецов Ю. В., Штейников Ю. Н. О некоторых свойствах непрерывных периодических дробей с небольшой длиной периода, связанных с гиперэллиптическими полями и S-единицами // Чебышевский сборник. 2017. Т. 18, № 4. С. 260-267.

REFERENCES

1. Mazur, B. 1977, "Rational points on modular curves" *Modular Funct. one Var. V, Proc. Int. Conf., Bonn 1976* Lect. Notes Math., vol. 601, pp. 107-148.
2. Kubert, D.S. 1976, "Universal bounds on the torsion of elliptic curves" *Proc. London Math.Soc. (3)*, vol. 33, no. 2, pp. 193-237.
3. Kubert, D.S. 1979, "Universal bounds on the torsion of elliptic curves" *Compositio Mathematica*, vol. 38, no. 1, pp. 121-128.
4. Adams W. W., Razar M. J. 1980, "Multiples of points on elliptic curves and continued fractions", *Proc. London Math. Soc.*, vol. 41, no. 3, pp. 481-498.
5. Van Der Poorten A. J., Tran X. C. 2002, "Periodic continued fractions in elliptic function fields", *International Algorithmic Number Theory Symposium*. – Springer, Berlin, Heidelberg, pp. 390-404.
6. Platonov, V. P., Fedorov, G. V. 2017, "On the periodicity of continued fractions in elliptic fields", *Dokl. Math.*, vol. 96, no. 1, pp. 332-335.
7. Platonov, V. P., Fedorov, G. V. 2018, "On the problem of periodicity of continued fractions in hyperelliptic fields", *Sb. Math.*, vol. 209, no. 4, pp. 519-559.
8. Platonov, V. P., Fedorov, G. V. 2019, "The criterion of the periodicity of continued fractions of key elements in hyperelliptic fields", *Chebyshevskii Sbornik*, vol. 20, no. 1, pp. 246-258 (In Russ.)
9. Fedorov, G. V. 2019, "On boundedness of period lengths of continued fractions of key elements hyperelliptic fields over the field of rational numbers", *Chebyshevskii Sbornik*, vol. 20, no. 4, pp. 321-334 (In Russ.)
10. Kamienny, S. 1986, "Torsion points on elliptic curves over all quadratic fields" *Duke Math. J.*, vol. 53, no. 1, pp. 157-162.
11. Kenku, M. A, Momose, F. 1988, "Torsion points on elliptic curves defined over quadratic fields" *Nagoya Math. J.*, vol. 109, pp. 125-149.
12. Platonov, V. P., Zhgoon, V. S., Fedorov, G. V. 2016, "On the Periodicity of Continued Fractions in Hyperelliptic Fields over Quadratic Constant Field", *Dokl. Math.*, vol. 98, no. 2, pp. 430-434.
13. Platonov, V. P., Zhgoon, V. S., Petrunin, M. M., Shteinikov, Yu. N. 2018, "On the Finiteness of Hyperelliptic Fields with Special Properties and Periodic Expansion of $\sqrt{f}$ ", *Dokl. Math.*, vol. 98, no. 3, pp. 641-645.
14. Platonov, V. P., Petrunin, M. M., Shteinikov, Yu. N. 2019, "On the Finiteness of the Number of Elliptic Fields with Given Degrees of S-Units and Periodic Expansion of $\sqrt{f}$ ", *Dokl. Math.*, vol. 100, no. 2, pp. 1-5.
15. Merel, L. 1996, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres" *Invent. Math.*, vol. 124, no. 1-3, pp. 437-449.

16. Howe, E. W. 2015, "Genus-2 Jacobians with torsion points of large order" *Bull. London Math. Soc.*, vol. 47, pp. 127-135.
17. Platonov, V. P. 2014, "Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field", *Russian Math. Surveys*, vol. 69, no. 1, pp. 1-34.
18. Petrunin, M. M. 2015, "Calculation of the fundamental S-units in hyperelliptic fields of genus 2 and the torsion problem in the jacobians of hyperelliptic curves", *Chebyshevskii Sbornik*, vol. 16, no. 4, pp. 250-283 (In Russ.)
19. Platonov, V. P., Fedorov, G. V. 2018, "An infinite family of curves of genus 2 over the field of rational numbers whose jacobian varieties contain rational points of order 28", *Dokl. Math.*, vol. 98, no. 2, pp. 468-471.
20. Benyash-Krivets, V. V., Platonov, V. P. 2009, "Groups of S-units in hyperelliptic fields and continued fractions", *Sb. Math.*, vol. 200, no. 11, pp. 1587-1615.
21. Platonov, V. P., Fedorov, G. V. 2015, "S-Units and Periodicity of Continued Fractions in Hyperelliptic Fields", *Dokl. Math.*, vol. 92, no. 3, pp. 752-756.
22. Platonov, V. P., Petrunin, M. M. 2016, "S-Units and periodicity in quadratic function fields", *Russian Math. Surveys*, vol. 71, no. 5, pp. 973-975.
23. Platonov, V. P., Petrunin, M. M. 2016, "S-units in hyperelliptic fields and periodicity of continued fractions", *Dokl. Math.*, vol. 94, no. 2, pp. 532-537.
24. Platonov, V. P., Fedorov, G. V. 2017, "On the periodicity of continued fractions in hyperelliptic fields", *Dokl. Math.*, vol. 95, no. 3, pp. 254-258.
25. Platonov, V. P., Petrunin, M. M. 2018, "Groups of S-units and the problem of periodicity of continued fractions in hyperelliptic fields", *Proc. Steklov Inst. Math.*, vol. 302, pp. 336-357.
26. Fedorov, G. V. 2020, "On S-units for second degree valuations in hyperelliptic fields *Izv. Ross. Akad. Nauk Ser. Mat.*, vol. 84, no. 2 (in press).
27. Fedorov, G. V. 2018, "Periodic continued fractions and S-units with second degree valuations in hyperelliptic fields", *Chebyshevskii Sbornik*, vol. 19, no. 3., pp. 283-298 (In Russ.)
28. Zhgoon V. S. 2017, "On generalized jacobians and rational continued fractions in the hyperelliptic fields", *Chebyshevskii Sbornik*, vol. 18, no. 4, pp. 208-220. (In Russ.)
29. Platonov, V. P., Zhgoon, V. S., Fedorov, G. V. 2016, "Continued Rational Fractions in Hyperelliptic Fields and the Mumford Representation", *Dokl. Math.*, vol. 94, no. 3, pp. 692-696.
30. Kuznetsov, Y. V., Shteinikov, Y. N. 2017, "On some properties of continued periodic fractions with small length of period related with hyperelliptic fields and S-units", *Chebyshevskii Sbornik*, vol. 18, no. 4, pp. 260-267 (In Russ.)

Получено 16.01.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 21. Выпуск 1.

УДК 511.3

DOI 10.22405/2226-8383-2020-21-1-341-356

**Об одной теореме о среднем значении
кратных тригонометрических сумм**

В. Н. Чубариков (г. Москва)

Чубариков Владимир Николаевич — доктор физико-математических наук, профессор, заведующий кафедрой математических и компьютерных методов анализа, президент механико-математического факультета, Московский государственный университет имени М. В. Ломоносова (г. Москва).
e-mail: chubarik1@mech.math.msu.su

Аннотация

Доказана теорема о среднем для кратных тригонометрических сумм, обобщающая теорему Г. И. Архипова [12, 13]. Первая теорема подобного типа лежит в сердцевине метода И. М. Виноградова [2]. В работе найден вариант теоремы с "равноправными" длинами промежутков изменения переменных. Интересным приложением метода И. М. Виноградова являются оценки дзетовых сумм вида

$$\sum_{n \leq P} n^{it}.$$

Подобным приложением теоремы о среднем, доказанной нами, служат оценки сумм вида

$$\sum_{n \leq P_1} \cdots \sum_{n \leq P_r} (n_1 \dots n_r + k)^{it}, \sum_{n \leq P} \tau_s(n)(n + k)^{it}, \sum_{p \leq P} (p + k)^{it}.$$

Ключевые слова: теоремы о среднем И. М. Виноградова, Г. И. Архипова; многомерная функция делителей; простые числа; дзетовая сумма.

Библиография: 17 названий.

Для цитирования:

В. Н. Чубариков. Об одной теореме о среднем значении кратных тригонометрических сумм // Чебышевский сборник, 2020, т. 21, вып. 1, с. 341–356.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.3

DOI 10.22405/2226-8383-2020-21-1-341-356

On a mean-value theorem for multiple trigonometric sums

V. N. Chubarikov

Chubarikov Vladimir Nikolaevich — doctor of physical and mathematical sciences, professor, head of the Department of mathematical and computer methods of analysis, president of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: chubarik1@mech.math.msu.su

Abstract

A mean-value theorem for multiple trigonometric generalizing from the G. I. Arkhipov's theorem [12, 13] was proved. The first theorem of the similar type lies in the core of the I. M. Vinogradov's method [2]. In the paper the version of theorem with "similar" lengths of changing intervals of variables. Estimates of zeta-sums of the form

$$\sum_{n \leq P} n^{it}.$$

are the interesting application of the I.M. Vinogradov's method. The similar application of the mean-value theorem proving by us serve the estimate of sums of the form

$$\sum_{n \leq P_1} \cdots \sum_{n \leq P_r} (n_1 \dots n_r + k)^{it}, \sum_{n \leq P} \tau_s(n)(n+k)^{it}, \sum_{p \leq P} (p+k)^{it}.$$

Keywords: the mean-value theorem of I. M. Vinogradov and G. I. Arkhipov, the multivariate divisor function, prime numbers, the zeta-sum.

Bibliography: 17 titles.

For citation:

V. N. Chubarikov, 2020, "On a mean-value theorem for multiple trigonometric sums", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 341–356.

1. Введение

В настоящей статье дано обобщение теоремы Г. И. Архипова о среднем значении степени модуля кратной тригонометрической суммы [12]. Первая теорема о среднем, лежащая в основе метода тригонометрических сумм, найдена И. М. Виноградовым. Наиболее совершенное изложение её дано в монографии [2]. Ю. В. Линнику [7] принадлежит p -адический вариант доказательства этой теоремы, усовершенствованный впоследствии А. А. Карацубой, Н. М. Коробовым [10, 11], Г. И. Архиповым [13] и другими.

Интересное применение метода тригонометрических сумм найдено Д. Е. Литтлвудом [1] в теории дзета-функции Римана, что позволило уточнить остаток Валле-Пуссена в асимптотической формуле для числа простых, не превосходящих любой наперёд заданной границы. Основным моментом доказательства этого утверждения лежит оценка дзетовой суммы вида

$$S = S(P; t) = \sum_{n \leq P} n^{it}.$$

Дальнейшие улучшения оценки дзетовой суммы связаны с применением метода И. М. Виноградова [5, 6, 3, 8].

Нами найдены оценки для любого целого k , отличного от нуля, подобных кратных тригонометрических сумм вида

$$\sum_{n \leq P_1} \cdots \sum_{n \leq P_r} (n_1 \dots n_r + k)^{it}, \sum_{n \leq P} \tau_s(n)(n + k)^{it}, \sum_{p \leq P} (p + k)^{it},$$

где $\tau_s(n)$ — многомерная функция делителей числа n , выражающая число решений уравнения $n_1 \dots n_s = n$ в натуральных числах $n_1, \dots, n_s$; а переменная p пробегает последовательность всех простых чисел.

В качестве первого шага получения этих оценок дадим доказательство теоремы о среднем для многочленов от нескольких переменных заданной степени.

Пусть $J = J(\mathbf{P}; n, k, r)$ обозначает число решений системы диофантовых уравнений вида

$$\sum_{j=1}^{2k} (-1)^j x_{1,j}^{t_1} \dots x_{r,j}^{t_r} = 0, \quad 0 \leq t_1 + \dots + t_r \leq n, \quad t_1, \dots, t_r \geq 0,$$

где каждое неизвестное $x_{i,j}$, $1 \leq i \leq r$, $1 \leq j \leq 2k$, принимает все целые значения от 1 до P_j , причём $1 < P_1 \leq P_2 \leq \dots \leq P_r \leq 2P_1$, $\mathbf{P} = (P_1, \dots, P_r)$, а величины n, k, r являются натуральными числами. Очевидно, что

$$J = J(\mathbf{P}; n, k, r) = \int \cdots \int_{\Omega} |S(A)|^{2k} dA,$$

где

$$S(A) = S(A; \mathbf{P}; n, k, r) = \sum_{x_1=1}^{P_1} \cdots \sum_{x_r=1}^{P_r} \exp \{2\pi i f(x_1, \dots, x_r)\},$$

причём $\mathbf{x} = (x_1, \dots, x_r)$,

$$f(\mathbf{x}) = f(x_1, \dots, x_r) = \sum_{\substack{t_1=0 \\ t_1+\dots+t_r \leq n}}^n \cdots \sum_{t_r=0}^n \alpha(t_1, \dots, t_r) x_1^{t_1} \dots x_r^{t_r},$$

число коэффициентов многочлена $f(\mathbf{x})$ равно $m = \binom{n+r}{r}$, символ Ω обозначает куб размерности m следующего вида

$$0 \leq \alpha(t_1, \dots, t_r) < 1, \quad 0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n,$$

буква A обозначает набор вещественных коэффициентов

$$\alpha(t_1, \dots, t_r), \quad 0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n,$$

многочлена $f(x_1, \dots, x_r)$ степени n от r переменных $x_1, \dots, x_r$, наконец,

$$d\Omega = \prod_{\substack{t_1=0 \\ t_1+\dots+t_r \leq n}}^n \cdots \prod_{t_r=0}^n d\alpha(t_1, \dots, t_r).$$

ТЕОРЕМА. Пусть $3 \leq n$, $2 \leq r$, — натуральные числа, $0 \leq \tau$ — целое число, $m = \binom{n+r}{r}$, $m_1 = \frac{nr m}{r+1}$, и пусть $k \geq m\tau$. Тогда для величины $J = J(\mathbf{P}; n, k, r)$ имеем оценку

$$J \leq D(\tau) P_1^{2rk - \Delta(\tau)},$$

где

$$\Delta(\tau) = m_1(1 - (1 - 1/n)^\tau), \quad D(\tau) = (2^{nr}(n+1^n)km^{-1})^{2k}.$$

2. Леммы

ЛЕММА 1. Пусть q — простое число, T_0 — число решений системы сравнений

$$\sum_{j=1}^{2m} (-1)^j x_{1j}^{t_1} \dots x_{rj}^{t_r} \equiv 0 \pmod{q}$$

$$0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n, m = \binom{n+r}{r},$$

где каждая неизвестная x_{ij} пробегает значения из полной системы вычетов по модулю q .

Тогда для величины T_0 справедлива оценка

$$T_0 \leq (n(n+1))^{r-1} q^{2mr-m+1}, m = \binom{n+r}{r}.$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$T_0 = q^{-m} \sum_{a(0,\dots,0)=1}^q \dots \sum_{a(t_1,\dots,t_r)=1}^q \dots \sum_{a(0,\dots,n)=1}^q \left| \sum_{x_1=1}^q \dots \sum_{x_r=1}^q e^{2\pi i F_A(x_1,\dots,x_r)/q} \right|^{2m},$$

где

$$F_A(x_1, \dots, x_r) = \sum_{t_1=0}^n \dots \sum_{t_r=0}^n a(t_1, \dots, t_r),$$

$$t_1 + \dots + t_r \leq n$$

причём A — целочисленный набор $a(t_1, \dots, t_r)$, $0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n$.

Произведём следующую замену переменных суммирования

$$\begin{cases} x_1 = y_1, \\ x_2 = y_2 + y_1^{n+1}, \\ \dots \quad \dots \\ x_r = y_r + y_1^{(n+1)^{r-1}}. \end{cases}$$

Поскольку в сумме для T_0 переменные $x_1, \dots, x_r$ пробегают полные системы вычетов по модулю q , переменные $y_1, \dots, y_r$ будут пробегать полные системы вычетов по модулю q , и наоборот. Следовательно,

$$T_0 = q^{-m} \sum_{a(0,\dots,0)=1}^q \dots \sum_{a(t_1,\dots,t_r)=1}^q \dots \sum_{a(0,\dots,n)=1}^q 1 \times$$

$$\times \left| \sum_{y_1=1}^q \dots \sum_{y_r=1}^q e^{2\pi i F_A(y_1, y_2 + y_1^{n+1}, \dots, y_r + y_1^{(n+1)^{r-1}})/q} \right|^{2m}.$$

Далее при $p > 1$ воспользуемся неравенством Гёльдера в виде

$$(\sum_{\nu} |a_{\nu}|)^p \leq (\sum_{\nu} 1)^{p-1} \sum_{\nu} |a_{\nu}|^p.$$

При $p = 2m$ получим

$$\left| \sum_{y_1=1}^q \dots \sum_{y_r=1}^q e^{2\pi i F_A(y_1, y_2 + y_1^{n+1}, \dots, y_r + y_1^{(n+1)^{r-1}})/q} \right|^{2m} \leq$$

$$\leq q^{(r-1)(2m-1)} \sum_{y_2=1}^q \dots \sum_{y_r=1}^q \left| \sum_{y_1=1}^q e^{2\pi i F_A(y_1, y_2 + y_1^{n+1}, \dots, y_r + y_1^{(n+1)^{r-1}})/q} \right|^{2m}.$$

Отсюда находим

$$T_0 \leq q^{(r-1)(2m-1)} U,$$

где

$$U = \sum_{y_2=1}^q \cdots \sum_{y_r=1}^q 1 \times \\ \times q^{-m} \sum_{a(0,\dots,0)=1}^q \cdots \sum_{a(t_1,\dots,t_r)=1}^q \cdots \sum_{a(0,\dots,n)=1}^q \left| \sum_{y_1=1}^q e^{2\pi i F_A(y_1, y_2 + y_1^{n+1}, \dots, y_r + y_1^{(n+1)^{r-1}})} \right|^{2m}.$$

Имеем

$$U = \sum_{y_2=1}^q \cdots \sum_{y_r=1}^q U(y_2, \dots, y_r),$$

где $U(y_2, \dots, y_r)$ равно числу решений следующей системы сравнений

$$\sum_{j=1}^{2m} (-1)^j y_{1,j}^{t_1} (y_2 + y_{1,j}^{n+1})^{t_2} \cdots (y_r + y_{1,j}^{(n+1)^{r-1}})^{t_r} \equiv 0 \pmod{q},$$

$$0 \leq t_1, \dots, t_r, t_1 + \cdots + t_r \leq n,$$

причём неизвестные $y_{1,j}$, $1 \leq j \leq 2m$ принимают значения из полной системы вычетов по модулю q .

Заметим, что величина $U^* = U(y_2, \dots, y_r)$ не зависит от переменных $y_2, \dots, y_r$, так как вместе с решением $(y_{1,j}, y_2 + y_{1,j}^{n+1}, \dots, y_r + y_{1,j}^{(n+1)^{r-1}})$ предыдущей системы сравнений её решением является $(y_{1,j}, y_{1,j}^{n+1}, \dots, y_{1,j}^{(n+1)^{r-1}})$, и наоборот. В этом легко убеждаемся, предположив, что $x_{i,j}$, $1 \leq i \leq r$, $1 \leq j \leq 2m$, решение системы сравнений, тогда $x_{i,j} + a_i$, $1 \leq i \leq r$, $1 \leq j \leq 2m$, также будет решением системы сравнений. Действительно,

$$\begin{aligned} & \sum_{j=1}^{2m} (-1)^j (x_{1,j} + a_1)^{t_1} \cdots (x_{r,j} + a_r)^{t_r} = \\ & = \sum_{j=1}^{2m} (-1)^j \sum_{v_1=0}^{t_1} \binom{t_1}{v_1} a_1^{t_1-v_1} x_{1,j}^{v_1} \cdots \sum_{v_r=0}^{t_r} \binom{t_r}{v_r} a_r^{t_r-v_r} x_{r,j}^{v_r} = \\ & = \sum_{v_1=0}^{t_1} \cdots \sum_{v_r=0}^{t_r} \binom{t_1}{v_1} a_1^{t_1-v_1} \cdots \binom{t_r}{v_r} a_r^{t_r-v_r} \sum_{j=1}^{2m} (-1)^j x_{1,j}^{v_1} \cdots x_{r,j}^{v_r} \equiv 0 \pmod{q}. \end{aligned}$$

Следовательно, положив $(a_1, a_2, \dots, a_r) = (0, -y_2, \dots, -y_r)$, получим эквивалентную систему сравнений

$$\begin{aligned} & \sum_{j=1}^{2m} (-1)^j y_{1,j}^{t_1+t_2(n+1)+\cdots+t_r(n+1)^{r-1}} \equiv 0 \pmod{q}, \\ & 0 \leq t_1, t_2, \dots, t_r, t_1 + t_2 + \cdots + t_r \leq n. \end{aligned}$$

Так как любое значение t вида

$$t = t_1 + t_2(n+1) + \cdots + t_r(n+1)^{r-1}, 0 \leq t_1, \dots, t_r, t_1 + \cdots + t_r \leq n,$$

Принимается не более одного раза, то последнюю систему сравнений можно переписать в виде

$$\sum_{j=1}^{2m} (-1)^j z_j^t \equiv 0 \pmod{q}, t = t_1 + t_2(n+1) + \cdots + t_r(n+1)^{r-1},$$

$$0 \leq t_1, t_2, \dots, t_r, 1 \leq t_1 + t_2 + \cdots + t_r \leq n.$$

Количество сравнений в этой системе сравнений равно $m-1$, где $m = \binom{n+r}{r}$. Степени многочленов её не превосходят $n(n+1)^{r-1}$. Занумеруем числа t , представимые в виде

$$t = t_1 + t_2(n+1) + \cdots + t_r(n+1)^{r-1}, 0 \leq t_1, \dots, t_r, 1 \leq t_1 + \cdots + t_r \leq n,$$

в порядке возрастания $1 = s_1 < s_2 < \dots < s_{m-1} = n(n+1)^{r-1}$.

Таким образом, число решений U^* рассматриваемой системы сравнений можно представить в виде

$$V = q^{-m+1} \sum_{b_{s_1}=1}^q \dots \sum_{b_{s_{m-1}}=1}^q \left| \sum_{z=1}^q e^{2\pi i f_B(z)/q} \right|^{2m}, f_B(z) = \sum_{u=1}^{m-1} b_t z^{s_u}.$$

Используя оценку А.Вейля, получим

$$U^* \leq q^{m+1} + (n(n+1)^r - 1)^{2m} q^m \leq (n(n+1))^{r-1}^{2m} q^{m+1}.$$

Отсюда находим

$$U = \sum_{y_2=1}^q \dots \sum_{y_r=1}^q U^* = q^{r-1} U^* \leq (n(n+1))^{r-1}^{2m} q^{m+r}, \quad T_0 \leq (n(n+1))^{r-1}^{2m} q^{2mr-m+1}.$$

Лемма 1 доказана. $\square$

Докажем несколько полезных тождеств.

ЛЕММА 2. Пусть $t_1, \dots, t_r$ — неотрицательные целые числа. Тогда имеем тождества

$$\begin{aligned} m^* &= m^*(n, r) = \sum_{t_1=0}^n \dots \sum_{\substack{t_r=0 \\ t_1+\dots+t_r=n}}^n 1 = \binom{n+r-1}{r-1}; \\ m &= m(n, r) = \sum_{t_1=0}^n \dots \sum_{\substack{t_r=0 \\ t_1+\dots+t_r \leq n}}^n 1 = \binom{n+r}{r}; \\ m_1^* &= m_1^*(n, r) = \sum_{t_1=0}^n \dots \sum_{\substack{t_r=0 \\ t_1+\dots+t_r=n}}^n (t_1 + \dots + t_r) = r \left(\binom{n+r}{r} - \binom{n+r-1}{r-1} \right); \\ m_1 &= m_1(n, r) = \sum_{t_1=0}^n \dots \sum_{\substack{t_r=0 \\ t_1+\dots+t_r \leq n}}^n (t_1 + \dots + t_r) = \frac{rn}{r+1} \binom{n+r}{r}. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим при $|z| < 1$ производящую функцию $F(z)$ для последовательности m_0 . Имеем

$$F(z) = \sum_{n=0}^{\infty} m^*(n, r) z^n = \sum_{t_1=0}^{\infty} \dots \sum_{t_r=0}^{\infty} z^{t_1+\dots+t_r} = \left(\sum_{t_1=0}^{\infty} z^{t_1} \right) \dots \left(\sum_{t_r=0}^{\infty} z^{t_r} \right) = \frac{1}{(1-z)^r}.$$

Следовательно,

$$m^* = m^*(n, r) = \frac{1}{n!} \frac{d^n}{dz^n} \frac{1}{(1-z)^r} \Big|_{z=0} = \frac{r(r+1) \dots (r+n-1)}{n!} = \binom{n+r-1}{r-1}.$$

Далее величина $m = m(n, r) = \sum_{k=0}^n m^*(k, r)$ равна числу решений уравнения $t_1 + \dots + t_{r+1} = n$ в целых неотрицательных числах $t_1, \dots, t_{r+1}$, т.е.

$$m = m(n, r) = m^*(n, r+1) = \binom{n+r}{r}.$$

Рассмотрим теперь при $|z| < 1$ производящую функцию $F_1(z)$ последовательности $m_1^*(n, r)$. Находим

$$F_1(z) = \sum_{n=0}^{\infty} m_1^*(n, r) z^n = \sum_{t_1=0}^{\infty} \dots \sum_{t_r=0}^{\infty} (t_1 + \dots + t_r) z^{t_1+\dots+t_r} =$$

$$= rz \left(\frac{1}{1-z} \right)' r \frac{z}{(1-z)^{r-1}} = r \frac{z}{(1-z)^{r+1}} = r \left(\frac{1}{(1-z)^{r+1}} - \frac{1}{(1-z)^r} \right).$$

Отсюда и из вида производящей функции $F(z)$ имеем

$$m_1^*(n, r) = r \left(\binom{n+r}{r} - \binom{n+r-1}{r-1} \right).$$

Наконец, используя при $0 \leq k \leq n$ формулу для $m_1^*(k, r)$ и для $m(k, r)$, имеем

$$m_1(n, r) = \sum_{k=0}^n m_1^*(k, r) = r \binom{n+r+1}{r+1} - r \binom{n+r}{r} = \frac{rn}{r+1} \binom{n+r}{r}.$$

Лемма доказана. $\square$

Перейдём к формулировке и доказательству леммы о числе решений полной системы сравнений.

ОПРЕДЕЛЕНИЕ. Пусть задана матрица M , имеющая $m = \binom{n+r}{r}$ строк и $k \geq 1$ столбцов,

$$M = (x_{1,j}^{t_1} \dots x_{r,j}^{t_r}),$$

где

$$0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n, 1 \leq j \leq k.$$

Набор векторов $\mathbf{x}_1, \dots, \mathbf{x}_k$, где $\mathbf{x}_s = (x_{1,s}, \dots, x_{r,s})$, $1 \leq s \leq k$, называют **регулярным по модулю q** , если ранг матрицы M , элементами которой являются вычеты $x_{1,j}^{t_1} \dots x_{r,j}^{t_r}$ по простому модулю q , будет максимален. В частности, при $k \geq m$, он равен m .

ЛЕММА 3. Пусть p — простое число, T — число решений системы сравнений

$$\sum_{j=1}^{2m} (-1)^j x_{1,j}^{t_1} \dots x_{r,j}^{t_r} \equiv 0 \pmod{p^{t_1+\dots+t_r}},$$

$$0 \leq t_1, \dots, t_r, 1 \leq t_1 + \dots + t_r \leq n,$$

где неизвестные $x_{s,j}$, $1 \leq s \leq r$, $1 \leq j \leq k$, пробегает значения из полной системы вычетов по модулю p^n , например, $0 \leq x_{s,j} < p^n$, и пусть векторы $\mathbf{x}_j$, $j = 2, 4, \dots, 2m$, удовлетворяют условию регулярности по модулю p .

Тогда справедлива следующая оценка

$$T \leq (n+1)^{2rm} p^A, A = 2rnm - m_1, \quad m = \binom{n+r}{r}, \quad m_1 = \frac{rn}{r+1} \binom{n+r}{r}.$$

ДОКАЗАТЕЛЬСТВО. Можно считать, что $p > n$, так как в противном случае решения системы сравнений, удовлетворяющие условию регулярности, отсутствуют.

Представим каждую неизвестную $x_{s,j}$, $1 \leq s \leq r$, $1 \leq j \leq 2m$, в виде

$$x_{s,j} = \sum_{l=0}^{n-1} p^l x_{s,j,l}, 0 \leq x_{s,j,l} < p,$$

и подставим эти выражения в систему сравнений.

Сначала отметим, что сравнения полученной системы обязаны выполняться по модулю p , т.е.

$$\sum_{j=1}^{2m} (-1)^j x_{1,j,0}^{t_1} \dots x_{r,j,0}^{t_r} \equiv 0 \pmod{p},$$

$$0 \leq t_1, \dots, t_r, 1 \leq t_1 + \dots + t_r \leq n,$$

и неизвестные $\mathbf{x}_{2v,0} = (x_{1,2v,0}, \dots, x_{r,2v,0})$, $1 \leq v \leq m$, удовлетворяют условию регулярности. Число решений этой системы сравнений обозначим через T_0 . По лемме 1 имеем

$$T_0 \leq (n(n+1))^{r-1} 2^m p^{2mr-m+1}, m = \binom{n+r}{r}.$$

Итак, неравенство для величины T_0 даёт оценку сверху количества нулевых координат $x_{s,j,0}$, удовлетворяющих системе сравнений из условия леммы. Оценку числа других координат проведем по индукции по параметру ν . При $\nu = 0$ такая оценка получена выше.

Далее первоначальную систему сравнений рассмотрим по модулю $p^{\nu+1}$, $1 \leq \nu \leq n$. Положим

$$u_{s,j,\nu} = \sum_{\mu=0}^{\nu} p^{\mu} x_{s,j,\mu} = u_{s,j,\nu-1} + p^{\nu} x_{s,j,\nu}, u(s, j, 0) = x(s, j, 0).$$

Имеем $x_{s,j} \equiv u(s, j, \nu) \pmod{p^{\nu+1}}$. Следовательно, обязана выполняться система сравнений вида

$$\sum_{j=1}^{2m} (-1)^j u_{1,j,\nu}^{t_1} \dots u_{r,j,\nu}^{t_r} \equiv 0 \pmod{p^{\nu+1}},$$

$$0 \leq t_1, \dots, t_r, \nu + 1 \leq t_1 + \dots + t_r \leq n,$$

и неизвестные $\mathbf{x}_{2\nu,0} = (x_{1,2\nu,0}, \dots, x_{r,2\nu,0})$, $1 \leq \nu \leq m$, удовлетворяют условию регулярности по модулю p . Число решений этой системы сравнений обозначим через T_{ν} .

Предположим, что справедлива оценка $T_{\nu-1}$. Зафиксируем любое решение $u_{s,j,\nu-1}$, $1 \leq s \leq r$, $1 \leq j \leq 2m$. Для этого фиксированного решения оценим величину $T(\nu)$.

Поскольку

$$u_{1,j,\nu}^{t_1} \dots u_{r,j,\nu}^{t_r} \equiv u_{1,j,\nu-1}^{t_1} \dots u_{r,j,\nu-1}^{t_r} + p^{\nu} \psi_j(t_1, \dots, t_r),$$

где

$$\psi_j(t_1, \dots, t_r) = \sum_{\lambda=1}^r t_{\lambda} u_{1,j,\nu-1}^{t_1} \dots u_{\lambda,j,\nu-1}^{t_{\lambda}-1} \dots u_{r,j,\nu-1}^{t_r} x_{\lambda,j,\nu} \pmod{p},$$

где при $t_{\lambda} = 0$ соответствующее слагаемое в последней сумме равно 0.

Отсюда приходим к системе сравнений с неизвестными $x_{s,j,\nu}$, $1 \leq s \leq r$, $1 \leq j \leq 2m$,

$$\sum_{j=1}^{2m} (-1)^j \psi_j(t_1, \dots, t_r) \equiv p^{-\nu} \sum_{j=1}^{2m} (-1)^j u_{1,j,\nu-1}^{t_1} \dots u_{r,j,\nu-1}^{t_r} \equiv \lambda(t_1, \dots, t_r) \pmod{p},$$

$$0 \leq t_1, \dots, t_r, \nu + 1 \leq t_1 + \dots + t_r \leq n,$$

причём набор векторов $\mathbf{u}_{2j,\nu-1} = (u_{1,2j,\nu-1}, \dots, u_{r,2j,\nu-1})$, $1 \leq j \leq m$, удовлетворяет условию регулярности по модулю p .

Для оценки $T(\nu)$ из предыдущей системы сравнений составим r подсистем сравнений. В первую подсистему войдут сравнения с условиями $t_1 \geq \nu + 1, t_2 = \dots = t_r = 0$, во вторую те сравнения, для которых $t_1 + t_2 \geq \nu + 1, t_2 \neq 0, t_3 = \dots = t_r = 0$, и т.д., наконец, в r -ю подсистему включим сравнения с условиями $t_1 + \dots + t_r \geq \nu + 1, t_r \neq 0$.

Пусть $R_s(\nu + 1)$ обозначает число решений в целых числах неравенств $\nu + 1 \leq t_1 + \dots + t_s \leq n$, $0 \leq t_1, \dots, t_s$. Тогда в первую подсистему войдут $R_1(\nu + 1)$ сравнений, во вторую — войдут $R_2(\nu + 1) - R_1(\nu + 1)$, и т.д., в r -ю войдут сравнения в количестве $R_r(\nu + 1) - R_{r-1}(\nu + 1)$.

Первая подсистема будет состоять из сравнений вида

$$\sum_{j=1}^{2m} (-1)^j x_{1,j,0}^{t_1-1} x_{1,j,\nu} \equiv \lambda(t_1, 0, \dots, 0) \pmod{p}, \nu + 1 \leq t_1 \leq n,$$

с неизвестными $x_{1,j,\nu}$, $1 \leq j \leq 2m$, и с условием регулярности по модулю p , которое означает, что матрица её коэффициентов имеет максимальный ранг по модулю p . Последнее означает, что найдутся $\rho = R_1(\nu + 1)$ коэффициентов с номерами $1 \leq j_1 \leq j_{\rho} \leq 2m$, таких, что определитель матрицы

$$\begin{pmatrix} x_{1,j_1,0}^{\nu+1} & \dots & x_{1,j_{\rho},0}^{\nu+1} \\ \dots & \dots & \dots \\ x_{1,j_1,0}^n & \dots & x_{1,j_{\rho},0}^n \end{pmatrix}$$

не сравним с 0 по модулю p . Следовательно, первая подсистема сравнений имеет не более $p^{2m-R_1(\nu+1)}$ решений.

Рассмотрим теперь s -ю подсистему сравнений. Она приводится к виду

$$\sum_{j=1}^{2m} (-1)^j x_{1,j,0}^{t_1} \dots x_{s,j,0}^{t_s-1} x_{s,j,\nu} \equiv \lambda'(t_1, \dots, t_s, 0, \dots, 0) \pmod{p}, \nu+1 \leq t_1 \leq n,$$

$$\nu+1 \leq t_1 + \dots + t_s \leq n, t_s \neq 0, 0 \leq t_1, \dots, t_s,$$

с неизвестными $x_{1,j,\nu}, 1 \leq j \leq 2m$, из полной системы по модулю вычетов p , и с условием регулярности по модулю p , т.е. с условием линейной независимости сравнений системы по модулю p . Как и раньше, получим, что число решений этой системы сравнений не превосходит $p^{R_s(\nu+1)-R_{s-1}(\nu+1)}$.

Таким образом, число решений ν -й системы сравнений не превосходит

$$T_\nu \leq p^{2m-R_1(\nu+1)} \prod_{s=2}^r p^{R_s(\nu+1)-R_{s-1}(\nu+1)} = p^{2mr-R_r(\nu+1)}.$$

Следовательно,

$$T \leq \prod_{\nu=0}^{n-1} T_\nu \leq (n(n+1)^{r-1})^{2m} p^{2mrn-R}, R = \sum_{\nu=1}^n R_r(\nu).$$

Найдём значение величины R . Имеем

$$\begin{aligned} R &= \sum_{\nu=1}^n R_r(\nu) = \sum_{\nu=1}^n \sum_{k=\nu}^n R_r^*(k) = \sum_{k=1}^n R_r^*(k) \sum_{\nu=1}^k 1 = \sum_{k=1}^n k R_r^*(k) = \\ &= \sum_{\substack{t_1=0 \\ t_1+\dots+t_r \leq n}}^n \dots \sum_{\substack{t_r=0 \\ t_1+\dots+t_r \leq n}}^n (t_1 + \dots + t_r) = \frac{rn}{r+1} \binom{n+r}{r} = m_1. \end{aligned}$$

□

Теперь докажем лемму о рекуррентном неравенстве.

ЛЕММА 4. Пусть $n \geq 2, r \geq 1, k \geq 2m, 1 \leq P_1 \leq \dots \leq P_r \leq 2P_1$. Тогда существует такое число p из отрезка $[P_1^{1/n}, 2P_1^{1/n}]$, что

$$J = J(\mathbf{P}; n, k, r) \leq D_1 p^{2r(k-m)+2mrn-m_1} J(\mathbf{Q}; n, k-m, r) + D_2 P_1^{2kr-2k+2m-2},$$

$$m_1 = \frac{rn}{r+1} \binom{n+r}{r}, D_1 = 2n^2 J_0 \leq 2n^2 (n+1)^{2rm} \left(\frac{k}{m} \right)^2, D_2 = 2^{2nm+2nk(r-1)+1} n^{2nk},$$

где $\mathbf{Q} = (Q_1, \dots, Q_r), Q_s = P_s p^{-1} + 1, 1 \leq s \leq r$.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности будем считать, что $(P_1 \dots P_r)^{m_1} > D_2$, поскольку в противном случае оценка величины J становится тривиальной. При этом условии на отрезке вида $[P_1^{1/n}, 2P_1^{1/n}]$ находится по крайней мере n различных простых чисел ([14], гл. III, лемма 8, с. 105–107). Пусть $p_1, \dots, p_n$ обозначают любые n различных таких простых чисел, $\mathbf{x}_j = (x_{1,j}, \dots, x_{r,j})$. Представим J в виде

$$J = \int \dots \int_{\Omega} \left| \sum_{\mathbf{x}_1} \sum_{\mathbf{x}_3} \dots \sum_{\mathbf{x}_{2k-1}} e^{2\pi i(f(\mathbf{x}_1)+f(\mathbf{x}_3)+\dots+f(\mathbf{x}_{2k-1}))} \right|^2 d\Omega,$$

где координаты векторов $\mathbf{x}_j = (x_{1,j}, \dots, x_{r,j})$ принимают значения целых чисел, причём $1 \leq x_{s,j} \leq P_s, 1 \leq s \leq r$.

Наборы векторов $\{\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}\}$ разобьём на два класса. Первый класс A будет состоять только из тех наборов, которые удовлетворяют условию регулярности по модулю $p = p_s$ при некотором $s, 1 \leq s \leq r$. Определение регулярности набора векторов по простому модулю дано перед формулировкой леммы 3. Все остальные наборы отнесём ко второму классу B .

Пусть

$$\sum_A = \sum_{\mathbf{x}_1} \sum_{\mathbf{x}_3} \dots \sum_{\substack{\mathbf{x}_{2k-1} \\ \{\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}\} \in A}} e^{2\pi i(f(\mathbf{x}_1)+f(\mathbf{x}_3)+\dots+f(\mathbf{x}_{2k-1}))}.$$

Сумма $\sum_B$ определяется аналогично. Тогда справедливо неравенство

$$J = \int \cdots \int_{\Omega} \left| \sum_A + \sum_B \right|^2 d\Omega \leq 2J_1 + 2J_2,$$

где

$$J_1 = \int \cdots \int_{\Omega} \left| \sum_A \right|^2 d\Omega, \quad J_2 = \int \cdots \int_{\Omega} \left| \sum_B \right|^2 d\Omega.$$

Оценим J_1 . Класс A разобьём на n совокупностей $A_1, \dots, A_n$. Для всякого $s, 1 \leq s \leq n$, совокупность A_s будет состоять только из тех наборов векторов $\{\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}\}$, которые удовлетворяют условию регулярности по модулю p_s , и не входят в совокупности $A_1, \dots, A_{s-1}$. По неравенству Коши имеем

$$J_1 = \int \cdots \int_{\Omega} \left| \sum_{s=1}^n \sum_{A_s} \right|^2 d\Omega \leq n \sum_{s=1}^n J_1 = \int \cdots \int_{\Omega} \left| \sum_{A_s} \right|^2 d\Omega \leq n^2 J_0,$$

где J_0 обозначает ту совокупность A_t , для которой при $1 \leq s \leq n$ интеграл

$$J_s = \int \cdots \int_{\Omega} \left| \sum_{A_s} \right|^2 d\Omega$$

имеет наибольшее значение.

Рассмотрим те наборы $\{\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}\}$, которые удовлетворяют условию регулярности по модулю p_t , причём первые m столбцов соответствующей матрицы M , отвечающей набору векторов $\{\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2m-1}\}$, являются линейно независимыми по модулю p_t . Совокупность таких наборов векторов обозначим $A_{t,0}$. Поскольку все другие наборы векторов из совокупности A_t отличаются только номером для линейно независимых столбцов матрицы M , получим неравенство

$$J_0 \leq \binom{k}{m}^2 \int \cdots \int_{\Omega} \left| \sum_{A_{t,0}} \right|^2 d\Omega.$$

Преобразуем сумму

$$\sum_{A_{t,0}} = \left\{ \sum_{\mathbf{x}_1} \cdots \sum_{\mathbf{x}_{2m-1}} \right\}' \sum_{\mathbf{x}_{2m+1}} \cdots \sum_{\mathbf{x}_{2k-1}},$$

где штрих в знаке суммы означает, что первые m векторов характеризуют условие регулярности по модулю $p = p_t$.

Заметим, что для остальных $r - m$ векторов $\mathbf{x}_j, j = 2m + 1, \dots, 2k - 1$, их координаты произвольным образом изменяются в соответствующих промежутках. Представим эти векторы $\mathbf{x}_j$ в виде $\mathbf{x}_j = \mathbf{y}_j + p\mathbf{z}_j$, где при $1 \leq s \leq r, j = 2m + 1, \dots, 2k - 1$, их координаты $y_{s,j}$ пробегает целые значения от 1 до p , а $z_{s,j}$ — от 0 до $P_s p^{-1}$.

Применяя неравенство Гёльдера, найдем

$$\begin{aligned} \left| \sum_{A_{t,0}} \right|^2 &\leq \left| \left\{ \sum_{\mathbf{x}_1} \cdots \sum_{\mathbf{x}_{2m-1}} \right\}' \right|^2 \left| \sum_{\mathbf{y}} \sum_{\mathbf{z}} \right|^{2(k-m)} \leq \\ &\leq p^{2r(k-m)-r} \sum_{\mathbf{y}} \left| \left\{ \sum_{\mathbf{x}_1} \cdots \sum_{\mathbf{x}_{2m-1}} \right\}' \right|^2 \left| \sum_{\mathbf{z}} \right|^{2(k-m)}. \end{aligned}$$

Следовательно,

$$J_0 \leq \binom{k}{m}^2 p^{2r(k-m)} \max_{\mathbf{y}} \int \cdots \int_{\Omega} \left| \left\{ \sum_{\mathbf{x}_1} \cdots \sum_{\mathbf{x}_{2m-1}} \right\}' \right|^2 \left| \sum_{\mathbf{z}} \right|^{2(k-m)} d\Omega.$$

Отсюда при некотором $\mathbf{y} = \mathbf{y}_0 = (y_{1,0}, \dots, y_{r,0})$ интеграл в левой части последнего неравенства представляет собой число решений следующей системы диофантовых уравнений

$$\sum_{j=1}^{2m} (-1)^j x_{1,j}^{t_1} \dots x_{r,j}^{t_r} = \sum_{j=2m+1}^{2k} (-1)^j (y_{1,0} + pz_{1,j})^{t_1} \dots (y_{r,0} + pz_{r,j})^{t_r},$$

$$0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n,$$

где неизвестные векторы $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2m-1}$, удовлетворяют условию регулярности по модулю p , а неизвестные $z_{s,j}$, $1 \leq s \leq r, j = 2m+1, 2m+2, \dots, 2k$ пробегает все целые значения от 0 до $P_s p^{-1}$.

Не изменяя числа решений в этой системе, произведём сдвиг векторов неизвестных на вектор $-\mathbf{y}_0$. Получим следующую систему уравнений

$$\sum_{j=1}^{2m} (-1)^j (x_{1,j} - y_{1,0})^{t_1} \dots (x_{r,j} - y_{r,0})^{t_r} = p^{t_1 + \dots + t_r} \sum_{j=2m+1}^{2k} (-1)^j z_{1,j}^{t_1} \dots z_{r,j}^{t_r},$$

$$0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n.$$

Так как число $J(\Lambda)$ решений системы уравнений

$$\sum_{j=2m+1}^{2k} (-1)^j z_{1,j}^{t_1} \dots z_{r,j}^{t_r} = \lambda(t_1, \dots, t_r), (0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n),$$

не превосходит числа решений подобной системы уравнений при $\lambda(t_1, \dots, t_r) = 0$ для всех $0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n$, то имеем

$$J(\Lambda) \leq J(\mathbf{Q}; n, k-m, r).$$

Пусть T обозначает число решений системы сравнений

$$\sum_{j=1}^{2m} (-1)^j (x_{1,j} - y_{1,0})^{t_1} \dots (x_{r,j} - y_{r,0})^{t_r} \equiv 0 \pmod{p^{t_1 + \dots + t_r}},$$

$$0 \leq t_1, \dots, t_r, t_1 + \dots + t_r \leq n,$$

причём переменные $\mathbf{x}_1, \dots, \mathbf{x}_r$, удовлетворяют условию регулярности по модулю p и пробегает полные системы вычетов по модулю p^n .

Воспользуемся оценкой величины T из леммы 3. Находим

$$J_0 \leq \binom{k}{m}^2 p^{2r(k-m)} T J(\mathbf{Q}; n, k-m, r),$$

$$J_1 \leq n^2 J_0 \leq n^2 (n+1)^{2rm} \binom{k}{m}^2 p^{2r(k-m) + 2mrn - m_1} J(\mathbf{Q}; n, k-m, r).$$

Перейдём к оценке J_2 . Для любого $1 \leq s \leq n$ наборы векторов $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}$, входящие в класс B , не являются регулярными по модулю p_s . Следовательно, найдутся целые числа $c_s(t_1, \dots, t_r)$, не все сравнимые с нулём по модулям p_s , $1 \leq s \leq n$, такие, что справедливы сравнения

$$\sum_{\substack{t_1=0 \\ t_1 + \dots + t_r \leq n}}^n \dots t_r = 0^n c_s(t_1, \dots, t_r) x_{1,j}^{t_1} \dots x_{r,j}^{t_r} \equiv 0 \pmod{p_s},$$

$$j = 1, 3, \dots, 2k-1.$$

Отсюда имеем, что при фиксированном наборе $c_s(t_1, \dots, t_r), t_1 + \dots + t_r \leq n$, отличном от нулевого по модулю p_s , число решений $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}$ предыдущего сравнения не превосходит $(np_s^{r-1})^k$. Число указанных наборов $c_s(t_1, \dots, t_r), t_1 + \dots + t_r \leq n$, не превосходит $2p_s^{m-1}$, поскольку можно считать, что $c_s(0, \dots, 0)$ может принимать лишь два значения 0 или 1. Таким образом, количество всех возможных наборов $\mathbf{x}_1(p_s), \mathbf{x}_3(p_s), \dots, \mathbf{x}_{2k-1}(p_s)$ вычетов по модулю p_s не превосходит $2p_s^{m-1} (np_s)^k$.

Итак, для всякого набора $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}$ из B и любого $p_s, 1 \leq s \leq n$, найдётся $\mathbf{x}_j(p_s)$ такое, что

$$\mathbf{x}_j \equiv \mathbf{x}_j(p_s) \pmod{p_s}.$$

Зафиксируем любой набор вычетов векторов

$$\mathbf{x}_j(p_s) \equiv \mathbf{a}_{p_s}, 1 \leq s \leq n, j = 1, 3, \dots, 2k-1.$$

Тогда по китайской теореме найдётся единственный набор векторов $\mathbf{a}_j$ по модулю $p_1 \dots p_n$ такой, что

$$\mathbf{x}_j \equiv \mathbf{a}_j \pmod{p_1 \dots p_n}.$$

Таким образом, число наборов векторов $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{2k-1}$, входящие в класс B , не превосходит

$$U = \prod_{s=1}^n (2p_s^{m-1} (np_s^r)^k).$$

Поскольку для любого $1 \leq s \leq n$ справедливо неравенство $p_s \leq 2P_1^{1/n}$, имеем

$$U \leq 2^{n+n(m-1)+kn(r-1)} n^{nk} P_1^{kr-k+m-1}.$$

Так как модуль сравнения $p_1 \dots p_n$ не превосходит P_1 , то соответствующие сравнения эквивалентны равенствам

$$\mathbf{x}_j = \mathbf{a}_j, j = 1, 3, \dots, 2k-1.$$

Это означает, что число элементов в классе B не превосходит U .

Следовательно,

$$J_2 \leq U^2 \leq 2^{2nm+2nk(r-1)} n^{2nk} P_1^{2kr-2k+2m-2}$$

Лемма 4 доказана. $\square$

3. Доказательство теоремы

Проведем индукцию по параметру $\tau \geq 0$. Пусть $\tau = 0$. Тогда $\Delta(\tau) = 0$ и выполняется тривиальная оценка $J \leq (P_1 \dots P_r)^{2k}$.

Пусть, теперь, $\tau = 1$. Так как $k \geq m$, то, очевидно, имеем

$$J(\mathbf{P}; n, k, r) \leq (P_1 \dots P_r)^{2(k-m)} J(\mathbf{P}; n, m, r), \Delta(1) = m_1/n = \frac{r}{r+1} \binom{n+r}{r} = \frac{r}{r+1} m.$$

Возьмём простое число q из отрезка $[P_r, 2P_r], 1 < P_1 \leq P_2 \leq \dots \leq P_r \leq 2P_1$. Из леммы 1 находим

$$\begin{aligned} J(\mathbf{P}; n, m, r) &\leq (n(n+1)^{r-1})^{2m} q^{2mr-m+1} \leq (n+1)^{2mr} (4P_1)^{2mr-m+1} \leq \\ &\leq 4^{2mr-m+1} (n+1)^{2mr} (P_1 \dots P_r)^{2m} P_1^{-m+1} \leq 4^{2mr-m+1} (n+1)^{2mr} (P_1 \dots P_r)^{2m} P_1^{-\Delta(1)}. \end{aligned}$$

Следовательно,

$$J(\mathbf{P}; n, k, r) \leq D(1) (P_1 \dots P_r)^{2k} P_1^{-\Delta(1)}.$$

Утверждение теоремы достаточно доказать при $k = m\tau$. Предположим, что утверждение справедливо при $\tau = l \geq 1$. Докажем, что оно имеет место при $\tau = l+1$. Применим лемму 4. Получим

$$\begin{aligned} J(\mathbf{P}; n, m(l+1), r) &\leq 2n^2 (n+1)^{2rm} \binom{m(l+1)}{m}^2 p^{2rml+2mrn-m_1} J(\mathbf{Q}; n, ml, r) + \\ &+ 2^{2nm+2nm(l+1)(r-1)+1} n^{2nm(l+1)} P_1^{2m(l+1)r-2m(l+1)+2m-2}, \end{aligned}$$

где $P_1^{1/n} \leq p \leq 2P_1^{1/n}, Q_s = P_s p^{-1} + 1$.

Для оценки величины $J(\mathbf{Q}; n, ml, r)$ воспользуемся предположением индукции:

$$J(\mathbf{Q}; n, ml, r) \leq D_0(l) (Q_1 \dots Q_r)^{2ml} Q_1^{-\Delta(l)}.$$

Используя эту оценку и предыдущее неравенство, находим

$$J(\mathbf{P}; n, m(l+1), r) \leq W_1 + W_2,$$

где

$$W_1 = A(l+1)D_0(l)p^{2rml+2mrn-m_1}(Q_1 \dots Q_r)^{2ml}Q_1^{-\Delta(l)} = A(l+1)D_0(l)R,$$

$$A(l+1) = 2n^2(n+1)^{2rm} \binom{m(l+1)}{m}^2,$$

$$W_2 \leq 2^{2nm+2nm(l+1)(r-1)+1} n^{2nm(l+1)} P_1^{2m(l+1)r-2m(l+1)+2m-2}.$$

Достаточно доказать, что $W_1 \leq 0,5W_0$, $W_2 \leq 0,5W_0$, где

$$W_0 = D(l+1)(P_1 \dots P_r)^{2m(l+1)} P_1^{-\Delta(l+1)}, D(l+1) \geq D_0(l+1).$$

Оценим W_1 . Имеем

$$R = p^{2rml+2mrn-m_1}(Q_1 \dots Q_r)^{2ml}Q_1^{-\Delta(l)} = R_0 B,$$

$$R_0 = p^{2mrn-m_1+\Delta(l)}(P_1 \dots P_r)^{2ml}P_1^{-\Delta(l)}, B = 2^{2mr} \prod_{s=1}^r (1 + pP_s^{-1})^{2ml},$$

где

$$Q_s = P_s p^{-1} + 1, 1 \leq s \leq r; P_1^{1/n} \leq p \leq 2P_1^{1/n}; 1 < P_1 \leq P_2 \leq \dots \leq P_r \leq 2P_1.$$

Преобразуем R_0 . Находим

$$p^{2mrn-m_1+\Delta(l)} \leq (2P_1)^{2mr-\frac{m_1}{n}(1-\frac{1}{n})^l}.$$

Следовательно,

$$R_0 \leq 2^{2mr}(P_1 \dots P_r)^{2m(l+1)} P_1^{-\Delta(l)-\frac{m_1}{n}(1-\frac{1}{n})^l}.$$

Так как

$$\begin{aligned} \Delta(l) + \frac{m_1}{n} \left(1 - \frac{1}{n}\right)^l &= m_1 - m_1 \left(1 - \frac{1}{n}\right)^l + \frac{m_1}{n} \left(1 - \frac{1}{n}\right)^l = \\ &= m_1 - m_1 \left(1 - \frac{1}{n}\right)^{l+1} = \Delta(l+1), \end{aligned}$$

то

$$R_0 \leq 2^{2mr}(P_1 \dots P_r)^{2m(l+1)} P_1^{-\Delta(l+1)}.$$

Оценим теперь величину B . Будем считать, что $P_1 \geq (2ml)^2$. В противном случае утверждение теоремы справедливо тривиально. Тогда, учитывая, что $n \geq 3, l \geq 2$, получим

$$pP_s^{-1} \leq pP_1^{-1} \leq 2P_1^{\frac{1}{n}-1} \leq 2(2ml)^{2(\frac{1}{n}-1)} \leq (2ml)^{-1}.$$

Таким образом, имеем

$$B \leq 2^{mr} e^r \leq 2^{r(m+2)}.$$

Собирая вместе оценки для R_0 и B , находим

$$W_1 = R_0 B \leq D_0(l)A(l+1)2^{r(m+2)}(P_1 \dots P_r)^{2m(l+1)} P_1^{-\Delta(l+1)}.$$

Покажем, что

$$D_0(l)A(l+1)2^{r(m+2)} \leq 0,5D(l+1).$$

Действительно, имеем цепочку неравенств

$$D(l+1) \geq D_0(l+1) \geq 2D_0(l)A(l+1)2^{r(m+2)},$$

$$D_0(l) \geq 2D_0(l-1)A(l)2^{r(m+2)},$$

... ..

$$D_0(2) \geq 2D_0(1)A(2)2^{r(m+2)}.$$

Перемножая их, получим

$$D(l+1) \geq D_0(1) (2n^2 2^{2rm})^l \left(\binom{2m}{m} \dots \binom{m(l+1)}{m} \right)^2 2^{lr(m+2)+r},$$

где

$$D_0(1) \geq 2n^2 2^{2rm}.$$

Поскольку из полиномиальной формулы Ньютона

$$(a_1 + \dots + a_k)^n = \sum_{\substack{t_1 \\ t_1 + \dots + t_k = n}}^n \dots \sum_{t_k}^n \frac{n!}{t_1! \dots t_k!} a_1^{t_1} \dots a_k^{t_k}$$

следует неравенство

$$\frac{(m(l+1))!}{(m!)^{l+1}} \leq (l+1)^{m(l+1)},$$

получим

$$\binom{2m}{m} \dots \binom{m(l+1)}{m} = \frac{(m(l+1))!}{(m!)^{l+1}} \leq (l+1)^{m(l+1)}.$$

Следовательно, для $D(l+1)$ выполняется неравенство

$$D(l+1) \geq D_0(l+1) \geq \left(2^{r(m+2)+1} (n+1)^{2mr} (l+1)^{2m} \right)^{l+1},$$

т.е. $W_1 \leq 0,5W_0$.

Перейдём теперь к оценке W_2 . Из определения W_2 имеем равенство

$$W_2 = A_1(l+1)P_1^{2mr(l+1)-2m(l+1)+2m-2},$$

где

$$A_1(l+1) = 2^{2nm+2nm(l+1)(r-1)+1} n^{2nm(l+1)}.$$

Достаточно доказать, что $W_2 \leq 0,5W_0$, т. е.

$$\begin{aligned} A_1(l+1)P_1^{2mr(l+1)-2m(l+1)+2m-2} &\leq A_1(l+1)(P_1 \dots P_r)^{2m(l+1)} P_1^{-2m(l+1)+2m-2} \leq \\ &\leq 0,5D(l+1)(P_1 \dots P_r)^{2m(l+1)} P_1^{-\Delta(l+1)}. \end{aligned}$$

Очевидно, что $A_1(l+1) \leq 0,5D(l+1)$. Утверждение будет доказано, если будет доказана справедливость неравенства

$$P_1^{-2m(l+1)+2m-2} \leq P_1^{-\Delta(l+1)},$$

т. е.

$$m_1 - m_1 \left(1 - \frac{1}{n} \right)^{l+1} \leq 2ml + 2, m_1 = \frac{rnm}{r+1}.$$

Из неравенства Бернулли получим

$$1 - \left(1 - \frac{1}{n} \right)^{l+1} \leq \frac{l+1}{n}.$$

Достаточно проверить при $l \geq 1, r \geq 2$, справедливость следующих неравенств

$$m_1 \frac{l+1}{n} \leq 2ml + 2, \frac{rnm(l+1)}{r+1} \leq 2ml + 2, \frac{2l}{l+1} \geq 1 > \frac{r}{r+1}.$$

Теорема доказана.

4. Заключение

Найденная в работе теорема возникла в связи с приближением гладкой функции от нескольких переменных многочленом Тейлора, который представляет собой сумму форм различных степеней, являющихся дифференциалами данной функции. Здесь рассматривается случай, когда переменные "равноправны". Другими словами, длины промежутков изменения их имеют один и тот же порядок. Для оценок сумм, подобных дзетовой, нам понадобятся суммы с "неравноправными" длинами промежутков суммирования. Соответствующая теорема о среднем нами доказана и будет опубликована в ближайшее время.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Littlewood J. E. Researches in the theory of Riemann ζ -function // *Proc. London Math. Soc.*(2), 1922, Том. 20, XXII-XXVIII.
2. Виноградов И. М. Метод тригонометрических сумм в теории чисел. 2-е изд., исправленное и дополненное — М.: Физматлит. 1980, 144 с.
3. Виноградов И. М. Новая оценка функции $\zeta(1+it)$ // *Изв. АН СССР, сер. матем.*, 1958, Том. 22, № 2, 161–164.
4. Виноградов И. М. К вопросу об оценке тригонометрических сумм // *Изв. АН СССР, сер. матем.*, 1965, Том. 29, № 3, 493–504.
5. Чудаков Н. Г. О функциях $\zeta(s)$ и $\pi(x)$ // *Докл. АН СССР*, 1938, Том. 21, 425–426.
6. Titchmarsh E. C. On $\zeta(s)$ and $\pi(x)$ // *Quart. J. Math.*, 1938, Том. 9, 97–108.
7. Линник Ю. В. Новые оценки сумм Вейля // *Докл. АН СССР*, 1942, Том. 34, № 7.
8. Коробов Н. М., Оценки тригонометрических сумм и их приложения // *Успехи матем. наук*, 1958, Том. 13, № 4, 185–192.
9. Walfisz A. Weylsche Exponentialsummen in der Neueren Zahlentheorie. — VEB Deutscher Verlag der WissenSchaften: Berlin. 1963, S. 231.
10. Карацуба А. А., Коробов Н. М. О теореме о среднем // *Докл. АН СССР*, 1963, Том. 149, № 2.
11. Карацуба А. А. Теоремы о среднем и полные тригонометрические суммы // *Изв. АН СССР, сер. матем.*, 1966, Том. 30, № 1.
12. Архипов Г. И. Кратные тригонометрические суммы // *Докл. АН СССР*, 1974, Том. 219, № 5.
13. Архипов Г. И. Избранные труды. — Орёл: Изд-во Орловского ун-та, 2013, 464 с.
14. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Теория кратных тригонометрических сумм. — М.: Наука. Гл. ред. физ.-мат. лит. 1987, 368 с.
15. Arkhipov G. I., Chubarikov V. N., Karatsuba A. A. Trigonometric sums in number theory and analysis. De Gruyter expositions in mathematics; 39 — Berlin, New York: Walter de Gruyter, 2004, pp. 554.
16. Чубариков В. Н. Кратные тригонометрические суммы с простыми числами // *Докл. АН СССР*, 1984, Том. 278, № 2, 302–304.
17. Чубариков В. Н. Оценки кратных тригонометрических сумм с простыми числами // *Изв. АН СССР, сер. матем.*, 1985, Том. 49, № 5, 1031–1067.

REFERENCES

1. Littlewood J. E, 1922, "Researches in the theory of Riemann ζ -function", *Proc. London Math. Soc.*(2), vol. 20, XXII-XXVIII.
2. Vinogradov I. M., 1980, *The method of trigonometric sums in the theory of numbers. 2nd Edition., correct. and supplement*, Moscow: Fizmatlit. pp. 144.

3. Vinogradov I. M., 1958, The new estimation of function $\zeta(1 + it)$, *Izvestija. AN SSSR, Ser.Mathem.*, vol. 22, № 2, 161–164.
4. Vinogradov I. M., 1965, "To the question on the estimation of trigonometric sums", *Izvestija. AN SSSR, Ser.Mathem.*, vol. 29, № 3, 493–504.
5. Chudakov N. G., 1938, "On functions $\zeta(s)$ and $\pi(x)$ ", *Doklady AN SSSR*, vol. 21, 425–426.
6. Titchmarsh E. C., 1938, "On $\zeta(s)$ and $\pi(x)$ ", *Quart. J. Math.*, vol. 9, 97–108.
7. Linnik J. V., 1942, "New estimation of Weyl's sums", *Doklady AN SSSR*, vol. 34, № 7.
8. Korobov N. M., 1958, "Estimations of trigonometric sums and their applications", *Uspehi mathem. nauk*, vol. 13, № 4, 185–192.
9. Walfisz A., 1963, "Weylsche Exponentialsummen in der Neueren Zahlentheorie", *VEB Deutscher Verlag der WissenSchaften: Berlin*, p. 231.
10. Karatsuba A. A., Korobov N. M. 1963, "On the mean-value theorem", *Doklady AN SSSR*, vol. 149, № 2.
11. Karatsuba A. A., 1966, "Mean-value theorem and complete trigonometric sums", *Izvestija. AN SSSR, Ser.Mathem.*, vol. 30, № 1.
12. Arkhipov G. I., 1974, "Multiple trigonometric sums", *Doklady AN SSSR*, vol. 219, № 5.
13. Arkhipov G. I., 2013, *Selected papers*, Orjol: Publ.House of the Orjol University, pp. 464.
14. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N., 1987, *The theory of multiple trigonometric sums*, Moscow.: Nauka. Fizmatlit. 368 c.
15. Arkhipov G. I., Chubarikov V. N., Karatsuba A. A., 2004, "Trigonometric sums in number theory and analysis. De Gruyter expositions in mathematics", 39 — *Berlin, New York: Walter de Gruyter*, pp. 554.
16. Chubarikov V. N., 1984, "Multiple trigonometric sums with primes", *Doklady AN SSSR*, vol. 278, № 2, 302–304.
17. Chubarikov V. N., 1985, "Estimates of multiple trigonometric sums with primes", *Izvestija. AN SSSR, Ser.Matem.*, vol. 49, № 5, 1031–1067.

Получено 22.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 517

DOI 10.22405/2226-8383-2020-21-1-357-363

О размере множества произведения множеств рациональных чисел

Ю. Н. Штейников

Ю. Н. Штейников Федеральный научный центр «Научно-исследовательский институт мистемных исследований РАН» (г. Москва).

e-mail: yuriisht@gmail.com

Аннотация

Впервые в статье [1] были установлены нетривиальные нижние оценки на размер множества произведений рациональных чисел, числители и знаменатели которых ограничены некоторой величиной Q . Грубо говоря, было показано, что размер произведения отклоняется от максимального не меньше чем в $\exp\left\{(9+o(1))\frac{\log Q}{\sqrt{\log \log Q}}\right\}$ раз. В статье [7] показатель у $\log \log Q$ был улучшен со значения $1/2$ до значения 1 и доказательство основного результата о множестве произведений дробей было принципиально другим. Это доказательство, его аргумент был основыван на поиске специального большого подмножества исходного множества рациональных чисел, у множество числителей и знаменателей которых являлись попарно взаимно простыми числами. Главным инструментом было рассмотрение случайных подмножеств. Была получена нижняя оценка математического ожидания величины размера этого случайного подмножества. Там же удалось получить верхнюю оценку на мультипликативную энергию рассматриваемого множества. Нижняя оценка на число произведений и верхняя оценка на мультипликативную энергию множества являются близкими к оптимальным результатам. В данной статье мы предлагаем следующую схему. Мы в общем и целом следуем схеме доказательства статьи [1], при этом модифицируем некоторые шаги и привносим некоторые дополнительные оптимизации и тоже улучшаем показатель со значения $1/2$ до значения $1 - \varepsilon$ для произвольного положительного $\varepsilon > 0$.

Ключевые слова: рациональные числа, делимость, дроби, случайное множество, энергия, число представлений, функция делителей, гладкие числа, преобразование Абеля, подмножество.

Библиография: 18 названий.

Для цитирования:

Ю. Н. Штейников. О размере множества произведения множеств рациональных чисел // Чебышевский сборник, 2020, т. 21, вып. 1, с. 357–363.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 517

DOI 10.22405/2226-8383-2020-21-1-357-363

On the size of the set of the product of sets of rational numbers

Yu. N. Shteinikov

Yu. N. Shteinikov Scientific Research Institute of System Analysis (Moscow).

e-mail: yuriisht@gmail.com

Abstract

For the first time in the article [1] was established non-trivial lower bounds on the size of the set of products of rational numbers, the numerators and denominators of which are limited to a certain quantity Q . Roughly speaking, it was shown that the size of the product deviates from the maximum by no less than $\exp\left\{(9 + o(1))\frac{\log Q}{\sqrt{\log \log Q}}\right\}$ times. In the article [7], the index of $\log \log Q$ was improved from $1/2$ to 1 , and the proof of the main result on the set of fractions was fundamentally different. This proof, its argument was based on the search for a special large subset of the original set of rational numbers, the set of numerators and denominators of which were pairwise mutually prime numbers. The main tool was the consideration of random subsets. A lower estimate was obtained for the mathematical expectation of the size of this random subset. There, it was possible to obtain an upper bound for the multiplicative energy of the considered set. The lower bound for the number of products and the upper bound for the multiplicative energy of the set are close to optimal results. In this article, we propose the following scheme. In general, we follow the scheme of the proof of the article [1], while modifying some steps and introducing some additional optimizations, we also improve the index from $1/2$ to $1 - \varepsilon$ for an arbitrary positive $\varepsilon > 0$.

Keywords: rational numbers, divisibility, fractions, random set, energy, number of representations, divisor function, smooth numbers, Abel transformation, subset.

Bibliography: 18 titles.

For citation:

Yu. N. Shteinikov 2020, "On the size of the set of the product of sets of rational numbers", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 357–363.

1. Введение

Пусть дано положительное достаточно большое Q и пусть A, B являются множествами рациональных чисел:

$$A, B \subseteq F_Q = \left\{ \frac{r}{s} : 1 \leq r, s \leq Q \right\}.$$

По определению произведение множеств A и B это

$$AB = \{ab : a \in A, b \in B\}.$$

Ж. Бургейн, С.В. Конягин и И.Е. Шпарлинский [1] установили следующий результат.

ТЕОРЕМА 1. Если $A, B \subseteq F_Q$, тогда имеет место оценка

$$|AB| \geq |A||B| \exp\left\{(-9 + o(1))\frac{\log Q}{\sqrt{\log \log Q}}\right\}, Q \rightarrow \infty. \quad (1)$$

Этот результат далее использовался этими и другими авторами для важных теоретико-числовых задач, заинтересованных читателей мы отсылаем к статьям [1], [2], [3], [5], [6]. Х. Силлеруело [2] доказал Теорему 1 и улучшил показатель 9 в формулировке Теоремы 1. Далее автор этой статьи с помощью подхода, отличного от [1], в работе [7] вывел такую оценку.

ТЕОРЕМА 2. *Существует абсолютная константа $C > 0$, такая что если $A, B \subseteq F_Q$, тогда справедлива оценка*

$$|AB| \geq |A||B| \exp\left\{(-C + o(1)) \frac{\log Q}{\log \log Q}\right\}, Q \rightarrow \infty, \quad (2)$$

и в качестве C можно взять $8 \log 2$.

В случае если $A = B$ можно взять $C = 6 \log 2$ и константа C не может быть взята меньше чем $4 \log 2$.

В данной же статье мы будем следовать рассуждениям из [1] с добавлением идей и модификациям и выведем из них такой результат.

ТЕОРЕМА 3. *Существует абсолютная константа $C > 0$ такая что если $A, B \subseteq F_Q$ тогда справедливо неравенство*

$$|AB| \geq |A||B| \exp\left\{(-C + o(1)) \frac{\log Q \log \log \log Q}{\log \log Q}\right\}, Q \rightarrow \infty, \quad (3)$$

Мы отмечаем, что основной результат слабее предыдущего. Однако главной задачей и целью является демонстрация самого метода [1] и его некоторая оптимизация.

Работа организована следующим образом. Во втором разделе собраны вспомогательные утверждения, в третьем мы доказываем основную теорему.

2. Предварительные результаты

Как обычно через $\tau(n)$ будем обозначать число делителей числа n . Напомним известную оценку на $\tau(n)$, которая может быть найдена в книге [10], Theorem 5.2, Kapitel 1.

$$\tau(n) \leq 2^{\frac{(1+o(1)) \log n}{\log \log n}}, n \rightarrow \infty. \quad (4)$$

Нам необходимы некоторые дополнительные утверждения и леммы. Начнем с определения гладких чисел. Для целого n пусть $P^+(n)$ обозначает наибольший простой делитель n , и $P^+(1) = 1$. Для $x \geq y \geq 2$ пусть

$$\psi(x, y) = |\{n \leq x : P^+(n) \leq y\}|.$$

Это множество называется множеством y -гладких чисел, не превосходящих x . Мы приводим верхние оценки на $\psi(x, y)$, которые могут быть в точности представлены в [12], Theorem 1.4, которые мы приводим ниже.

ЛЕММА 1. *Равномерно для $x \geq y \geq 2$, справедливо*

$$\log \psi(x, y) = Z \left\{ 1 + O\left(\frac{1}{\log y} + \frac{1}{\log \log x}\right) \right\},$$

где

$$Z = Z(x, y) = \frac{\log x}{\log y} \log\left(1 + \frac{y}{\log x}\right) + \frac{y}{\log y} \log\left(1 + \frac{\log x}{y}\right).$$

Пусть $\tau(n, z)$ обозначает число делителей числа n , которые не превосходят z , то есть

$$\tau(n, z) = |\{d : d|n, d \leq z\}|.$$

Приведем далее такую лемму.

ЛЕММА 2. *Количество делителей числа $n < Q$, не превосходящих z , не превосходит*

$$\psi(z, (1 + o(1)) \log Q), Q \rightarrow \infty.$$

ДОКАЗАТЕЛЬСТВО. Пусть $p_1^{t_1} \dots p_s^{t_s}$ разложение на простые множители, причем $p_1 < p_2 < \dots < p_s$. Рассмотрим отображение делителей числа n

$$\sigma : p_1^{l_1} \dots p_s^{l_s} \rightarrow p_{(1)}^{l_1} \dots p_{(s)}^{l_s},$$

где $p_{(i)}$ — i -ое простое число в натуральном ряду, то есть $p_{(1)} = 2, p_{(2)} = 3, p_{(3)} = 5, \dots$

Это отображение инъективно. Также, $\sigma(d) \leq d \leq z$.

Известно, что если $n := p_1^{t_1} \dots p_s^{t_s} < Q$ то $p_{(s)} \leq (1 + o(1)) \log Q$. Отсюда количество чисел в образе отображения σ , которые не превосходят z не больше $\psi(z, (1 + o(1)) \log Q)$. А это и есть исходное утверждение. Лемма доказана. $\square$

Из предыдущих двух лемм можно вывести такое лемму. Она нам понадобится в дальнейшем при доказательстве основной теоремы.

ЛЕММА 3. Пусть C_1 — некоторая фиксированная константа, Q — достаточно большое натуральное число, $n \leq Q$ и $s \in [\exp\{C \frac{\log Q}{\log \log Q}\}, Q]$. Тогда существует такая фиксированная константа $C_2 > 0$, что выполнено неравенство

$$\tau(n, s) \leq s^{\frac{(C_2 + o(1)) \log \log \log Q}{\log \log Q}}, Q \rightarrow \infty.$$

3. Доказательство основных результатов.

Теорема 3

ДОКАЗАТЕЛЬСТВО. Схема доказательства аналогична доказательству работы [1]. Введем параметры M_1, γ .

$$M_1 = \exp\left\{\frac{\log Q}{\log \log Q}\right\}; \gamma = \frac{c_0 \log \log \log Q}{\log \log Q},$$

где c_0 — некоторая абсолютная константа, которую определим позже. Мы утверждаем, что существует такое подмножество $B_0 \subseteq F_Q$ размера

$$|B_0| \geq |B|Q^{2\gamma}$$

и $\xi \in \mathbb{Q}$, что $\xi B_0 \subseteq B$ и для любого числа $m > 1$ справедливо

$$|\{r/s \in B_0 : \gcd(r, s) = 1, m|r \text{ or } m|s\}| \leq \frac{2}{m^\gamma} |B_0|. \quad (5)$$

Конструкция построения такого множества следующая. Для положительного действительного R определим

$$E_R = \left\{\frac{r}{s} : r, s \in \mathbb{N}, \gcd(r, s) = 1, rs \leq R\right\}.$$

Ясно, что $F_Q \subseteq E_{R^2}$. Если $B_0 = B$ не удовлетворяет неравенству, то по определению существует такое $m_1 > 1 \in \mathbb{Z}$ (5) и подмножество $B_1 \subseteq E_{Q^2/m_1}$ и размера $|B_1| \geq |B|/m_1^\gamma$ что либо

$$m_1 B_1 \subseteq B_0,$$

либо

$$\frac{1}{m_1} B_1 \subseteq B_0.$$

Далее повторяем итеративно эту процедуру со множеством B_1 вместо B_0 . И так далее. После проведения k шагов мы получим множество B_k такое, что

$$B_k \subseteq E_{Q^2/\prod_i m_i}; \xi B_k \subseteq B, \xi \in \mathbb{Q}, |B_0| \geq |B|/(\prod_i m_i)^\gamma. \quad (6)$$

удовлетворяющее условию (5). Так как мы знаем, что $(\prod_i m_i) \leq Q^2$, то

$$B_k \geq |B|Q^{2\gamma}.$$

Из этого неравенства следует, что наша процедура завершится на каком-то шаге k и множество B_k будет удовлетворять нашему требованию. Положим $B_0 = B_k$. Далее, установим нижнюю оценку на размер множества AB_k . Для $\alpha = r/s \in F_Q$, $\gcd(r, s) = 1$ обозначим

$$B_0(\alpha) = \{u/v \in B_0 : u, v \in \mathbb{N}, \gcd(u, v) = 1, \gcd(u, s) \leq M_1, \gcd(v, r) \leq M_1\}.$$

Докажем, что при правильно подобранной константе c_0 для любого $\alpha \in F_Q$ справедливо $|B_0(\alpha)| \geq |B_0|/2$. Для этого оценим дополнение

$$|B_0 \setminus B_0(\alpha)| \leq |B_0| \left(\sum_{d|r, d > M_1} 1/d^\gamma + \sum_{d|s, d > M_1} 1/d^\gamma \right).$$

Для оценки каждой суммы применим будем применять преобразование Абеля. Продемонстрируем это на примере первой суммы. Пусть $\chi(d)$ обозначает характеристическую функцию множества делителей числа r , а $X(s) = \sum_{M_1 < d \leq s} \chi(d)$.

$$\sum_{d|r, d > M_1} 1/d^\gamma = \sum_{M_1 < d \leq Q} \chi(d)/d^\gamma = X(Q)/Q^\gamma + \gamma \int_{M_1}^Q X(s)/s^{\gamma+1} ds.$$

Далее, заметим, что $X(Q) \leq \tau(r)$. А по Лемме 3 имеет место неравенство

$$X(s) \leq \tau(r, s) \leq s^{\frac{(C_2 + o(1)) \log \log \log Q}{\log \log Q}}.$$

Подставим эти неравенства в последнее выражение и получим, что при достаточно большом, но фиксированном c_0 (в определении γ) мы имеем

$$\sum_{d|r, d > M_1} 1/d^\gamma + \sum_{d|s, d > M_1} 1/d^\gamma < 1/2.$$

Поэтому для любого $\alpha \in F_Q$ верно $|B_0(\alpha)| \geq |B_0|/2$. $\square$

Теперь оценим снизу размер множества AB . Легко видеть, что

$$|AB| \geq |AB_0| \geq \left| \bigcup_{\alpha \in A} \{\alpha\beta : \beta \in B_0(\alpha)\} \right| \geq \frac{|A||B_0|}{2L},$$

где по определению $L = \max_{\xi} |\{(\alpha, \beta) : \alpha \in A, \beta \in B_0(\alpha), \alpha\beta = \xi\}|$. Оценим сверху L . Пусть

$$\xi \in F_{Q^2}, \xi = x/y, \alpha = r/s, \beta = u/v, \gcd(x, y) = \gcd(r, s) = \gcd(u, v) = 1.$$

Пусть $\gcd(r, u) = m_1, \gcd(u, s) = m_2$. Тогда, во-первых, по построению множества $B_0(\alpha)$ имеем $m_1, m_2 \leq M_1$. Обозначим $r' = r/m_1, s' = s/m_2, u' = u/m_2, v' = v/m_1$. Тогда $r'u' = x, s'v' = y$. Число возможных четверок (r', s', u', v') не превосходит $\tau(x)\tau(y)$. Число же пар (m_1, m_2) не превосходит M_1^2 . Подставляя известные оценки получаем, что для некоторой фиксированной абсолютной константы $C > 0$

$$L \leq \exp\left\{(-C + o(1)) \frac{\log Q}{\log \log Q}\right\}, Q \rightarrow \infty.$$

Остается заметить, что $|B_0| \geq |B| \exp\left\{(-C + o(1)) \frac{\log Q \log \log \log Q}{\log \log Q}\right\}$ для некоторой фиксированной абсолютной константы $C > 0$. Подставляя все эти оценки мы получаем утверждение Теоремы 3. Эти мы завершаем доказательство теоремы.

4. Заключение

Отметим, что некоторые результаты о произведениях и частных подмножеств натуральных чисел содержатся в работах [4] – [13] и в приведенной ниже литературе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bourgain J., Konyagin S.V., Shparlinski I.E. Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm // *Int. Math Research Notices*. 2008. rnn 090, P. 1-29.
2. Cilleruelo J. A note on product sets of rationals // *International Journal of Number Theory*. 2016. Vol. 12, № 05, P. 1415-1420.
3. Cilleruelo J., Garaev M. Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications // *Math. Proc. Cambridge Phil. Soc.* 2016. Vol. 160, Issue 03, P. 477-494.
4. Cilleruelo J., Ramana D. S., Ramare O. Quotients and product sets of thin subsets of the positive integers // *Proceedings of the Steklov Institute of Mathematics*. 2017, Vol 296, P. 58–71.
5. Cilleruelo J., Ramana D. S., Ramare O. The number of rational numbers determined by large sets of integers // *Bull. of the London Math. Soc.* 2010. Vol 42, №3 P. 517-526.
6. Штейников Ю.Н. Оценки тригонометрических сумм по подгруппам и некоторые их приложения // *Матем. заметки*. 2015. Том 98, выпуск 4, С. 606–625.
7. Штейников Ю.Н. О произведении множеств рациональных чисел // *Тр. МИАН*. 2017. Т. 296, С. 252–259.
8. Tao T., Vu V. Additive combinatorics // Cambridge University Press 2006, P. 1-530.
9. Конягин С.В., Шкредов И.Д. Новые результаты о суммах и произведениях в $\mathbb{R}$ // *Тр. МИАН*, Т. 294, С. 87–98 .
10. Prachar K. Primzahlverteilung // Springer-Verlag Berlin-Göttingen-Heidelberg, 1957.
11. Shnirel'man L.G. Über additive Eigenschaften von Zahlen // *Mathematische Annalen*. 1933. Vol. 107, P. 649-690.
12. Adolf Hildebrand, Gerald Tenenbaum. Integers without large prime factors // *Journal de Theorie des Nombres de Bordeaux*. 1993. Vol. 5, P.411-484.
13. Штейников Ю.Н. Дополнение к работе Х.Силлеруело, Д.С. Раманы, О. Рамаре "Частные и произведения подмножеств нулевой плотности множества натуральных чисел" // *Тр. МИАН*, 2017, Т. 296, С. 260–264 .
14. Штейников Ю. Н. О распределении элементов полугрупп натуральных чисел // *Чебышевский сб.*, Т. 13, №3, С. 91–99 .
15. Штейников Ю. Н. О распределении элементов полугрупп натуральных чисел II // *Чебышевский сб.*, Т. 17, №3, С. 197–203 .

REFERENCES

1. Bourgain J., Konyagin S.V., Shparlinski I.E. "Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm", *Int. Math Research Notices.*, rnn 090, pp. 1-29.
2. Cilleruelo J. A note on product sets of rationals *International Journal of Number Theory* vol. 12, no. 5, pp. 1415-1420.
3. Cilleruelo J., Garaev M. "Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications" *Math. Proc. Cambridge Phil. Soc.*, vol. 160, Issue 03, pp. 477-494.
4. Cilleruelo J., Ramana D. S., Ramare O. "Quotients and product sets of thin subsets of the positive integers" *Proceedings of the Steklov Institute of Mathematics*, vol. 296, pp. 58-71.
5. Cilleruelo J., Ramana D. S., Ramare O. "The number of rational numbers determined by large sets of integers" *Bull. of the London Math. Soc.*, vol. 42, no. 3, pp. 517-526.

6. Shteinikov Yu. N. ‘Estimates of Trigonometric Sums over Subgroups and Some of Their Applications’ *Math. Notes*, vol 98, no. 4, pp. 667-684.
7. Shteinikov Yu. N. “On the product sets of rational numbers” *Proc. Steklov Inst. Math.*, vol. 296, pp. 243–250.
8. Tao T., Vu V. Additive combinatorics *Cambridge University Press.*, 2006, pp.1-530.
9. Konyagin S. V., Shkredov I. D. “New results on sums and products in $\mathbb{R}$ ” *Proc. Steklov Inst. Math.*, vol 294, pp. 78–88.
10. Prachar K. “Primzahlverteilung” *Springer-Verlag Berlin-Göttingen-Heidelberg*, 1957.
11. Shnirel'man L.G. “Über additive Eigenschaften von Zahlen” *Mathematische Annalen*, vol. 107, pp. 649-690.
12. Adolf Hildebrand, Gerald Tenenbaum. “Integers without large prime factors” *Journal de Theorie des Nombres de Bordeaux*, vol. 5, pp.411-484.
13. Shteinikov Yu. N. “Addendum to J. Cilleruelo, D.S. Ramana, and O. Ramare’s Paper ‘Quotient and Product Sets of Thin Subsets of the Positive Integers’” *Proc. Steklov Inst. Math.*, vol 296, pp. 251-255.
14. Shteinikov, Yu. N. “On the distribution of elements of semigroups of natural numbers” *Chebyshevskii Sb.* vol. 13, no. 3, pp. 91-99.
15. Shteinikov, Yu. N. “On the distribution of elements semigroups of natural numbers II”, *Chebyshevskii Sb.* , vol.17, no. 3, pp. 197-203.

Получено 18.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.35, 517.15

DOI 10.22405/2226-8383-2020-21-1-364-367

О значениях последовательности Битти в арифметической прогрессии¹

А. В. Бегунц, Д. В. Горяшин

Бегунц Александр Владимирович — кандидат физико-математических наук, доцент кафедры математического анализа, механико-математический факультет, Московский государственный университет имени М. В. Ломоносова (г. Москва).

e-mail: ab@rector.msu.ru

Горяшин Дмитрий Викторович — кандидат физико-математических наук, доцент кафедры математического анализа, механико-математический факультет, Московский государственный университет имени М. В. Ломоносова (г. Москва).

e-mail: goryashin@mech.math.msu.su

Аннотация

В статье доказана асимптотическая формула для числа значений последовательности Битти в арифметической прогрессии с растущей разностью. Пусть $\alpha > 1$ — иррациональное число и β — вещественное число из промежутка $[0; \alpha)$, a и d — целые числа, $d \geq 2$, $0 \leq a < d$, x — достаточно большое натуральное число. Обозначим через $N_d(x)$ число значений последовательности Битти $[\alpha n + \beta]$, $1 \leq n \leq x$, принадлежащих арифметической прогрессии $(a + kd)$, $k \in \mathbb{N}$. Тогда если неполные частные непрерывной дроби числа α ограничены, то при $x \rightarrow \infty$ справедлива асимптотическая формула $N_d(x) = \frac{x}{d} + O(d \ln^3 x)$, где постоянная в знаке O абсолютная. Разность прогрессии может расти вместе с x , причём результат нетривиален, если $d \ll \sqrt{x} \ln^{-3/2-\varepsilon} x$, $\varepsilon > 0$.

Ключевые слова: последовательность Битти, арифметическая прогрессия, асимптотическая формула.

Библиография: 4 названия.

Для цитирования:

А. В. Бегунц, Д. В. Горяшин О значениях последовательности Битти в арифметической прогрессии // Чебышевский сборник, 2020, т. 21, вып. 1, с. 364–367.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.35, 517.15

DOI 10.22405/2226-8383-2020-21-1-364-367

On the values of Beatty sequence in an arithmetic progression

A. V. Begunts, D. V. Goryashin

Begunts Aleksandr Vladimirovich — candidate of physical and mathematical sciences, associate professor, Lomonosov Moscow State University, Department of mathematics and mechanics (Moscow).

e-mail: ab@rector.msu.ru

Goryashin Dmitry Viktorovich — candidate of physical and mathematical sciences, associate professor, Lomonosov Moscow State University, Department of mathematics and mechanics (Moscow).

e-mail: goryashin@mech.math.msu.su

¹Работа выполнена при поддержке Московского государственного университета имени М. В. Ломоносова (грант «Современные проблемы фундаментальной математики и механики»).

Abstract

In the paper, we consider $N_d(x) = N(x; \alpha, \beta; d, a)$, $x \in \mathbb{N}$, which is the number of values of Beatty sequence $[\alpha n + \beta]$, $1 \leq n \leq x$, for $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0; \alpha)$, in an arithmetic progression $(a + kd)$, $k \in \mathbb{N}$. We prove the asymptotic formula $N_d(x) = \frac{x}{d} + O(d \ln^3 x)$ as $x \rightarrow \infty$, where the implied constant is absolute. For growing difference d the result is non-trivial provided $d \ll \sqrt{x} \ln^{-3/2-\varepsilon} x$, $\varepsilon > 0$.

Keywords: Beatty sequence, arithmetic progression, asymptotic formula.

Bibliography: 4 titles.

For citation:

A. V. Begunts, D. V. Goryashin, 2020, "On the values of Beatty sequence in an arithmetic progression", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 364–367.

В настоящей заметке продолжено исследование свойств последовательности Битти (см., например, [1], [2]) и изучен вопрос о распределении её значений в заданной арифметической прогрессии с растущей разностью. Основным результатом является следующее утверждение.

ТЕОРЕМА. Пусть $\alpha > 1$ — иррациональное число и β — вещественное число из промежутка $[0; \alpha)$, a и d — целые числа, $d \geq 2$, $0 \leq a < d$, x — достаточно большое натуральное число. Обозначим через

$$N_d(x) = N(x; \alpha, \beta; d, a) = \sum_{\substack{1 \leq n \leq x \\ [\alpha n + \beta] \equiv a \pmod{d}}} 1$$

число значений последовательности Битти $[\alpha n + \beta]$, $1 \leq n \leq x$, принадлежащих арифметической прогрессии $(a + kd)$, $k \in \mathbb{N}$. Тогда если неполные частные непрерывной дроби числа α ограничены, то справедлива асимптотическая формула

$$N_d(x) = \frac{x}{d} + O(d \ln^3 x) \quad \text{при } x \rightarrow \infty,$$

где постоянная в знаке O абсолютная.

Данный результат является нетривиальным для всех $d \ll \sqrt{x} \ln^{-3/2-\varepsilon} x$, где $\varepsilon > 0$. Отметим также, что аналогичным образом доказывается асимптотическая формула с остаточным членом $O(d \ln^4 x)$ для случая почти всех $\alpha > 1$ в смысле меры Лебега.

Нам потребуется следующее утверждение.

ЛЕММА 1 ([3], лемма 19). Пусть α — положительное иррациональное число, действительное число β лежит в промежутке $[0; \alpha)$ и функция ξ определена на множестве натуральных чисел. Тогда для любого целого числа $L \geq 2$ при $N \rightarrow \infty$ справедлива оценка

$$\sum_{n \leq N} \xi([\alpha n + \beta]) - \frac{1}{\alpha} \sum_{n \leq \alpha N + \beta} \xi(n) \ll |\Sigma_1| + |\Sigma_2| + |R_{N,\alpha}|, \quad (1)$$

где

$$|\Sigma_1| \ll \sum_{1 \leq m \leq L} \frac{1}{m} \left| \sum_{n \leq \alpha N + \beta} \xi(n) e^{2\pi i \lambda m n} \right|, \quad (2)$$

$$|\Sigma_2| \ll \frac{\ln L}{L} \left(\sum_{1 \leq m \leq L \ln L} \left| \sum_{n \leq \alpha N + \beta} \xi(n) e^{2\pi i \lambda m n} \right| + \sum_{n \leq \alpha N + \beta} |\xi(n)| \right), \quad (3)$$

$$|R_{N,\alpha}| \ll \max_{n \leq \alpha N + \beta} |\xi(n)| \quad (4)$$

и $\lambda = \frac{1}{\alpha k}$, причём k — наименьшее натуральное число, для которого $\alpha k > 1$.

Применим утверждение данной леммы к функции $\xi(n) = \delta_{a,d}(n)$, равной характеристической функции арифметической прогрессии $a + kd$, $k \in \mathbb{N}$, т. е.

$$\delta_{a,d}(n) = \begin{cases} 1, & \text{если } n \equiv a \pmod{d}, \\ 0, & \text{если } n \not\equiv a \pmod{d}. \end{cases}$$

Получим

$$N_d(x) = \frac{1}{\alpha} \sum_{\substack{1 \leq n \leq \alpha x + \beta \\ n \equiv a \pmod{d}}} 1 + O(R) = \frac{1}{\alpha} \left(\frac{\alpha x + \beta}{d} + O(1) \right) + O(R) = \frac{x}{d} + O(R),$$

где $R = R_1 + R_2 + 1$,

$$R_1 = \sum_{1 \leq m \leq L} \frac{1}{m} \left| \sum_{n \leq \alpha x + \beta} \delta_{a,d}(n) e^{2\pi i \lambda m n} \right|, \quad \lambda = \frac{1}{\alpha},$$

$$R_2 = \frac{\ln L}{L} \left(\sum_{1 \leq m \leq L \ln L} \left| \sum_{n \leq \alpha x + \beta} \delta_{a,d}(n) e^{2\pi i \lambda m n} \right| + \sum_{n \leq \alpha x + \beta} \delta_{a,d}(n) \right).$$

Докажем обобщение леммы 3.3 книги [4], используя обозначение $\|x\| = \min_{n \in \mathbb{Z}} |x - n|$.

ЛЕММА 2. Пусть λ — положительное иррациональное число и ψ — такая неубывающая положительная функция, что при всех натуральных m верно неравенство $\|\lambda m\| \geq \frac{1}{m\psi(m)}$. Тогда для любых $d, L \geq 1$:

- а) существует такое $\delta > 0$, что на промежутке $[0; \delta)$ не попадёт ни одного значения $\|\lambda d m\|$, $1 \leq m \leq L$, причём можно положить $\delta = (2dL\psi(2dL))^{-1}$;
 б) при $L \rightarrow \infty$ справедливы оценки

$$\sum_{1 \leq m \leq L} \frac{1}{\|\lambda d m\|} \ll dL\psi(2dL) \ln L, \quad \sum_{1 \leq m \leq L} \frac{1}{m\|\lambda d m\|} \ll d\psi(2dL) \ln L + d \sum_{1 \leq m \leq L} \frac{\psi(2dm) \ln m}{m}.$$

ДОКАЗАТЕЛЬСТВО. Следуя доказательству леммы 3.3 книги [4], воспользуемся тем, что для любого $\delta > 0$ из неравенств $\|x \pm y\| \geq \delta$ вытекает неравенство $\|x\| - \|y\| \geq \delta$. Рассмотрим произвольные целые числа m_1, m_2 с условием $0 \leq m_2 < m_1 \leq L$. Тогда поскольку

$$\|\lambda d m_1 \pm \lambda d m_2\| = \|\lambda d(m_1 \pm m_2)\| \geq \frac{1}{d(m_1 \pm m_2)\psi(d(m_1 \pm m_2))} \geq \frac{1}{2dL\psi(2dL)} = \delta,$$

получаем, что $\|\lambda d m_1\| - \|\lambda d m_2\| \geq \delta$. Полагая $m_2 = 0$, получаем утверждение п. а). Следовательно, точки $\|\lambda d m\|$, $1 \leq m \leq L$, расположены на полуинтервале $(0; \frac{1}{2}]$ так, что расстояние между любыми соседними не меньше δ , при этом на промежутке $[0; \delta)$ ни одной такой точки нет. Значит,

$$S_L = \sum_{1 \leq m \leq L} \frac{1}{\|\lambda d m\|} \leq \sum_{1 \leq m \leq L} \frac{1}{m\delta} \ll dL\psi(2dL) \ln L.$$

Далее, пользуясь преобразованием Абеля, получаем

$$\sum_{1 \leq m \leq L} \frac{1}{m\|\lambda d m\|} = \frac{S_L}{L+1} + \sum_{1 \leq m \leq L} \frac{S_m}{m(m+1)} \ll d\psi(2dL) \ln L + d \sum_{1 \leq m \leq L} \frac{\psi(2dm) \ln m}{m}.$$

Лемма доказана.

Оценим теперь суммы R_1 и R_2 . Поскольку при $\|t\| \neq 0$ для всякого $x > 0$ верна оценка

$$\left| \sum_{k \leq x} e^{2\pi i k t} \right| \leq \frac{1}{2\|t\|},$$

получаем

$$R_1 = \sum_{1 \leq m \leq L} \frac{1}{m} \left| \sum_{k \leq \frac{\alpha x + \beta - a}{d}} e^{2\pi i \lambda m(a + kd)} \right| = \sum_{1 \leq m \leq L} \frac{1}{m} \left| \sum_{k \leq \frac{\alpha x + \beta - a}{d}} e^{2\pi i \lambda m d k} \right| \leq \frac{1}{2} \sum_{1 \leq m \leq L} \frac{1}{m\|\lambda d m\|}.$$

Аналогично имеем

$$R_2 = \frac{\ln L}{L} \sum_{1 \leq m \leq L \ln L} \left| \sum_{k \leq \frac{\alpha x + \beta - a}{d}} e^{2\pi i \lambda m(a + kd)} \right| + \frac{x}{dL} \ln L \ll \frac{\ln L}{L} \sum_{1 \leq m \leq L \ln L} \frac{1}{\|\lambda d m\|} + \frac{x}{dL} \ln L.$$

Далее воспользуемся утверждением леммы 2. Если неполные частные непрерывной дроби числа α (а значит, и числа $\lambda = \frac{1}{\alpha}$) ограничены, то соответствующая функция ψ равна константе (см. [4, с. 134–135]). Получаем оценки

$$|R_1| \ll d \ln^2 L, \quad |R_2| \ll d \ln^3 L + \frac{x}{dL} \ln L,$$

что при $L = x$ даёт требуемый результат.

Авторы благодарят профессора В. Н. Чубарикова за поддержку и внимание к работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Technau, M., 2018, “On Beatty sets and some generalisations thereof”, Würzburg, Würzburg University Press. doi: 10.25972/WUP-978-3-95826-089-4
2. Бегунц А. В., Горяшин Д. В. Актуальные задачи, связанные с последовательностями Битти // Чебышевский сборник. **18**. Вып. 4. 2017. 97–105. doi: 10.22405/2226-8383-2017-18-4-97-105
3. Бегунц А. В. О распределении значений сумм мультипликативных функций на обобщенных арифметических прогрессиях // Чебышевский сборник. **6**. Вып. 2. 2005. 52–74.
4. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей: Пер. с англ. — М.: Наука, 1985. — 408 с.

REFERENCES

1. Technau, M., 2018, “*On Beatty sets and some generalisations thereof*”, Würzburg, Würzburg University Press. urn:nbn:de:bvb:20-opus-163303
2. Begunts, A. V., Goryashin, D. V., 2017, “Topical problems concerning Beatty sequences”, *Chebyshevskii Sb.*, vol. 18, no. 4, pp. 97–105. doi: 10.22405/2226-8383-2017-18-4-97-105
3. Begunts, A. V., 2005, “On the distribution of the values of sums of multiplicative functions on generalized arithmetic progressions”, *Chebyshevskii Sb.*, vol. 6, no. 2, pp. 52–74.
4. Kuipers, L., Niederreiter, H., 1974, *Uniform Distribution of Sequences*, Wiley, New York.

Получено 21.09.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 512

DOI 10.22405/2226-8383-2020-21-1-368-373

Канонический базис Гензеля — Шафаревича для формальных модулей Хонды¹

С. В. Востоков, Р. П. Востокова, Е. В. Иконникова

Востоков Сергей Владимирович — доктор физико-математических наук, профессор, профессор кафедры высшей алгебры и теории чисел, Санкт-Петербургский государственный университет (г. Санкт-Петербург).

e-mail: sergei.vostokov@gmail.com

Востокова Регина Петровна — старший преподаватель, кафедра общей математики и информатики, Санкт-Петербургский государственный университет (г. Санкт-Петербург).

e-mail: rvostokova@yandex.ru

Иконникова Елена Валерьевна — инженер-исследователь, факультет математики и компьютерных наук, Санкт-Петербургский государственный университет (г. Санкт-Петербург).

e-mail: ikonnikovaev@gmail.com

Аннотация

В данной работе мы строим систему образующих Гензеля — Шафаревича для формальных модулей Хонды над многомерным полем. В дальнейшем это даст возможность вычисления символа Гильберта в описанной ситуации.

Ключевые слова: формальные группы, формальные модули

Библиография: 14 названий.

Для цитирования:

С. В. Востоков, Р. П. Востокова, Е. В. Иконникова. Канонический базис Гензеля — Шафаревича для формальных модулей Хонды // Чебышевский сборник, 2020, т. 21, вып. 1, с. 368–373.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 512

DOI 10.22405/2226-8383-2020-21-1-368-373

The Hensel–Shafarevich canonical basis in Honda formal modules

S. V. Vostokov, R. P. Vostokova, E. V. Ikonnikova

Vostokov Sergey Vladimirovich — doctor of physical and mathematical Sciences, Professor, Professor of algebra and number theory Department of St. Petersburg University (Saint Petersburg).

e-mail: sergei.vostokov@gmail.com

Vostokova Regina Petrovna — Senior Lecturer, Department of General Mathematics and Computer Science, St. Petersburg State University (Saint Petersburg).

e-mail: rvostokova@yandex.ru

Ikonnikova Elena Valerevna — Research Engineer, Faculty of Mathematics and Computer Science, St. Petersburg State University (Saint Petersburg).

e-mail: ikonnikovaev@gmail.com

¹Работа выполнена при поддержке Российского научного фонда, грант 16-11-10200

Abstract

In this paper, we construct Hensel–Shafarevich generating set in Honda formal modules over a higher dimensional field. Later, that should allow us to compute Hilbert symbol in this case.

Keywords: formal groups, formal modules

Bibliography: 14 titles.

For citation:

S. V. Vostokov, R. P. Vostokova, E. V. Ikonnikova, 2020, "The Hensel–Shafarevich canonical basis in Honda formal modules", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 368–373.

1. Введение

При изучении формальных модулей важную роль играют их системы образующих. В данной работе мы построим систему образующих Шафаревича для формальных модулей Хонды над многомерным полем. В дальнейшем это даст возможность вычисления символа Гильберта в описанной ситуации.

2. Обозначения

Пусть k — локальное поле характеристики 0, с полем вычетов $\bar{k} = \mathbb{F}_q$, $q = p^f$, $p \neq 2$. Пусть k'/k — конечное неразветвленное расширение с униформизирующей π . Рассмотрим K — n -мерное локальное поле, т.е., цепочку полей $K = K_n, K_{n-1}, \dots, K_1, K_0$, где каждое следующее поле является полем вычетов предыдущего, и предположим, что при этом $K_1 = k'$. Тогда $K = k'((t_2)) \dots ((t_n))$, $(\pi, t_2, \dots, t_n)$ — система локальных параметров.

Обозначим за L конечное расширение K . Тогда $L = L_1((T_2)) \dots ((T_n))$, L_1 — конечное расширение K_1 . Системой локальных параметров при этом будет $(\Pi, T_2, \dots, T_n)$, где Π — униформизирующая в K . Пусть $L_i = L_1((T_2)) \dots ((T_i))$ и T_0 — подполе инерции в L_1/k .

Нам понадобится отображение $\sigma : K \rightarrow K$, действующее на локальные параметры t_i как $\sigma(t_i) = t_i^p$, а на k' совпадающее с автоморфизмом Фробениуса, и оператор Δ на $K[[X]]$:

$$\Delta(\sum c_i X^i) = \sum \sigma(c_i) X^{pi}$$

Обозначим через $\mathcal{D}$ кольцо степенных рядов от Δ с коэффициентами из $\mathcal{O}_K$, на котором введем умножение

$$\Delta \cdot a = \sigma(a) \cdot \Delta$$

3. Предварительные сведения

3.1. Тип формальной группы

Пусть $F(X, Y) \in \mathcal{O}_K[[X, Y]]$ — формальная группа. Тогда F строго изоморфна p -типической формальной группе F_p , т.е., такой формальной группе, логарифм которой имеет вид $\lambda_p(X) = \sum_{i=0}^{\infty} c_i X^{p^i}$.

ПРЕДЛОЖЕНИЕ 1. Пусть F_p — p -типическая формальная группа. Тогда существует единственный $u_p(\Delta) \in \pi + \mathcal{D}\Delta$ (будем называть его типом F_p), такой что

$$\lambda_p(X) = (\pi u_p^{-1}(\Delta))(X).$$

Обратно, пусть $u \in \pi + \mathcal{D}\Delta$. Тогда ряд $\lambda(X) = \pi u^{-1}(\Delta) \circ X$ будет логарифмом некоторой p -типической формальной группы над $\mathcal{O}_K$.

ДОКАЗАТЕЛЬСТВО. По теории Хонды существует $u(\Delta) \in \pi + \mathcal{D}\Delta$ со свойством $u(\Delta) \circ \lambda_p(X) \equiv 0 \pmod{\pi}$. Тогда $u \circ \Lambda = \pi \varepsilon(\Delta)$, и $\varepsilon \in 1 + \mathcal{D}\Delta$. Теперь можно взять $u_p = \varepsilon^{-1} \circ u$.

Обратно, ряд $\lambda(X)$ удовлетворяет сравнению. $\square$

3.1.1. Оператор $\mathcal{A}$

Из теории Хонды выводится следующее утверждение:

ПРЕДЛОЖЕНИЕ 2. В классе изоморфных формальных групп высоты h можно выделить канонический представитель – группу Артина-Хассе F_c с логарифмом $\lambda_c(X) = \pi u_c^{-1}(\Delta) \circ X$, где $u_c = \pi - \sum_{i=1}^h a_i \Delta^i$.

ТЕОРЕМА 1. Пусть F – p -типическая формальная группа над $\mathcal{O}_K$ типа $u = \pi - a_h B \Delta^h$, $B \in 1 + \mathcal{D}\Delta$, и пусть $\lambda_1(X) = (\pi u^{-1}(\Delta))(X)$, где $u_1 = u^{\sigma^h} \circ B^{-1}$. Тогда

1. λ_1 является логарифмом некоторой p -типической формальной группы F_1 над $\mathcal{O}_K$;
2. существует $[\pi a_h^{-1}]_{F, F_1} \in \text{Hom}_{\mathcal{O}_K}(F, F_1)$, такой что

$$[\pi a_h^{-1}]_{F, F_1}(X) \equiv X^{p^h} \pmod{\pi}$$

3. если u_c – канонический тип F , то $u_{c,1} = a_h^{-1} u_c a_h$ – канонический тип F_1 .

ДОКАЗАТЕЛЬСТВО.

1. $u_1 = u^{\sigma^h} \circ B^{-1} \in \pi + \mathcal{D}\Delta$ Следовательно, u_1 – логарифм некоторой формальной группы F_1 над $\mathcal{O}_K$.
2. Рассмотрим группу F'_1 с логарифмом $\lambda'_1 = \pi u_1'^{-1} \circ X$, где $u'_1 = B u_1$. Учитывая, что $B \equiv 1 \pmod{\Delta}$, F'_1 будет строго изоморфна F_1 .

Легко проверить, что

$$[\pi a_h^{-1}]_{F, F_1} = [\pi a_h^{-1}]_{F, F'_1} \circ [1]_{F'_1, F_1}$$

– гомоморфизм, удовлетворяющий условию.

- 3.

$$u_{c,1} = (a_h^{-1} \varepsilon a_h)(a_h^{-1} u a_h) = (a_h^{-1} \varepsilon a_h) B u_1$$

Т.е., $u_{c,1} = \eta u_1$, где $\eta \in 1 + \mathcal{D}\Delta$.

□

Таким образом мы получаем последовательность формальных групп и гомоморфизмов f_i

$$F \rightarrow F_1 \rightarrow \dots \rightarrow F_M$$

$$f^{(m)} = f_{m-1} \circ \dots \circ f_1 \circ f$$

3.1.2. Отображение Артина-Хассе

Определим отображения

$$\bullet E_F : T_0[[X]]_0 \rightarrow F(T_0[[X]]_0)$$

$$E_F(\varphi) = \lambda^{-1}(\pi u_0^{-1} \circ \varphi)$$

$$\bullet l_F : F(T_0[[X]]_0) \rightarrow T_0[[X]]_0$$

$$l_F(\psi) = \frac{u_0}{\pi} \circ \lambda(\psi)$$

(“экспоненту и логарифм”).

ЛЕММА 1. E_F и l_F задают обратные друг другу изоморфизмы $\mathcal{O}_K$ -модулей $\mathcal{O}_{T_0}[[X]]_0$ и $F(\mathcal{O}_{T_0}[[X]]_0)$, а также $T_0[[X]]_0$ и $F(T_0[[X]]_0)$.

ДОКАЗАТЕЛЬСТВО. Непосредственной проверкой. □

3.1.3. Примарные элементы

DEFINITION 5. Элемент $\omega \in F_M(\mathfrak{M})$ называется примарным, если $K(\tilde{\omega})/K$ неразветвлено (где $f^{(M)}(\tilde{\omega}) = \omega$).

- $W_F^M = \text{Ker}[\pi^M]_F \subset F(\mathfrak{M})$
- $\{z_1, \dots, z_h\}$ — множество образующих W_F^M (как модуля над $\mathcal{O}_K$)
- $s = f^{(M)} \circ \underline{z}$, где $\underline{z}$ — разложение одной из образующих в ряд по локальным параметрам
- $\hat{b} = b + b^\Delta + \dots + b^{\Delta^{h-1}}$

ПРЕДЛОЖЕНИЕ 3.

$$\omega(b) = E_M(\hat{b}\lambda_M(s))|_{X=\Pi}$$

— корректно определенный элемент $F_M(\mathfrak{M})$, и, более того, является примарным.

ДОКАЗАТЕЛЬСТВО. Аналогично доказательству из [4], свойства ряда $\hat{b}\lambda_M(s)$ позволяют подставлять в него элемент Π . $\square$

3.2. Основные результаты

Определим многочлены Эньяра:

$$g_0 = \pi_{M-1}X + X^{p^h}$$

$$g_{\rho,a} = \pi_{M-1}X + \pi_{M-1}aX^{p^\rho} + X^{p^h}, a \in \mathcal{O}_K, 1 \leq \rho < fh$$

Пусть u_{M-1} — канонический тип группы F_{M-1} . Тогда существуют единственные (с точностью до изоморфизма) формальные группы $G_0, G_{\rho,a}$, для которых $g_0, g_{\rho,a}$ являются допустимыми изогениями в группы $G'_0, G'_{\rho,a}$ соответственно. Тогда u_M — тип групп $G'_0, G'_{\rho,a}$, следовательно, они изоморфны F_N . Обозначим соответствующие изоморфизмы за $\mathcal{E}_M^0, \mathcal{E}_M^{\rho,a}$.

ТЕОРЕМА 2. Элементы

$$\omega_i(b), b \in \mathcal{O}_K, \quad 1 \leq i \leq h,$$

$$\mathcal{E}_M^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}),$$

$$\mathcal{E}_M^{\rho,a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}),$$

$\theta \in \mathcal{R}, a \in \mathcal{O}_K^*, 1 \leq \rho < fh, p \nmid \vec{i}, 0 < i_n \leq e_* = p^h e_n / (p^h - 1)$ являются множеством образующих для $F_M(\mathfrak{M})$.

ДОКАЗАТЕЛЬСТВО. Достаточно проверить это утверждение для одной формальной группы типа u , например, $F = \mathcal{A}^{-M+1}G_0$. Обозначим логарифм G_0 за λ_0 и логарифм $G_{\rho,a}$ за μ . Тогда

$$(B_{n-1}\lambda_0^{\Delta^h}) \circ g_0 = \pi_{n-1}\lambda_0,$$

$$(B_{n-1}\mu^{\Delta^h}) \circ g_{\rho,a} = \pi_{n-1}\mu,$$

то есть

$$(B_{n-1}\lambda_0^{\Delta^h})(\pi_{n-1}x) \equiv \pi_{n-1}\lambda_0(x) \bmod \deg p^\rho + 1$$

$$(B_{n-1}\mu^{\Delta^h})(\pi_{n-1}x) \equiv \pi_{n-1}\mu(x) \bmod \deg p^\rho + 1$$

Таким образом, если мы определим V как элемент, удовлетворяющий условию

$$V - V^{\Delta^h} \pi_{n-1}^{p^\rho-1} = a,$$

то $\mu \equiv \lambda_0 + Vx^{p^\rho}$. Рассмотрев логарифмы $\mathcal{A}G_0$ и $\mathcal{A}G_{\rho,a}$, делаем вывод, что

$$E_M^{\rho,a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}) - \theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n} \equiv$$

$$\equiv V^{\Delta^h} \theta^{p^\rho} \Pi^{ip^\rho} T_2^{i_2} \dots T_n^{i_n} \bmod \Pi^{ip^{\rho+1}} T_2^{i_2} \dots T_n^{i_n}$$

Теперь заметим, что достаточно добавить примарные элементы, чтобы получить полную систему образующих. $\square$

Положим

$$\begin{aligned}\tilde{\mathcal{E}}^0 &= [\pi^M / \pi_1^{(M)}]_{AG_0, F} \\ \tilde{\mathcal{E}}^{\rho, a} &= [\pi^M / \pi_1^{(M)}]_{AG_{\rho, a}, F}\end{aligned}$$

ТЕОРЕМА 3. *Элементы*

$$\begin{aligned}\tilde{\omega}_i(b), b \in \mathcal{O}_K, \quad 1 \leq i \leq h, \\ \tilde{\mathcal{E}}^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}), \\ \tilde{\mathcal{E}}^{\rho, a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}),\end{aligned}$$

$\theta \in \mathcal{R}$, $a \in \mathcal{O}_K^*$, $1 \leq \rho < fh$, $p \nmid i$, $0 < i_n \leq e_* = p^h e_n / (p^h - 1)$ являются множеством образующих для $F(\mathfrak{M})$.

ДОКАЗАТЕЛЬСТВО. Следует из предыдущей теоремы и того, что

$$\begin{aligned}[\pi^M / \pi_1^{(M)}]_{F_M, F} \mathcal{E}_M^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}) &= \tilde{\mathcal{E}}^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}) \\ [\pi^M / \pi_1^{(M)}]_{F_N, F} \mathcal{E}_M^{\rho, a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}) &= \tilde{\mathcal{E}}^{\rho, a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n})\end{aligned}$$

$\square$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Ivan B. Fesenko, S. V. Vostokov, "Local fields and their extensions", AMS Bookstore, 2002.
2. M. Hazewinkel, "Formal Groups and Applications", Pure Appl. Math., 78, Academic Press, New York, 1978.
3. J. Lubin, J. Tate, "Formal complex multiplication in local fields", Annals of Mathematics. Second Series 81, 1965 380–387.
4. М. В. Бондарко, С. В. Востоков, Ф. Лоренц, "Спаривание Гильберта для формальных групп над σ -кольцами", Вопросы теории представлений алгебр и групп. 11, Зап. научн. сем. ПОМИ, 319, ПОМИ, СПб., 2004, 5–58.
5. С. В. Востоков, "Норменное спаривание в формальных модулях", Известия АН СССР, Сер.матем., 1979, т. 43, № 4, с. 706–794.
6. С. В. Востоков, "Канонический базис Гензеля–Шафаревича в полных дискретно-нормированных полях", Вопросы теории представлений алгебр и групп, 22, Зап. научн. сем. ПОМИ, 394, ПОМИ, СПб., 2011, 174–193.
7. С. В. Востоков, И. Л. Климовицкий, "Примарные элементы в формальных модулях", Математика и информатика, 2, К 75-летию со дня рождения Анатолия Алексеевича Карацубы, Совр. пробл. матем., 17, МИАН, М., 2013, 153–163.
8. Д. Г. Бенуа, С. В. Востоков, "Норменное спаривание в формальных группах и представления Галуа", Алгебра и Анализ, том 2, вып. 6, 1990, с. 69–97.
9. О. В. Демченко, "Формальные группы Хонды: арифметика группы точек", Алгебра и Анализ, том 12, вып. 1, 2000, с. 132–149.
10. О. В. Демченко, "Новое в отношениях формальных групп Любина–Тэйта и формальных групп Хонды", Алгебра и анализ, 10:5 (1998), 77–84;
11. С. С. Афанасьева, Р. П. Востокова, "Логарифмы формальных A -модулей в малом ветвлении" Алгебра и анализ, 27:6 (2015), 6–13.
12. Ikonnikova, E.V., Shaverdova, E.V. The Shafarevich basis in higher dimensional local fields. (2014) Journal of Mathematical Sciences (United States), 202 (3), pp. 410–421.
13. Ikonnikova, E.V. "The Hensel-Shafarevich canonical basis in Lubin-Tate formal modules", 2016 Journal of Mathematical Sciences (United States), 219 (3), pp. 462–472.
14. Afanaseva, S.S., Ikonnikova, E.V., "Arithmetic of π_0 -critical module", 2017, Lobachevskii Journal of Mathematics, 38 (1), pp. 131–136.

REFERENCES

1. Ivan B. Fesenko, S. V. Vostokov, "Local fields and their extensions", AMS Bookstore, 2002.
2. M. Hazewinkel, "Formal Groups and Applications", Pure Appl. Math., 78, Academic Press, New York, 1978.
3. J. Lubin, J. Tate, "Formal complex multiplication in local fields", *Annals of Mathematics. Second Series* 81, 1965 380–387.
4. M.V.Bondarko, S.V.Vostokov, F.Lorenz, "The Hilbert pairing for formal groups over σ -rings", *Problems in the theory of representations of algebras and groups. Part 11*, *Zap. Nauchn. Sem. POMI*, 319, POMI, St. Petersburg, 2004, 5–58; *J. Math. Sci. (N. Y.)*, 134:6 (2006), 2445–2476
5. S. V. Vostokov, "A norm pairing in formal modules", *Izv. Akad. Nauk SSSR Ser. Mat.*, 43:4 (1979), 765–794; *Math. USSR-Izv.*, 15:1 (1980), 25–51
6. S. V. Vostokov, "Canonical basis of Hensel–Shafarevich in complete discrete valuation fields", *Problems in the theory of representations of algebras and groups. Part 22*, *Zap. Nauchn. Sem. POMI*, 394, POMI, St. Petersburg, 2011, 174–193; *J. Math. Sci. (N. Y.)*, 188:5 (2013), 570–581
7. S. V. Vostokov, I. L. Klimovitskii, "Primary Elements in Formal Modules", *Mathematics and Informatics*, 2, Dedicated to 75th Anniversary of Anatolii Alekseevich Karatsuba, *Sovrem. Probl. Mat.*, 17, Steklov Math. Institute of RAS, Moscow, 2013, 153–163; *Proc. Steklov Inst. Math.*, 282, suppl. 1 (2013), S140–S149
8. D. G. Benois, S. V. Vostokov, "Norm pairing in formal groups and Galois representations", *Algebra i Analiz*, 2:6 (1990), 69–97; *Leningrad Math. J.*, 2:6 (1991), 1221–1249
9. O. V. Demchenko, "Formal Honda groups: the arithmetic of the group of points", *Algebra i Analiz*, 12:1 (2000), 132–149; *St. Petersburg Math. J.*, 12:1 (2001), 101–115
10. O. V. Demchenko, "New relationships between formal Lubin–Tate groups and formal Honda groups", *Algebra i Analiz*, 10:5 (1998), 77–84; *St. Petersburg Math. J.*, 10:5 (1999), 785–789
11. S. S. Afanas'eva, R. P. Vostokova, "Logarithms of formal A-modules in the case of small ramification", *Algebra i Analiz*, 27:6 (2015), 6–13; *St. Petersburg Math. J.*, 27:6 (2016), 863–868
12. Ikonnikova, E.V., Shaverdova, E.V. The Shafarevich basis in higher dimensional local fields. (2014) *Journal of Mathematical Sciences (United States)*, 202 (3), pp. 410–421.
13. Ikonnikova, E.V. "The Hensel-Shafarevich canonical basis in Lubin-Tate formal modules", 2016 *Journal of Mathematical Sciences (United States)*, 219 (3), pp. 462–472.
14. Afanaseva, S.S., Ikonnikova, E.V., "Arithmetic of π_0 -critical module", 2017, *Lobachevskii Journal of Mathematics*, 38 (1), pp. 131–136

Получено 28.11.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 517.5+511.3

DOI 10.22405/2226-8383-2020-21-1-374-380

Обобщение определения среднего

Р. В. Почеревин

Почеревин Роман Владимирович — аспирант кафедры математических и компьютерных методов анализа, Московский государственный университет им. М. В. Ломоносова (г. Москва).

e-mail: pocherevin-roman@rambler.ru

Аннотация

В статье приводится решение задачи нахождения общего вида среднего в случае отсутствия симметричности по всем переменным. В 1930 году А. Н. Колмогоров дал общий вид среднего значения. Он сформулировал четыре аксиомы среднего: непрерывность и монотонность по каждой переменной, симметричность по каждой переменной, равенство среднего от одинаковых значений этому значению и возможность замены некоторой группы значений их собственным средним без изменения общего среднего. Все переменные в теореме Колмогорова равноправны, это предполагает, что среднее является симметрической функцией по всем переменным. В. Н. Чубариковым была поставлена задача обобщения результата А. Н. Колмогорова на случай отсутствия симметричности по всем аргументам. Теперь переменные разбиваются на группы, и среднее будет симметрично отдельно по каждой из групп переменных. Если такая группа единственна, то исследуемое среднее удовлетворяет аксиомам А. Н. Колмогорова, поэтому результат статьи является обобщением теоремы Колмогорова. В статье найден общий вид функции среднего в этой задаче, отмечена связь с равномерным распределением по модулю единица.

Ключевые слова: Теорема Колмогорова о понятии среднего, равномерное распределение по модулю единица

Библиография: 2 названия.

Для цитирования:

Р. В. Почеревин. Обобщение определения среднего // Чебышевский сборник, 2020, т. 21, вып. 1, с. 374–380.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 517.5+511.3

DOI 10.22405/2226-8383-2020-21-1-374-380

On generalization of mean value

R. V. Pocherevin

Pocherevin Roman Vladimirovich — Ph.D. student of the department of Mathematical and Computer Methods of Analysis, M. V. Lomonosov Moscow State University (Moscow).

e-mail: pocherevin-roman@rambler.ru

Abstract

In paper we discuss the solution of mean value general form problem in case of all variables symmetry absence. In 1930 A. N. Kolmogorov proved the formula for general form of mean value. He formulated four axioms: continuity and monotony on each variable, symmetry on each variable, mean value of equal variables is equal to these variables, any substitution of any group of variables with their mean value does not change the mean value. In Kolmogorov's theorem all arguments are equitable, this means that the mean value is symmetric on each variable. V. N. Chubarikov set the task of generalization to this result in case of all variables symmetry absence. We divide all the variables on groups and the mean value is a symmetric function for variables in each group separately. For example, if we have only one group the mean value will be Kolmogorov's mean value, so we have a generalization of Kolmogorov's theorem. In paper we show the general form of mean value in our case and we note the connection with uniform distribution modulo 1.

Keywords: Kolmogorov's mean value theorem, uniform distribution modulo 1

Bibliography: 2 titles.

For citation:

R. V. Pocherevin, 2020, "On generalization of mean value", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 374–380.

1. Введение

В 1930 году А. Н. Колмогоров дал общий вид среднего значения n величин [1]. В его работе "Об определении среднего" было доказано, что каждый тип среднего, если он удовлетворяет нескольким естественным условиям, имеет определенный вид. А. Н. Колмогоров представил эти аксиомы в следующем виде:

I. $M(x_1, x_2, \dots, x_n)$ непрерывна и монотонна по каждому переменному. Для определенности будет считать, что M возрастает по каждому переменному.

II. $M(x_1, x_2, \dots, x_n)$ — симметрическая функция.

III. Среднее от одинаковых чисел равно их общему значению:

$$\forall x \ M(x, x, \dots, x) = x.$$

IV. Можно заменить некоторую группу значений их собственным средним, не меняя общего среднего:

$$M(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) = M_{n+m}(x, \dots, x, y_1, y_2, \dots, y_n),$$

где $x = M(x_1, x_2, \dots, x_m)$

Из них он вывел общую формулу, которая имеет вид:

$$M(x_1, x_2, \dots, x_n) = \psi \left(\frac{\phi(x_1) + \phi(x_2) + \dots + \phi(x_n)}{n} \right),$$

где ϕ — непрерывная строго монотонная функция, а ψ — обратная к ней.

Все переменные в теореме Колмогорова равноправны, это предполагает, что среднее является симметрической функцией по всем переменным.

Применением теоремы А. Н. Колмогорова является критерий равномерного распределения последовательности по модулю единица [2].

В настоящей статье мы решаем более общую задачу, постановка которой принадлежит В. Н. Чубарикову. В общих словах она состоит в том, чтобы дать общий вид среднего значения величин, объединенных в некоторые группы, по которым происходит осреднение. Переменные разбиваются на группы, и среднее будет симметрично отдельно по каждой из групп переменных. В данной работе приводится общий вид среднего в этой задаче.

2. Формулировка теоремы

Переходим к формулировке основного результата работы. Следуя А. Н. Колмогорову приведем аксиомы I'-IV'

I'. $M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m})$ непрерывна и монотонна по каждому переменному. Для определенности будет считать, что M возрастает по каждому переменному.

II'. $M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m})$ — симметрическая функция отдельно по каждой группе переменных $x_1, x_2, \dots, x_{n_1}; \dots; z_1, z_2, \dots, z_{n_m}$.

III'. Среднее от одинаковых чисел равно их общему значению:

$$\forall x \in [a, b] \quad M(x, \dots, x; x, \dots, x; x, \dots, x) = x.$$

IV'. Можно заменить некоторую группу значений их собственным средним, не меняя общего среднего:

$$M(x_1, x_2, \dots, x_{k_1}, \dots, x_{n_1}; y_1, y_2, \dots, y_{k_2}, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{k_m}, \dots, z_{n_m}) =$$

$$= M_{n_1, \dots, n_m}(t, \dots, t, x_{k_1+1}, \dots, x_{n_1}; t, \dots, t, y_{k_2+1}, \dots, y_{n_2}; \dots; t, \dots, t, z_{k_m+1}, \dots, z_{n_m})$$

где $t = M(x_1, x_2, \dots, x_{k_1}; y_1, y_2, \dots, y_{k_2}; \dots; z_1, z_2, \dots, z_{k_m})$

ТЕОРЕМА 1. При $x_1, \dots, x_{n_1}, y_1, \dots, y_{n_2}, \dots, z_{n_m} \in [a, b]$ и выполнении условий I' - IV' среднее $M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m})$ имеет вид

$$M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) =$$

$$= g(f_1(x_1) + \dots + f_1(x_{n_1}) + \dots + f_m(z_1) + \dots + f_m(z_{n_m})),$$

где g — функция, обратная к функции $n_1 f_1 + n_2 f_2 + \dots + n_m f_m$.

3. Вспомогательные утверждения

В основе доказательства лежат следующие леммы:

ЛЕММА 1. Обозначим через $q \cdot x$ набор из q повторений переменной x : $x, \dots, x$. В данных обозначениях имеет место следующее утверждение:

$$\forall q \in \mathbb{N} \quad M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) =$$

$$= M(q \cdot x_1, q \cdot x_2, \dots, q \cdot x_{n_1}; q \cdot y_1, q \cdot y_2, \dots, q \cdot y_{n_2}; \dots; q \cdot z_1, q \cdot z_2, \dots, q \cdot z_{n_m})$$

ДОКАЗАТЕЛЬСТВО. Разобьем переменные в правой части равенства леммы на q наборов $x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}$. Тогда, используя свойства I' - IV', приходим к следующей цепочке равенств:

$$M(q \cdot x_1, q \cdot x_2, \dots, q \cdot x_{n_1}; q \cdot y_1, q \cdot y_2, \dots, q \cdot y_{n_2}; \dots; q \cdot z_1, q \cdot z_2, \dots, q \cdot z_{n_m}) =$$

$$= M_{qn_1, \dots, qn_m}(t, t, \dots, t; t, t, \dots, t; \dots; t, t, \dots, t) = t,$$

где $t = M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m})$

Лемма 1 доказана. $\square$

Теперь определим для каждого рационального r , $0 \leq r = \frac{p}{q} \leq 1$, функцию $\psi(r)$ следующим образом:

$$\psi(r) = M(p \cdot b, (q-p) \cdot a; p \cdot b, (q-p) \cdot a; \dots; p \cdot b, (q-p) \cdot a)$$

Это определение корректно, поскольку для любого представления рационального числа имеем: $r = \frac{p}{q} = \frac{p_0}{q_0}$, где $(p_0, q_0) = 1$. Введем обозначение: $d = (p, q)$, тогда по лемме 1:

$$\begin{aligned}\psi\left(\frac{p_0}{q_0}\right) &= M(p_0 \cdot b, (q_0 - p_0) \cdot a; p_0 \cdot b, (q_0 - p_0) \cdot a; \dots; p_0 \cdot b, (q_0 - p_0) \cdot a) = \\ &= M(dp_0 \cdot b, d(q_0 - p_0) \cdot a; dp_0 \cdot b, d(q_0 - p_0) \cdot a; \dots; dp_0 \cdot b, d(q_0 - p_0) \cdot a) = \\ &= M(p \cdot b, (q - p) \cdot a; p \cdot b, (q - p) \cdot a; \dots; p \cdot b, (q - p) \cdot a) = \psi\left(\frac{p}{q}\right)\end{aligned}$$

ЛЕММА 2. Функция $\psi(r)$, как функция рационального числа r , является возрастающей.

ДОКАЗАТЕЛЬСТВО. Действительно, пусть $r' > r$. Представим r' и r как дроби с одинаковым знаменателем $r' = \frac{p'}{q}$, $r = \frac{p}{q}$, $p' > p$, и тогда в силу свойства монотонности Γ получим неравенство

$$\begin{aligned}\psi(r') &= M(p' \cdot b, (q - p') \cdot a; p' \cdot b, (q - p') \cdot a; \dots; p' \cdot b, (q - p') \cdot a) > \\ &> M(p \cdot b, (q - p) \cdot a; p \cdot b, (q - p) \cdot a; \dots; p \cdot b, (q - p) \cdot a) = \psi(r)\end{aligned}$$

Лемма 2 доказана. $\square$

ЛЕММА 3. Функцию $\psi(r)$ можно доопределить до непрерывной возрастающей функции на отрезке $[0, 1]$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим случай $r_* \notin \{0, 1\}$. Для точек $r \in \{0, 1\}$ заключение аналогично.

Пусть $r_* \notin \mathbb{Q}$ и пусть $\forall n \in \mathbb{N} \ r_n, r'_n \in \mathbb{Q}$, $r_n \rightarrow r_* - 0$, $r'_n \rightarrow r_* + 0$, причем $\frac{r_n + r'_n}{2} < r_*$

Допустим противное: $\lim_{r_n \rightarrow r_* - 0} \psi(r_n) = A < B = \lim_{r'_n \rightarrow r_* + 0} \psi(r'_n)$. Тогда

$$\begin{aligned}\psi\left(\frac{r_n + r'_n}{2}\right) &= \psi\left(\frac{\frac{p_n}{q_n} + \frac{p'_n}{q_n}}{2}\right) = \psi\left(\frac{p_n + p'_n}{2q_n}\right) = \\ &= M((p_n + p'_n) \cdot b, (2q_n - (p_n + p'_n)) \cdot a; \dots; (p_n + p'_n) \cdot b, (2q_n - (p_n + p'_n)) \cdot a) = \\ &= M(p_n \cdot b, (q_n - p_n) \cdot a, p'_n \cdot b, (q_n - p'_n) \cdot a; \dots; p_n \cdot b, (q_n - p_n) \cdot a, p'_n \cdot b, (q_n - p'_n) \cdot a) = \\ &= M_{2q_n, \dots, 2q_n}(t_1, \dots, t_1, t_2, \dots, t_2; \dots; t_1, \dots, t_1, t_2, \dots, t_2) = \\ &= M_{2q_n, \dots, 2q_n}(t, \dots, t; \dots; t, \dots, t) = t,\end{aligned}$$

$$t_1 = M_{q_n, \dots, q_n}(p_n \cdot b, (q_n - p_n) \cdot a; \dots; p_n \cdot b, (q_n - p_n) \cdot a) = \psi\left(\frac{p_n}{q_n}\right) = \psi(r_n) \rightarrow A$$

$$t_2 = M_{q_n, \dots, q_n}(p'_n \cdot b, (q_n - p'_n) \cdot a; \dots; p'_n \cdot b, (q_n - p'_n) \cdot a) = \psi\left(\frac{p'_n}{q_n}\right) = \psi(r'_n) \rightarrow B$$

$$t = M(t_1, t_2; \dots; t_1, t_2) \rightarrow M(A, B; \dots; A, B) > M(A, A; \dots; A, A) = A$$

Таким образом, $\lim_{n \rightarrow +\infty} \psi\left(\frac{r_n + r'_n}{2}\right) > A$. С другой стороны, $\frac{r_n + r'_n}{2} < r_*$ и поэтому

$$\lim_{n \rightarrow +\infty} \psi\left(\frac{r_n + r'_n}{2}\right) = A.$$

Противоречие, следовательно функцию $\psi(r)$ можно доопределить до непрерывной возрастающей функции на отрезке $[0, 1]$.

Лемма 3 доказана. $\square$

Таким образом, используя результат леммы 3, можно однозначно определить обратную к ψ функцию ϕ , и при этом ϕ будет возрастающей непрерывной функцией.

ЛЕММА 4. Пусть

$$t = M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}).$$

Тогда

$$\begin{aligned} & M(x_1, x_2, \dots, x_{n_1}, t; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) = \\ & = M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}, t; \dots; z_1, z_2, \dots, z_{n_m}) = \dots \\ & = M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}, t) = t \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Действительно, докажем для первой группы (по свойству IV’):

$$\begin{aligned} & M(x_1, x_2, \dots, x_{n_1}, t; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) = \\ & M_{n_1+1, n_2, \dots, n_m}(t, t, \dots, t, t; t, t, \dots, t; \dots; t, t, \dots, t) = t \end{aligned}$$

Для остальных групп доказательство аналогично. Лемма 4 доказана. $\square$

4. Доказательство теоремы 1 при равном количестве переменных в группах

Пусть $n_1 = n_2 = \dots = n_m = n$, в этом случае можно сгруппировать переменные с одинаковыми номерами и, воспользовавшись свойствами II’ и IV’, получить

$$\begin{aligned} & M(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n; \dots; z_1, z_2, \dots, z_n) = \\ & = M(t_1, t_2, \dots, t_n; t_1, t_2, \dots, t_n; \dots; t_1, t_2, \dots, t_n), \end{aligned}$$

где $t_i = M(x_i; y_i; \dots; z_i)$.

Теперь рассмотрим такие $t_i = \psi(r_i)$, где $r_i \in \mathbb{Q}$. Представим r_i как дроби с одинаковым знаменателем: $r_i = \frac{p_i}{q}$, тогда

$$t_i = \psi(r_i) = M(p_i \cdot b, (q - p_i) \cdot a; p_i \cdot b, (q - p_i) \cdot a; \dots; p_i \cdot b, (q - p_i) \cdot a)$$

и

$$\begin{aligned} & M(t_1, t_2, \dots, t_n; t_1, t_2, \dots, t_n; \dots; t_1, t_2, \dots, t_n) = \\ & = M(q \cdot \psi(r_1), q \cdot \psi(r_2), \dots, q \cdot \psi(r_n); \dots; q \cdot \psi(r_1), q \cdot \psi(r_2), \dots, q \cdot \psi(r_n)) = \\ & = M((p_1 + \dots + p_n) \cdot b, (nq - (p_1 + \dots + p_n)) \cdot a; \dots; (p_1 + \dots + p_n) \cdot b, (nq - (p_1 + \dots + p_n)) \cdot a) = \\ & = \psi\left(\frac{p_1 + \dots + p_n}{nq}\right) = \psi\left(\frac{r_1 + \dots + r_n}{n}\right) = \psi\left(\frac{\phi(t_1) + \dots + \phi(t_n)}{n}\right) = \\ & = \psi\left(\frac{\phi(M(x_1; y_1; \dots; z_1)) + \dots + \phi(M(x_n; y_n; \dots; z_n))}{n}\right) \end{aligned}$$

Уточним последнюю формулу:

$$M(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n; \dots; z_1, z_2, \dots, z_n) =$$

$$\begin{aligned}
&= M(x_1, x_2, \dots, x_n; y_2, y_1, \dots, y_n; \dots; z_1, z_2, \dots, z_n) \Leftrightarrow \\
&\Leftrightarrow \psi \left(\frac{\phi(M(x_1; y_1; \dots; z_1)) + \phi(M(x_2; y_2; \dots; z_2)) + \dots + \phi(M(x_n; y_n; \dots; z_n))}{n} \right) = \\
&= \psi \left(\frac{\phi(M(x_1; y_2; \dots; z_1)) + \phi(M(x_2; y_1; \dots; z_2)) + \dots + \phi(M(x_n; y_n; \dots; z_n))}{n} \right) \Leftrightarrow \\
&\Leftrightarrow \phi(M(x_1; y_1; \dots; z_1)) + \phi(M(x_2; y_2; \dots; z_2)) = \phi(M(x_1; y_2; \dots; z_1)) + \phi(M(x_2; y_1; \dots; z_2)) \Leftrightarrow \\
&\Leftrightarrow \phi(M(x_1; y_1; \dots; z_1)) - \phi(M(x_2; y_1; \dots; z_2)) = \phi(M(x_1; y_2; \dots; z_1)) - \phi(M(x_2; y_2; \dots; z_2))
\end{aligned}$$

Таким образом, функция $\phi(M(x_1; y; \dots; z)) - \phi(M(x_2; y; \dots; z))$ не зависит от y . Аналогично можно показать, что эта функция зависит только от x_1 и x_2 . То есть

$$\phi(M(x; y; \dots; z)) - \phi(M(a; y; \dots; z)) = f_1(x)$$

Точно такими же рассуждениями можно получить

$$\phi(M(a; y; \dots; z)) - \phi(M(a; a; \dots; z)) = f_2(y)$$

.....

$$\phi(M(a; a; \dots; z)) - \phi(M(a; a; \dots; a)) = f_m(z)$$

Если сложить все полученные равенства, то мы придем к

$$\phi(M(x; y; \dots; z)) = f_1(x) + f_2(y) + \dots + f_m(z)$$

А значит формула для среднего представляется в виде

$$\begin{aligned}
&M(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n; \dots; z_1, z_2, \dots, z_n) = \\
&= \psi \left(\frac{f_1(x_1) + \dots + f_1(x_n) + f_2(y_1) + \dots + f_2(y_n) + \dots + f_m(z_1) + \dots + f_m(z_n)}{n} \right),
\end{aligned}$$

$$\begin{aligned}
&\text{причем } \phi(M(x; x; \dots; x)) = f_1(x) + f_2(x) + \dots + f_m(x) \Leftrightarrow x = \psi(f_1(x) + f_2(x) + \dots + f_m(x)) \Leftrightarrow \\
&\Leftrightarrow \psi = (f_1 + \dots + f_m)^{-1}
\end{aligned}$$

Следовательно

$$\begin{aligned}
&M(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n; \dots; z_1, z_2, \dots, z_n) = \\
&= (f_1 + \dots + f_m)^{-1} \left(\frac{f_1(x_1) + \dots + f_1(x_n) + \dots + f_m(z_1) + \dots + f_m(z_n)}{n} \right) = \\
&= (nf_1 + \dots + nf_m)^{-1} (f_1(x_1) + \dots + f_1(x_n) + \dots + f_m(z_1) + \dots + f_m(z_n))
\end{aligned}$$

По лемме 3 значения $\psi(r)$ при $r \in \mathbb{Q}$ образуют плотное множество, а значит доказанная формула верна по непрерывности при всех значениях переменных.

5. Доказательство теоремы 1 при произвольном количестве переменных в группах

С помощью леммы 4 мы можем сравнивать количества переменных в группах. Допустим, что n_m - наибольшая, тогда:

$$M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) = t =$$

$$M_{n_m, n_m, \dots, n_m}(x_1, x_2, \dots, x_{n_1}, t, \dots, t; y_1, y_2, \dots, y_{n_2}, t, \dots, t; \dots; z_1, z_2, \dots, z_{n_m}) =$$

К последнему выражению мы уже можем применить предыдущий результат:

$$= (n_m(f_1 + \dots + f_m))^{-1}(f_1(x_1) + \dots + f_1(x_{n_1}) + (n_m - n_1)f_1(t) +$$

$$+ f_2(y_1) + \dots + f_2(y_{n_2}) + (n_m - n_2)f_2(t) + \dots + f_m(z_1) + \dots + f_m(z_{n_m}))$$

Выразив из последней цепочки равенств t , получим

$$n_m f_1(t) + n_m f_2(t) + \dots + n_m f_m(t) = f_1(x_1) + \dots + f_1(x_{n_1}) + (n_m - n_1)f_1(t) +$$

$$+ f_2(y_1) + \dots + f_2(y_{n_2}) + (n_m - n_2)f_2(t) + \dots + f_m(z_1) + \dots + f_m(z_{n_m}) \Leftrightarrow$$

$$\Leftrightarrow n_1 f_1(t) + n_2 f_2(t) + \dots + n_m f_m(t) =$$

$$= f_1(x_1) + \dots + f_1(x_{n_1}) + f_2(y_1) + \dots + f_2(y_{n_2}) + \dots + f_m(z_1) + \dots + f_m(z_{n_m}) \Leftrightarrow$$

$$\Leftrightarrow M(x_1, x_2, \dots, x_{n_1}; y_1, y_2, \dots, y_{n_2}; \dots; z_1, z_2, \dots, z_{n_m}) = t =$$

$$= (n_1 f_1 + n_2 f_2 + \dots + n_m f_m)^{-1}(f_1(x_1) + \dots + f_1(x_{n_1}) + \dots + f_m(z_1) + \dots + f_m(z_{n_m}))$$

6. Заключение

Доказанная теорема обобщает результат А. Н. Колмогорова на более широкий класс средних. В дальнейшем предполагается распространить понятие неравноправия переменных с использованием группы подстановок.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Колмогоров, А. Н. Избранные труды. Математика и механика / А. Н. Колмогоров. - Москва: Наука, 1985. - 470 с.
2. Чубариков, В. Н. Замечание к определению среднего / В. Н. Чубариков // Вестник Московского университета. сер. 1. Математика и механика - 2003 - №1. С. 30-33.

REFERENCES

1. Kolmogorov, A. N., 1985, Izbrannie trudy. Matematika i mehanika [Selected Works. Mathematics and Mechanics], Nauka, Moscow, pp. 136-138.
2. Chubarikov, V. N., 2003, "A remark on definition of mean value Vestnik Moscovskogo Univ. Seriya 1: Matematika. Mehanika, no. 1, pp. 30-33.

Получено 21.09.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 21. Выпуск 1.

УДК 512.772.1

DOI 10.22405/2226-8383-2020-21-1-381-387

Минимальные морсификации функций
двух вещественных переменных¹

И. А. Проскурнин

Проскурнин Иван Андреевич — аспирант кафедры высшей геометрии и топологии, Московский государственный университет имени М. В. Ломоносова (г. Москва).
e-mail: dazai131@yahoo.com

Аннотация

В статье даётся явный метод построения морсификаций с минимально топологически возможным числом вещественных критических точек для функций двух переменных с гладкими ветвями множества уровня, а также для полуквазиоднородных функций двух переменных.

Ключевые слова: особенности кривых, деформации особенностей, вещественные кривые, полуквазиоднородные функции.

Библиография: 7 названий.

Для цитирования:

И. А. Проскурнин. Минимальные морсификации функций двух вещественных переменных // Чебышевский сборник, 2020, т. 21, вып. 1, с. 381–387.

CHEBYSHEVSKII SBORNIK
Vol. 21. No. 1.

UDC 512.772.1

DOI 10.22405/2226-8383-2020-21-1-381-387

Minimal morsifications for functions of two real variables

I. A. Proskurnin

Proskurnin Ivan Andreevich — Ph.D. student of the department of Higher Geometry and Topology, M. V. Lomonosov Moscow State University (Moscow).
e-mail: dazai131@yahoo.com

Abstract

In this paper we give an explicit construction of morsifications with the smallest topologically possible number of real critical points for functions of two variables with smooth level-set branches, as well as for semiquasihomogenous functions of two real variables.

Keywords: curve singularities, deformations of singularities, real curves, semiquasihomogenous functions.

Bibliography: 7 titles.

For citation:

I. A. Proskurnin, 2020, "Minimal morsifications for functions of two real variables", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 381–387.

¹Работа выполнена за счет гранта РФФИ-20-01-00579 и гранта Международного Центра фундаментальной и прикладной математики.

1. Введение

Известно (см., например, работу В. И. Арнольда [1]), что если $f : (\mathbb{R}^2, 0) \rightarrow (\mathbb{R}, 0)$ — росток аналитической функции с изолированной критической точкой в начале координат, то индекс критической точки равен $1 - r$, где r — число неприводимых компонент ростка вещественного аналитического множества $\{f = 0\}$. В частности, это означает, что если росток $\tilde{f}$ — морсификация f , т. е. деформация, имеющая только невырожденные критические точки, то $\tilde{f}$ имеет не менее $|r - 1|$ вещественных критических точек в окрестности нуля.

ОПРЕДЕЛЕНИЕ 1. *Морсификация называется минимальной, если у неё ровно $|r - 1|$ вещественных критических точек.*

В работах [2], [3] С. М. Гусейн-Заде было доказано существование минимальных морсификаций в случае $r = 1$. В работе [4] был дан явный метод построения минимальных морсификаций в частном случае $r = 1$ для некоторых конкретных характеристических экспонент. Мы построим явные минимальные морсификации для функций f таких, что все неприводимые компоненты кривой $\{f = 0\}$ — гладкие, а также для полуквазиоднородных f .

2. Предварительные замечания

Неприводимые компоненты ростка аналитической кривой называются ветвями. Известно (см. [5], [6]), что множество уровня ростка аналитической функции состоит из не более чем конечного числа ветвей, любая ветвь может быть параметризована аналитическими функциями, и любая ветвь может быть задана как множество нулей некоторого ростка аналитической функции, определенного однозначно с точностью до умножения на обратимые ростки. Ветвь кривой $\{f = 0\}$ называется кратной, если она совпадает с множеством нулей ростка h , который входит в разложение f на множители с кратностью более 1.

Деформация функции может рассматриваться как деформация ее градиентного отображения, при которой отображение остается градиентным. Докажем вспомогательную лемму о деформациях ростков отображений плоскости в себя.

ЛЕММА 1. *Пусть $F : (\mathbb{R}^2, 0) \rightarrow (\mathbb{R}^2, 0)$ — росток отображения плоскости с изолированным нулём в начале координат, (f, g) — его компоненты. Рассмотрим деформацию $F_\lambda = (f + \lambda, g)$. Ее нули лежат на кривой $\{g = 0\}$. Тогда при достаточно малых λ те из нулей, которые лежат на некратных ветвях этой кривой — невырожденные.*

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi : (\mathbb{R}, 0) \rightarrow (\mathbb{R}^2, 0)$ — параметризация какой-нибудь некратной ветви множества $\{g = 0\}$. Функция одной переменной $f(\varphi(t))$ не может иметь критических точек в достаточно малой проколотовой окрестности нуля, т.к. иначе f было бы постоянно (и равно нулю) на некоторой ветви $\{g = 0\}$, а тогда отображение F имело бы неизолированный нуль. Пусть (v_1, v_2) — касательный вектор к $\{g = 0\}$. Условие отсутствия у $f(\varphi(t))$ критических точек означает, что в некоторой проколотовой окрестности нуля в $\mathbb{R}^2$ на множестве $\{g = 0\}$ величина $\frac{\partial f}{\partial x}v_1 + \frac{\partial f}{\partial y}v_2$ не равна нулю. Вектор (v_1, v_2) удовлетворяет равенству $\frac{\partial g}{\partial x}v_1 + \frac{\partial g}{\partial y}v_2 = 0$, причем вектор $(\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y})$ (в силу некратности выбранной нами ветви) не зануляется в некоторой проколотовой окрестности нуля. Значит, векторы $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ и $(\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y})$ в некоторой проколотовой окрестности нуля на выбранной ветви линейно независимы. Матрица, составленная из компонент этих векторов — якобиан отображения F (равный якобиану F_λ), поэтому все нули F_λ на некратной кривой невырожденные. $\square$

В частности, если $\{g = 0\}$ — приведенная кривая (или, что то же самое, функция g имеет в нуле конечное число Милнора), то деформация F_λ будет иметь только невырожденные нули.

Если F — градиентное отображение какой-нибудь функции h , то рассмотренной выше деформации F_λ соответствует, конечно, деформация $h - \lambda x$. Практически всегда мы будем пользоваться деформациями именно такого вида.

3. Функции с гладкими ветвями множества уровня.

Пусть $f : (\mathbb{R}^2, 0) \rightarrow (\mathbb{R}, 0)$ — аналитическая функция, имеющая в нуле изолированную критическую точку, и $\{f = 0\}$ состоит из объединения r гладких кривых. Без ограничения общности

неприводимые компоненты $\{f = 0\}$ можно считать графиками возрастающих аналитических функций: i -тая кривая есть $\{y - g_i(x) = 0\}$, $\frac{dg_i}{dx}(0) > 0$, $g_i(0) = 0$. Тогда f разлагается в произведение $f = u(\prod_{i=1}^r (y - g_i(x)))$, где u — функция, не принимающая в $\mathbb{R}^2$ нулевого значения нигде, кроме, возможно, начала координат (в некоторой окрестности нуля). Также можно считать, что $u(0) \neq 0$ — иначе можно рассмотреть деформацию $f_\lambda = (u + \lambda)(\prod_{i=1}^r (y - g_i(x)))$. Как показано в [2], при таком шевелении не рождается новых вещественных критических точек (при правильном выборе знака λ). Мы будем рассматривать только случай $r > 2$. Если множество уровня функции состоит из двух гладких кривых, то квадратичная часть ряда Тейлора этой функции ненулевая. К такой функции можно применить лемму Морса с параметрами и привести её к виду $\pm x^2 \pm y^k$. В этом случае минимальная морсификация строится очевидным образом. В случае одной гладкой ветви критическая точка просто отсутствует.

Выясним, как устроены множества $\{f_x = 0\}$ и $\{f_y = 0\}$.

ЛЕММА 2. $\{f_x = 0\}$ — приведенная кривая, являющаяся объединением $r-1$ вещественных гладких ветвей.

ДОКАЗАТЕЛЬСТВО. Члены наименьшей степени в разложении f в ряд Тейлора образуют однородный полином f^{hom} степени r . f^{hom} содержит все мономы от двух переменных степени r с ненулевыми коэффициентами: мы условились, что $\{f = 0\}$ состоит из графиков $g_i(x)$, $\frac{dg_i}{dx}(0) > 0$, а коэффициенты мономов f^{hom} суть (с точностью до знака) симметрические функции от $\frac{dg_i}{dx}(0)$. Поэтому члены наименьшей степени у f_x образуют однородный полином степени $r-1$, что означает, в частности, что у множества $\{f_x = 0\}$ не может быть более $r-1$ ветвей. Однако, ветвей также не может быть менее $r-1$, поскольку вещественный индекс векторного поля (f_x, f_y) в нуле равен $1-r$. Значит, их ровно $r-1$. Эти ветви должны быть гладкими, поскольку их $r-1$, что совпадает со степенью начальных членов ряда Тейлора функции f_x , т.е. уравнение каждой из ветвей обязано иметь ненулевую линейную часть. $\square$

Очевидно, $\{f_y = 0\}$ устроено аналогичным образом. Теперь выясним взаимное расположение множеств $\{f_x = 0\}$ и $\{f_y = 0\}$ в плоскости $\mathbb{R}^2$. Пусть $\gamma \in \mathbb{R}^2$ — какая-нибудь ветвь ростка аналитической кривой в окрестности начала координат. Начало координат делит γ на две компоненты связности, называемые полуветвями.

ОПРЕДЕЛЕНИЕ 2. Будем говорить, что у двух ростков кривых g_1 и g_2 правильное чередование, если множества $\{g_1 = 0\} \cap \mathbb{R}^2$ и $\{g_2 = 0\} \cap \mathbb{R}^2$ имеют одинаковое число неприводимых компонент, и каждая компонента связности дополнения к $\{g_2 = 0\} \cap \mathbb{R}^2$ содержит ровно одну полуветвь множества $\{g_1 = 0\} \cap \mathbb{R}^2$.

Например, $y^3 - 5x^4y$ и $3xy^2 - x^5$ имеют правильное чередование.

ЛЕММА 3. Если $\{f = 0\}$ состоит из гладких вещественных ветвей, то в подходящей системе координат f_x и f_y имеют правильное чередование.

ДОКАЗАТЕЛЬСТВО. Зафиксируем окружность малого радиуса с центром в начале координат. При прохождении по этой окружности вектор (f_x, f_y) обязан повернуться $r-1$ раз. Рассмотрим дугу этой окружности, начинающуюся на одной из компонент множества $\{f_x = 0\}$, проходящую через соседнюю компоненту того же множества и кончающуюся на следующей. При проходе по такой дуге вектор (f_x, f_y) не может сделать более одного оборота, т.к. на этой дуге знак f_x ровно один раз меняется и возвращается к изначальному. Но вся окружность состоит из $r-1$ таких дуг. Значит, при прохождении каждой такой дуги вектор (f_x, f_y) должен сделать ровно один оборот. Из этого следует, что каждая дуга пересекает ровно две ветви множества $\{f_y = 0\}$. Это означает, что либо между каждыми двумя соседними ветвями $\{f_x = 0\}$ лежит ровно одна кривая $\{f_y = 0\}$ (как нам и надо), либо одно из множеств $\{f_x > 0\} \cap \{f_y = 0\}$, $\{f_x < 0\} \cap \{f_y = 0\}$ пусто. Если выполняется вторая возможность, то (считая без ограничения общности, что пусто $\{f_x > 0\} \cap \{f_y = 0\}$) деформация $f_\lambda = f - \lambda x$, $\lambda > 0$ не будет иметь вещественных критических точек, чего не может быть. $\square$

В частности, рассмотренные выше ростки $y^3 - 5x^4y$ и $3xy^2 - x^5$ являются частными производными ростка $xy^3 - yx^5$.

Воспользовавшись этими двумя леммами, можно следующее утверждение.

ТЕОРЕМА 1. Деформация $f_\lambda = f + \lambda x$, $\lambda > 0$ будет иметь $r-1$ невырожденных критических точек в $\mathbb{R}^2$.

ДОКАЗАТЕЛЬСТВО. Невырожденность критических точек следует из леммы 1, поэтому достаточно посчитать их количество. Кривая $\{f_x = 0\} \cap \mathbb{R}^2$ делит малую окружность с центром в нуле на $2r - 2$ сектора. Критические точки рассматриваемой деформации f_λ могут лежать только в половине этих секторов, где $f_x < 0$. Тогда критические точки могут лежать только на $r - 1$ (из всего $2r - 2$) полуветвей множества $\{f_y = 0\}$. У множества $\{f_x = -\lambda\}$ $r - 1$ компонента связности, причем в силу леммы 3, каждая полуветвь множества $\{f_y = 0\}$ может пересекаться только с одной из компонент $\{f_x = -\lambda\}$. Осталось доказать, что пересечение данной полуветви с данной компонентой единственно. Как показано в лемме 1, гессиан функции f не зануляется на множестве $\{f_y = 0\}$ (в заранее выбранной достаточно малой окрестности нуля). Пересечения $\{f_y = 0\}$ и $\{f_x = -\lambda\}$ — трансверсальные пересечения гладких кривых. Это означает, что если пересечений несколько, то при движении по $\{f_y = 0\}$ от одной точки пересечения до другой гессиан обязан менять знак, поскольку соседние точки пересечения обязаны иметь разную ориентацию, что приводит нас к противоречию.

□

4. Квазиоднородные функции.

ОПРЕДЕЛЕНИЕ 3. Функция f называется квазиоднородной с весами $\alpha, \beta \in \mathbb{N}$ и квазистепеню $d \in \mathbb{N}$, если для любого $\lambda \in \mathbb{C}$ $f(\lambda^\alpha x, \lambda^\beta y) = \lambda^d f(x, y)$.

ОПРЕДЕЛЕНИЕ 4. Квазиоднородная функция невырождена, если её число Милнора в начале координат конечно (или, что то же самое, росток её множества нулей в начале координат не имеет кратных ветвей).

Мы будем рассматривать только квазиоднородные полиномы с вещественными коэффициентами. Заметим, что, на самом деле, функция не должна быть квазиоднородной, а достаточно только, чтобы вещественные ветви её множества уровня задавались некоторой квазиоднородной функцией: пусть вещественные нули задаются некоторой квазиоднородной функцией, а комплексные произвольны. Тогда функция имеет с точностью до знака вид gu , где g — квазиоднородная функция, а u строго положительно вне начала координат. Как известно, при деформации $f_\lambda = g(u + \lambda)$, $\lambda > 0$ не появляется новых особых точек, а комплексные ветви ростка кривой исчезают. При этом в локальных координатах $(\tilde{x}, \tilde{y}) = (x(u + \lambda)^{\frac{\alpha}{d}}, y(u + \lambda)^{\frac{\beta}{d}})$ имеем

$$g(\tilde{x}, \tilde{y}) = g(x(u + \lambda)^{\frac{\alpha}{d}}, y(u + \lambda)^{\frac{\beta}{d}}) = (u + \lambda)g(x, y) = f_\lambda.$$

Поэтому любой росток, вещественные нули которого могут быть заданы квазиоднородным уравнением, с точки зрения нашей задачи считается просто квазиоднородным.

ЛЕММА 4. Пусть число ветвей множества $\{f = 0\}$ равно $r > 1$. Тогда росток алгебраического многообразия $\{f_x = 0\}$ (множества нулей частной производной) имеет самое большее r ветвей.

ДОКАЗАТЕЛЬСТВО. Известно, что число неприводимых компонент одинаково у всех невырожденных квазиоднородных функций данной квазистепени (см., например, [1], [7]), а у вырожденных оно может быть только меньше. Но xf_x — функция той же квазистепени, что и f , имеющая не меньше ветвей, чем $\{f_x = 0\}$. □

Аналогично, множество $\{f_y = 0\}$ имеет не более r ветвей.

ЛЕММА 5. Пусть хотя бы одна из частных производных f_x, f_y является невырожденной функцией. Тогда существует минимальная деформация f .

ДОКАЗАТЕЛЬСТВО. Предположим, что частная производная f_y невырожденная. Хотя бы в одном из множеств $\{f_x > 0\}$ и $\{f_x < 0\}$ лежит не более чем r полуветвей множества $\{f_y = 0\}$. Пусть это будет $\{f_x > 0\}$. Рассмотрим деформацию $f_\lambda = f - \lambda x$, $\lambda > 0$. По первой лемме, эта деформация является морсификацией. Ее критические точки лежат на полуветвях $\{f_y = 0\}$, находящихся в множестве $\{f_x > 0\}$, которых у нас не более r штук. Заметим, что на каждой полуветви не более одной критической точки: поскольку функция f_y квазиоднородна, полуветви $\{f_y = 0\}$ являются орбитами группы гиперболических поворотов $\sigma(x, y) = (e^{\alpha\sigma}x, e^{\beta\sigma}y)$. Поэтому если бы на какой-нибудь полуветви было две критические точки, то их можно было бы перевести друг в друга гиперболическим поворотом. Но этот поворот изменил бы значение функции f_x , которая квазиоднородна с теми же весами. Таким

образом, все критические точки невырожденные и их не более r и не менее $r - 1$. Их суммарный индекс равен $r - 1$. Для невырожденных критических точек суммарный индекс по четности обязан совпадать с количеством критических точек (поскольку индекс есть разность числа минимумов и максимумов и числа седел, а количество — сумма), т.е. их $r - 1$. $\square$

5. Плохие квазистепени.

Осталось рассмотреть многочлены, у которых обе частные производные вырождены. Заметим, что множество квазиоднородных полиномов, имеющих хотя одну невырожденную частную производную, всегда открыто по Зарисскому в пространстве функций данной квазистепени. Поэтому если есть хотя бы один полином данной квазистепени, у которого хотя одна производная невырождена, то всегда можно перейти к невырожденной производной малым шевелением. Это шевеление не будет менять ни числа Милнора, ни числа ветвей, поскольку, как известно, у квазиоднородных полиномов при малом шевелении эти инварианты не меняются. Таким образом, нужно рассмотреть только случай “плохих квазистепеней”, при которых ни одного полинома с невырожденными производными не бывает. Примером может служить семейство многочленов $ax^8 + bx^4y^3 + cy^6$ — все они имеют вырожденные производные.

ЛЕММА 6. *Невырожденный квазиоднородный многочлен плохой квазистепени всегда имеет вид $ax^k + x^3y^3g(x, y) + by^l$, $ab \neq 0, k, l \geq 3$.*

ДОКАЗАТЕЛЬСТВО. Вырожденность производных у всех квазиоднородных многочленов данной квазистепени d равносильна тому, что пространства квазиоднородных многочленов степеней $d - \alpha$ и $d - \beta$ (с теми же весами α, β) состоят исключительно из вырожденных многочленов. Пространство многочленов данной квазистепени от двух переменных содержит только вырожденные полиномы в том и только в том случае, когда все мономы данной квазистепени делятся на x^2 , либо на y^2 — иначе в пространстве есть либо мономы x^a, y^b , либо мономы $x^a y, y^b$, либо мономы $x^a y, x y^b$, из которых всегда можно составить невырожденную квазиоднородную функцию. Если все мономы квазистепени $d - \alpha$ делятся на y^2 , то тогда и все мономы квазистепени d делятся на y^2 , и все полиномы квазистепени d вырождены. Вырожденные полиномы мы не рассматриваем, поэтому можно считать, что все мономы квазистепени $d - \alpha$ делятся на x^2 . Аналогично, все полиномы квазистепени $d - \beta$ делятся на y^2 .

Если все мономы квазистепени $d - \alpha$ делятся на x^2 , то мономы квазистепени d либо не делятся на x совсем, либо делятся на x^3 . Точно таким же образом, мономы квазистепени d либо совсем не делятся на y , либо делятся на y^3 . Это означает, что любой невырожденный квазиоднородный многочлен плохой квазистепени имеет вид $ax^k + x^3y^3g(x, y) + by^l$, где $g(x, y)$ — квазиоднородная функция квазистепени $d - 3\alpha - 3\beta, ab \neq 0, k = \frac{d}{\alpha}, l = \frac{d}{\beta}$. $\square$

Итак, у множества $\{f_y = 0\}$ есть кратная ветвь $\{y = 0\}$. Заметим, что всегда можно добиться того, чтобы $\{y = 0\}$ было единственной кратной ветвью кривой $\{f_y = 0\}$, немного пошевелив f в пространстве квазиоднородных полиномов степени d . Будем считать, что это так и есть, т.е., что на других ветвях множества $\{f_y = 0\}$ градиент функции f_y ненулевой в некоторой проколотой окрестности начала координат.

ТЕОРЕМА 2. *У невырожденных квазиоднородных полиномов плохой квазистепени есть минимальные морсификации.*

ДОКАЗАТЕЛЬСТВО. Построение минимальной морсификации полинома плохой квазистепени совершается в два этапа. На первом этапе мы действуем в точности так же, как в простом случае. Повторю приведенную ранее конструкцию.

Хотя бы в одном из множеств $\{f_x > 0\}$ и $\{f_x < 0\}$ лежит не более чем r полуветвей множества $\{f_y = 0\}$. Пусть это будет $\{f_x > 0\}$. Рассмотрим деформацию $f_\lambda = f - \lambda x, \lambda > 0$. Ее критические точки лежат на полуветвях $\{f_y = 0\}$, находящихся в множестве $\{f_x > 0\}$, которых у нас не более r штук. Заметим, что на каждой полуветви не более одной критической точки: поскольку функция f_y квазиоднородна, полуветви $\{f_y = 0\}$ являются орбитами группы гиперболических поворотов $\sigma(x, y) = (e^{\alpha\sigma}x, e^{\beta\sigma}y)$. Поэтому если бы на какой-нибудь полуветви было бы две критические точки, то их можно было бы перевести друг в друга гиперболическим поворотом. Но этот поворот изменил бы значение функции f_x , которая также квазиоднородна с теми же весами. Таким образом, у этой деформации не более r критических точек.

В отличие от простого случая мы не можем утверждать, что все эти критические точки невырожденные. Однако, по лемме 1 невырождены все критические точки, лежащие на некротных ветвях $\{f_y = 0\}$. Но мы условились, что у $\{f_y = 0\}$ только одна кратная ветвь, а именно $\{y = 0\}$. По сказанному выше, на этой ветви лежит не более двух критических точек (по одной на каждой полуветви), и они являются единственными вырожденными критическими точками нашей деформации f_λ .

Второй этап построения морсификации заключается в том, чтобы морсифицировать эти критические точки, лежащие на прямой $\{y = 0\}$. Зафиксируем малое $\lambda = \lambda_0$, и пусть

$$\tilde{f} = f_{\lambda_0} = ax^k + x^3y^3g(x, y) + by^l - \lambda_0x.$$

Вырожденные критические точки имеют координаты $(\pm(\frac{\lambda_0}{ka})^{\frac{1}{k-1}}, 0)$. Вторая производная $\tilde{f}_{xx}$ в этой точке ненулевая, т.е. гессиан $\tilde{f}$ имеет ранг как минимум один. Воспользовавшись леммой Морса с параметрами, можно представить $\tilde{f}$ в окрестности этой точки в виде $\tilde{x}^2 \pm \tilde{y}^m$, причём координаты $\tilde{x}, \tilde{y}$ можно выбрать так, чтобы $\tilde{y}$ отличалась от y только умножением на константу. Но такая особенность всегда имеет морсификацию с максимум одной критической точкой, а именно $\tilde{x}^2 \pm \tilde{y}^m + \varepsilon\tilde{y}$. Более того, такая деформация морсифицирует сразу обе вырожденные критические точки $\tilde{f}$ (если их две), поскольку, как говорилось, $\tilde{y}$ отличается от y разве что умножением на константу, т.е. в окрестностях обоих критических точек $\tilde{y}$ те же самые. Поскольку все остальные критические точки $\tilde{f}$ были невырожденными, малое шевеление рассматриваемой критической точки не изменит их числа и вида. Таким образом, полученная деформация f имеет не более, чем r вещественных критических точек, причем все они невырожденные. Теперь можно повторить использованный ранее аргумент: критических точек не более r , не менее $r - 1$, они невырождены, их суммарный индекс равен $1 - r$. Следовательно, этих точек $r - 1$. $\square$

6. Полуквазиоднородные функции.

ОПРЕДЕЛЕНИЕ 5. Функция f полуквазиоднородна, если она представляется в виде суммы $f_0 + f_1$, где f_0 — невырожденная квазиоднородная, а в f_1 все мономы имеют квазистепень строго выше, чем у f_0 (с теми же, что и у f_0 весами). Полином f_0 при этом называется главной частью функции f .

ТЕОРЕМА 3. У любой полуквазиоднородной вещественной функции есть минимальная морсификация.

ДОКАЗАТЕЛЬСТВО. По доказанному выше, минимальная морсификация может быть построена для любой квазиоднородной функции. Пусть f — полуквазиоднородная функция с главной частью f_0 . Построенная ранее морсификация f_0 имеет вид $f_0^\lambda = f_0 + a(\lambda)x + b(\lambda)y$ (для большинства рассматриваемых случаев, как показано выше, минимальной морсификацией будет $f_0^\lambda = f_0 + \lambda x$. В случаях “плохой квазистепени” необходимо также прибавить моном, линейный по y). Поскольку деформация заключается в прибавлении линейных по x, y членов, гессиан f_0^λ не отличается от гессиана f_0 . Заметим, что условие минимальности морсификации равносильно тому, что во всех критических точках этой морсификации гессиан морсификации принимает отрицательные значения. Координаты критических точек f_0^λ могут быть разложены в ряд Пуизо по степеням λ . При подставлении этих рядов в гессиан f_0 получается степенной ряд (вообще говоря, дробно-степенной), принимающий при малых λ строго отрицательные значения, а, значит, имеющий строго отрицательный член наименьшей степени. Теперь рассмотрим деформацию $f_\lambda = f_0^\lambda + f_1$. f отличается от f_0 только членами строго большего порядка, чем f_0 , а поэтому гессиан f_λ не зависит от λ и имеет те же члены наименьшей квазистепени, что и гессиан f_0 . Аналогично, ряд Пуизо для критических точек f_λ обязан в членах наименьшей степени совпадать с рядом Пуизо для критических точек f_0^λ . Но это означает, что если гессиан f_0 принимает при малых λ строго отрицательные значения в критических точках f_0^λ , то и гессиан f_λ будет при малых λ принимать в критических точках f_λ строго отрицательные значения, т.е. f_λ — минимальная морсификация. $\square$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Арнольд В. И. Индекс особой точки векторного поля, неравенства Петровского–Олейник и смешанные структуры Ходжа // Функц. анализ и его приложения. 1978. Том 12, № 1. стр.1-14.

2. Гусейн-Заде С. М. On a problem of B.Teissier // Topics in Singularity Theory: V. I. Arnold's 60th Anniversary Collection. Am. Math. Soc. Providence, Rhode Island. 1997. P. 117-141.
3. Гусейн-Заде С. М. О существовании деформаций без критических точек (задача Тессье для функций двух переменных) // Функц. анализ и его приложения. 1997. Том 31, № 1. стр. 74-77.
4. Gonzalez-Ramirez J. A., Luengo I. Deformations of functions without real critical points // Communications in Algebra. 2003. Vol. 31, № 9, P.42-55.
5. Casas-Alvero E. Singularities of plane curves. 2000. Cambridge university press.
6. Milnor J. Singular Points of Complex Hypersurfaces. 1968. Princeton university press.
7. Damon J. On the number of branches for real and complex weighted homogeneous curve singularities // Topology. 1991. Vol.30, № 2. P.223-229.

REFERENCES

1. V. I. Arnol'd, V. I. 1978, "Index of a singular point of a vector field, the Petrovskii–Oleinik inequality, and mixed Hodge structures", *Funct. Anal. Appl.*, vol.12, no.1, pp. 1–12.
2. Gusein-Zade, S. M. 1997, "On a problem of B.Teissier", in A. Khovanskii(ed.), A. Varchenko(ed.), V. Vassiliev(ed.), *Topics in Singularity Theory: V. I. Arnold's 60th Anniversary Collection*, Providence, Rhode Island, Am. Math. Soc., 1997, pp. 117-141.
3. Gusein-Zade, S. M. 1997, "On the Existence of Deformations without Critical Points (the Teissier problem for functions of two variables)", *Funct. Anal. Appl.*, vol. 31, no. 1, pp. 58–60.
4. Gonzalez-Ramirez, J. A., Luengo, I. 2003, "Deformations of functions without real critical points", *Communications in Algebra*, vol. 31, no. 9, pp. 42-55.
5. Casas-Alvero, E. *Singularities of plane curves*, New York, Cambridge university press, 2000.
6. Milnor, J. *Singular Points of Complex Hypersurfaces*, Princeton, New Jersey, Princeton university press, 1968.
7. Damon, J. 1991, "On the number of branches for real and complex weighted homogeneous curve singularities" *Topology*, vol. 30, no. 2, pp. 223-229.

Получено 24.09.2019 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 511.9

DOI 10.22405/2226-8383-2020-21-1-388-403

О русской научной школе диофантовых приближений¹

Ю. А. Басалов

Басалов Юрий Александрович — аспирант кафедры алгебры, математического анализа и геометрии, Тульский государственный педагогический университет им. Л. Н. Толстого (г. Тула)
e-mail: basalov_yurij@mail.ru

Аннотация

Теория диофантовых приближений, как раздел математики, начала активно формироваться в XIX веке. Значительный вклад в ее развитие внесли русские и советские математики. В данной работе мы дадим исторический обзор некоторых результатов в области диофантовых приближений, полученных русской и советской научной школой теории чисел.

Одним из первых, задачами теории диофантовых приближений заинтересовался во второй половине XIX века П. Л. Чебышев. Эти исследования были продолжены его учениками А. Н. Коркиным и Е. Н. Золотарёвым. А в 1880 году, ученик А. Н. Коркина, академик А. А. Марков-старший в своей магистерской диссертации блестяще решил задачу описания классов плохоприближаемых неопределенных квадратичных форм. Другой ученик П. Л. Чебышева — Г. Ф. Вороной, наряду с Г. Минковским, заложил основы нового, тесно связанного с диофантовыми приближениями раздела математики — геометрии чисел.

В развитие метрической теории цепных дробей внес значительный вклад А. Я. Хинчин. В 1936 году им была получена *постоянная Хинчина* — значение среднего геометрического элементов разложения в цепную дробь, для почти всех вещественных чисел. Поразительность этого факта отмечается математиками всего мира.

Значительный вклад в развитие метрической теории диофантовых приближений принадлежит белорусским математикам. В 1964 году В. Г. Спринджук получил доказательство гипотезы о мере множества S -чисел. Исследования в этой области были продолжены В. И. Берником.

Интересных результатов в области геометрии чисел и свойств приближения алгебраических чисел были получены во 70–80-ых годах XX века Б. Ф. Скубенко. В частности, в его работах представлена оценка константы наилучших диофантовых приближений для двумерного случая. Исследования в области приближения действительных чисел и теории цепных дробей были продолжены в 1990–2010-ых годах Н. Г. Мощевитиным, О. Н. Германом, А. Д. Брюно, Н. М. Добровольским и Н. Н. Добровольским.

Ключевые слова: история диофантовых приближений, русская школа теории чисел.

Библиография: 45 названия.

Для цитирования:

Ю. А. Басалов. О русской научной школе диофантовых приближений // Чебышевский сборник, 2020, т. 21, вып. 1, с. 388–403.

¹Исследование выполнено при финансовой поддержке РФФИ: (грант 16-41-710194_р_центр_а).

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 511.9

DOI 10.22405/2226-8383-2020-21-1-388-403

About the Russian scientific school of diophantine approximations

Yu. A. Basalov

Basalov Yuriy Aleksandrovich — Postgraduate Student, Tula State Pedagogical University of Leo Tolstoy, Department of Algebra, Mathematical Analysis and Geometry (Tula).

e-mail: basalov_yuriy@mail.ru

Abstract

The theory of diophantine approximations, as a branch of mathematics, began to take shape in the 19th century. A significant contribution to its development was made by Russian and Soviet mathematicians. In this paper, we give a historical review of some results in the field of Diophantine approximations obtained by the Russian scientific school of number theory.

One of the first, P. L. Chebyshev became interested in the problems of the theory of diophantine approximations in the second half of the 19th century. These studies were continued by his students A. N. Korkin and E. N. Zolotarev. In 1880 academician A. A. Markov (the student of A. N. Korkin) in his master thesis brilliantly solved the problem of describing classes of poorly approximating indefinite quadratic forms. Another student of P. L. Chebyshev — G. F. Voronoi, along with G. Minkowski, laid the foundations for a new, closely related to Diophantine approximations section of mathematics — the geometry of numbers.

A. I. Hinchin made a significant contribution to the development of the metric theory of continued fractions. In 1936, he obtained *the Khinchin constant* — the value of the geometric mean of the decomposition into a continued fraction, for almost all real numbers. The awesomeness of this fact is noted by mathematicians around the world.

A significant contribution to the development of the metric theory of diophantine approximations belongs to Belarusian mathematicians. In 1964 V. G. Sprindzhuk obtained a proof of the hypothesis on the measure of the set of S -numbers. Research in this area was continued by V. I. Bernik.

Interesting results in the field of geometry of numbers and the approximation properties of algebraic numbers were obtained in the 70–80s of the XX century by B. F. Skubenko. In particular his work presents an estimate of the constant of the best Diophantine approximations for the two-dimensional case. Research in the field of approximation of real numbers and the theory of continued fractions was continued in the 1990–2010s by N. G. Moshchevitin, O. N. German, A. D. Bruno, N. M. Dobrovol'skii and N. N. Dobrovol'skii.

Keywords: history of diophantine approximations, Russian school of number theory.

Bibliography: 45 titles.

For citation:

Yu. A. Basalov, 2020, "About the Russian scientific school of diophantine approximations", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 388–403.

1. Введение

Теория диофантовых приближений сформировалась как естественное развитие теории цепных дробей, которая активно развивалась в XVII–XIX веках. Исследованию непрерывных дробей посвящали свои работы Л. Эйлер, Ж. Л. Лагранж, Ж. Лиувиль, К. Ф. Гаусс. Ключевой особенностью цепных дробей является то, что они обеспечивают наилучшие приближения действительного числа рациональными дробями, обладая при этом простой и изящной алгебраической и геометрической структурой.

Теория диофантовых приближений интересуется более общими вопросами аппроксимации в целых числах. Многие проблемы теории диофантовых приближений исходят из фундаментального утверждения, полученного П. Г. Дирихле в 1842 году [4]

ТЕОРЕМА 1. Пусть $\alpha_{ij} (1 \leq i \leq n, 1 \leq j \leq m)$ и Q — произвольные действительные числа, причем $Q > 1$. Тогда найдутся целые числа $q_1, q_2, \dots, q_m$ и $p_1, p_2, \dots, p_n$ такие, что $1 \leq \max(|q_1|, |q_2|, \dots, |q_m|) < Q^{\frac{n}{m}}$ и

$$\left| \sum_{j=1}^m \alpha_{ij} \cdot q_j - p_i \right| \leq \frac{1}{Q}, \quad (1 \leq i \leq n).$$

В данной работе мы дадим краткий обзор русской школы теории диофантовых приближений. С более частным вопросом истории оценки константы наилучших совместных диофантовых приближений можно ознакомиться в работе [16].

2. Петербургская школа

Петербургской, а вместе с ней и русской, научной школе в области диофантовых приближений более полутора веков. К первым исследованиям русских ученых в этой области можно отнести работу П. Л. Чебышева 1866 года «Об одном арифметическом вопросе» [63]. В этой работе он получает оценку степени приближения для неоднородной линейной формы. А именно, показывает, что для произвольных чисел a, b существует бесконечное количество пар целых чисел x, y таких, что

$$|x - ay - b| < \frac{2}{y}.$$

Изучение этого вопроса было затем продолжено Ш. Эрмитом [8], а позднее Г. Минковским [11].

В теории бинарных квадратичных форм известно следующее утверждение. Если $\varphi(x, y) = ax^2 + bxy + cy^2$ — бинарная форма с произвольными коэффициентами a, b, c и определителем $\Delta = b^2 - 4ac \neq 0$ (если $\Delta = 0$, то бинарная форма приводится к линейной), то переменным x, y можно дать такие целые, не равные одновременно нулю, значения, что

$$\varphi(x, y) \leq \sqrt{\frac{1}{3}|\Delta|} \quad \text{для определенных квадратичных форм, где } \Delta < 0 \quad (1)$$

и

$$\varphi(x, y) \leq \sqrt{\frac{1}{5}|\Delta|} \quad \text{для неопределенных квадратичных форм, где } \Delta > 0 \quad (2)$$

Указанное утверждение впервые было четко сформулировано учениками П. Л. Чебышева, А. Н. Коркиным и Е. Н. Золотарёвым [9]. При исследовании этого вопроса ими была обнаружена принципиальная разница между случаями $\Delta < 0$ и $\Delta > 0$. При $\Delta > 0$ равенство $\varphi(x, y) = \sqrt{\frac{1}{5}|\Delta|}$ достигается на некотором классе эквивалентных квадратичных форм. Если исключить этот класс из рассмотрения, то можно усилить неравенство (2) как

$$\varphi(x, y) \leq \sqrt{\frac{1}{8}|\Delta|},$$

где равенство также достигается на определенном классе квадратичных форм. Этот процесс можно продолжать далее. В тоже время, для $\Delta < 0$, после исключения из рассмотрения класса эквивалентных форм для которых $\varphi(x, y) = \sqrt{\frac{1}{3}|\Delta|}$, для любого $\lambda < \frac{1}{3}$ можно будет найти формы для которых достигается $\varphi(x, y) < \sqrt{\lambda|\Delta|}$.

Задача дальнейшего продолжения ряда описанных выше констант $\frac{1}{5}, \frac{1}{8}, \dots$ (при $\Delta > 0$) была решена учеником Коркина, академиком А. А. Марковым в 1880 году в магистерской диссертации «О бинарных квадратичных формах положительного определителя» [40]. А. А. Марков доказал, что ряд чисел $\frac{1}{5}, \frac{1}{8}, \frac{25}{221}, \dots$ бесконечный и стремится к пределу $\frac{4}{9}$. По сути, этот ряд и соответствующие каждому члену квадратичные формы описывает классы плохоприближаемых неопределенных квадратичных

форм. Фундаментальность этой работы отмечает Б. Н. Делоне в работе [35]. В этой же работе он дает интересную геометрическую интерпретацию задачи А. А. Маркова и ее обобщения.

Разрешив полностью проблему Коркина для неопределенных бинарных форм, А. А. Марков в работах «О неопределенных тройничных квадратичных формах» (1901 г.) [41], «О неопределенных квадратичных формах с четырьмя переменными» (1902 г.) [42] ставит аналогичную проблему для неопределенных тройничных и четвертичных форм. Позднее исследования в этом направлении продолжил Б. А. Венков в работе [28] от 1945 года.

Значительный вклад в тесно связанный с диофантовыми приближениями разделы геометрии чисел внес другой ученик П. Л. Чебышева — Г. Ф. Вороной. Он подошел к вопросу изучения квадратичных форм с точки зрения геометрии [30]. В своей докторской диссертации «Об одном обобщении алгоритма непрерывных дробей» (1896 г.) [29], удостоенной, премии имени В. Я. Буняковского, он построил и обосновал новые алгоритмы вычисления основных единиц кубического поля алгебраических чисел.

Важным понятием геометрии чисел является

ОПРЕДЕЛЕНИЕ 1. Пусть $\mathbb{F}$ — точечное тело. Если решетка Λ не имеет в $\mathbb{F}$ отличных от $\mathcal{O}$ точек ($\mathcal{O} \in \mathbb{F}$), то Λ допустима для $\mathbb{F}$. Точную нижнюю грань

$$\Delta(\mathbb{F}) = \inf d(\Lambda)$$

определителей $d(\Lambda)$ всех $\mathbb{F}$ -допустимых решеток Λ называют критическим определителем множества $\mathbb{F}$.

Вычисление критического определителя произвольного тела $\mathbb{F}$ является сложной задачей. Вопросам оценки значений некоторых критических определителей посвящены исследования А. В. Малышева. В своих работах он активно использовал метод Л. Дж. Морделла (1973 г.) [39]. В сочетании с использованием ЭВМ это позволило ему достичь значительных результатов в доказательстве гипотезы Минковского о критическом определителе области $|x|^p + |y|^p < 1$ [38, 34].

В работе 1962 года «О представлении целых чисел положительными квадратичными формами» [38] А. В. Малышевым дается исчерпывающее описание задачи целочисленного представления чисел квадратичными формами $f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{i,j} x_i x_j$ с целыми коэффициентами, в частности определение количества таких представлений. Некоторые асимптотические формулы количества представлений целого числа квадратичными формами можно найти в работе 1979 года Е. В. Подсыпанина «Количество целых точек в эллиптической области (замечание к одной теореме А. В. Малышева)» [49].

В работе [47] Е. В. Подсыпанин проводит подробное исследование одного из вариантов обобщения цепных дробей — алгоритма Вигго Бруна — исследует его сходимость, получает выражение знаменателя n -ых подходящих дробей как функции неполных частных $a_1, \dots, a_n, \varepsilon_1, \dots, \varepsilon_n$. В работе [48] Е. В. Подсыпанин получает оценку для длины периода квадратичной иррациональности, сформулированную в следующей теореме

ТЕОРЕМА 2. Пусть

$$D = \begin{cases} f^2 d, & \text{если } d \equiv 1 \pmod{4}, \\ 4f^2 d, & \text{если } d \equiv 2, 3 \pmod{4}, \end{cases}$$

где $d > 1$ — бесквадратное число, $L(1, \chi)$ — L -функция Дирихле, h — число классов вещественного квадратичного поля $\mathbb{Q}(\sqrt{d})$. Тогда длина l периода квадратичной иррациональности дискриминанта D удовлетворяет следующему неравенству

$$l < \frac{C\sqrt{D}L(1, \chi)}{h},$$

где

$$D = \begin{cases} 1/\left(2 \log \frac{1+\sqrt{5}}{2}\right), & \text{если } f = 1, \\ 1/\log \frac{1+\sqrt{5}}{2}, & \text{если } f > 1. \end{cases}$$

Нельзя не отметить вклад в развитие теории диофантовых приближений и цепных дробей в нашей стране А. Я. Хинчина. В 1936 году в работе «Метрические задачи теории иррациональных чисел» [60]

им было доказано существование постоянной Хинчина. Пусть

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

разложение в цепную дробь, a_0 целое, а остальные a_i натуральные, тогда для почти всех вещественных чисел x выполняется, что среднее геометрическое элементов этого разложения равно

$$\lim_{n \rightarrow \infty} (a_1 a_2 \dots a_n)^{1/n} = K_0 = 2,6854520010 \dots$$

При этом постоянную Хинчина K_0 можно выразить в виде бесконечного произведения

$$K_0 = \prod_{r=1}^{\infty} \left(1 + \frac{1}{r(r+2)} \right)^{\log_2 r}.$$

Значимость этого результата сложно переоценить. Если каким-либо образом случайно выбирать элементы последовательности натуральных чисел, то среднее геометрическое элементов, вообще говоря, совершенно не обязательно будет одним и тем же для всех или почти всех получаемых последовательностей. Поэтому существование постоянной Хинчина — то обстоятельство, что среднее геометрическое элементов разложения в цепную дробь оказывается одним и тем же для почти всех вещественных чисел — это один из самых поразительных фактов в математике (по мнению профессора MIT С. Финча в книге [6]).

Также, нельзя не отметить монографию А. Я. Хинчина «Цепные дроби» [62], где дается исчерпывающее описание теории непрерывных дробей. В частности, в этой работе подробно показывается связь цепных дробей и диофантовых приближений одного действительного числа. В работе «Принцип Дирихле в теории диофантовых приближений» [61] излагается ряд методических вопросов, связанных с применением принципа Дирихле.

С течением времени, исследования в области диофантовых приближений и в области цепных дробей стали развиваться в различных направлениях. Далее мы рассмотрим результаты в области диофантовых приближений и геометрии чисел, а затем вернемся к вопросам связанным с исследованием цепных дробей.

Известна следующая гипотеза Минковского: в R^n для любой решетки Λ и любой точки L в множестве $\Lambda + L$ содержится точка $Y = (y_1, \dots, y_n)$, для которой будет выполнено

$$M = \prod_{i=1}^n |y_i| \leq 2^{-n} |\det \Lambda|.$$

Вопросу ее доказательства посвящено множество работ. Первый значительный результат был получен в 1934 году Н. Г. Чеботаревым в работе «Заметки по алгебре и теории чисел» [64]. Он получил оценку

$$M \leq 2^{-n/2} |\det \Lambda|.$$

Исследованиям связанными с гипотезой Минковского посвящены работы Б. Ф. Скубенко. В 1972–1976 годах в работах [50, 51, 52] он излагает доказательства гипотезы Минковского для $n \leq 5$. В частности он вводит и использует понятие «парус» — границу замкнутой выпуклой оболочки множества $(\Lambda \setminus 0)^f$, которое строится как отображение f множества $\Lambda \setminus 0$, полученного из Λ путем отбрасывания точки 0. Отображение f переводит точку $X = (x_1, \dots, x_n)$ в точку $X^f = (x_1^2, \dots, x_n^2)$. Парус состоит из $(n-1)$ -мерных граней, соприкасающихся по $(n-2)$ -мерным граням. Грани являются выпуклыми конечными многогранниками. В работе «К гипотезе Минковского при больших n » [53] он дает оценку

$$M < 2^{n/2} e^2 \left(\frac{\log^2 n}{n} \right)^{1/3},$$

для достаточно больших n .

В работе 1982 года «К совместным приближениям алгебраических иррациональностей» [54] Б. Ф. Скубенко дает ряд интересных результатов для совместных приближений чисел чисто вещественных алгебраических, и в частности кубических полей. Пусть расстояние до ближайшего целого определяется как

$$||q\theta|| = \min_{a \in \mathbb{Z}} |q\theta - a|,$$

а константой наилучших диофантовых приближений называют наименьшее C_n для которого существует $\theta_1, \dots, \theta_n$, что для бесконечного количества q выполняется

$$\max_{i=1, n} ||q\theta_i|| \leq C_n q^{-1/n}.$$

В этой работе Б. Ф. Скубенко во-первых повторяет полученную в 1955 году Дж. В. С. Касселсом [3] оценку для константы наилучших диофантовых приближений для чисел из чисто вещественного кубического поля

$$\max(||q\theta_1||, ||q\theta_2||) \leq \frac{2}{7} q^{-1/2},$$

где θ_1, θ_2 принадлежит полю $\mathbb{Q}(2 \cos \frac{2\pi}{7})$. Во-вторых, Б. Ф. Скубенко дает оценку

$$||q\theta_i|| \cdot ||q\theta_j|| < \alpha_{ij} (q \log q)^{-1}$$

для произвольного целого q , θ_i, θ_j из чисто вещественного кубического поля, и числа α_{ij} , зависящего только от θ_i, θ_j .

Известна следующая обобщенная теорема Рота–Шмидта [14].

ТЕОРЕМА 3. Пусть $\theta_1, \dots, \theta_n$ вещественные алгебраические числа, такие что $1, \theta_1, \dots, \theta_n$ линейно независимы над полем рациональных чисел. Тогда для любого $\varepsilon > 0$ существует только конечное количество натуральных чисел q таких, что

$$||q\theta_1|| \cdot \dots \cdot ||q\theta_n|| < q^{-1-\varepsilon}.$$

В работе «К обобщенной теореме Рота–Шмидта» [55] Б. Ф. Скубенко дает следующее дополнение описанной выше теоремы.

ТЕОРЕМА 4. Пусть $\theta_1, \dots, \theta_n$ вещественные алгебраические числа из чисто вещественного алгебраического поля степени n . Тогда существует $C > 0$, что

$$||q\theta_1|| \cdot \dots \cdot ||q\theta_n|| \leq C (q \log q)^{-1}.$$

для бесконечного числа натуральных чисел q .

3. Белорусская школа

Значительных результатов в теории диофантовых приближений достигли белорусские ученые. В. Г. Спринджук в 1964 году [56] было получено доказательство гипотезы Малера о мере множества S -чисел. Суть этого утверждения в следующем. Пусть ω – трансцендентное число. Для данного натурального n определим $w_n(\omega)$ – точную верхнюю грань тех чисел w , для которых существует бесконечное количество целочисленных полиномов P степени не более n , удовлетворяющих неравенству

$$|P(\omega)| < h^{-w}, \quad (h \rightarrow \infty)$$

где h – высота полинома P . Положим

$$\frac{1}{n} w_n(\omega) = \begin{cases} \theta_n(\omega), & \text{если } \omega \text{ вещественно,} \\ \nu_n(\omega), & \text{если } \omega \text{ комплексно.} \end{cases}$$

Известно, что

$$\theta_n(\omega) \geq 1, \quad \nu_n(\omega) \geq \frac{1}{2} - \frac{1}{2n}, \quad n \geq 1.$$

Гипотеза Малера утверждает, что для почти всех (в смысле меры Лебега) вещественных и комплексных чисел

$$\sup_n \theta_n(\omega) = 1, \quad \sup_n \nu_n(\omega) = \frac{1}{2}.$$

В работах [57, 58] В. Г. Спринджук проводит исследование значений в алгебраических точках для расширения класса E функций Зигеля. В. Г. Спринджук вводит класс E^* функций

$$\varphi(z) = \sum_{v=0}^{\infty} c_v \cdot \frac{z^v}{v!}$$

обладающих следующими свойствами

- число c_v – алгебраические и принадлежат полю конечной степени над полем рациональных чисел $\mathbb{Q}$;
- существует число $\alpha, 0 < \alpha < 1$, для которого $|c_v| < c(\varepsilon)(v!)^{\alpha+\varepsilon}$;
- для фиксированного n пусть q_{nm} – наименьшее натуральное число q , для которого все числа $q c_{v_1} c_{v_2} \dots c_{v_n}$, $v_1 + v_2 + \dots + v_n \leq m$ – целые; существует последовательность чисел $\beta_n, 0 \leq \beta_n = o(\sqrt{n})$ при $n \rightarrow \infty$ для которых $q_{nm} < c(n, \varepsilon)(m!)^{\beta_n + \varepsilon}$ при любом $\varepsilon > 0$.

Исследования в области метрической теории диофантовых приближений были продолжены В. И. Берником [17]. В работе «Метрическая теорема о совместном приближении нуля значениями целочисленных многочленов» в 1980 году им было доказано предложенное В. Г. Спринджук обобщение гипотезы Малера.

ТЕОРЕМА 5. Пусть $w_n(\bar{\omega})$ – точная верхняя грань тех $w > 0$, для которых неравенство

$$\prod_{i=1}^k |P(\omega_i)| < h^{-w}$$

имеет бесконечное число решений в полиномах $P(x)$. Тогда для почти, всех со $\bar{\omega}$

$$w_n(\bar{\omega}) = n - k + 1.$$

Продолжением этих исследований стало доказательство в 1984 году гипотезы А. Бэйкера [18] и доказательство В. И. Берником [19] и В. И. Бересневичем [2] аналога метрической теоремы Хинчина для многочленов произвольной степени. Дальнейшие исследования в этой области были направлены на переход от степенной функции в правой части оценки к логарифмической. Это позволяет получить многие тонкие характеристики классических множеств, возникающих в теории трансцендентных чисел. В работе 1997 года «Совместная аппроксимация нуля значениями целочисленных полиномов» [20] В. И. Берником и В. Н. Борбатов была получена двумерная оценка следующего вида:

ТЕОРЕМА 6. Пусть $P(x)$ – многочлен с целыми коэффициентами, h – его высота, функция $\Psi(x)$ монотонно убывает при $x > 0$ и $\sum_{t=1}^{\infty} \Psi(t) < \infty$. Тогда система неравенств

$$\begin{cases} |P(\omega_1)| < h^{-w_1} \Psi^{v_1}(h), \\ |P(\omega_2)| < h^{-w_2} \Psi^{v_2}(h), \end{cases}$$

где $w_1 + w_2 = n - 2$, $v_1 + v_2 = 1$, имеет для почти всех $(w_1, w_2) \in \mathbb{R}^2$ лишь конечное число решений в полиномах $P(x) \in \mathbb{Z}[x]$.

4. Современная школа

В 1992 году Н. Г. Мошевитин в работе «О совместных приближениях алгебраических чисел» [43], основываясь на работах Б. Ф. Скубенко, вместо оценки совместного произведения получил оценку для отдельных сомножителей, сформулированную в следующей теореме

ТЕОРЕМА 7. Пусть натуральное q задает совместные приближения к числам $\theta_1, \dots, \theta_n$:

$$||q\theta_i|| < cq^{-1/s}, \quad i = \overline{1, n}$$

где $c > 0$ — некоторая константа. Тогда

$$||q\theta_i|| > Cq^{-1/s} \log^{-\beta} q, \quad i = \overline{1, n}$$

с константами $C, \beta > 0$, зависящими от $\theta_1, \dots, \theta_n$ и c .

В работе 2002 года «К теореме Бlichфельда — Мюллера — Спона о совместных приближениях» [45] развивает, полученную В. Спонам [15] (1968 г.) и В. Г. Новаком [13] (1993 г.), оценку сверху константы наилучших диофантовых приближений

$$C_n \leq \frac{1}{\beta_n}, \quad \beta_n \geq n \cdot 2^{n+1} \left(\int_0^1 \frac{u^{n-1} du}{(1+u)^n + (1+u^n)} + \varepsilon_n \right), \quad \varepsilon_n > 0.$$

Н. Г. Мощевитин получил оценку для остаточного члена

$$\varepsilon_n = \frac{1}{2(\log 2\pi)^3 en^2 \cdot 2^{2n+7}} \left(1 - \frac{2^{1/m}}{2} \right)^{n+2} > 0, \quad n \geq 2.$$

При ее доказательстве он использовал следующее свойство совместных диофантовых приближений, полученное Дж. К. Лагариасом [10] в 1982 году.

ЛЕММА 1. Пусть знаменатели q n -мерных наилучших совместных приближений образуют бесконечную последовательность $q_1 < \dots < q_\mu < q_{\mu+1} < \dots$. Тогда $q_{\mu+2^{n+1}} > 2q_\mu$.

В 1982 году Дж. К. Лагариас ввел величину, показывающую скорость роста знаменателей совместных приближений

$$g(\alpha) = \lim_{\alpha \in \mathbb{R}^n} \inf_{\nu \rightarrow \infty} q_\nu^{1/\nu},$$

где $q_1 < \dots < q_i < q_{i+1} < \dots$ последовательные знаменатели совместных диофантовых приближений и получил оценку

$$g(\alpha) \geq \theta \left(\frac{8 + 13\theta}{\theta^{13}} \right)^{1/11} \approx 1.28040 \dots$$

В работе 2005 года «О наилучших двумерных совместных диофантовых приближениях в $\sup$ -норме» [46] Н. Г. Мощевитин улучшил оценку $g(\alpha)$ для двух чисел

$$g(\alpha) \geq \theta = \sqrt{\frac{1 + \sqrt{5}}{2}} \approx 1.2720 \dots,$$

Несколько иной подход к задачам теории диофантовых приближений состоит в рассмотрении понятия диофантовых экспонент. О. Н. Герман излагает это понятие следующим образом [31]. Пусть дана вещественная матрица

$$\Theta = \begin{pmatrix} \theta_{11} & \theta_{12} & \dots & \theta_{1m} \\ \theta_{21} & \theta_{22} & \dots & \theta_{2m} \\ \dots & \dots & \dots & \dots \\ \theta_{n1} & \theta_{n2} & \dots & \theta_{nm} \end{pmatrix},$$

тогда

ОПРЕДЕЛЕНИЕ 2. Точная вещественных чисел γ , для которых существует бесконечно много таких $x_1, \dots, x_m \in \mathbb{Z}$ одновременно не равных 0 и $y_1, \dots, y_n \in \mathbb{Z}$ что

$$\max_{1 \leq i \leq n} \left| \sum_{1 \leq j \leq m} \theta_{ij} x_j - y_i \right| \leq \left(\max_{1 \leq i \leq m} |x_i| \right)^{-\gamma}$$

называется (регулярной) диофантовой экспонентой матрицы Θ и обозначается $\beta(\Theta)$.

ОПРЕДЕЛЕНИЕ 3. Точная вещественных чисел γ , для которых существует бесконечно много таких $x_1, \dots, x_m \in \mathbb{Z}$ одновременно не равных 0 и $y_1, \dots, y_n \in \mathbb{Z}$ что

$$\prod_{1 \leq i \leq n} \left| \sum_{1 \leq j \leq m} \theta_{ij} x_j - y_i \right| \leq \left(\prod_{1 \leq i \leq m} \max(1, |x_i|) \right)^{-\gamma}$$

называется (регулярной) мультипликативной диофантовой экспонентой матрицы Θ и обозначается $\beta_M(\Theta)$.

В работе [31] О. Н. Герман указывает на тесную связь этого понятия с теоремами переноса. Например, известный принцип переноса Хинчина изящно выражается в описанных выше терминах

ТЕОРЕМА 8. Если $n = 1$, то

$$\frac{\beta(\Theta)}{(m-1)\beta(\Theta) + m} \leq \beta(\Theta^T) \leq \frac{\beta(\Theta) - m + 1}{m},$$

где Θ^T — транспонированная матрица Θ .

В работе «Усиление теоремы переноса Малера» [7] (2012 год) О. Н. Германом получены следующие теоремы переноса

ТЕОРЕМА 9. Пусть пространство целочисленных решений системы

$$\Theta \vec{x} = \vec{y}$$

не одномерно. Тогда для всех натуральных n, m , не равных одновременно 1, справедливы три неравенства

$$\begin{aligned} \beta(\Theta^T) &\geq \frac{n\beta(\Theta) + n - 1}{(m-1)\beta(\Theta) + m}, \\ \beta(\Theta^T) &\geq \frac{(n-1)(1 + \beta(\Theta)) - (1 - \alpha(\Theta))}{(m-1)(1 + \beta(\Theta)) + (1 - \alpha(\Theta))}, \\ \beta(\Theta^T) &\geq \frac{(n-1)(1 + \beta(\Theta)^{-1}) - (1 - \alpha(\Theta)v)}{(m-1)(1 + \beta(\Theta)^{-1}) + (1 - \alpha(\Theta)^{-1})}, \end{aligned}$$

где $\alpha(\Theta)$ это равномерная диофантова экспонента матрицы Θ — точная верхняя грань вещественных чисел γ , для которых при любом достаточно большом t система неравенств

$$\max_{1 \leq i \leq n} \left| \sum_{1 \leq j \leq m} \theta_{ij} x_j - y_i \right| \leq t^{-\gamma}, \quad \max_{1 \leq i \leq m} |x_i| \leq t$$

имеет ненулевое решение $\vec{x} \in \mathbb{Z}^m$, $\vec{y} \in \mathbb{Z}^n$.

Дальнейшее развитие этих исследований можно найти в работе О. Н. Германа Диофантовы экспоненты решеток» [32].

Как уже ранее отмечалось, теория диофантовых приближений тесно связана с теорией непрерывных дробей. В последнее время активные исследования в области цепных дробей велись В. И. Парусниковым и А. Д. Брюно. Ими в серии работ был дано обобщение алгоритма цепных дробей в начале на трехмерный [21, 22] (1994–1997 гг.), а потом и на многомерный случай [23, 24, 25, 26] (2004–2015 гг.).

Изложим суть этого обобщения. Пусть в n -мерном вещественном пространстве $\mathbb{R}^n$ с координатами $X = (x_1, \dots, x_n)$ заданы m однородных вещественных форм (т. е. многочленов от переменных) $f_1(X), \dots, f_m(X)$. Модули $g_i(X) = |f_i(X)|$ форм $f_i(X)$, $i = \overline{1, m}$, задают отображение $G(X) = (g_1(X), \dots, g_m(X))$ пространства $\mathbb{R}^n$ в положительный ортант $S = \mathbb{R}_+^m$ в m -мерном пространстве $\mathbb{R}^m$ с координатами

$$S = (s_1, \dots, s_m) : s_i = g_i(X) = |f_i(X)|, i = \overline{1, \dots, m}$$

При этом целочисленная решётка $\mathbb{Z}^n \subset \mathbb{R}^n$ отображается в некоторое множество $\mathbb{Z} \subset \mathbb{S}$. Замыкание выпуклой оболочки $\mathbb{H}$ множества $\mathbb{Z} \setminus 0$ является выпуклым множеством. Все целочисленные точки $X \in \mathbb{Z}^n \setminus 0$, отображающиеся на границу $\partial\mathbb{H}$ множества $\mathbb{H}$, назовём граничными. Ограничимся случаями, когда выпуклое множество $\mathbb{H}$ является многогранным, т.е. его граница $\partial\mathbb{H}$ состоит из вершин, рёбер, граней различных размерностей и не содержит непрерывных «кривых» частей. В этих случаях граница $\partial\mathbb{H}$ вычисляется с помощью стандартных программ для вычисления выпуклых многогранных оболочек [1]. Это и даёт алгоритмическое обобщение цепной дроби на любую размерность.

В работе «Вычисление основных единиц числовых колец с помощью обобщенной цепной дроби» [27] А. Д. Брюно сводит вычисление основных единиц кольца $\mathbb{Z}[\lambda]$ для целого неприводимого в $\mathbb{Q}$ вещественного многочлена и к вычислению куска границы $\partial\mathbb{H}$, содержащий $(m-1)$ -мерную грань.

Исследованиями, связанными с разложением алгебраических чисел в цепные дроби, в настоящее время занимаются Н. М. Добровольский и Н. Н. Добровольский. В работах [5, 36, 37] ими было проведено исследование, поведения остаточных дробей и их сопряжённых чисел для разложения алгебраических чисел в цепные дроби, например, что начиная с некоторого места все остаточные дроби являются приведёнными алгебраическими числами. В этих работах излагаются свойства минимальных многочленов остаточных дробей. В частности установлена связь значений минимальных многочленов и неполных частных разложений алгебраических чисел, сформулированная в следующей теореме

ТЕОРЕМА 10. Пусть $\alpha = \alpha_0$ — вещественный корень неприводимого целочисленного многочлена

$$f_0(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x], a_n > 0,$$

и число α имеет разложение в цепную дробь

$$\alpha = \alpha_0 = q_0 + \frac{1}{q_1 + \frac{1}{\dots + \frac{1}{q_k + \frac{1}{\dots}}}}.$$

Пусть последовательность минимальных многочленов $f_m(x)$ для остаточных дробей α_m задана формулами и номер $m_0 = m_0(\alpha, \varepsilon)$ определен из неравенства

$$\frac{2(n-1)}{Q_{m_0-1}\delta(\alpha)} < \varepsilon,$$

тогда для любого $m > m_0$ справедливы равенства

$$q_m = \begin{cases} q_m^*, & \text{если } f_m(q_{m+1}^*) > 0 \text{ и } f_m(q_m^*) < 0 \\ q_{m+1}^*, & \text{если } f_m(q_{m+1}^*) < 0 \\ q_{m-1}^*, & \text{если } f_m(q_m^*) > 0 \end{cases}$$

где

$$q_m^* = \left[-\frac{f'_{m-1}(q_{m-1})}{f_{m-1}(q_{m-1})} + \frac{(n-1)Q_{m-2}}{Q_{m-1}} \right].$$

В работе [37] была предложена классификация чисто-вещественных алгебраических иррациональностей с точки зрения разложения их в цепные дроби.

5. Заключение

Русская научная школа внесла значительный вклад в развитие теории диофантовых приближений. Фундаментальные результаты А. А. Маркова [40], А. Я. Хинчина [60], В. Г. Спринджук [56] дали мощный толчок к развитию теории чисел во всем мире. Значительный вклад в исследование свойств приближения алгебраических и действительных чисел внес во второй половине XX века Б. Ф. Скубенко [50, 51, 52, 53, 54, 55], а в развитие метрической теории диофантовых приближений белорусские ученые [17, 18, 20, 56, 57, 58, 59].

Активные исследования в этой области продолжают проводиться российскими учеными и в настоящее время [26, 27, 31, 7, 32, 36, 5, 37].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Barber C. B., Dobkin D. P., Huhdanpaa H. T., The Quickhull algorithm for convex hulls // ACM Trans. on Mathematical Software. 1996. Vol. 22. No. 4. P. 469–483.
2. Beresnevich V. V. On approximation of real numbers by real algebraic numbers // Acta Arithmetica. 1999. Vol. 90. P. 97–112.
3. Cassels J. W. S. Simultaneous Diophantine approximation // J. London Math. Soc. 1955. Vol. 30. P. 119–121.
4. Dirichlet L. G. P. Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen // S. B. Preuss. Akad. Wiss. 1842, P. 93–95.
5. Dobrovol'skii N. M., Balaba I. N., Rebrova I. Yu., Dobrovol'skii N. N. On Lagrange algorithm for reduced algebraic irrationalities // Bul. Acad. Stiinte Repub. Mold. Mat. 2016, No. 2. pp. 27–39.
6. Finch S. R. Mathematical Constants. Cambridge University Press, 2003 (Encyclopedia of Mathematics and its Applications, Book 94).
7. German O. N. On Diophantine exponents and Khintchine's transference principle // Moscow Journal of Combinatorics and Number Theory. 2012. Vol. 2. No. 2. pp. 22–51.
8. Hermite C. Sur une extension donnee a la theorie des fractions continues par M. Tchebychev // J. reine angew. Math. 1879. Vol. 88 P. 10–15.
9. Korkine A., Zolotareff G. Sur les formes quadratiques // Mathematische Annalen. 1873. Vol. 6. P. 366–389.
10. Lagarias J. S. Best simultaneous Diophantine approximation I. Growth rates of best approximation denominators // Trans. Amer. Math. Soc. 1982. Vol. 272. P. 545–554.
11. Minkovski H. Geometrie der Zahlen. Berlin: Teubner, 1896.
12. Mordell L. Lattice points in some n-dimensional non-convex regions. I, II // Kon. Nederl. Akad. Wetensch. Proc. Sect. Sci. 1946. Vol. 49. P. 773–781, 782–792.
13. Nowak W. G. A remark concerning the s-dimensional simultaneous Diophantine approximation constants // Graz. Math. Ber. 1993. Vol. 318. P. 105–110.
14. Schmidt W. M. Simultaneous approximation to algebraic numbers by rationals // Acta Math. 1970. Vol. 125. P. 189–201.
15. Spohn W. G. Blichfeldt's theorem and simultaneous Diophantine approximation // Amer. J. Math. 1968. Vol. 90. P. 885–894.
16. Ю. А. Басалов. Об истории оценок константы наилучших совместных диофантовых приближений // Чебышевский сборник, Т. 19, Вып. 2, 2018, С. 388–405. <https://doi.org/10.22405/2226-8383-2018-19-2-394-411>
17. Берник В. И. Метрическая теорема о совместном приближении нуля значениями целочисленных многочленов // Изв. АН СССР. Сер. матем. 1980. Том 44. Вып. 1. С. 24–45.
18. Берник В. И. Доказательство гипотезы А. Бэйкера в метрической теории трансцендентных чисел // Докл. АН СССР. 1984. Том 277. Номер 5. С. 1036–1039.
19. Берник В. И. О точном порядке приближения нуля значениями целочисленных многочленов // Acta Arithmetica. 1989. Том 53. С. 17–28.
20. Берник В. И., Борбат В. Н. Совместная аппроксимация нуля значениями целочисленных полиномов // Тр. МИАН. 1997. Том 218. С. 58–73.
21. Брюно А. Д., Парусников В. И. Многогранники Клейна для двух кубических форм Давенпорта // Матем. заметки. 1994. Том 56. С. 9–27.
22. Брюно А. Д., Парусников В. И. Сравнение разных обобщений цепных дробей // Матем. заметки. 1997. Том 61. С. 339–348.

23. Брюно А. Д. Алгоритм обобщенной цепной дроби // Препринт N45. М.: ИПМ им. М. В. Келдыша. 2004.
24. Брюно А. Д. Структура наилучших диофантовых приближений // ДАН. 2005. Том 402. Номер 4.
25. Брюно А. Д. Алгоритм обобщенной цепной дроби // ДАН. 2005. Том 402. Номер 6.
26. Брюно А. Д. Универсальное обобщение алгоритма цепной дроби // Чебышевский сборник. 2015. Том 16. С. 35–65.
27. Брюно А. Д. Вычисление основных единиц числовых колец с помощью обобщенной цепной дроби / Программирование. 2019. Номер 2. С. 17–31.
28. Венков Б. А. Об экстремальной проблеме Маркова для неопределенных тройничных квадратичных форм // Изв. АН СССР. 1945. Сер. матем., Том 9, вып. 6. С. 429–494.
29. Вороной Г. Ф. Об одном обобщении алгоритма непрерывных дробей // Вороной Г. Ф. Собрание сочинений. Т. 1. — Киев.: Изд-во АН Укр. ССР. 1952. С. 200–394.
30. Вороной Г. Ф. О некоторых свойствах положительных совершенных квадратичных форм // Вороной Г. Ф. Собрание сочинений. Т. 2. — Киев.: Изд-во АН Укр. ССР. 1952. С. 174–241.
31. Герман О. Н. Плохо приближаемые матрицы и диофантовы экспоненты // Чебышевский сб. 2013. Том 14. Вып. 4. С. 38–79.
32. Герман О. Н. Диофантовы экспоненты решеток // Совр. пробл. матем. 2016. Вып. 23. С. 35–42.
33. Глазунов Н. М., Голованов А. С., Малышев А. В. Доказательство гипотезы Минковского о критическом определителе области $|x|^p + |y|^p < 1$ // Зап. научн. сем. ЛОМИ. 1986. вып. 151. С. 40–53.
34. Гришмановская К. И., Малышев А. В., Пачев У. М., Фидарова А. М. Доказательство гипотезы минковского о критическом определителе области $|x|^p + |y|^p < 1$ в случае $5 < p < 6$ // Зап. научн. сем. ЛОМИ. 1977. вып. 67. С. 95–107.
35. Делоне Б. Н. О работе А. А. Маркова "О бинарных квадратичных формах положительного определителя" // УМН. 1948. Том 3. Вып. 5. С. 3–5.
36. Добровольский Н. М., Добровольский Н. Н. О минимальных многочленах остаточных дробей для алгебраических иррациональностей // Чебышевский сб. 2015. Том 16. Вып. 3. С. 147–182.
37. Добровольский Н. М., Добровольский Н. Н., Соболев Д. К., Соболева В. Н. Классификация чисто-вещественных алгебраических иррациональностей // Чебышевский сб. 2017. Том 18. Вып. 2. С. 98–128.
38. Малышев А. В. О представлении целых чисел положительными квадратичными формами // Тр. МИАН СССР. 1962. Том 65. С. 3–212.
39. Малышев А. В. Метод Морделла взаимных решеток в геометрии чисел // Зап. научн. сем. ЛОМИ. 1973. вып. 33. С. 97–115.
40. Марков А. А. О бинарных квадратичных формах положительного определителя // Марков А. А. Избранные труды. — М.: Изд. АН СССР, 1951. С. 9–85.
41. Марков А. А. О неопределенных тройничных квадратичных формах // Известия Императорской Академии Наук. 1901. Т. 14. вып. 5. С. 509–523.
42. Марков А. А. О неопределенных квадратичных формах с четырьмя переменными // Известия Императорской Академии Наук. 1902. Т. 16. вып. 3. С. 97–108.
43. Мощевитин. Н. Г. О совместных приближениях алгебраических чисел // Матем. заметки. 1992. Том 51. С. 72–80.
44. Мощевитин. Н. Г. О совместных диофантовых приближениях. Векторы заданного диофантова типа // Матем. заметки. 1997. Том 61. С. 706–716.
45. Мощевитин. Н. Г. К теореме Бlichфельда-Мюллера-Спона о совместных приближениях // Тр. МИАН. 2002. Том 239. С. 268–274.

46. Мощевитин Н. Г. О наилучших двумерных совместных диофантовых приближениях в $\sup$ -норме // Вестн. Моск. ун-та. Сер. 1. Матем., мех. 2005. Том 6. С. 50–53.
47. Подсыпанин Е. В. Об одном обобщении алгоритма цепных дробей, связанном с алгоритмом Вигго Бруна // Зап. научн. сем. ЛОМИ. 1977. Том 67. С. 184–194.
48. Подсыпанин Е. В. О длине периода квадратичной иррациональности // Зап. научн. сем. ЛОМИ. 1979. Том 82. С. 95–99.
49. Подсыпанин Е. В. Количество целых точек в эллиптической области (замечание к одной теореме А. В. Малышева) // Зап. научн. сем. ЛОМИ. 1979. Том 82. С. 100–102.
50. Скубенко Б. Ф. К гипотезе Минковского для $n = 5$ // Докл. АН СССР. 1972. Том 205. С. 1304–1305.
51. Скубенко Б. Ф. Доказательство гипотезы Минковского о произведении n линейных неоднородных форм от n переменных для $n \leq 5$ // Зап. научн. сем. ЛОМИ. 1973. Том 33. С. 6–36.
52. Скубенко Б. Ф. Новый вариант доказательства неоднородной гипотезы Минковского для $n = 5$ // Тр. МИАН СССР. 1976. Том 142. С. 240–253.
53. Скубенко Б. Ф., К гипотезе Минковского при больших n // Тр. МИАН СССР. 1978. Том 148. С. 218–224.
54. Скубенко Б. Ф. К совместным приближениям алгебраических иррациональностей // Зап. научн. сем. ЛОМИ. 1982. Том 116. С. 142–154.
55. Скубенко Б. Ф. К обобщенной теореме Рота–Шмидта // Зап. научн. сем. ЛОМИ. 1984. Том 134. С. 226–231.
56. Спринджук В. Г. Доказательство гипотезы Малера о мере множества S -чисел // Изв. АН СССР. Сер. матем. 1965. Том 29. Вып. 2. С. 379–436.
57. Спринджук В. Г. Конечность числа рациональных и алгебраических точек на некоторых трансцендентных кривых // Докл. АН СССР. 1967. Том 177. Номер 3. С. 524–527.
58. Спринджук В. Г. Иррациональность значений некоторых трансцендентных функций // Изв. АН СССР. Сер. матем. 1968. Том 32. Вып. 1. С. 93–107.
59. Спринджук В. Г. Достижения и проблемы теории диофантовых приближений // УМН. 1980. Том 35. Вып. 4. С. 3–68.
60. Хинчин А. Я. Метрические задачи теории иррациональных чисел // УМН. 1936. Вып. 1. С. 7–32.
61. Хинчин А. Я. Принцип Дирихле в теории диофантовых приближений // УМН. 1948. Т. 3. Вып. 3. С. 3–28.
62. Хинчин А. Я. Цепные дроби. — М.: Физматгиз, 1961.
63. Чебышев П. Л. Об одном арифметическом вопросе.— СПб., 1866 // Чебышев П. Л. Избранные труды. — М.: Изд. АН СССР, 1955. С. 55–105.
64. Чеботарев Н. Г. Заметки по алгебре и теории чисел. — Уч. зап. КГУ, 1934, // Чеботарев Н. Г. Собрание сочинений. Том 1. — М.-Л.: Изд. АН СССР, 1949. С. 208–221.

REFERENCES

1. Barber C. B., Dobkin D. P., Huhdanpaa H. T., 1996, “The Quickhull algorithm for convex hulls“, *ACM Trans. on Mathematical Software*, vol. 22, no. 4, pp. 469–483.
2. Beresnevich V. V. 1999, “On approximation of real numbers by real algebraic numbers“, *Acta Arithmetica*, vol. 90, pp. 97–112.
3. Cassels J. W. S. 1955, “Simultaneous Diophantine approximation“, *J. London Math. Soc.*, vol. 30, pp. 119–121.

4. Dirichlet L. G. P. 1842, “Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen“, *S. B. Preuss. Akad. Wiss.*, pp. 93–95.
5. Dobrovol'skii N. M., Balaba I. N., Rebrova I. Yu., Dobrovol'skii N. N. 2016, “On Lagrange algorithm for reduced algebraic irrationalities“, *Bul. Acad. Stiinte Repub. Mold. Mat.*, no. 2, pp. 27–39.
6. Finch S. R. 2003, *Mathematical Constants*, Cambridge University Press (Encyclopedia of Mathematics and its Applications, Book 94).
7. German O. N. 2012, “On Diophantine exponents and Khintchine’s transference principle“, *Moscow Journal of Combinatorics and Number Theory*, vol. 2, no. 2, pp. 22–51.
8. Hermite C. 1879, “Sur une extension donnee a la theorie des fractions continues par M. Tchebychev“, *J. reine angew. Math.* Vol. 88, pp. 10–15.
9. Korkine A., Zolotareff G. 1873, “Sur les formes quadratiques“ *Mathematische Annalen*, vol. 6, pp. 366–389.
10. Lagarias J. S. 1982, “Best simultaneous Diophantine approximation I. Growth rates of best approximation denominators“, *Trans. Amer. Math. Soc.*, vol. 272, pp. 545–554.
11. Minkovski H. 1896, *Geometrie der Zahlen* Berlin, Teubner.
12. Mordell L. 1946, “Lattice points in some n-dimensional non-convex regions. I, II“, *Kon. Nederl. Akad. Wetensch. Proc. Sect. Sci.*, vol. 49, pp. 773–781, 782–792.
13. Nowak W. G. 1993, “A remark concerning the s-dimensional simultaneous Diophantine approximation constants“, *Graz. Math. Ber.*, vol. 318, pp. 105–110.
14. Schmidt W. M. 1970, “Simultaneous approximation to algebraic numbers by rationals“, *Acta Math.*, vol. 125, pp. 189–201.
15. Spohn W. G. 1968, “Blichfeldt’s theorem and simultaneous Diophantine approximation“, *Amer. J. Math.*, vol. 90, pp. 885–894.
16. Basalov Yu. A. 2018, “On the history of estimates of the constant of the best joint diophantine approximations“, *Chebyshevskii sbornik*, vol. 19, issue 2, pp. 388–405. <https://doi.org/10.22405/2226-8383-2018-19-2-394-411>
17. Bernik V. I. 1980, “Metric theorem on the joint approximation of zero by values of integer polynomials“, *Izv. USSR Academy of Sciences, Ser. math.*, vol. 44, issue 1, pp. 24–45.
18. Bernik V. I. 1984, “Proof of A. Baker’s conjecture in the metric theory of transcendental numbers“, *Dokl. USSR Academy of Sciences*, Volume 277, no. 5, pp. 1036–1039.
19. Bernik V. I. 1989, “On the exact order of approximation of zero by the values of integer polynomials“, *Acta Arithmetica*, vol. 53, pp. 17–28.
20. Bernik V. I., Borbat V. N. 1997, “Joint approximation of zero by the values of integer polynomials“, *Proceedings of the Steklov Mathematical Institute*, vol. 218, pp. 58–73.
21. Bruno A. D., Parusnikov V. I., 1994, “Klein polyhedra for two cubic forms of Davenport“, *Math. notes*, vol. 56, pp. 9–27.
22. Bruno A. D., Parusnikov V. I., 1997, “Comparison of different generalizations of continued fractions//“, *Math. notes*, vol. 61, pp. 339–348.
23. Bruno A. D. 2004, “Generalized continued fraction algorithm“, *Preprint No. 45 Keldysh IAM*.
24. Bruno A. D. 2005, “The structure of the best diophantine approximations“, *Proceedings FAS*, vol. 402, no. 4.
25. Bruno A. D. 2005, “Generalized continued fraction algorithm“, *Proceedings FAS*, vol. 402, no. 6.
26. Bruno A. D. 2015, “Universal generalization of the continued fraction algorithm“ *Chebyshevskii sbornik*, vol. 16, pp. 35–65.

27. Bruno A. D. 2019, "Calculation of the basic units of number rings using a generalized continued fraction", *textitProgramming*, No 2, pp. 17–31.
28. Venkov B. A. 1945, "On the Markov extremal problem for indefinite trigeminal quadratic forms", *Izv. USSR Academy of Sciences*, Ser. math., vol. 9, issue 6, pp. 429–494.
29. Voronoi G. F. 1952, "On a generalization of the algorithm for continued fractions", *Collected Works*, vol. 1, Kiev, Publishing house of the Academy of Sciences of Ukraine SSR. pp. 200–394.
30. Voronoi G. F. 1952, "On some properties of positive perfect quadratic forms", *Collected Works*, vol. 2, Kiev, Publishing house of the Academy of Sciences of Ukraine SSR. pp. 174–241.
31. German O. N. 2013, "Poorly approximate matrices and Diophantine exponents", *Chebyshevskii sbornik*, vol. 14, issue 4, pp. 38–79.
32. German O. N. 2016, "Diophantine exponents of lattices" *Modern problem of math.*, issue 23, pp. 35–42.
33. Glazunov N. M., Golovanov A. S., Malyshev A. V. 1986, "Proof of the Minkowski conjecture on the critical determinant of a domain $|x|^p + |y|^p < 1$ ", *Notes of the LOMI Scientific Seminar*, issue 151, pp. 40–53.
34. Grishmanovskaya K. I., Malyshev A. V., Pachev U. M., Fidarova A. M. 1977, "Proof of the Minkowski conjecture on the critical determinant of the domain $|x|^p + |y|^p < 1$ in the case $5 < p < 6$ ", *Notes of the LOMI Scientific Seminar*, issue 67. pp. 95–107.
35. Delone B. N. 1948, "On the work of A. A. Markov "On binary quadratic forms of positive determinants"", *Uspekhi Mat. Nauk*, vol. 3, issue 5, pp. 3–5.
36. Dobrovol'skii N. M., Dobrovol'skii N. N. 2015, "On minimal polynomials of residual fractions for algebraic irrationalities", *Chebyshevskii sbornik*, vol. 16, issue 3, pp. 147–182.
37. Dobrovol'skii N. M., Dobrovol'skii N. N., Sobolev D. K., Soboleva V. N. 2017, "Classification of purely real algebraic irrationalities", *Chebyshevskii sbornik*, vol. 18, issue 2, pp. 98–128.
38. Malyshev A. V. 1962, "On the representation of integers by positive quadratic forms", *Transactions of Steklov Mathematical Institute of the USSR*, vol. 65, pp. 3–212.
39. Malyshev A. V. 1973, "Mordell method of reciprocal lattices in the geometry of numbers", *Notes of the LOMI Scientific Seminar*, issue 33. pp. 97–115.
40. Markov A. A. 1880, "On binary quadratic forms positive determinant", *Selected Works*, Publishing USSR Academy of Sciences, pp. 9–85.
41. Markov A. A. 1901, "On indefinite trigeminal quadratic forms", *Proceedings of the Imperial Academy of Sciences*, vol. 14, issue 5, pp. 509–523.
42. Markov A. A. 1902, "On indefinite quadratic forms with four variables" *Proceedings of the Imperial Academy of Sciences*, vol. 16, issue 3, pp. 97–108.
43. Moshchevitin N. G. 1992, "On joint approximations of algebraic numbers", *Mat. notes*, vol. 51, pp. 72–80.
44. Moshchevitin N. G. 1997, "On joint diophantine approximations. Vectors of a given Diophantine type", *Mat. notes*, vol. 61. pp. 706–716.
45. Moshchevitin N. G. 2002, "To the Blichfeldt-Mullender-Spohn theorem on simultaneous approximations", *Proceedings of the Steklov Mathematical Institute*, vol. 239, pp. 268–274.
46. Moshchevitin N. G. 2005, "On the best two-dimensional joint Diophantine approximations in the sup-norm", *Bulletin of the Moscow University*, Ser. 1. Vol. 6, pp. 50–53.
47. Podsypanin E. V. 1977, "On a generalization of the continued fraction algorithm associated with the Wiggo Brun algorithm" *Notes of the LOMI Scientific Seminar*, Volume 67, pp. 184–194.
48. Podsypanin E. V. 1979, "On the length of the period of quadratic irrationality" *Notes of the LOMI Scientific Seminar*, 1Vol. 82, pp. 95–99.
49. Podsypanin E. V. 1979, "The number of integer points in an elliptic region (remark on a theorem of A. V. Malyshev)" *Notes of the LOMI Scientific Seminar*, vol. 82, pp. 100–102.

50. Skubenko B. F. 1972, "To the Minkowski conjecture for $n = 5$ ", *Dokl. USSR Academy of Sciences*, vol. 205, pp. 1304–1305.
51. Skubenko B. F. 1973, "Proof of the Minkowski hypothesis on the product of n linear inhomogeneous forms of n variables for $n \leq 5$ ", *Notes of the LOMI Scientific Seminar*, vol. 33, pp. 6–36.
52. Skubenko B. F. 1976, "A new version of the proof of the heterogeneous Minkowski hypothesis for $n = 5$ ", *Proceedings of the Steklov Mathematical Institute of the USSR*, vol. 142, pp. 240–253.
53. Skubenko B. F. 1978, "To the Minkowski conjecture for large n ", *Proceedings of the Steklov Mathematical Institute of the USSR*, vol. 148, pp. 218–224.
54. Skubenko B. F. 1982, "To joint approximations of algebraic irrationalities", *Notes of the LOMI Scientific Seminar*, vol. 116, pp. 142–154.
55. Skubenko B. F. 1984, "To the generalized Roth-Schmidt theorem", *Notes of the LOMI Scientific Seminar*, vol. 134, pp. 226–231.
56. Sprindzhuk V. G. 1965, "Proof of Mahler's conjecture on the measure of the set of S-numbers", *Izv. USSR Academy of Sciences, Ser. math.*, vol. 29, issue 2, pp. 379–436.
57. Sprindzhuk V. G. 1967, "Finiteness of the number of rational and algebraic points on some transcendental curves", *Dokl. USSR Academy of Sciences*, vol. 177, no. 3, pp. 524–527.
58. Sprindzhuk V. G. 1968, "Irrationality of values some transcendental functions", *Izv. USSR Academy of Sciences, Ser. math.*, vol. 32, issue 1, pp. 93–107.
59. Sprindzhuk V. G. 1980, "Achievements and problems of theory Diophantine approximations", *Advances in Mathematical Sciences*, vol. 35, issue 4, pp. 3–68.
60. Hinchin A. I. 1936, "Metric problems of the theory of irrational numbers", *Advances in Mathematical Sciences*, issue 1, pp. 7–32.
61. Hinchin A. I. 1948, "Dirichlet principle in the theory of diophantine approximations", *Advances in Mathematical Sciences*, vol. 3, Issue 3, pp. 3–28.
62. Hinchin A. I. 1961, *Continued fractions*, Mir.
63. Chebyshev P. L. 1866, "On an arithmetic question", *Selected Works*, Publishing USSR Academy of Sciences, pp. 55–105.
64. Chebotarev N. G. 1934, "Notes on algebra and number theory", *Collected Works*, vol. 1, Publishing USSR Academy of Sciences, pp. 208–221.

Получено 28.01.2020 г.

Принято в печать 20.03.2020 г.

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 21. Выпуск 1.

УДК 517

DOI 10.22405/2226-8383-2020-21-1-404-414

Василий Ильич Нечаев. К 100-летию юбилею

В. Н. Чубариков, В. Г. Чирский, Е. И. Деза, Ю. Н. Баулина, Л. В. Котова, Е. В. Неискашова,
В. С. Ванькова, Н. М. Добровольский, И. Ю. Реброва, А. Л. Рощеня

Чубариков Владимир Николаевич — доктор физико-математических наук, профессор, заведующий кафедрой математических и компьютерных методов анализа, президент механико-математического факультета Московского государственного университета имени М. В. Ломоносова (г. Москва).
e-mail: chubarik1@mech.math.msu.su

Чирский Владимир Григорьевич — доктор физико-математических наук, доцент, заведующий кафедрой теории чисел Московского педагогического государственного университета, профессор механико-математического факультета Московского государственного университета имени М. В. Ломоносова (г. Москва).
e-mail: vgchirskii@yandex.ru

Деза Елена Ивановна — доктор педагогических наук, кандидат физико-математических наук, доцент, профессор кафедры теоретической информатики и дискретной математики, Московский педагогический государственный университет (г. Москва).
e-mail: elena.deza@gmail.com

Баулина Юлия Николаевна — кандидат физико-математических наук, Институт математики и информатики, Московский педагогический государственный университет (г. Москва).
e-mail: jbaulina@mail.ru

Котова Лидия Владимировна — кандидат педагогических наук, доцент кафедры теории чисел Института математики и информатики, Московский педагогический государственный университет (г. Москва).
e-mail: kolv@inbox.ru

Неискашова Елена Валентиновна — кандидат педагогических наук, доцент, заведующий кафедрой высшей математики, Российский государственный аграрный университет — Московская сельскохозяйственная академия имени К. А. Тимирязева (г. Москва).
e-mail: neiskashova@gmail.com

Ванькова Валентина Сергеевна — кандидат физико-математических наук, доцент кафедры информатики и информационных технологий, Тульский государственный педагогический университет им. Л. Н. Толстого (г. Тула).
e-mail: vsvankova@gmail.com

Добровольский Николай Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры, математического анализа и геометрии Тульского государственного педагогического университета им. Л. Н. Толстого (г. Тула).
e-mail: dobrovol@tspu.ru

Реброва Ирина Юрьевна — кандидат физико-математических наук, декан факультета математики, физики и информатики, доцент кафедры алгебры, математического анализа и геометрии, Тульский государственный педагогический университет им. Л. Н. Толстого (г. Тула).
e-mail: i_rebrova@mail.ru

Рощеня Алла Леностовна — кандидат физико-математических наук, доцент кафедры педагогики, дисциплин и методик начального образования, Тульский государственный педагогический университет им. Л. Н. Толстого (г. Тула).
e-mail: kpdmmo@tspu.ru

Аннотация

11 января 2020 года исполняется сто лет со дня рождения Василия Ильича Нечаева — известного советского математика, доктора физико-математических наук, профессора, ведущего научного сотрудника Математического института имени В. А. Стеклова Академии наук СССР (РАН), заведующего кафедрой теории чисел Московского педагогического государственного университета (МПГУ) с 1978 по 1999 годы.

Василий Ильич Нечаев внес значительный вклад в развитие отечественной научной школы по теории чисел. Наиболее известны исследования профессора В. И. Нечаева и его учеников в области аналитической теории чисел и ее приложений.

Неоценимы заслуги Василия Ильича Нечаева и в развитии высшего образования России. В. И. Нечаев много лет руководил научным семинаром по аналитической теории чисел в МПГУ, создал собственную научную школу. Многие его ученики стали кандидатами и докторами физико-математических или педагогических наук, активно работают в системе отечественного высшего образования, занимают высокие административные посты, проводят научные исследования по дидактике высшей школы в областях, связанных с преподаванием избранных вопросов теории чисел и ее приложений, воспитывают своих учеников.

Василий Ильич опубликовал большое количество научных и методических работ, перевел на русский язык несколько фундаментальных научных монографий. Он долгие годы являлся членом редколлегии журнала "Математические заметки", был членом программных комитетов многих международных конференций по алгебре и теории чисел.

Ключевые слова: теория чисел, криптография, дидактика высшей школы.

Библиография: 25 названий.

Для цитирования:

В. Н. Чубариков, В. Г. Чирский, Е. И. Деца, Ю. Н. Баулина, Л. В. Котова, Е. В. Неискашова, В. С. Ванькова, Н. М. Добровольский, И. Ю. Реброва, А. Л. Рощеня. Василий Ильич Нечаев. К 100-летию юбилею // Чебышевский сборник, 2020, т. 21, вып. 1, с. 404–414.

CHEBYSHEVSKII SBORNIK

Vol. 21. No. 1.

UDC 517

DOI 10.22405/2226-8383-2020-21-1-404-414

Vassiliy Ilyich Nechaev. To the 100-th anniversary

V. N. Chubarikov, V. G. Cherskii, E. I. Deza, I. N. Baoulina, L. V. Kotova, E. V. Neiskashova, V. S. Vankova, N. M. Dobrovolskii, I. Yu. Rebrova, A. L. Roshchenya

Chubarikov Vladimir Nikolaevich — doctor of physical and mathematical sciences, professor, head of the Department of mathematical and computer methods of analysis, president of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University (Moscow).

e-mail: chubarik2009@live.ru

Chirsky Vladimir Grigoryevich — doctor of physical and mathematical sciences, associate professor, head of number theory's chair of the Moscow Pedagogical State University, professor of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University (Moscow).

e-mail: vgchirskii@yandex.ru

Deza Elena Ivanovna — doctor of pedagogical Sciences, candidate of physical and mathematical Sciences, associate Professor, Professor of the Department of theoretical Informatics and discrete mathematics, Moscow State Pedagogical University (Moscow).

e-mail: elena.deza@gmail.com

Baoulina Ioulia Nikolaevna — candidate of physical and mathematical sciences, Institute of Mathematics and Computer Science, Moscow State Pedagogical University (Moscow).

e-mail: jbaulina@mail.ru

Kotova Lidia Vladimirovna — candidate of Pedagogical Sciences, Associate Professor, Department of Number Theory, Institute of Mathematics and Computer Science, Moscow State Pedagogical University (Moscow).

e-mail: kolv@inbox.ru

Neiskashova Elena Valentinovna — candidate of pedagogical Sciences, associate Professor, head of higher mathematics chair of Russian State Agrarian University-Moscow Timiryazev Agricultural Academy (Moscow).

e-mail: neiskashova@gmail.com

Vankova Valentina Sergeevna — candidate of physical and mathematical Sciences, associate professor, Tula State L. N. Tolstoy Pedagogical University (Tula).

e-mail: vsvankova@gmail.com

Dobrovolsky Nikolai Mihailovich — doctor of physical and mathematical sciences, professor, head of the Department algebra, calculus and geometry of the Tula State L. N. Tolstoy Pedagogical University (Tula).

e-mail: dobrovol@tspu.ru

Rebrova Irina Yuryevna — candidate of physical and mathematical Sciences, associate professor, dean of the faculty of mathematics, physics and computer science, Tula State L. N. Tolstoy Pedagogical University (Tula).

e-mail: i_rebrova@mail.ru

Roshchenya Alla Lenstovna — candidate of physical and mathematical Sciences, associate professor, Tula State L. N. Tolstoy Pedagogical University (Tula).

e-mail: kpdmmo@tspu.ru

Abstract

January 11, 2020 marks the centenary of the birth of Vassiliy Ilyich Nechaev, a well-known Soviet mathematician, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Number Theory of Moscow Pedagogical State University (MSPU).

Vassiliy Ilyich Nechaev has made a significant contribution to Development of Russian scientific school on number theory. The research of Professor V. I. Nechaev and his disciples in the field of analytical number theory and its applications is very considerable.

Moreover, the scientific and educational activities of Professor V.I. Nechaev have been very influential in the development of methods of teaching mathematics at colleges for teacher education. V. I. Nechaev was a leading figure at the scientific school and the organizer of the analytic number theory research seminar at the Moscow State Pedagogical University. Among his many students received their PhD and doctoral degrees. Vassiliy Ilyich Nechaev has published a large number of scientific and methodical works, was a translator of several fundamental scientific monographs. He was for many years a member of the editorial board of the journal "Mathematical Notes" and served as a member of the program committees of many international conferences on algebra and number theory.

Keywords: number theory, cryptography, didactics of the higher education.

Bibliography: 25 titles.

For citation:

V. N. Chubarikov, V. G. Cherskii, E. I. Deza, I. N. Baoulina, L. V. Kotova, E. V. Neiskashova, V. S. Vankova, N. M. Dobrovolskii, I. Yu. Rebrova, A. L. Roshchenya, 2020, "Vassiliy Ilyich Nechaev. To the 100-th anniversary", *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 404–414.

1. Введение

Василий Ильич Нечаев родился 11 января 1920 года в Москве. Его интерес к математике и математический талант были очевидны еще в школе. Школьные годы стали для него и временем активного

самообразования. В 1937 году он поступил на физико-математический факультет Московского городского педагогического института имени В. П. Потемкина (высшее учебное заведение, существовавшее в Москве с 1931 по 1960 год) и окончил его с отличием в июне 1941 года.

15 октября 1941 года, в труднейшие дни исторической битвы за Москву, В. И. Нечаев добровольцем ушел в Красную Армию. Прошел с боями всю войну, закончив ее младшим лейтенантом. Участвовал в сражениях на Западном и Сталинградском фронтах в составе 241-го Гвардейского Особого разведывательного батальона, дважды был тяжело ранен. За боевые заслуги был награжден орденами Красного Знамени и Отечественной войны II степени, многочисленными медалями.

В. И. Нечаев был женат на Клавдии Тырковой (Нечаевой), имел двух дочерей (Нечаева Тамара Васильевна, 1951 г. р. и Шитова (Нечаева) Людмила Васильевна, 1960 г. р.) и четырех внуков.

2. Трудовая деятельность

После войны В. И. Нечаев приступает к активной научной работе, и вся его последующая деятельность связана с МГПИ им. В. И. Ленина и Математическим институтом им. В. А. Стеклова АН СССР (РАН).

Демобилизовавшись из армии, он возвращается в Московский городской педагогический институт имени В. П. Потемкина и учится в аспирантуре под руководством профессора Михаила Кузьмича Гребенчи (1897–1948). По окончании аспирантуры в 1949 году по рекомендации академика Ивана Матвеевича Виноградова становится заведующим кафедры алгебры и элементарной математики Московского городского педагогического института, сменив на этом посту своего учителя М. К. Гребенчу.

В 1960 году Московский городской педагогический институт имени В. П. Потемкина был объединен с Московским государственным педагогическим институтом имени В. И. Ленина. Кафедра алгебры и элементарной математики стала называться кафедрой алгебры и теории чисел, возглавил ее профессор Александр Адольфович Бухштаб.

В 1962 году, после отделения кафедры алгебры под руководством профессора Леонида Яковлевича Куликова, кафедра алгебры и теории чисел стала называться кафедрой теории чисел и вычислительной математики. Несколько позже, после создания кафедры вычислительной математики и программирования под руководством Владимира Вениаминовича Щенникова, кафедра теории чисел и вычислительной математики стала кафедрой теории чисел.

Именно на этой кафедре, кафедре теории чисел математического факультета МГПИ (позднее — МПГУ), почти сорок лет проработал В. И. Нечаев, более 20 лет, с 1978 года и до конца жизни, являясь ее заведующим.

В разное время на кафедре преподавали выдающиеся ученые, профессора А. Б. Шидловский, Н. М. Коробов, С. М. Воронин, А. И. Павлов, Кафедра теории чисел МГПИ им. В. И. Ленина все эти годы тесно сотрудничала с кафедрой теории чисел МГУ имени М. В. Ломоносова. Кафедры проводили совместный научно-исследовательский семинар и являлись ведущими научными центрами по теории чисел в СССР. Традиции кафедры теории чисел, ее дух сохраняются и сегодня. с 1999 по 2006 годы кафедрой руководил доктор физико-математических наук, профессор Д. А. Митькин. С 2006 года по настоящее время заведующим кафедрой является доктор физико-математических наук, профессор В. Г. Чирский. Молодые перспективные преподаватели — С. В. Орлова, О. Ю. Баженова, Ю. В. Нестеренко, М. Е. Чанга, Е. В. Крупицын — предлагая свои курсы и методики, внося новую струю в преподавание математических дисциплин, бережно относятся к наследию своих предшественников.

С 1948 года Василий Ильич Нечаев — кандидат физико-математических наук, с 1975 года — доктор физико-математических наук, профессор.

С 1963 года — старший, а затем — ведущий научный сотрудник Математического института имени В. А. Стеклова Академии наук СССР (позднее РАН).

3. Научная деятельность

Василий Ильич Нечаев всегда был на острие математической науки и внес значительный вклад в развитие ряда важнейших теоретических и прикладных вопросов современной математики.

Василию Ильичу принадлежат важные результаты в области аналитической теории чисел:

- новые верхние и нижние оценки в проблеме Варинга для специальных целозначных многочленов $\frac{x(x+1)\dots(x+n-1)}{n!}$;
- правильные по порядку оценки сверху полных рациональных тригонометрических сумм, улучшающие оценки Хуа Локена;
- оценки полных тригонометрических сумм и сумм с характеристиками с рекуррентными функциями.

Кроме того, Василий Ильич получил ряд значительных результатов в теории линейно-рекуррентных последовательностей над конечными полями. Его идеи оказали существенное влияние на развитие этой ветви прикладной математики. Ему принадлежат и результаты по разработке и оценке детерминированных алгоритмов вычисления дискретного логарифма над конечным полем. Эти задачи возникли во второй половине прошлого столетия в связи с созданием новейших цифровых систем защиты информации. В эти годы криптография как наука переживала второе рождение, и В. И. Нечаев внес большой вклад в ее становление.

Научные труды В. И. Нечаева хорошо известны как в нашей стране, так и за рубежом. За работу в области прикладной математики он награжден орденом "Знак Почета".

4. Педагогическая деятельность

В. И. Нечаев был одним из крупнейших специалистов по вопросам высшего педагогического образования, автором учебных программ по алгебре, теории чисел, числовым системам, элементарной математике, прикладным вопросам теории чисел; автором нескольких учебников, многочисленных статей в Математической энциклопедии, Детской и Школьной математических энциклопедиях.

На протяжении многих лет профессор В. И. Нечаев являлся членом редколлегии журнала "Математические заметки", членом Совета математического факультета МПГУ, членом специализированного Совета по присуждению ученых степеней и членом секции алгебры и теории чисел научно-методического Совета по математике и вычислительной технике УМО на базе МПГУ.

За многолетнюю работу по совершенствованию дидактики высшей школы, существенный вклад в дело подготовки отечественных педагогических кадров он был награжден знаком "Отличник народного просвещения".

В. И. Нечаев стоял у истоков внедрения в образовательный процесс высшей и общеобразовательной школы компьютерных технологий. Он был создателем первой программы для ЭВМ, позволяющей проверить вычислительные навыки школьников. Эта работа была отмечена Золотой медалью ВДНХ.

Разработанный В. И. Нечаевым курс "Числовые системы" и написанный на его основе учебник для студентов педагогических вузов [14] давно стал классикой предметной подготовки учителей математики и информатики и до сих пор активно внедряется в образовательный процесс Института математики и информатики (до 2018 года — математического факультета) МПГУ.

Программы по элементарной математике (арифметика и комбинаторика), разработанные на кафедре теории чисел под руководством В. И. Нечаева, послужили основой для создания нескольких учебных пособий указанной тематики, в том числе пособия В. Л. Топунова "Комбинаторика", пособия Л. Л. Степановой и А. В. Жмулевой "Арифметика: практикум по решению задач". В 2008 году последнее пособие было переиздано при активном участии Московского центра непрерывного математического образования и до сих пор активно используется в образовательной практике. Пользуется постоянным спросом и вызывает непреходящий интерес у студентов пособие Л. Л. Степановой "Дополнительные главы теории чисел".

В. И. Нечаев был инициатором введения в образовательные программы математических факультетов педагогических вузов дисциплины "Основы дискретной математики", автором первой программы по дискретной математике для педагогических вузов. Указанный курс давно и прочно занял важное место в учебных планах, в 2010 году на его основе было создано учебное пособие Е. И. Де́за и Д. Л. Моделя "Основы дискретной математики".

В. И. Нечаев много лет работал в области прикладной математики. Будучи ведущим отечественным специалистом в вопросах защиты информации, он внес большой вклад не только в развитие, но и в популяризацию новой науки, создав первое в своем роде пособие по криптографии для студентов педагогических вузов, осветив в нем исторические аспекты и математические основы последних достижений. Он был одним из инициаторов включения дисциплины "Криптография. Основы защиты информации" в учебную программу математического факультета МПГУ. Цикл лекций, прочитанный

им по прикладным вопросам теории чисел — элементам криптографии — лег в основу пособия "Элементы криптографии (Основы теории защиты информации)" [25]. Будучи тяжело болен, он до последних дней жизни продолжал работать над этой книгой.

Первая часть книги содержит краткие сведения о различных приемах шифрования: квадрат Полибия, шифр Цезаря, шифр Тритемиуса, решетка Кардано, маршрутная и постолбцовая транспозиции, квадрат Виженера, перемешанные алфавиты, одноразовый шифровальный блокнот, шифр "по книге", тюремный шифр, парный шифр, шифр "по стихотворению". Вторая часть книги знакомит с современными методами шифрования: открытый ключ, электронная подпись. Третья часть книги включает необходимые сведения из теории конечных полей. Она включает также следующие вопросы: дискретный логарифм, экспоненциальный открытый ключ, оценка сложности детерминированных алгоритмов вычисления дискретного логарифма, конструкция псевдослучайной последовательности на основе ненулевого решения линейного рекуррентного уравнения, локация удаленных и быстро движущихся объектов, псевдослучайные последовательности и криптография.

Редактором этой книги стал ректор МГУ имени М. В. Ломоносова, академик Российской академии наук В. А. Садовничий. В предисловии к ней он отметил, что "особенность отечественной школы состоит в сочетании четкости рассуждений с глубиной содержания и простотой, доступностью, конкретностью изложения материала", а "практическое воплощение данных идей подразумевает наличие высококвалифицированных и творчески мыслящих преподавателей". "Математическое образование и математическая культура составляют стержень научного знания, и значение математики как основы фундаментальных исследований постоянно возрастает. Для решения этих задач требуются учебники, отражающие в определенной полноте современное состояние исследований и мировоззренческие принципы данной области науки. Книга В. И. Нечаева "Элементы криптографии (Основы теории защиты информации)" является первым учебным пособием по теории защиты информации, фундаментом которой является прикладная теория чисел. Книга отличается широтой охвата материала в области защиты информации. Она доступна широкому кругу читателей, начиная с учащихся старших классов математических школ."

В течение последних двадцати лет работа по внедрению элементов криптографии в образовательный процесс значительно продвинулась. Сегодня соответствующие курсы читаются практически на всех направлениях подготовки, реализуемых Институтом математики и информатики МПГУ. В 2018 году вышло учебное пособие Е. И. Деза и Л. В. Котовой "Теоретико-числовые основы защиты информации", основанное на идеях В. И. Нечаева. Оно опирается на теперь уже многолетний опыт практической работы преподавателей кафедры в этой области, работы, начало которой было положено В. И. Нечаевым.

5. Научная школа В. И. Нечаева

В. И. Нечаев придавал огромное значение научному преемничеству, воспитанию и поддержке талантливой молодежи. Его многочисленные ученики, в разных городах и странах мира, продолжают его дело.

Василий Ильич руководил аспирантами по трем различным направлениям. У него много учеников по прикладным вопросам теории чисел, для широкого круга ученых хорошо известны результаты его учеников по аналитической теории чисел и по методике преподавания математики.

Многие годы основу кафедры теории чисел Московского педагогического государственного университета составляли выпускники математического факультета МПГУ и ученики Василия Ильича: Баулина Ю. Н., Гладкова Е. Б., Деза Е. И. (Пантелеева), Жмулева А. В., Иконникова Т. К., Киселева Л. В., Котова Л. В., Топунов В. Л., Степанова Л. Л., Юрченко А. Л.

Большинство из них защитили по руководством В. И. Нечаева кандидатские диссертации:

- Жмулева Алевтина Васильевна "Теория делимости целых чисел. Факультативный курс" (МППИ им. В. И. Ленина, 1980 г.);
- Киселева Лариса Владимировна "О количестве нулей дзета-функции Римана на коротких промежутках критической прямой" (МППИ им. В. И. Ленина, 1989 г.);
- Пантелеева (Деза) Елена Ивановна "О проблеме делителей Дирихле и ее аналогах в числовых полях" (МПГУ, 1993 г.);

- Неискашова Елена Валентиновна "Профессиональная направленность обучения студентов педагогических вузов в процессе углубленного изучения понятия числа" (МПГУ, 1999 г.);
- Баулина Юлия Николаевна "Формулы для числа решений уравнений марковского типа в конечных полях" (МПГУ, 2001 г.);

Работа по развитию научных идей В. И. Нечаева никогда не прерывалась. Продолжается она и сегодня.

Жмулева Алевтина Васильевна, профессор, кандидат физико-математических наук, проработала на кафедре 58 лет. Бывшую выпускницу Василий Ильич сам пригласил работать на кафедру. Она стала его первой защищенной аспиранткой, а разработанный ею факультативный курс "Теория делимости" и сейчас активно востребован в педагогической практике. На протяжении всех лет работы Алевтина Васильевна отмечала, что является ученицей Василия Ильича и продолжателем его идей. За это время она внесла огромный вклад в развитие преподавания арифметики и теории чисел не только в МПГУ, но и в системе отечественного педагогического образования в целом. Она была одним из основных авторов разработанного на кафедре теории чисел курса "Практикум по решению задач: арифметика и комбинаторика", принимала активное участие в разработке и внедрению в учебный процесс таких классических сегодня курсов, как "Теория чисел" и "Числовые системы".

В декабре 2012 года Елена Ивановна Деза защитила в МПГУ диссертацию на соискание степени доктора педагогических наук по теме "Индивидуальные траектории фундаментальной подготовки учителя математики в условиях вариативного образования". Работа была основана на исследовании теоретико-числовой и дискретной содержательных линий подготовки будущего учителя математики и опиралась на многолетний опыт работы автора на кафедре теории чисел.

В 2018 году, продолжая дело Василия Ильича по освещению и популяризации современных математических достижений в области криптографии, защитила кандидатскую диссертацию "Профессиональная направленность математической подготовки учителей информатики при обучении методам и средствам защиты информации" Котова Лидия Владимировна.

Хочется отметить, что кафедра теории чисел, возглавляемая В. И. Нечаевым, послужила trampolinem к плодотворной научной, преподавательской, административной деятельности для многих выпускников матфака МГПИ-МПГУ. Так, Д. Л. Модель, выпускник матфака 2001 года, ученик Е. И. Деза, является сегодня директором государственного бюджетного общеобразовательного учреждения города Москвы "Школа № 2101", ведет активную исследовательскую работу в области дидактики высшего и общего образования. Ученица В. И. Нечаева, выпускница матфака 1991 года Е. В. Неискашова сегодня — заведующая кафедрой высшей математики Российского государственного аграрного университета МСХА имени К. А. Тимирязева, кандидат педагогических наук, почетный работник высшего профессионального образования Российской Федерации. А. Л. Чекин, выпускник матфака 1979 года, ученик А. А. Бухштаба, возглавляет в настоящее время кафедру математики и информатики в начальной школе Института детства МПГУ; кандидат физико-математических наук (диссертация "Двумерное решето с весами и некоторые его теоретико-числовые приложения" (МПГИ, 1988)), доктор педагогических наук ("Профессиональная подготовка учителя начальных классов к обучению математике на основе интегративного подхода" (МПГУ, 2006)).

Те, кому довелось знать Василия Ильича Нечаева или учиться у него, всегда будут с восхищением и благодарностью вспоминать не только блеск его интеллекта, эрудицию, широту культурных интересов и интеллектуальную независимость, но и его высокие душевные качества, непоколебимое благородство, сочетавшееся с терпимостью и вниманием к людям.

Б. П. Гейдман, московский учитель и автор известных учебников по математике для начальной школы, вспоминая студенческие годы, проведенные в пединституте, так описывает качества характера и стиль преподавания Василия Ильича: "Высшую алгебру читал Василий Ильич Нечаев. Это изумительнейший математик, он читал лекции тихо, спокойно, обдумывая каждую фразу. Мы не могли найти лишнего слова в его лекциях. Алгебра проходила на встречной интеллектуальной волне, во встречном взаимодействии учеников и преподавателя. Выдающийся математик!"

Е. В. Неискашова, вспоминая годы учебы в аспирантуре под руководством В. И. Нечаева, пишет: "Нечаев Василий Ильич... В памяти сразу всплывают две картинки. Одна из них — мой первый приход к нему домой с подготовленным материалом по диссертации. Его рабочий кабинет и мое изумление — все стены комнаты от пола до потолка заняты стеллажами с книгами, ими же занят и коридор в квартире. Книги всегда были моей страстью и любовь Василия Ильича к ним подарила мне надежду, что наша совместная работа будет интересной. Другая картинка в моей памяти, связанная с Нечаевым,

день защиты моей диссертации. К сожалению, на защиту я выходила уже без Василия Ильича (июнь 1999 года) и, безусловно, испытывала, помимо присущего этому событию волнения, волнение и от того, что на защите не будет присутствовать мой научный руководитель. К началу мероприятия, заметив в аудитории людей, которых не было в числе приглашенных, начала потихоньку волноваться. Каково же было мое изумление, когда в процессе заседания стало понятно, что это пришли ученики и некоторые коллеги Василия Ильича поддержать на защите меня — его ученицу, тем самым включив меня в свой клан — учеников Нечаева. Мало кому удастся воспитать таких учеников, которые и после ухода учителя будут его помнить и уважать, поддерживая его начинания. Нечаев В. И. был из таких людей, немногословный, с обостренным чувством справедливости, умеющий объединять вокруг себя людей с общими интересами и похожими взглядами на жизнь.“

6. В. И. Нечаев и Тульская школа теории чисел

Определенные научные связи с Тульской школой теории чисел у Василия Ильича Нечаева установились ещё 50 лет тому назад, когда В. Д. Подсыпанин и М. Н. Добровольский выступали с докладами по результатам своих исследований по полиномам Туэ и матричным разложениям алгебраических иррациональностей на научно-исследовательском семинаре кафедры теории чисел МГУ под руководством член-корреспондента АН СССР А. О. Гельфонда в 1965 году. Он давал доброжелательные комментарии и справки во время их выступления. Развитие этих связей было продолжено уже в 1986 году, когда Василий Ильич согласился взять к себе соискателем В. С. Ванькову, преподавателя Тульского государственного педагогического института им. Л. Н. Толстого. Благодаря профессору М. Д. Гриндлингеру, который в 1981–1983 годах позволил Н. М. Добровольскому в аспирантуре продолжать заниматься теорией чисел по тематике профессора Н. М. Коробова в области теоретико-числового метода в приближенном анализе, и профессору В. И. Нечаеву, который согласился сотрудничать в области подготовки специалистов по теоретико-числовому методу приближенного анализа с Тульским государственным педагогическим институтом им. Л. Н. Толстого и МГУ имени М. В. Ломоносова, в Туле после десятилетнего перерыва начала возрождаться теоретико-числовая научная школа, основанная В. Д. Подсыпаниным в 1949 году. У всех тульских аспирантов Василия Ильича остались самые теплые воспоминания о домашних консультациях, которые он ежемесячно проводил для них. На этих консультациях Василий Ильич прежде всего сосредотачивал свои усилия на тщательной подготовке аспирантов по программе кандидатского экзамена по специальности. Огромное впечатление на тульских аспирантов производила научная библиотека профессора, в которой он быстро находил нужную справку по любому научному вопросу, возникавшему в процессе занятий. Со стороны МПГУ это сотрудничество осуществлялось профессорами: В. И. Нечаевым, Д. А. Митькиным, С. М. Ворониным, В. Г. Чирским, А. В. Жмулевой. Благодаря этому сотрудничеству были подготовлены кандидатские диссертации по теории чисел:

- В. С. Ванькова "Многомерные теоретико-числовые сетки" (МПГУ, 1992 г. рук. В. И. Нечаев);
- А. Л. Рошня "Аналитическое продолжение гиперболической дзета-функции решеток" (МПГУ, 1998 г. рук. В. И. Нечаев);
- И. Ю. Реброва "Пространство решеток и функции на нем (МПГУ, 2000 г. рук. В. И. Нечаев, Н. М. Добровольский);
- О. В. Родионова "Обобщенные параллелепипедальные сетки и их приложения" (МПГУ, 2000 г. рук. Д. А. Митькин, Н. М. Добровольский);
- Г. Т. Вронская "Квадратичное отклонение плоских сеток" (МПГУ, 2005 г. рук. Н. М. Добровольский);
- Л. П. Добровольская "Алгоритмы вычисления оптимальных коэффициентов" (МПГУ 2009 г. рук. В. Н. Чубариков);
- А. С. Герцог "Чисто-вещественные биквадратичные алгебраические поля и их приложения" (МПГУ 2012 г. рук. Н. М. Добровольский);
- Е. Д. Ребров "Некоторые теоретико-числовые методы приближенных вычислений" (МГУ 2013 г. рук. Н. М. Добровольский).

Отметим один интересный факт. На семинаре под руководством Н. М. Коробова в МГУ в 1992 году в процессе обсуждения диссертации В. С. Ваньковой Василий Ильич вместе с Николаем Михайловичем сформулировали задачу получения асимптотических формул для плоских сеток. Эта задача стала известна как задача Коробова-Нечаева. Ее удалось решить Г. Т. Вронской в своей кандидатской диссертации.

Сотрудничество между кафедрой теории чисел МПГУ и кафедрой алгебры, математического анализа и геометрии ТГПУ им. Л. Н. Толстого по подготовке аспирантов успешно продолжается и сейчас.

Другое важное направление научного сотрудничества связано с организацией и проведением научных конференций сначала по теории чисел, а потом по алгебре и теории чисел. Василий Ильич Нечаев активно участвовал в организации и проведении этих Международных конференций.

7. Заключение

Василия Ильича Нечаева не стало 18 февраля 1999 года. Это была тяжелая утрата не только для родных и близких, но и для математической общественности. Он являлся образцом служения на профессорском поприще, олицетворяя честь и достоинство русского интеллигента и ученого математика.

В год 75-летия Победы в Великой Отечественной войне можно только удивляться той жизненной силе, которая позволила старшему поколению преодолеть все испытания самой страшной войны человечества и продолжить созидательную деятельность на благо МИРА. Василий Ильич Нечаев солдатом защищал Отечество на поле брани, а профессором — на ниве образования. Светлая ему память!

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. В. И. Нечаев Представлении натуральных чисел суммой слагаемых вида $\frac{x(x+1)\dots(x+n-1)}{n!}$. // ДАН СССР. 1949. Т. 64. С. 159–162.
2. В. И. Нечаев Проблема Варинга для многочленов // Тр. МИАН СССР. 1951. Т. 38, № 1. С. 190–243.
3. В. И. Нечаев О представлении натуральных чисел суммой слагаемых вида $\frac{x(x+1)\dots(x+n-1)}{n!}$ // Изв. АН СССР. Сер. матем. 1953. Т. 17, № 6. С. 485–498.
4. В. И. Нечаев Группы невырожденных матриц над конечными полями и рекуррентные последовательности // ДАН СССР. 1963. Т. 152. С. 275–277.
5. В. И. Нечаев Неулучшаемая оценка тригонометрических сумм с рекуррентными функциями с непостоянными коэффициентами // ДАН СССР. 1964. Т. 154, pp. 520–522.
6. В. И. Нечаев, А. М. Полосуев О распределении невычетов и первообразных корней в последовательности, удовлетворяющей конечноразностному уравнению с полиномиальными коэффициентами // Вестн. Моск.ун-та. Серия 1. 1964. № 6. С. 75–84.
7. В. И. Нечаев, Л. Л. Степанова Распределение невычетов и первообразных корней в рекуррентных последовательностях над полем алгебраических чисел // УМН 1965. Т. 20, № 3. С. 197–203.
8. В. И. Нечаев Линейные рекуррентные сравнения с периодическими коэффициентами // Математические заметки. 1968. Т. 3, № 6. С. 625–632.
9. В. И. Нечаев Рекуррентные последовательности // Алгебра и теория чисел: Московский гос. пед. ин-тут, учен. записки. 1971. 375. С. 103–123.
10. В. И. Нечаев Линейные сравнения относительно степени простого идеала, и линейные рекуррентные последовательности // Алгебра и теория чисел: Московский гос. пед. ин-тут, учен. записки. 1971. 375. С. 124–132.
11. В. И. Нечаев Тригонометрические суммы для рекуррентных последовательностей // ДАН СССР. 1972. Т. 206, № 2. С. 811–814.
12. В. И. Нечаев Тригонометрические суммы для рекуррентных последовательностей элементов конечных полей // Мат. заметки. 1972. Т. 11. С. 597–607.
13. В. И. Нечаев Оценка полной рациональной тригонометрической суммы // Математические заметки. 1975. Т. 17, № 6. С. 839–849.

14. В. И. Нечаев Числовые системы: [учебное пособие для студентов физико-математических факультетов педагогических институтов] / М.: Просвещение, 1975. — 198 с.
15. В. И. Нечаев К вопросу о представлении натуральных чисел суммой слагаемых вида $\frac{x(x+1)\dots(x+n-1)}{n!}$ // Тр. МИАН СССР. 1976. Т. 142, № 1. С. 195–197.
16. В. И. Нечаев, В. Л. Топунов Оценка модуля полных рациональных тригонометрических сумм третьей и четвертой степени // Тр. МИАН. 1981. Т. 158, № 1. С. 125–129.
17. В. И. Нечаев Иван Матвеевич Виноградов // Математика в школе. 1983. № 3. С. 79–80.
18. В. И. Нечаев О верхней оценки модуля полных тригонометрических сумм третьей и четвертой степени // Исследования по теории чисел: Саратов 1988. С. 71–76.
19. Й. П. Кубилис, В. И. Нечаев, С. Б. Стечкин, А. Б. Шидловский Бухштаб Александр Адольфович (некролог) // УМН. 1991. Т. 46, № 1(277). С. 201–202.
20. Nechaev, V. I. On solutions of linear congruences // New trends in probability and statistics, Vol. 2 (Palanga, 1991). VSP, Utrecht. 1992. pp. 69–71.
21. В. И. Нечаев К вопросу о сложности детерминированного алгоритма для дискретного логарифма // Математические заметки. 1994. Т. 55. Вып. 2. С. 91–101.
22. В. И. Нечаев Сложность дискретного логарифма // Научные труды МПГУ. 1994. С. 46–49.
23. В. И. Нечаев Распределение на части периода линейной рекуррентной последовательности над конечным полем // Тезисы III Международной конференции “Современные проблемы теории чисел и ее приложения”. Тула, 1996. С. 107.
24. В. И. Нечаев Распределение знаков в последовательности прямоугольных матриц над конечным полем // Тр. МИАН. 1996. Т. 218. С. 335–342.
25. В. И. Нечаев Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В. А. Садовниченко - М.: Высш. шк., 1999. 109 с.

REFERENCES

1. Nechaev, V. I. 1949, "The representation of integers by sums of terms of the form $\frac{x(x+1)\dots(x+n-1)}{n!}$ ", Doklady Akad. Nauk SSSR (N.S.), vol. 64, pp. 159–162. (Russian)
2. Nechaev, V. I. 1951, "Waring's problem for polynomials", Trudy Mat. Inst. Steklov, Moscow, vol. 38, № 1. pp. 190–243. (Russian)
3. Nechaev, V. I. 1953, "On the representation of natural numbers as a sum of terms of the form $\frac{x(x+1)\dots(x+n-1)}{n!}$ ", Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 17, № 6, pp. 485–498. (Russian)
4. Nechaev, V. I. 1963, "The group of non-singular matrices over a finite field, and recurrent sequences", Dokl. Akad. Nauk SSSR, vol. 152, pp. 275–277. (Russian)
5. Nechaev, V. I. 1964, "A best-possible estimate of trigonometric sums for recurrent functions with non-constant coefficients", Dokl. Akad. Nauk SSSR, vol. 154, pp. 520–522. (Russian)
6. Nechaev, V. I. & Polosuev, A. M. 1964, "The distribution of non-residues and primitive roots in a sequence which satisfies a finite-difference equation with polynomial coefficients", Vestnik Moskov. Univ. Ser. I Mat. Meh., no. 6, pp. 75–84. (Russian)
7. Nechaev, V. I. & Stepanova, L. L. 1965, "The distribution of nonresidues and primitive roots in recurrence sequences over a field of algebraic numbers", Uspehi Mat. Nauk, vol. 20, № 3 (123), pp. 197–203. (Russian)
8. Nechaev, V. I. 1968, "Linear recurrent congruences with periodic coefficients", Mat. Zametki, vol. 3, № 6, pp. 625–632. (Russian)
9. Nechaev, V. I. 1971, "Recurrent sequences", Algebra and number theory. Moscow. Gos. Ped. Inst. Uchen. Zap., № 375, pp. 103–123. (Russian)

10. Nechaev, V. I. 1971, "Linear congruences with respect to a power of a prime ideal, and linear recurrent sequences", Algebra and number theory. Moskov. Gos. Ped. Inst. Uchen. Zap., № 375, pp. 124–132. (Russian)
11. Nechaev, V. I., 1972, "Trigonometric sums for recurrent sequences", Dokl. Akad. Nauk SSSR, vol. 206, pp. 811–814. (Russian)
12. Nechaev, V. I. 1972, "Trigonometric sums for recurrent sequences of elements of a finite field", Mat. Zametki, vol. 11, pp. 597–607. (Russian)
13. Nechaev, V. I. 1975, "An estimate of the complete rational trigonometric sum", Mat. Zametki, vol. 17, № 6, pp. 839–849. (Russian)
14. Nechaev, V. I. 1975, "Numeric system [textbook for students of physics and mathematics departments of pedagogical institutes]", Prosveshenie, Moscow, 198 p. (Russian)
15. Nechaev, V. I. 1976, "On the question of representing natural numbers by a sum of terms of the form $\frac{x(x+1)\dots(x+n-1)}{n!}$. Number theory, mathematical analysis and their applications. Trudy Mat. Inst. Steklov., vol. 142 (1976), 195–197, 270. (Russian)
16. Nechaev, V. I. & Topunov, V. L. 1981, "Estimation of the modulus of complete rational trigonometric sums of degree three and four", Analytic number theory, mathematical analysis and their applications. Trudy Mat. Inst. Steklov, vol. 158, pp. 125–129, 229. (Russian)
17. Nechaev, V. I. 1983, "Ivan Matveevich Vinogradov", Mat. v Shkole, № 3, pp. 79–80. (Russian)
18. Nechaev, V. I. 1988, "On the least upper bound on the modulus of complete trigonometric sums of degrees three and four", Investigations in number theory, pp. 71–76, Saratov. Gos. Univ., Saratov. (Russian)
19. Kubilis, I. P., Nechaev, V. I., Stechkin, S. B. & Shidlovskii, A. B. 1991, "Aleksandr Adol'fovich Bukhshtab", Uspekhi Mat. Nauk, vol. 46, № 1(277), pp. 201–202. (Russian); translation in Russian Math. Surveys 46 (1991), № 1, 241–243.
20. Nechaev, V. I. 1992, "On solutions of linear congruences", New trends in probability and statistics, Vol. 2 (Palanga, 1991), pp. 69–71, VSP, Utrecht.
21. Nechaev, V. I. 1994, "On the complexity of a deterministic algorithm for a discrete logarithm", Mat. Zametki, vol. 55, № 2, 91–101, 189; translation in Math. Notes 55, № 1–2, pp. 165–172. (Russian)
22. Nechaev, V. I. 1994, "The complexity of the discrete logarithm", Uchen. Trudy MPGU, pp. 46–49. (Russian)
23. Nechaev, V. I. 1996, "Distribution on the part of the period of linear recurring sequences over a finite field", Abstracts of the III International Conference "Modern Problems in Number Theory and its Applications", Tula, p. 107. (Russian)
24. Nechaev, V. I. 1996, "Distribution of signs in a sequence of rectangular matrices over a finite field", Tr. Mat. Inst. Steklova, vol. 218, Anal. Teor. Chisel i Prilozh., pp. 335–342. (Russian); translation in Proc. Steklov Inst. Math. 1997, № 3 (218), pp. 332–339.
25. Nechaev, V. I. 1999, "Elementy kriptografii" [Elements of cryptography] Osnovy teorii zashchity informatsii. [Fundamentals of information security] Vysshaya Matematika. [Higher Mathematics] Vyssh. Shkola, Moscow, 110 pp. (Russian)

Получено 16.01.2020 г.

Принято в печать 20.03.2020 г.

РЕДКОЛЛЕГИЯ

Том 21 Выпуск 1

ГЛАВНЫЙ РЕДАКТОР

Чубариков Владимир Николаевич — доктор физико-математических наук, профессор, заведующий кафедрой математических и компьютерных методов анализа, президент механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: chubarik1@mech.math.msu.su

ЗАМЕСТИТЕЛИ ГЛАВНОГО РЕДАКТОРА

Добровольский Николай Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры, математического анализа и геометрии Тульского государственного педагогического университета им. Л. Н. Толстого.
e-mail: dobrovol@tspu.ru

Михалев Александр Васильевич — доктор физико-математических наук, профессор механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: mikhalev@shade.msu.ru

Нижников Александр Иванович — доктор педагогических наук, профессор, заведующий кафедрой математической физики Московского педагогического государственного университета, заслуженный работник высшей школы РФ.
e-mail: ainizhnikov@mail.ru, nizhnikov.ai@mail.ru

ОТВЕТСТВЕННЫЕ СЕКРЕТАРИ

Добровольский Николай Николаевич — кандидат физико-математических наук, ассистент кафедры прикладной математики и информатики Тульского государственного университета; доцент кафедры алгебры, математического анализа и геометрии Тульского государственного педагогического университета им. Л. Н. Толстого.
e-mail: cheb@tspu.tula.ru, nikolai.dobrovolsky@gmail.com

Реброва Ирина Юрьевна — кандидат физико-математических наук, декан факультета математики, физики и информатики, доцент кафедры алгебры, математического анализа и геометрии Тульского государственного педагогического университета им. Л. Н. Толстого.
e-mail: i_rebrova@mail.ru

ЧЛЕНЫ РЕДКОЛЛЕГИИ

Артамонов Вячеслав Александрович — доктор физико-математических наук, профессор, заведующий кафедрой высшей алгебры механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: viacheslav.artamonov@gmail.com

Быковский Виктор Алексеевич — доктор физико-математических наук, член-корреспондент РАН, заместитель директора по научной работе Института прикладной математики Дальневосточного отделения Российской академии наук (ИПМ ДВО РАН), директор Хабаровского отделения ИПМ ДВО РАН.
e-mail: vab@iam.khv.ru

Востоков Сергей Владимирович — доктор физико-математических наук, профессор, профессор кафедры алгебры и теории чисел Санкт-Петербургского университета, президент фонда им. Л. Эйлера.
e-mail: sergei.vostokov@gmail.com

Гвоздев Александр Евгеньевич — доктор технических наук, профессор, профессор кафедры технологии и сервиса Тульского государственного педагогического университета им. Л. Н. Толстого.
e-mail: gwozdew.alexandr2013@yandex.ru

Георгиевский Дмитрий Владимирович — доктор физико-математических наук, профессор, заведующий кафедрой теории упругости механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: georgiev@mech.math.msu.su

Гриценко Сергей Александрович — доктор физико-математических наук, профессор кафедры математики 1-го Финансового университета при Правительстве РФ; профессор механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: s.gritsenko@gmail.com

Демидов Сергей Сергеевич — доктор физико-математических наук, профессор, профессор кафедры теории вероятностей механико-математического факультета Московского государственного университета; заведующий кабинетом истории и методологии математики и механики, заведующий отделом истории физико-математических наук Института истории естествознания и техники РАН; главный редактор журнала «Историко-математические исследования»; президент Международной академии истории науки.
e-mail: serd42@mail.ru

Дурнев Валерий Георгиевич — доктор физико-математических наук, профессор, заведующий кафедрой компьютерной безопасности и математических методов обработки информации Ярославского государственного университета.
e-mail: durnev@univ.uniyar.ac.ru

Зубков Андрей Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой математической статистики и случайных процессов механико-математического факультета Московского государственного университета имени М. В. Ломоносова; заведующий отделом дискретной математики Математического института им. В. А. Стеклова РАН.
e-mail: zubkov@mi.ras.ru

Иванов Валерий Иванович — доктор физико-математических наук, профессор, заведующий кафедрой прикладной математики и информатики Института прикладной математики и компьютерных наук Тульского государственного университета.
e-mail: ivaleryi@mail.ru

Карташов Владимир Константинович — кандидат физико-математических наук, профессор, заведующий кафедрой высшей математики и физики Волгоградского государственного социально-педагогического университета.
e-mail: kartashovvk@yandex.ru

Королёв Максим Александрович — доктор физико-математических наук, старший научный сотрудник Математического института им. В. А. Стеклова РАН.
e-mail: korolevma@mi.ras.ru

Кузнецов Валентин Николаевич — доктор технических наук, профессор, профессор кафедры прикладной математики и системного анализа Саратовского государственного технического университета им. Ю. А. Гагарина.
e-mail: kuznetsovn@info.sgu.ru

Латышев Виктор Николаевич — доктор физико-математических наук, профессор, профессор кафедры высшей алгебры механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: latyshev@basis.math.msu.su

Матиясевич Юрий Владимирович — доктор физико-математических наук, профессор, академик Российской академии наук, советник РАН Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН, президент Санкт-Петербургского математического общества.
e-mail: yumat@pdmi.ras.ru

Мищенко Сергей Петрович — доктор физико-математических наук, профессор, заведующий кафедрой алгебро-геометрических вычислений Ульяновского государственного университета.
e-mail: mishchenkosp@mail.ru

Нестеренко Юрий Валентинович — доктор физико-математических наук, профессор, член-корреспондент РАН, заведующий кафедрой теории чисел механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: nester@mi.ras.ru

Панин Владимир Алексеевич — доктор физико-математических наук, профессор, член-корреспондент РАН, действительный член академии информатизации образования, ректор Тульского государственного педагогического университета имени Л. Н. Толстого.
e-mail: tgpu@tula.net

Пачев Урусби Мухамедович — доктор физико-математических наук, профессор кафедры алгебры и дифференциальных уравнений Кабардино-Балкарского государственного университета

им. Х. М. Бербекова.

e-mail: urusbi@rambler.ru

Семёнов Алексей Львович — доктор физико-математических наук, профессор, академик Российской академии наук, академик Российской академии образования, заведующий кафедрой математической логики и теории алгоритмов Московского государственного университета имени М. В. Ломоносова.

e-mail: alsemno@ya.ru

Фомин Александр Александрович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры Московского педагогического государственного университета.

e-mail: alexander.fomin@mail.ru

Чирский Владимир Григорьевич — доктор физико-математических наук, доцент, заведующий кафедрой теории чисел Московского педагогического государственного университета; профессор механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

e-mail: vgchirskii@yandex.ru

Аллаков Исмаил — доктор физико-математических наук, профессор, профессор Термезского университета (Узбекистан).

e-mail: iallakov@mail.ru

Белов Алексей Яковлевич — доктор физико-математических наук, федеральный профессор математики, профессор университета Бар-Илана (Израиль).

e-mail: Kanelster@gmail.com

Берник Василий Иванович — доктор физико-математических наук, профессор, главный научный сотрудник Института математики НАН Беларуси (Белоруссия).

e-mail: bernik@im.bas-net.by

Касьянов Павел Олегович — доктор физико-математических наук, профессор Учебно-научного комплекса «Институт прикладного системного анализа» НТУУ «КПИ» МОН и НАН Украины (Украина).

e-mail: kasyanov@i.ua

Лауринчикас Антанас — доктор физико-математических наук, профессор, действительный член АН Литвы, заведующий кафедрой теории вероятностей и теории чисел Вильнюсского университета (Литва).

e-mail: antanas.laurincikas@mif.vu.lt

Лю Юнпин — доктор наук, профессор, руководитель Исследовательского центра современного математического анализа Пекинского педагогического университета (Китай).

e-mail: ypliu@bnu.edu.cn

Мисир Джумаил оглы Марданов — доктор физико-математических наук, профессор, директор Института математики и механики Национальной академии наук Азербайджана (Азербайджан).

e-mail: rmi@lan.ab.az

Мусин Олег Рустамович — доктор физико-математических наук, профессор факультета математики Техасского университета в Браунсвилле (США).

e-mail: oleg.musin@utb.edu, omusin@gmail.com

Рахмонов Зарулло Хусейнович — доктор физико-математических наук, профессор, член-корреспондент АН Республики Таджикистан, директор Института математики Таджикской АН (Таджикистан).

e-mail: zarullo_r@tajik.net, zarullo-r@rambler.ru

Салиба Холем Мансур — кандидат физико-математических наук, доцент факультета естественных и прикладных наук университета Нотр-Дам-Луэз (Ливан).

e-mail: qwe123@rocketmail.com

Табари Абдулло Хабибулло — доктор физико-математических наук, профессор, член корреспондент Академии наук Таджикистана; ректор Кулябского государственного университета имени Абуабдуллаха Рудаки (Таджикистан).

e-mail: rektor@kgu.tj

Фукшанский Леонид Евгеньевич — доктор математических наук, профессор, Колледж Клермонт Маккенна (США).

e-mail: lenny@cmc.edu

Шяучюнас Дарюс — профессор, доктор математических наук, старший научный сотрудник Научного института Шяуляйского университета (Литва).

e-mail: darius.siauciunas@su.lt

THE EDITORIAL BOARD

Volume 21 Issue 1

THE MAIN EDITOR

Chubarikov Vladimir Nikolaevich — doctor of physical and mathematical sciences, professor, head of the Department of mathematical and computer methods of analysis, president of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: chubarik1@mech.math.msu.su

THE ASSISTANTS OF THE MAIN EDITOR:

Dobrovolsky Nikolai Mihailovich — doctor of physical and mathematical sciences, professor, head of the Department algebra, calculus and geometry of the Tula State L. N. Tolstoy Pedagogical University.
e-mail: dobrovol@tspu.ru

Mihalev Alexander Vasilyevich — doctor of physical and mathematical sciences, professor, head of the chair of theoretical Informatics of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: mikhalev@shade.msu.ru

Nijnikov Alexander Ivanovich — doctor of pedagogical sciences, professor, head of chair of the mathematical physics of the Moscow Pedagogical State University, honored worker of the higher school of the Russian Federation.

e-mail: ainizhnikov@mail.ru, nizhnikov.ai@mail.ru

THE EXECUTIVE SECRETARY:

Dobrovolsky Nikolai Nikolaevich — candidate of physical and mathematical sciences, assistant of the department of applied mathematics and computer science of the Tula State University; associate Professor of algebra, mathematical analysis and geometry of the Tula State L. N. Tolstoy Pedagogical University.

e-mail: cheb@tspu.tula.ru, nikolai.dobrovolsky@gmail.com

Rebrova Irina Yuryevna — candidate of physical and mathematical Sciences, associate professor, dean of the faculty of mathematics, physics and computer science, Tula State L. N. Tolstoy Pedagogical University, Tula.

e-mail: i_rebrova@mail.ru

THE MEMBERS OF THE EDITORIAL BOARD:

Artamonov Vyacheslav Alexandrovich — doctor of physical and mathematical sciences, professor, head of Higher algebra's chair of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: viacheslav.artamonov@gmail.com

Bykovsky Victor Alekseevich — doctor of physico-mathematical Sciences, correspondent member of RAS, Deputy Director of the Federal state institution of science, Institute of applied mathematics of the far Eastern branch of the Russian Academy of Sciences (IPM RAS) on scientific work, Director of the Khabarovsk branch of the IPM DVO RAS.

e-mail: vab@iam.khv.ru

Vostokov Sergey Vladimirovich — doctor of physical and mathematical Sciences, Professor, Professor of algebra and number theory Department of St. Petersburg University, President of the Foundation. L. Euler.

e-mail: sergei.vostokov@gmail.com

Gvozdev Alexander Evgenievich — doctor of technical sciences, professor, professor of Tula State Lev Tolstoy Pedagogical University.

e-mail: gvozdev.alexandr2013@yandex.ru

Georgievsky Dmitry Vladimirovich — Doctor of Physical and Mathematical Sciences, Professor, Head of Chair of Elasticity at Mechanical and Mathematical Department of the M. V. Lomonosov Moscow State University.

e-mail: georgiev@mech.math.msu.su

Gritsenko Sergey Alexandrovich — doctor of physical and mathematical sciences, professor of the chair Mathematics of the 1 Financial University under the Government of the Russian Federation, professor of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: s.gritsenko@gmail.com

Demidov Sergey Sergeyivich — doctor of physical and mathematical sciences, professor, professor of the department of probability theory of mechanics and mathematics of Moscow state University, head of the cabinet of history and methodology of mathematics and mechanics, head. department of history of physical and mathematical sciences of the Institute of history of science and technology RAS, editor-in-chief of "Historical and mathematical research president of the International Academy of history of science.

e-mail: serd42@mail.ru

Durnev Valery Georgievich — doctor of physical and mathematical Sciences, Professor, head of the Department of computer security and mathematical methods of data processing of the Yaroslavl state a public University. P. G. Demidov.

e-mail: durnev@univ.uniyar.ac.ru

Zubkov Andrey Mihailovich — doctor of physical and mathematical sciences, professor, full member of the Academy of cryptography of the Russian Federation, head of the chair of mathematical statistics and random processes mechanics and mathematics faculty Moscow state University of a name of M. of Century University, head of the Department of discrete mathematics Mathematical Institute. Century A. Steklov mathematical Institute RAS.

e-mail: zubkov@mi.ras.ru

Ivanov Valery Ivanovich — doctor of physical and mathematical sciences, professor, head of the chair of applied mathematics and Informatics of Institute of Applied Mathematics and Computer Science of the Tula State University.

e-mail: ivaleryi@mail.ru

Kartashov Vladimir Konstantinovich — candidate of physical and mathematical sciences, professor, head of the Department of algebra, geometry and Informatics of the Volgograd State Social and Pedagogical University.

e-mail: kartashovvk@yandex.ru

Korolev Maxim Aleksandrovich — doctor of physical and mathematical sciences, the leading researcher of the Department of Algebra and Number Theory of Steklov Mathematical Institute of RAS.

e-mail: korolevma@mi.ras.ru

Kuznetsov Valentin Nikolaevich — doctor of technical sciences, professor, professor of the department of applied mathematics and systems analysis, Saratov State Technical University.

e-mail: kuznetsovn@info.sgu.ru

Latyshev Viktor Nikolaevich — doctor of physical and mathematical sciences, professor, professor of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: latyshev@basis.math.msu.su

Matiyasevich Yuri Vladimirovich — doctor of physical and mathematical sciences, professor, full member of Russian Academy of Sciences, RAS Counselor of St. Petersburg department of Steklov Mathematical Institute of Russian Academy of Sciences, president of the St. Petersburg Mathematical society.

e-mail: yumat@pdmi.ras.ru

Mishchenko Sergey Petrovich — doctor of physical and mathematical sciences, professor, Professor, Department of applied mathematics of the Ulyanovsk State University.

e-mail: mishchenkosp@mail.ru

Nesterenko Yuri Valentinovich — doctor of physical and mathematical sciences, professor, corresponding member of RAS, head of number theory's chair of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: nester@mi.ras.ru

Panin Vladimir Alexeyevich — doctor of physical and mathematical sciences, professor, corresponding member Russian Academy of Natural Sciences, Rector of Tula State Lev Tolstoy Pedagogical University.

e-mail: tgpu@tula.net

Pachev Urusbi Mukhamedovich — doctor of physical and mathematical sciences, professor of algebra and differential equations Kabardino-Balkar State University. After H. M. Berbekov

e-mail: urusbi@rambler.ru

Semenov Alexey Lvovich — doctor of physico-mathematical Sciences, Professor, academician of the Russian Academy of Sciences, academician of the Russian Academy of education, head of Department of Mathematical logic and theory of algorithms, Moscow state University named after M. V. Lomonosov.

e-mail: alsemno@ya.ru

Fomin Aleksandr Aleksandrovich — doctor of physical and mathematical sciences, professor, head of the Department of algebra of the Moscow Pedagogical State University.

Chirsky Vladimir Grigoryevich — doctor of physical and mathematical sciences, associate professor, head of number theory's chair of the Moscow Pedagogical State University, professor of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.

e-mail: vgchirskii@yandex.ru

Allakov Ismail — doctor of physical and mathematical Sciences, Professor, Professor of Termez University, Uzbekistan.

e-mail: iallakov@mail.ru

Belov Alexey Yakovlevich — doctor of physical and mathematical sciences, federal professor, professor Bar Ilan University, Ramat Gan, Israel.

e-mail: Kanelster@gmail.com

Bernik Vasily Ivanovich (Belorussia) — doctor of physical and mathematical sciences, professor, the main researcher of the Belorussia Institute of Mathematics of NAS.

e-mail: bernik@im.bas-net.by

Kasyanov Pavel Olegovich (Ukraine) — doctor of physical and mathematical Sciences, head of the research department at Educational and Scientific Complex "Institute for Applied System Analysis" of the National Technical University of Ukraine "Kyiv Politechnic Institute" of the MES of Ukraine and NAS of Ukraine.

e-mail: kasyanov@i.ua

Laurinchikas Antanas (Lithuania) — Full member of the AS in Lithuania, doctor of physical and mathematical sciences, professor, head of probability theory's and number theory's chair of the Vilnius University.

e-mail: antanas.laurincikas@mif.vu.lt

Liu Yongping (China) — Ph.D, professor, head of the Research Center for Modern Analysis of Mathematics of the Beijing Normal University.

e-mail: ypliu@bnu.edu.cn

Misir Jumayil oglu Mardanov (Azerbaijan) — doctor of physical and mathematical sciences, professor, director of the institute of Mathematics and Mechanics of the National Academy of Sciences of Azerbaijan.

e-mail: rmi@lan.ab.az

Musin Oleg Rustamovich (USA) — doctor of physical and mathematical Sciences, Professor, Department of Mathematics, University of Texas at Brownsville, United States of America

e-mail: oleg.musin@utb.edu, omusin@gmail.com

Rahmonov Zarullo Huseinovich (Tajikistan) — doctor of physical and mathematical sciences, professor, corresponding member of the Republic of Tajikistan AS, director of the Institute of Mathematics of the Tajik AS.

e-mail: zarullo_r@tajik.net, zarullo-r@rambler.ru

Saliba Holem Mansour (Lebanon) — Ph.D. Assistant Professors of faculty of natural & applied sciences of Notre Dame University Louaize

e-mail: qwe123@rocketmail.com

Tabari Abdullo Habibullo (Tajikistan) — doctor of physical and mathematical sciences, professor, corresponding member of the Republic of Tajikistan AS, rector of the Kulob State University named after Abuabdullo Rudaki.

e-mail: rektor@kgu.tj

Fukshansky Lenny (USA) — Ph.D. in mathematics, Professor of mathematics, Claremont Mckenna College (California, USA).

e-mail: lenny@cmc.edu

Šiaučius Darius — professor, doctor of mathematics, senior researcher of Research Institute, Šiauliai University, Lithuania.

e-mail: darius.siauciunas@su.lt

THE MEMBERS OF THE INVITED EDITORIAL BOARD:

Bolsinov Alexey Viktorovich — doctor of science, professor, School of Mathematics, Loughborough University, GB, and Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: A.Bolsinov@lboro.ac.uk

Ivanov Alexander Olegovich — doctor of science, professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, and Chair FN-12, Bauman Moscow Technical University.

e-mail: aoiva@mech.math.msu.su

Kudryavtseva Elena Alexandrovna — doctor of science, professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: elena.a.kudryavtseva@gmail.com

Oshemkov Andrey Alexandrovich — doctor of science, professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: a@oshemkov.ru

Popelensky Theodore Yur'evich — candidate of science (PhD), assistant professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: popelens@gmail.com

Tuzhilin Alexey Avgustinovich — doctor of science, professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: tuz@mech.math.msu.su

Shafarevich Andrey Igorevich — corresponding member of RAS, doctor of science, professor, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

e-mail: shafarev@yahoo.com

TABLE OF CONTENTS

Volume 21 Issue 1

From the editor	3
T. Ayano, V. M. Buchstaber. Analytical and number-theoretical properties of the two-dimensional sigma function	9
A. Ya. Belov–Kanel, A. M. Elishev, F. Razavinia, Yu Jie–Tai, Wenchao Zhang. Noncommutative Białynicki-Birula Theorem	51
V. V. Beniash–Kryvets, A. N. Admiralova. On representation varieties of some one-relator products of cyclic groups	62
E. M. Vechtomov, D. V. Chuprakov. Finite cyclic semirings with semilattice additive operation defined by two-generated ideal of natural numbers	82
S. B. Gashkov, I. S. Sergeev. Multiplication	101
V. A. Gorelov. On algebraic identities between solution matrices of generalized hypergeometric equations	135
E. I. Deza, B. Mhanna. On special properties of some quasi-metrics	145
N. N. Dobrovol'skii, I. Yu. Rebrova, N. M. Dobrovol'skii. Inverse problem for a monoid with an exponential sequence of Prime numbers	165
V. G. Durnev, O. V. Zetkina, A. I. Zetkina. On elementary theories of algebraically closed groups	186
P. L. Ivankov. On representation varieties of some one-relator products of cyclic groups	200
N. I. Kalosha, I. A. Korlyukova, E. V. Guseva. Intervals of small measure containing an algebraic number of given height	213
M. A. Korolev. Kloosterman sums with primes and the solvability of one congruence with inverse residues — II	221
N. V. Maksimenko. The space of Dirichlet series to multivariate lattices and the algebra of Dirichlet series of grids, repetitive multiplication	233
I. A. Martyanov. Nikolskii constant for trigonometric polynomials with periodic Gegenbauer weight ...	247
Yu. V. Matiyasevich. Asymptotic structure of eigenvalues and eigenvectors of certain triangular Hankel matrices	259
V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov. Periodic elements $\sqrt{f}$ in elliptic fields with a field of constants of zero characteristic	273
V. I. Subbotin. On the completeness of the list of convex RR -polyhedra	297
L. A. Tolokonnikov, T. S. Nguyen. Determination of the displacement field in an inhomogeneous coating of an elastic plate when passing through her plane sound wave	310
G. V. Fedorov. On families of hyperelliptic curves over the field of rational numbers whose Jacobian contains torsion points of given orders	322
V. N. Chubarikov. On a mean-value theorem for multiple trigonometric sums	341
Yu. N. Shteinikov. On the size of the set of the product of sets of rational numbers	357
BRIEF MESSAGE	
A. V. Begunts, D. V. Goryashin. On the values of Beatty sequence in an arithmetic progression	364

S. V. Vostokov, R. P. Vostokova, E. V. Ikonnikova. The Hensel–Shafarevich canonical basis in Honda formal modules	368
R. V. Pocherevin. On generalization of mean value	374
I. A. Proskurnin. Minimal morsifications for functions of two real variables	381
HISTORY OF MATHEMATICS AND APPLICATIONS	
Yu. A. Basalov. About the Russian scientific school of diophantine approximations	388
MEMORABLE DATE	
V. N. Chubarikov, V. G. Cherskii, E. I. Deza, I. N. Baoulina, L. V. Kotova, E. V. Neiskashova, V. S. Vankova, N. M. Dobrovolskii, I. Yu. Rebrova, A. L. Roshchenya. Vassiliy Ilyich Nechaev. To the 100-th anniversary	404
РЕДКОЛЛЕГИЯ	415
THE EDITORIAL BOARD	419