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 XIX

Выпуск 3 (67)

Тула
2018

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

Каталог «Пресса России»
Подписной индекс 10642

Адрес редакции: 300026, г. Тула, пр. Ленина, 125, каб. 310
Тел: +79156812638, 8(4872)374051

E-mail: cheb@tsput.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.

Выпуск осуществлен при финансовой поддержке Минобрнауки России в рамках государственного контракта № 14.597.11.0035

Журнал выходит под эгидой Министерство 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 университета, Тульского государственного университета.

От редакции

Данный выпуск Чебышевского сборника посвящен выдающемуся советскому математику, академику АН СССР, доктору физико-математических наук, профессору
Юрию Владимировичу Линнику.

Сборник открывается статьёй о жизни и научной деятельности Юрия Владимировича Линника.

СОДЕРЖАНИЕ

Том 19 Выпуск 3

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 51(09) DOI 10.22405/2226-8383-2018-19-3-7-19

О жизни и творчестве Юрия Владимировича Линника

Ибрагимов Ильдар Абдуллович — Академик РАН, доктор физико-математических наук, профессор, Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН.
e-mail: ibr32@pdmi.ras.ru
Мороз Борис Зеликович — доктор физико-математических наук, профессор кафедры дискретной математики Московского Физико-Технического Института, Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН, Россия; Universität Bonn, Германия.
e-mail: moroz@pdmi.ras.ru

Аннотация

Статья посвящена жизни и научной деятельности выдающегося советского математика, академика АН СССР, доктора физико-математических наук, профессора Юрия Владимировича Линника.

Ключевые слова: Юрий Владимирович Линник.

Библиография: 9 названий.

Для цитирования:
И. А. Ибрагимов, Б. З. Мороз. О жизни и творчестве Юрия Владимировича Линника // Чебышевский сборник, 2018, т. 19, вып. 3, с. 7–19.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 51(09) DOI 10.22405/2226-8383-2018-19-3-7-19

On the life and work of Yuri Vladimirovich Linnik

Ibragimov Il'dar Abdullovich — Member of the Russian Academy of Sciences, Doctor of physico-mathematical sciences, Professor, St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences.
e-mail: ibr32@pdmi.ras.ru
Moroz Boris Zelikovich — Doctor of physico-mathematical sciences, St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Russia; Universität Bonn, Germany.
e-mail: moroz@pdmi.ras.ru

Abstract

The article is devoted to the life and scientific activity of the outstanding Soviet mathematician, academician of the USSR Academy of Sciences, doctor of physics and mathematics, Professor Yuri Vladimirovich Linnik.

Keywords: Yuri Vladimirovich Linnik.

Bibliography: 9 titles.

For citation:
I. A. Ibragimov, B. Z. Moroz, 2018, "On the life and work of Yuri Vladimirovich Linnik", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 7–19.

1.

Блестящий математик и замечательный широко образованный человек, Юрий Владимирович Линник (1915–1972) был ярким представителем петербургской школы теории чисел. В юности на него оказали некоторое влияние петербургские математики Борис Алексеевич Венков (1900–1962) и Владимир Абрамович Тартаковский (1901–1973), но он рано нашёл свою дорогу, став доктором физико-математических наук уже в 1940-м году.

Остановимся на некоторых этапах его жизненного пути (ср. [3]). Ю. В. Линник родился 8 января 1915 г. в городе Белая Церковь. Его родители — Владимир Павлович и Мария Абрамовна Линник были учителями. В. П. Линник (1889–1984), отец Юрия Владимировича, стал впоследствии известным физиком ("телескоп Линника") и был избран академиком АН СССР.

В 1932 г., возможно, под влиянием своего отца, Юрий Владимирович поступил на физический факультет Ленинградского университета, но по окончании третьего курса, "чувствуя неодолимое влечение к высшей арифметике" (как он писал в своей автобиографии), перешёл на математико-механический факультет ЛГУ, который и закончил в 1938 г.

Военные годы не обошли Ю. В. Линника. В 1939 г. он был призван в Красную Армию и зимой 1939–1940 гг. принимал участие в войне с Финляндией в качестве командира артиллерийского взвода (Юрий Владимирович всегда называл эту войну несправедливой в своих разговорах с И. А.). В июле 1941 г. он заболел дистрофией, был демобилизован и эвакуирован в Казань, где тогда располагался МИАН (стоит ещё раз упомянуть, что между двумя войнами, в 1940 г., Юрий Владимирович защитил кандидатскую диссертацию по теории чисел, за которую ему сразу была присуждена степень доктора физико-математических наук).

Ю. В. Линник вернулся в Ленинград в 1945 г., где до конца своих дней работал в ЛОМИ (:= Ленинградское отделение МИАН) и в Ленинградском университете.

В ЛОМИ работал семинар по теории чисел под руководством Юрия Владимировича. Этот семинар посещали, в частности, А. Н. Андрианов, А. И. Виноградов, Е. П. Голубева, А. Ф. Иванов, А. В. Малышев, Б. З. Мороз, Б. Ф. Скубенко, О. М. Фоменко, В. М. Цветков и Н. Г. Чудаков. Николай Григорьевич Чудаков (1904–1986) приехал в Ленинград из Саратова по приглашению Ю. В. Линника и проработал в ЛОМИ около десяти лет.

Ю. В. Линник создал и возглавил лабораторию статистических методов в ЛОМИ и кафедру теории вероятностей и математической статистики на математико-механическом факультете ЛГУ (заведование последней он позднее передал В. В. Петрову). Мы точно не знаем, когда был организован вероятностный семинар Ю. В. Линника. Когда И. А. начал посещать этот семинар осенью 1953 г., среди его участников были Н. Н. Воробьёв, Н. А. Сапогов, О. В. Сарманов, В. П. Скитович (незадолго до этого доказавший знаменитую "теорему Скитовича — Дармуа").

Юрий Владимирович уделял большое внимание преподавательской деятельности, общению с молодыми математиками. В ЛГУ он читал лишь вероятностые курсы – теорию случайных процессов (позднее Юрий Владимирович поручил читать этот курс И. А.), курс теории

вероятностей для механиков (почему-то он больше любил читать этот курс механикам, чем математикам), математическую статистику. Этот последний курс он особенно любил и читал его каждый год вплоть до своей кончины (Б. З. познакомился с Юрием Владимировичем после первого часа одной из лекций по математической статистике). В течение некоторого времени в ЛОМИ работал учебный семинар, организованный по инициативе (и с участием) Юрия Владимировича, целью которого было, разобраться в новейших работах по алгебраической геометрии. К сожалению, достичь этой цели участникам семинара не удалось. Начав с учебников по комбинаторной топологии, мы (Б. З. был одним из участников этого семинара) добрались до теории пучков, но не до схем Гротендика. Ю. В. Линник нашёл однако применение теории функций многих комплексных переменных и, в частности, теории пучков в математической статистике.

Когда в 60-х годах очередной административный приказ запретил сотрудникам Академии Наук совместительство в вузах, вплоть до отмены этого нелепого запрета, в течение 2-х лет, Юрий Владимирович преподавал бесплатно.

В середине 50-х годов начинают восстанавливаться связи советских математиков с зарубежными коллегами. К этому времени относится первый визит Ю. В. Линника за границу, в Индию. Юрий Владимирович всегда придавал большое значение личным контактам между учёными разных стран (позднее, в 60-е годы, на заседании семинара по теории чисел, он както, говоря о зарубежных математиках, между прочим, сказал: "Они не умнее нас, но у них — связь со всем миром"). Тесные, порою дружеские отношения установились у него со многими крупнейшими специалистами по теории чисел и теории вероятностей.

Ю. В. Линник был первым президентом Ленинградского математического общества (1959–1965).

Заслуги Ю. В. Линника были высоко оценены. Он был избран членом-корреспондентом АН СССР в 1954 г. и академиком в 1963 г. В 1947 г. ему была присуждена Государственная премия за работы по аналитической теории чисел, а в 1970 г. — Ленинская премия (совместно с И. А. Ибрагимовым, Ю. В. Прохоровым и Ю. А. Розановым) за работу по предельным теоремам теории вероятностей. В 1970 г. он был удостоен звания Героя Социалистического Труда. В 1962 г. Ю. В. Линник был приглашённым докладчиком на Международном Математическом Конгрессе в Стокгольме; в докладе на этом конгрессе Юрий Владимирович сформулировал свою знаменитую, до сих пор не доказанную гипотезу о суммах сумм Клоостермана. Многие университеты, академии, научные общества избрали Ю. В. Линника своим почётным членом.

Юрий Владимирович был очень ярким, разносторонне одарённом человеком. Он свободно владел многими языками и писал стихи на русском, французском и немецком языках. Имел обширнейшие познания в литературе и истории, особенно военной. Живо интересовался политическими событиями. Приведём одну из любимых шуток Юрия Владимировича.

Теорема. *Генеральная линия партии — прямая.*

Доказательство. Действительно, она вся состоит из точек перегиба.

Однако главным делом жизни Ю. В. Линника, которому он отдавался весь, отдавался страстно, темпераментно, было научное творчество. Трудолюбие его было необычайно, но труд этот был источником радости. Юрий Владимирович всегда любил ту работу, которой он был занят в данный момент и почти по-детски гордился, даже чуть-чуть хвастался своими достижениями данного момента. То, что уже было сделано, волновало его мало. При встрече Юрий Владимирович немедленно начинал рассказывать вам, какую замечательную вещь он сейчас придумал, лучшую в своей жизни. Иногда собеседник припоминал, что, кажется, лучшую в своей жизни вещь Юрий Владимирович сделал три дня назад. Юрий Владимирович искренне недоумевал: "О чём это Вы? Ах, это... Ну, это пустяки. Вот то, что я сейчас сделал, вот это да". К Ю. В. Линнику, как нельзя лучше, подходят слова Ф. Клейна: "И всё-таки тайна продвижения вперёд лежит в наивном творчестве, возникающем из чистой радости

того дела, к которому толкает творцов их мысль". Читая работы Ю.В. Линника, видишь в них те "орудия первооткрывателей" , в которых Г. Вейль отказал Ф. Клейну — "изощрённую тонкость математической мысли, головоломные трюки, позволяющие доказывать результаты, ещё определённо не созревшие для того, чтобы можно было уяснить их исходные принципы" (Г. Вейль, Феликс Клейн и современная математика. Избранные труды, М., Наука, 1984).

Скончался Юрий Владимирович Линник 30 июня 1972 года от инфаркта миокарда. Более 46-и лет отделяют нас от того знойного июньского дня, когда он ушёл из жизни. Оглядываясь назад, мы видим, сколь многим обязаны Ю. В. Линнику математики Ленинграда, круг же тех, на кого повлияли его идеи, созданные им методы исследования, много шире непосредственного круга его учеников и сотрудников.

2.

Вот что пишет о нашем учителе Аскольд Иванович Виноградов (1929–2005), один из лучших учеников и коллег Юрия Владимировича [2]:

"Всё творчество Ю. В. Линника в области теории чисел можно разбить на несколько периодов, в каждом из которых он интересовался определённым кругом проблем.

Самый первый юношеский интерес его связан с задачей представления целого числа тернарной квадратичной формой определённого типа. Здесь сказалось влияние проф. Б. А. Венкова, который читал тогда в ЛГУ курс теории чисел, и личные интересы которого лежали в этой области, восходящей ещё к Гауссу.

Затем его интересы начали смещаться в сторону кругового метода Харди — Литтльвуда и метода тригонометрических сумм И. М. Виноградова.

В 1940 г. он заинтересовался гипотезой И. М. Виноградова о наименьшем невычете, ставшей в дальнейшем одной из любимых его проблем, над которой он размышлял до конца жизни. В 1941 г. он публикует заметку в Докладах Академии наук СССР, где доказвает, что гипотеза И. М. Виноградова верна для всех модулей, кроме, быть может, ограниченного множества. Эта статья называлась большое решето, и её ждала блестящая судьба. Проблемы, которые были заключены в этой статье, породили целое научное направление, и к настоящему времени оно является ведущим в теории чисел, давшим сотни научных статей и десятки книг во всём мире. Идеи этой статьи позволили доказать в середине 60-х годов арифметический аналог расширенной гипотезы Римана (РГР), а так как с РГР связан почти необозримый круг проблем в теории чисел, то становится понятным, почему так необычна судьба этой маленькой заметки.

В военные годы Ю. В. Линник публикует ряд глубоких работ по методу И. М. Виноградова, где связывает этот метод с p-адической арифметикой локальных полей и получает оценку полиномиальной суммы Г. Вейля с понижающей степенью $1/n^2 \log n$, где n — степень полинома. Эти идеи получили дальнейшее развитие в работах А. А. Карацубы.

В эти же годы Юрий Владимирович изучает теорию L-рядов Дирихле и начинает сравнивать метод L-рядов с методом И. М. Виноградова. Он пытался в это время ответить на вопрос, можно ли получить оценку И. М. Виноградова для сумм по простым числам с помощью плотностных теорем для L-рядов. Такая постановка вопроса оказалась в высшей степени плодотворной. Она позволила ему создать новые методы как в мультипликативной, так и в аддитивной теории чисел. Эти поиски привели его в 1944 г. к ныне знаменитой теореме о наименьшем простом в арифметической прогрессии. В серии этих исследований он создал новый плотностной метод в d-аспекте, который потом усиленно развивался как у нас, так и за рубежом. Вышло в свет много работ, в которых авторы пытались снизить константу Линника (показатель степени модуля d, которого не превосходит минимальное простое).

Эта теорема Ю. В. Линника свидетельствует о благотворном влиянии метода И. М. Ви-

ноградова на мультипликативную теорию чисел. Но уже в 1946 г. Юрий Владимирович понял, что существует и обратная связь. К этому времени ему удалось доказать, что оценка И. М. Виноградова для простых чисел действительно может быть получена методом плотностных теорем. Это позволило ему дать новое доказательство знаменитой теоремы Виноградова — Гольдбаха о трёх простых. Тем самым он обогатил методы аддитивной теории чисел за счёт идей, заимствованных из мультипликативной теории чисел.

В этой серии работ Линник развил плотностной метод L-рядов в t-аспекте. Отметим, что t- и d-аспекты, развитые Ю. В. Линником в теории L-рядов, различны по своей природе. Первый аспект касается аналитической природы L-функций Дирихле, так как t — это мнимая часть аналитического параметра s. Второй аспект связан с арифметической природой L-рядов, так как d — это модуль характера Дирихле. Оба эти аспекты успешно развивались многими авторами, но шли параллельно друг другу, пока, наконец, в начале 70-х годов не объединились под шапкой "большого решета" в интерпретации Х. Монтгомери.

Надо отметить, что на военные годы (1943 г.) падает и его знаменитое элементарное решение проблемы Варинга, ставшее широко известным благодаря книге А. Я. Хинчина "Три жемчужины теории чисел".

В конце 40-х — начале 50-х годов Ю. В. Линник много размышлял над бинарной проблемой Гольдбаха. Он обнаружил, что круговой метод вместе с РГР не достаёт до этой проблемы. Не хватало совсем немного — последовательности логарифмической плотности. Эти размышления породили серию работ. Отметим две из них, которые являются итоговыми: "Некоторые условные теоремы, касающиеся бинарной проблемы Гольдбаха" (1952 г.) и "Складывание простых чисел со степенями одного и того же числа" (1953 г.).

В середине 50-х годов Юрий Владимирович снова возвращается к своим юношеским увлечениям тернарными формами. Он продолжает и развивает свои довоенные идеи. Главным отличием этих исследований от довоенных является их эргодический харатер. В это время его интересует не только общее количество целых точек на всей сфере, но и распределение их на отдельных кусках её. В этой серии работ ему удалось установить фундаментальный факт — равномерность распределения целых точек на сфере (совместно с А. В. Малышевым). Итоговым трудом этого цикла является его работа "Асимптотико-геометрические и эргодические свойства множества целых точек на сфере" (1957 г.).

В это же время он обдумывал и проблему распределения целых точек на гиперболоидах. Эта задача тесно связана с арифметикой бинарных квадратичных форм. Если взять класс таких форм с фиксированным дискриминантом, а коэффициенты этих форм трактовать как свободные параметры, то мы получим гиперболоид. Если ограничиться только приведёнными формами, то гауссовские условия приведения вырежут на гиперболоиде некомпактную область приведения. Число целых точек в этой области будет совпадать с числом различных форм с одним и тем же дискриминантом. Естественно поставить вопрос о том, сколько будет целых точек в некоторой части области приведения. Это аналог вопроса о целых точках на кусках сферы. Но если там можно было рассматривать сферу в обычном евклидовом пространстве, то здесь евклидова геометрия уже не работает. Нужно погрузить гиперболоид в неевклидово пространство и воспользоваться метрикой Лобачевского. Сама идея перехода к неевклидовой метрике была высказана Б. А. Венковым в 1951 г. Ю. В. Линник существенно развил её и дополнил. Отметим, что в этом направлении существует принципиальная разница между случаями двуполостного и однополостного гиперболоидов.

Первый случай отвечает положительно определённым бинарным квадратичным формам, или, другими словами, мнимым квадратичным полям.

Второй — неопределённым формам, или вещественным квадратичным полям. Принципиальную разницу вносит имеющая бесконечный порядок единица вещественного поля, которой нет в мнимых полях. Сам Юрий Владимирович исследовал эргодические свойства двуполост-

ного гиперболоида, а его ученик Б. Ф. Скубенко — однополостного. Отметим главную работу этой серии "Асимптотическое распределение приведённых бинарных квадратичных форм в связи с геометрией Лобачевского" (1955 г.).

В конце 50-х — начале 60-х годов Ю. В. Линник создаёт новый, дисперсионный метод в теории чисел. В 1960 г. он решил этим методом известную проблему Харди — Литтльвуда о представимости каждого целого числа суммой простого и двух квадратов. Суть этого метода кратко в следующем. Чаще всего мы не можем вычислить асимптотику арифметической функции в прогрессии с большим модулем. Но иногда возникает возможность вычислить дисперсию этой суммы по всем большим модулям. Юрий Владимирович заметил, что этого достаточно для многих проблем и, в частности, для проблемы Харди — Литтльвуда. Именно поэтому метод и был назван дисперсионным, хотя с вероятностными методами, по существу, нет никакой связи. Идеи этого метода были изложены им в серии работ конца 50-х — начала 60-х годов. Полное представление об этом методе можно получить, прочитав его монографию "Дисперсионный метод в бинарных аддитивных задачах" (1961 г.). С этого времени и до конца жизни он несколько раз возвращался к этому методу, развивая и дополняя его.

В середине 60-х годов Ю. В. Линник в третий раз вернулся к проблематике тернарных форм. На этот раз толчком к этому послужила короткая заметка в Докладах Академии наук СССР "Гиперэллиптические кривые и наименьший простой квадратичный вычет" (1966 г.). В ней было показано, что этот вычет имеет порядок корня 4-й степени из модуля. Это существенно упрощало всю теорию тернарных форм, развитую Ю. В. Линником в двух предыдущих периодах. В то время сильно сказывалась "нехватка" малых простых вычетов. Тогда не удавалось показать, что они лежат ниже корня квадратного из модуля. Это обстоятельство усложнило метод и сделало его громоздким в техническом отношении, так как приходилось "обходить" большие вычеты. После заметки 1966 г. эти сложности обхода пропали. Теория стала прозрачной и красивой. Юрий Владимирович изложил её в монографии "Эргодические свойства алгебраических числовых полей" (1967 г.). В это же время он обнаружил эргодические свойства дисперсионного метода. Это сочетание геометрии с дисперсионным методом породило серию работ, выполненных совместно с Б. М. Бредихиным. Отметим главную из них "Асимптотика и эргодические свойства решений обобщённого уравнения Харди — Литтльвуда" (1967 г.), где эти идеи изложены наиболее подробно.

В конце жизни он понял, что с помощью дисперсионного метода можно получить элементарное доказательство теоремы Виноградова — Гольдбаха о трёх простых. Эта находка изложена в его последней работе по теории чисел "Новый метод в аналитической теории чисел" совместно с Б. М. Бредихиным, которая вышла после его смерти, в 1974 г., в сборнике "Актуальные проблемы аналитической теории чисел" .

Сейчас ясно, что теоретико-числовые работы Ю. В. Линника во многом определили лицо современной теории чисел, особенно той её части, которая касается L-рядов и плотностных методов."

Эти строки были написаны 13 лет назад. Юрий Владимирович Линник по-прежнему остаётся одним из самых цитируемых ленинградских математиков.

3.

В 1947 г. вышла в свет первая работа Ю. В. Линника по теории вероятностей. С этого времени, не прекращая интенсивных и весьма плодоворных исследований по теории чисел, Юрий Владимирович не менее активно работал в теории вероятностей и статистике. Однажды И. А. спросил Юрия Владимировича, почему он начал работать в теории вероятностей. Отвечая, Ю. В. Линник сказал, что определённую роль тут сыграл А. Я. Хинчин, убеждавший его, что работать нужно по крайней мере в двух разных областях и что такой дополнитель-

ной областью могла бы быть теория вероятностей. Были, по-видимому, и другие причины. Ю. В. Линник был выдающимся аналитиком, которого привлекали трудные аналитические проблемы теории чисел и теории вероятностей.

Петербург—Петроград—Ленинград всегда был выдающимся центром исследований в области теории вероятностей. Достаточно заметить, что здесь работали, сменяя друг друга, П. Л. Чебышев, А. А. Марков, А. М. Ляпунов, С. Н. Бернштейн. Однако в военные и послевоенные годы, хотя в Ленинграде и работали прекрасные специалисты, ученики С. Н. Бернштейна, Н. А. Сапогов и О. В. Сарманов, организованная деятельность в области теории вероятностей как научная, так и образовательная, практически прекратилась. Можно смело сказать, что Петербургская—Ленинградская школа теории вероятностей была заново воссоздана Ю. В. Линником. Как отмечалось выше, им была создана кафедра теории вероятностей и математической статистики в Ленинградском университете, лаборатория статистических методов в ЛОМИ, заработал постоянный городской семинар по теории вероятностей (работа его продолжается и по сей день), появились молодые учёные, сперва ученики Линника, а потом и ученики его учеников.

Перечислим вкратце основные циклы работ Юрия Владимировича по теории вероятностей и статистике, остановившись более подробно на работах по теории больших уклонений и арифметике законов распределения (здесь мы следуем [3]).

3.1. Предельные теоремы для сумм независимых случайных величин.

Изучение предельного поведения распределений сумм

$$\xi = \sum_{j=1}^{n} \xi_j$$

независимых случайных величин ξ_j при $n \to \infty$ есть классический сюжет теории вероятностей. Допустим, что все ξ_j имеют одинаковое распределение, конечное среднее $a = \mathbf{E}\xi_j$ и дисперсию $\sigma^2 = \mathbf{D}\xi_j$. Пусть

$$Z_n = \frac{1}{\sigma n^{1/2}} \sum_{j=1}^{n} (\xi_j - a)$$

и

$$\Phi(x) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^{x} e^{-u^2/2} du.$$

В силу центральной предельной теоремы (в данном случае теоремы П. Леви)

$$\mathbf{P}(Z_n < x) \to \Phi(x) \ \text{ и } \ \mathbf{P}(Z_n \geq x) \to 1 - \Phi(x) \ \text{ при } \ n \to \infty. \tag{1}$$

Более того, если вдобавок $\mathbf{E}|\xi_j|^3 < \infty$, то (теорема Ессена !) разность между допредельным и предельным выражениями в (1) есть $O(n^{-1/2})$. Однако в целом ряде задач математической статистики и в ряде разделов современной теории вероятностей во многих случаях требуется знать поведение левых частей в (1) при бóльших x (т.е. при $x \to \infty$ вместе с n). Такие задачи называют задачами о вероятностях больших уклонений. Классические предельные теоремы (1) практически не дают никакой полезной информации, поскольку с ростом x функция $1-\Phi(x)$ убывает, как e^{-x^2}. Определённый выход из этого положения приносит теорема Г. Крамера, опубликованная в 1938 г. По воспоминаниям И. А. первый интерес Ю. В. Линника к задачам о вероятностях больших уклонений был связан с желанием понять, насколько необходимо в теореме Крамера весьма ограничительное условие

$$\mathbf{E}\exp(a|\xi_j|) < \infty \ \text{ для какого-нибудь положительного числа a.} \tag{C}$$

В определённом смысле до работ Ю. В. Линника в том, что касается поведения вероятностей больших уклонений для сумм независимых случайных величин, практически ничего, кроме теоремы Крамера не было (т.е. были, разумеется, различные обобщения теоремы Крамера, распространение этой теоремы на неодинаково распределённые слагаемые и т.д., но все они имели ту же структуру и существенно использовали условие (C)). Ю. В. Линник получил ряд новых предельных теорем. Мы приведём две самые простые по формулировке и очень красивые теоремы.

Теорема 1. *Пусть для любого* $\alpha < 1/2$

$$\frac{\mathbf{P}(Z_n > x)}{1 - \Phi(x)} \to 1 \quad и \quad \frac{\mathbf{P}(Z_n < -x)}{\Phi(-x)} \to 1 \quad при \quad n \to \infty \tag{2}$$

равномерно в интервале $0 \le x \le n^{\alpha}$. *Тогда случайные величины* ξ_j *нормальны.*

Теорема 2. *Пусть монотонно возрастающая функция* $\rho(n) \to \infty$. *Если* $\alpha < 1/6$ *и соотношение* (2) *выполняется равномерно в интервале* $0 \le x \le n^{\alpha}\rho(n)$, *то*

$$\mathbf{E}|\xi_j|^{4\alpha(2\alpha+1)^{-1}} < \infty. \tag{3}$$

Более того, условие (3) *достаточно для выполнения* (2) *равномерно в интервале* $0 \le x \le n^{\alpha}\rho(n)^{-1}$. *Если* $1/6 \le \alpha < 1/2$, *рассмотрим последовательность*

$$\{\frac{s+1}{2(s+3)} \mid s \in \mathbb{N}\}.$$

Пусть

$$\frac{s+1}{2(s+3)} \le \alpha < \frac{s+2}{2(s+4)}.$$

Если соотношение (2) *выполняется равномерно в интервале* $0 \le x \le n^{\alpha}\rho(n)$, *то выполнено* (3) , *и все моменты* $\mathbf{E}|\xi_j|^k$ *при* $k \le s+3$ *совпадают с моментами закона Гаусса.*

В последующих работах (С. В. Нагаев, Л. В. Осипов) удалось заменить $\rho(n)$ на 1.

3.2. Предельные теоремы для неоднородной цепи Маркова.

Проблема, заинтересовавшая Ю. В. Линника, восходит к исследованиям А. А. Маркова начала двадцатого века. В работе 1910 г. Марков рассматривает последовательность случайных величин $\{X_j\}$, связанных в неоднородную цепь Маркова с вероятностями перехода $p_{ij}^{(n)}$ и конечным числом состояний. Марков доказал, что если

$$\alpha(n) = \inf_{ij} p_{ij}^{(n)} \ge \alpha_0 > 0,$$

а число состояний равно двум, то к последовательности $\{X_j\}$ применима центральная предельная теорема (ЦПТ). Трудную задачу о применимости ЦПТ при нарушении его условий Марков оставил будущим исследователям.

Задача Маркова чрезвычайно заинтересовала С. Н. Бернштейна, который посвятил ей серию работ 20-30-х годов. Основной вопрос, рассмотренный в этих работах, сводится к следующему: может ли $\alpha(n)$ стремиться к нулю и если да, то как быстро? Пусть, например, $\alpha(n) \ge n^{-\beta}$. При каких показателях β выполняется ЦПТ? С. Н. Бернштейн показал, что условие $\beta \le 1/3$ необходимо. В серии работ 20-х годов С. Н. Бернштейн постепенно увеличивал показатель β: $1/7$, $1/5$,..., доведя его в итоге до $\beta \le 1/3$.

В перечисленных исследованиях всё время предполагалось, что число состояний равно двум, и это предположение было существенным. Проблема заключалась в том, что для цепей с бóльшим числом состояний не удавалось доказать, что дисперсия сумм

$$\sum_{j=1}^{n} X_j$$

с ростом n растёт достаточно быстро. Вообще при изучении предельных распределений для сумм зависимых величин анализ роста дисперсии и по сю пору — один из труднейших и важнейших аспектов проблемы. Лишь в 1936 г. С. Н. Бернштейн, создав новый метод исследования цепей Маркова ("метод сечений"), установил точные нижние границы дисперсии

$$B_n^2 = \mathbf{D}\sum_{j=1}^{n} X_j.$$

В 1949 г. Ю. В. Линник после глубокого обобщения метода сечений Бернштейна смог для цепей с произвольным конечным множеством состояний доказать достаточность условия $\beta \leq 1/3$. Тем самым 40-летняя история исследования задачи Маркова в определённом смысле завершилась.

3.3. Арифметика законов распределения.

Пусть X — случайная величина с функцией распределения F. Зададимся вопросом, когда X можно представить в виде суммы двух нетривиальных независимых случайных величин: $X = X_1 + X_2$. Так как функция распределения F есть свертка функций распределения F_1 и F_2 слагаемых X_1 и X_2, задаче можно придать следующую форму. Когда функцию распределения F можно представить в виде "произведения"$F = F_1 * F_2$ и каковы свойства множителей F_1, F_2? Так как свертке F_1 и F_2 соответствует произведение их характеристических функций $f_1(t)$ и $f_2(t)$, то исходный вопрос эквивалентен следующему. Когда характеристическую функцию $f(t)$ распределения F можно представить в виде произведения$f(t) = f_1(t)f_2(t)$ и каковы свойства компонент $f_1(t), f_2(t)$?

В 1936-м Г. Крамер доказал, что компоненты разложения F_1 и F_2 закона Гаусса F необходимо являются законами Гаусса, а годом позже Д. А. Райков доказал сходную теорему о распределениях Пуассона: компоненты разложения F_1 и F_2 закона Пуассона F необходимо являются законами Пуассона. Множество I всех вероятностных распределений на прямой образуют полугруппу относительно операции свертки. Пусть $F \in I$; естественно назвать F простым элементом полугруппы I, если его нельзя представить в виде $F = F_1 * F_2$ с нетривиальными F_1, F_2 из I. Обозначим через I_0 подмножество вероятностных распределений, не имеющих простых делителей. Из теорем Г. Крамера и Д. А. Райкова следует, что множество I_0 не пусто. По теореме А. Я. Хинчина (1937 г.), любой элемент F полугруппы I представим в виде

$$F = F_0 * F_1 * F_2 * ...,$$

где $F_0 \in I_0$, а $F_1, F_2, ...$ суть простые множители. Более того, А. Я. Хинчин доказал, что элементы множества I_0 безграничны делимы. В частности, если $F \in I_0$, то характеристическая функция $f(t)$ распределения F представима в виде

$$f(t) = \exp[i\alpha t - \frac{1}{2}\sigma^2 t^2 + \int_{-\infty}^{\infty}(e^{itu} - 1 - \frac{itu}{1+u^2})dG(u)], \tag{4}$$

где $\{\alpha, \sigma\} \subseteq \mathbb{R}$, $\sigma \geq 0$, а G — монотонно не убывающая непрерывная в нуле функция ограниченной вариации. Гауссовскому распределению соответствует в разложении (4) тождественно

равная нулю функция G; у распределения Пуассона $\sigma = 0$, а мера сосредочена в одной точке (отличной от нуля). Примерно таким было состояние арифметики законов распределения к 1940-му году, и вплоть до середины 1940-х годов, до работ Ю. В. Линника, ничего существенно нового здесь не прибавилось. В частности, были известны лишь два подмножества множества I_0 — множество распределений Гаусса и множество распределений Пуассона. Ю. В. Линник доказал, что всякая композиция законов Гаусса и Пуассона имеет своими делителями лишь композиции законов Гаусса и Пуассона. Доказательство этой теоремы в отличие от теорем Крамера и Райкова очень сложно. Впоследствии И. В. Островский нашёл более простые варианты доказательства, но и они достаточно сложны. Ю. В. Линник доложил об этом результате на семинаре В. И. Смирнова; во время его доклада кто-то сказал: "Я не понимаю, как Вы вообще могли до этого додуматься". Совершенно серьёзно и с некоторой гордостью Юрий Владимирович ответил: "Трое суток думал". Он действительно имел в виду трое суток, а не три дня. После результата о разложении законов Гаусса и Пуассона Ю. В. Линник занялся собственно арифметикой законов распределения, попытавшись разобраться в структуре множества I_0. В 1958 — 1959 гг. он публикует три большие работы под заглавием "Общие теоремы о разложении безгранично делимых законов" , посвящённые исследованию структуры этого множества. В частности, он получает следующий замечательный результат, теорему о принадлежности классу I_0 законов с ненулевой гауссовой компонентой (т.е. с $\sigma > 0$). Назовём множеством Линника множество вида

$$\{\mu_k, \lambda_k \mid k \in \mathbb{Z}, \{\mu_{k+1}\mu_k^{-1}, \lambda_{k+1}\lambda_k^{-1}\} \subseteq \mathbb{N} \setminus \{1\}\}$$

при некоторых вещественных $\mu_0 > 0$ и $\lambda_0 < 0$.

Теорема 3. *Для того чтобы распределение с характеристической функцией, задаваемой равенством* (4) *с* $\sigma > 0$, *принадлежало множеству* I_0, *необходимо, чтобы носитель функции* G *был подмножеством некоторого множества Линника.*

Класс безгранично делимых законов с характеристической функцией, задаваемой равенством (4), у которых носитель функции G есть множество Линника называется классом Линника и обозначается через $\mathcal{L}$. Доказательство этой теоремы сложно и даже сейчас занимает около 50-ти страниц. Полное обращение этой теоремы невозможно. Ю. В. Линник привёл примеры законов класса $\mathcal{L}$, не принадлежащих I_0. В то же время он показал, что если в представлении (4) закона класса $\mathcal{L}$ функция $G(u)$ убывает достаточно быстро с ростом $|u|$, то этот закон принадлежит множеству I_0; в частности, если у какого-либо распределения F класса $\mathcal{L}$ носитель функции G ограничен, то $F \in I_0$. Активную работу над теорией разложений вероятностных законов Ю. В. Линник прекратил в 1960 г. Его работы, безусловно, знаменовали начало нового этапа в развитии этой теории, явились мощным импульсом её развития, не ослабевающим до сих пор. В этом легко убедиться, хотя бы вкратце просмотрев обзоры результатов, полученных в этой области за последующие годы. Мы процитируем лишь один результат, касающийся принадлежности распределений класса $\mathcal{L}$ множеству I_0. Ю. В. Линник высказал гипотезу, что законы класса $\mathcal{L}$, характеристические функции которых суть целые аналитические функции, принадлежат I_0. В 1986 г. в очень трудной работе Г. П. Чистяков доказал эту гипотезу. Объединив теорему Линника с теоремой Чистякова, мы приходим к следующему поразительному результату.

Теорема 4. *Для того чтобы безгранично делимое распределение с целой характеристической функцией, имеющее ненулевую гауссову компоненту, не имело простых делителей, необходимо и достаточно, чтобы оно принадлежало классу* $\mathcal{L}$.

3.4. Математическая статистика.

До работ Ю. В. Линника исследования по математическая статистике в городе на Неве практически не велись. Именно с именем Юрия Владимировича связано создание ленинградской школы математической статистики. Очень скоро вокруг него образовалась группа молодых учёных, его учеников и сотрудников (А. А. Зингер, А. М. Каган, О. В. Шалаевский, И. Р. Судаков, И. В. Романовский, А. Л. Рухин и др.). Остановимся совсем вкратце на одном цикле работ, выполненных Ю. В. Линником в последнее десятилетие его жизни, на работах, посвящённых статистическим задачам с параметрами, а именно проблеме Беренса — Фишера. Проблема заключается в следующем. Наблюдаются две выборки

$$X_1, ..., X_{n^{(1)}}; Y_1, ..., Y_{n^{(2)}}$$

из нормальных распределений с параметрами $(a_1, \sigma_1), (a_2, \sigma_2)$ соответственно. По этим выборкам надлежит проверить гипотезу

$$H : a_1 = a_2.$$

При этом о параметрах σ_1, σ_2 ничего не известно и ничего не предполагается (это мешающие параметры). Вся выборочная информация о четырёх параметрах содержится в четырёх статистиках (статистика:=функция наблюдений):

$$\bar{X} = \sum_{1 \le i \le n^{(1)}} X_i, \bar{Y} = \sum_{1 \le i \le n^{(2)}} Y_i, s_1^2 = \sum_{1 \le i \le n^{(1)}} (\bar{X} - X_i)^2, s_2^2 = \sum_{1 \le i \le n^{(2)}} (\bar{Y} - Y_i)^2,$$

и потому все критерии имеют вид

$$G(\bar{X}, \bar{Y}, s_1^2, s_2^2) \ge 0.$$

При некоторых дополнительных естественных предположениях эти критерии принимают вид

$$G(\frac{\bar{X} - \bar{Y}}{s_2}, \frac{s_1}{s_2}) \ge 0.$$

В работах Ю. В. Линника и его сотрудников было доказано, что такие критерии существуют, но обязательно имеют плохие аналитические свойства границы критической зоны. Приведём, например, замечательный результат Юрия Владимировича относительно проблемы А. Вальда. Знаменитый американский статистик А. Вальд установил, что удовлетворяющие некоторым естественным статистическим требованиям критерии должны представляться в виде

$$\frac{|\bar{X} - \bar{Y}|}{s_2} \ge \varphi(\frac{s_1}{s_2}),$$

и поставил задачу построить такие критерии с аналитической функцией φ. Юрий Владимирович доказал, что не существует критериев Вальда не только с аналитической, но даже с дифференцируемой функцией φ !

Для исследования указанных выше задач Ю. В. Линник привлёк совершенно новые для статистики аналитические методы, в частности, теорию аналитических функций многих переменных, которые в статистике раньше никогда не применялись.

"Выдающийся талант Ю. В. Линника и совершенное владение аналитическими средствами современной математики позволили ему создать новое направление — направление, которое можно назвать "аналитической статистикой" "(акад. Ю. В. Прохоров).

Исследования Ю. В. Линника по аналитической статистике изложены им в двух монографиях [8], [9] .

4.

Эти заметки не претендуют на полноту. Полный список и подробный обзор работ Ю. В. Линника можно найти в посвящённом его памяти томе журнала Acta Arithmetica [1] и в его собрании сочинений [4] — [7].

То, что сделал Юрий Владимирович для своих учеников и, в частности, для авторов этих строк, трудно переоценить. Нам хотелось бы закончить нашу статью цитатой из известного стихотворения Н. А. Некрасова:

Учитель! перед именем твоим позволь смиренно преклонить колени!

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Acta Arithmetica, Том 27, 1975 г.
2. Виноградов А. И. Краткий очерк научной, педагогической и общественной деятельности Ю. В. Линника // Записки научных семинаров ПОМИ, Том 322, 2005 г. , стр. 5–9.
3. Ибрагимов И. А. Ю. В. Линник. Некоторые работы 50-х годов // Алгебра и Анализ, 3 (1991), 206-215.
4. Линник Ю. В. Избранные труды, Теория чисел (эргодический метод и L-функции) / Наука, М., 1979.
5. Линник Ю. В. Избранные труды, Теория чисел (L-функции и дисперсионный метод), / Наука, М., 1980.
6. Линник Ю. В. Избранные труды, Теория вероятностей / Наука, М.,1981.
7. Линник Ю. В. Избранные труды, Математическая статистика / Наука, М., 1982.
8. Линник Ю. В. Статистические задачи с мешающими параметрами / Наука, М., 1966.
9. Линник Ю. В. Лекции о задачах аналитической статистики / Физматлит, Наука, 1994.

REFERENCES

1. Acta Arithmetica, 1975, Vol 27.
2. Vinogradov A. I., 2005, "Kratkij ocherk nauchnoj, pedagogicheskoj i obshchestvennoj deyatel'nosti YU. V. Linnika" , *Zapiski nauchnyh seminarov POMI* Tom 322, pp. 5–9.
3. Ibragimov I. A., 1991, "YU.V.Linnik. Nekotorye raboty 50-h godov" , *Algebra i Analiz*, 3, 206-215.
4. Linnik YU. V., 1979, *Izbrannye trudy, Teoriya chisel (ehrgodicheskij metod i L-funkcii)*, Nauka, M.
5. Linnik YU. V., 1980, *Izbrannye trudy, Teoriya chisel (L-funkcii i dispersionnyj metod),* Nauka, M.
6. Linnik YU. V., 1981, *Izbrannye trudy, Teoriya veroyatnostej,* Nauka, M.
7. Linnik YU. V., 1982, *Izbrannye trudy, Matematicheskaya statistika,* Nauka, M.

8. Linnik YU. V., 1966, *Statisticheskie zadachi s meshayushchimi parametrami,* Nauka, M.

9. Linnik YU. V., 1994, *Lekcii o zadachah analiticheskoj statistiki,* Fizmatlit, Nauka.

Получено 05.07.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.176 DOI 10.22405/2226-8383-2018-19-3-20-34

Суммы Мертенса, требующие меньших значений функции Мёбиуса

Хаксли Мартин — почетный профессор математики, профессор, доктор наук, Кардиффский университет, Уэльс, Великобритания.
e-mail: huxley@cardiff.ac.uk
Уотт Найджел — доктор наук, Данфермлайн, Шотландия.
e-mail: wattn@btinternet.com

Аннотация

Обсудим некоторые тождества с участием $\mu(n)$ и $M(x) = \sum_{n\le x}\mu(n)$, функции Мёбиуса и Мертенса. Они позволяют вычислить $M(N^d)$ для $d = 1, 2, 3, \dots$ как сумму $O_d\left(N^d(\log N)^{2d-2}\right)$ членов, каждое произведение вида $\mu(n_1)\cdots\mu(n_r)$ с $r \le d$ и $n_1, \dots, n_r \le N$. Докажем более общее тождество, в котором $M(N^d)$ заменяется на $M(g, K) = \sum_{n\le K}\mu(n)g(n)$, где $g(n)$ – произвольная полностью мультипликативная функция, тогда как каждое n_j имеет собственный диапазон суммирования $1, \dots, N_j$. Это не ново, за исключением того, что в $N_1, \dots, N_d$ произвольны, но наше доказательство (вдохновленное тождественным равенством Э. Майсселя, 1854) является новым. Мы главным образом заинтересованы в случае $d = 2$, $K = N^2$, $N_1 = N_2 = N$, где тождество имеет вид $M(g, N^2) = 2M(g, N) - \mathbf{m}^{\mathrm{T}}A\mathbf{m}$, при этом A является матрицей $N \times N$ элементов $a_{mn} = \sum_{k\le N^2/(mn)} g(k)$, в то время как $\mathbf{m} = (\mu(1)g(1), \dots, \mu(N)g(N))^{\mathrm{T}}$. Наши результаты в разделах 2 и 3 данной статьи предполагают, что $g(n)$ равно 1 для всех n. Теорема Фробениуса—Перрона применяется в этом случае: мы находим, что A имеет одно большое положительное собственное значение, приблизительно $(\pi^2/6)N^2$, с собственным вектором приблизительно $\mathbf{f} = (1, 1/2, 1/3, \dots, 1/N)^{\mathrm{T}}$ T и что при больших значениях N второе наибольшее собственное значение лежит в $(-0.58N, -0.49N)$. Раздел 2 включает оценки для следов A и A^2 (хотя для $\mathrm{Tr}(A^2)$, мы пропустим часть доказательства). В разделе 3 обсуждаются способы аппроксимации $\mathbf{m}^{\mathrm{T}}A\mathbf{m}$, используя спектральное разложение A или (альтернативно) формулу Перрона: последний подход приводит к контурному интегралу, включающему дзета-функцию Римана. Мы также рассматриваем использование тождества $A = N^2\mathbf{f}\mathbf{f}^T - \frac{1}{2}\mathbf{u}\mathbf{u}^T + Z$, а Z — матрица $N \times N$ элементов $z_{mn} = -\psi(N^2/(mn))$, причем $\psi(x) = x - \lfloor x\rfloor - \frac{1}{2}$. Наши выводы представлены в разделе 4.

Ключевые слова: функция Мёбиуса, функция Мертенса, полностью мультипликативная функция, Майссель, тождество Линника, тождество Вогана, симметричная матрица, теорема Фробениуса-Перрона, собственное значение, собственный вектор, формула Перрона, дзета-функция Римана.

Библиография: 15 названий.

Для цитирования:
М. Хаксли, Н. Уотт. Суммы Мертенса, требующие меньших значений функции Мёбиуса // Чебышевский сборник, 2018, т. 19, вып. 3, с. 20–34.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.176 DOI 10.22405/2226-8383-2018-19-3-20-34

Mertens Sums requiring Fewer Values of the Möbius Function

Huxley Martin — Emeritus Professor of Mathematics, Professor and Ph.D., Cardiff University, Wales, United Kingdom.
e-mail: huxley@cardiff.ac.uk
Watt Nigel — Doctor of Philosophy, Dunfermline, Scotland.
e-mail: wattn@btinternet.com

Abstract

We discuss certain identities involving $\mu(n)$ and $M(x) = \sum_{n\le x}\mu(n)$, the functions of Möbius and Mertens. These allow calculation of $M(N^d)$, for $d = 1, 2, 3, \dots$, as a sum of $O_d\left(N^d(\log N)^{2d-2}\right)$ terms, each a product of the form $\mu(n_1)\cdots\mu(n_r)$ with $r \le d$ and $n_1, \dots, n_r \le N$. We prove a more general identity in which $M(N^d)$ is replaced by $M(g, K) = \sum_{n\le K}\mu(n)g(n)$, where $g(n)$ is an arbitrary totally multiplicative function, while each n_j has its own range of summation, $1, \dots, N_j$. This is not new, except perhaps in that $N_1, \dots, N_d$ are arbitrary, but our proof (inspired by an identity of E. Meissel, 1854) is new. We are mainly interested in the case $d = 2$, $K = N^2$, $N_1 = N_2 = N$, where the identity has the form $M(g, N^2) = 2M(g, N) - \mathbf{m}^{\mathrm{T}}A\mathbf{m}$, with A being the $N \times N$ matrix of elements $a_{mn} = \sum_{k\le N^2/(mn)} g(k)$, while $\mathbf{m} = (\mu(1)g(1), \dots, \mu(N)g(N))^{\mathrm{T}}$. Our results in Sections 2 and 3 of the paper assume that $g(n)$ equals 1 for all n. The Perron-Frobenius theorem applies in this case: we find that A has one large positive eigenvalue, approximately $(\pi^2/6)N^2$, with eigenvector approximately $\mathbf{f} = (1, 1/2, 1/3, \dots, 1/N)^{\mathrm{T}}$, and that, for large N, the second-largest eigenvalue lies in $(-0.58N, -0.49N)$. Section 2 includes estimates for the traces of A and A^2 (though, for $\mathrm{Tr}(A^2)$, we omit part of the proof). In Section 3 we discuss ways to approximate $\mathbf{m}^{\mathrm{T}}A\mathbf{m}$, using the spectral decomposition of A, or (alternatively) Perron's formula: the latter approach leads to a contour integral involving the Riemann zeta-function. We also discuss using the identity $A = N^2\mathbf{f}\mathbf{f}^T - \frac{1}{2}\mathbf{u}\mathbf{u}^T + Z$, where $\mathbf{u} = (1, \dots, 1)^{\mathrm{T}}$ and Z is the $N \times N$ matrix of elements $z_{mn} = -\psi(N^2/(mn))$, with $\psi(x) = x - \lfloor x\rfloor - \frac{1}{2}$.

Keywords: Möbius function, Mertens function, completely multiplicative function, Meissel, Linnik's identity, Vaughan's identity, symmetric matrix, Perron-Frobenius, eigenvalue, eigenvector, Perron's formula, Riemann zeta-function.

Bibliography: 15 titles.

For citation:
M. Huxley, N. Watt, 2018, "Mertens Sums requiring Fewer Values of the Möbius Function", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 20–34.

Dedicated to the memory of Yu. V. Linnik

1. Introduction

The sieve of Eratosthenes will find the prime numbers in $N+1, \dots, N^2$ provided that we know all the primes in $2, \dots, N$. In particular the sieve gives a relation for the function $\pi(x)$ that counts

the number of primes less than or equal to x:

$$\pi(N^2) = \pi(N) - 1 + \sum_{\substack{d \le N^2 \\ P(d) \le N}} \mu(d) \left[\frac{N^2}{d} \right], \tag{1}$$

where $\mu(d)$ is the Möbius function (which is $(-1)^\nu$ when d has ν prime factors, all different, but 0 when d has any prime factor repeated), while $P(d)$ is the greatest non-composite divisor of d, and $[x] = \max\{m \in \mathbb{Z} : m \le x\}$. The numbers d in (1) are constructed as products of the known primes in $2, \dots, N$, so the values $\mu(d)$ can be read off. In general, given a number n, it is very difficult to factorise n and so find $\mu(n)$. Thus the Mertens sum

$$M(x) = \sum_{n \le x} \mu(n) \tag{2}$$

is difficult to calculate from the definition. The Dirichlet series $\sum \mu(n)/n^s$ is $1/\zeta(s)$ (the reciprocal of the Riemann zeta function), and, according to folklore, the fastest method of calculating $M(x)$ is by Perron's contour integral formula for the sum of the coefficients of a Dirichlet series.

In this paper we discuss a family of identities which allow $M(N^d)$ to be calculated for each positive integer d as a sum of no more than $O_d\left(N^d (\log N)^{2d-2}\right)$ terms, each a product of the form $\mu(n_1) \cdots \mu(n_r)$ with $r \le d$ and $\{n_1, \dots, n_r\} \subseteq \{1, \dots, N\}$. In Theorem 1, below, we state a more complicated form of these identities, in which each of the variables of summation n_j $(j = 1, \dots, r)$ can have its own independent range of summation: $1, \dots, N_j$ (say).

We actually treat the more general Möbius sum

$$M(g, x) = \sum_{n \le x} \mu(n) g(n), \tag{3}$$

where $g(n)$ can be any totally multiplicative arithmetic function, that is, $g(rs) = g(r)g(s)$ holds for any positive integers r and s. The relevant identity when $d = 1$ is (of course) the definition (3). The case $d = 2$ is the next simplest. Let $\mathbf{m}(g, N)$ be the column-matrix $(\mu(1)g(1), \dots, \mu(N)g(N))^{\mathrm{T}}$, and let $A(g, N)$ be the $N \times N$ matrix with elements

$$a_{mn}(g, N) = \sum_{k \le \frac{N^2}{mn}} g(k) \quad (m, n \in \{1, \dots, N\}). \tag{4}$$

Then

$$M(g, N^2) = 2M(g, N) - (\mathbf{m}(g, N))^{\mathrm{T}} A(g, N) \mathbf{m}(g, N) \,. \tag{5}$$

In the general case, when $d, K, N \in \mathbb{N}$ satisfy $d \ge 2$ and $K \ge N > K^{1/d} - 1$, we have:

$$\begin{aligned} M(g, K) = {} & d M(g, N) \\ & - \sum_{r=2}^{d} (-1)^r \, {}_dC_r \sum_{n_1 \le N} \cdots \sum_{n_r \le N} \sum_{k_1} \cdots \sum_{k_{r-1}} g(k_1 \cdots k_{r-1}) \prod_{i=1}^{r} \mu(n_i) g(n_i) \,, \\ & \qquad n_1 n_2 \dots n_r k_1 k_2 \dots k_{r-1} \le K \end{aligned} \tag{6}$$

where ${}_dC_r = d(d-1)\cdots(d-(r-1))/(r!)$.

Note that (5) is just the special case $d = 2$, $K = N^2$ of (6). Moreover, (6) is itself a special case of another identity (that stated in Theorem 1, below), in which the single range of summation

$1, \ldots, N$ is replaced by d independent ranges of summation. In order to state this more general identity we require some more notation.

Let d be a positive integer greater than 1. Let $V = v_1 v_2 \ldots v_d$ be a word of length d in the alphabet $\{0, 1\}$. The support of a word V is the set of indices i for which $v_i = 1$. The weight $w(V)$ of a word V is the size of the support, so that $w(V) = \sum v_i$. The combinatorial Möbius function, which we write as μ^* to distinguish it from the number-theoretic function μ, is $\mu^*(V) = (-1)^{w(V)}$.

Let $N_1, \ldots, N_d$ be positive integers. For each word V, and each $L \in \mathbb{N}$, let the notatation $\sum_1^L(V)$ signify summation over $n_1, \ldots, n_d$ in the ranges $n_i = 1, \ldots, L$ when $v_i = 0$, but $n_i = 1, \ldots, N_i$ when $v_i = 1$. When $L = 1$ and $v_i = 0$, the variable of summation n_i effectively becomes 'frozen', meaning that its range of summation is then just the single-element set $\{1\}$.

Let K be a positive integer that is less than $(1 + N_1)(1 + N_2) \ldots (1 + N_d)$. If $n_1, \ldots, n_d$ are integers satisfying the condition $n_1 n_2 \ldots n_d \le K$, then $n_i \le N_i$ holds for at least one index i. It therefore follows by the inclusion-exclusion principle of combinatorics that if $f : \mathbb{N}^d \to \mathbb{C}$ is such that one has $|f(n_1, \ldots, n_d)| > 0$ only when $n_1 n_2 \cdots n_d \le K$, then

$$\sum_1^K (00\ldots0) f(n_1, \ldots, n_d) = \sum_{r=1}^{d} (-1)^{r-1} \sum_{V\,:\,\omega(V)=r} \sum_1^K (V) f(n_1, \ldots, n_d)\,, \tag{7}$$

or, to put it more elegantly, $\sum_V \mu^*(V) \sum_1^K (V) f(n_1, \ldots, n_d) = 0$.

THEOREM 1. *When $g(n)$ is a totally multiplicative arithmetic function, and d, $N_1, \ldots, N_d$ and K are as above, we have:*

$$\begin{aligned} M(g, K) = &\sum_{i=1}^{d} M(g, \min\{N_i, K\}) \\ &- \sum_{V\,:\,w(V)\ge 2} (-1)^{w(V)} \sum_1^1 (V) \sum_{k_1} \cdots \sum_{\substack{k_{\omega(V)-1} \\ k_1 \ldots k_{\omega(V)-1} \le \frac{K}{n_1 \ldots n_d}}} g(k_1 \cdots k_{\omega(V)-1}) \prod_{i=1}^{d} \mu(n_i) g(n_i)\,. \end{aligned} \tag{8}$$

Proof. We apply (7) with f given by:

$$f(n_1, \ldots, n_d) = \sum_{\substack{k_1 \\ k_1 \ldots k_{d-1} \le \frac{K}{n_1 \ldots n_d}}} \cdots \sum_{k_{d-1}} \mu(n_1) \ldots \mu(n_d) g(k_1 \ldots k_{d-1} n_1 \ldots n_d). \tag{9}$$

For the word $V = 11 \ldots 1$ with $w(V) = d$, we have

$$\sum_1^K (11\ldots1) = \sum_1^1 (11\ldots1).$$

All other words V have $v_j = 0$ for at least one index j, so the corresponding summand n_j runs over the full range from 1 to K. For these words V we carry out the following 'contraction step'. Take an index j for which $v_j = 0$. We sum over n_j and k_{d-1} first, observing that by Möbius inversion we have:

$$\sum_{n_j=1}^{K} \sum_{k_{d-1}\le \frac{K}{n_1\dots n_d k_1\dots k_{d-2}}} \mu(n_j) g(n_j k_{d-1}$$
$$= \sum_{m\le \frac{K}{n_1\dots n_{j-1}n_{j+1}\dots n_d k_1\dots k_{d-2}}} g(m) \sum_{n_j\mid m} \mu(n_j)$$
$$= \begin{cases} g(1)=\mu(1)g(1) & \text{if } n_1\dots n_{j-1}n_{j+1}\dots n_d k_1\dots k_{d-2}\le K,\\ 0 & \text{otherwise.}\end{cases}$$

We thereby find that the value of the relevant sum over $n_1,\dots,n_d$ and $k_1,\dots,k_{d-1}$ is unchanged when we omit k_{d-1} and freeze n_j as the fixed value $n_j=1$.

We repeat the contraction step for every index j with $v_j=0$, freezing the corresponding variable as $n_j=1$, and removing the last variable k_i. Exceptionally, when V is $00\dots0$, we can remove $k_{d-1},k_{d-2},\dots,k_1$, and freeze $n_d,n_{d-1},\dots,n_2$, but the sum over n_1 remains over the range $1,\dots,K$, giving the term $M(g,K)$ on the left of (8). The summation identity (7), when applied with f given by (9), contracts to give (8). ■

In (5), (6) and Theorem 1, we require the total multiplicativity of g only in order to 'separate variables' (as, in (6) for example, we separate $k_1,\dots,k_{r-1}$ from $n_1,\dots,n_r$ by means of the identity $g(k_1\cdots k_{r-1}n_1\cdots,n_r)=g(k_1\cdots k_{r-1})g(n_1)\cdots g(n_r)$). Indeed, (8) gives a formula for the Möbius function itself, for we can apply (8) to each term in the difference $M(g,K)-M(g,K-1)=\mu(K)g(K)$, and we can then divide through by $g(K)$ to obtain a formula for $\mu(K)$ that is independent of g. This formula for $\mu(K)$ may also be deduced from the identity

$$\frac{1}{\zeta(s)}\prod_{j=1}^{d}\Big(1-\zeta(s)\sum_{n=1}^{N_j}\frac{\mu(n)}{n^s}\Big)=\zeta^{d-1}(s)\prod_{j=1}^{d}\sum_{n=1+N_j}^{\infty}\frac{\mu(n)}{n^s}\quad(\mathrm{Re}(s)>1),\tag{10}$$

through multiplying out the brackets on the left-hand side, and then computing the coefficient of K^{-s} on each side of the resulting identity, subject to the hypothesis that the product $(1+N_1)\cdots(1+N_d)$ be greater than K. This approach yields a second proof of Theorem 1. We prefer the first proof due to its more obvious connection with Meissel's identity [**8** p 303],

$$\sum_{n\le x}\Big[\frac{x}{n}\Big]\mu(n)=\begin{cases}1 & if\ \ x\ge 1,\\ 0 & if\ \ 1>x>0,\end{cases}\tag{11}$$

which was the initial source of inspiration for our work.

Given any $K\in\mathbb{N}$, any integer $d\ge 2$, and any $\theta_1,\dots,\theta_d>0$ with $\theta_1+\cdots+\theta_d=1$, it follows from Theorem 1 that (8) will hold when one has also $N_j=[K^{\theta_j}]$, for $j=1,\dots,d$. Theorem 1 therefore offers considerably more flexibility of application than (6) does. Although we believe Theorem 1 to be new (in respect of the flexibility in the choice of $N_1,\dots,N_d$), the special cases of it that are displayed in (5) and (6) are known results. The result (5) is contained in Vaughan's (slightly more complicated) identity [**13** equation (18)] (essentially the special case when $u=\sqrt{X}$, and so $S_3=0$), and one can find in equation (13.38) of [**5**], for example, a formula for $\mu(n)$ that is equivalent to what we have in (6). It is, moreover, clear that even our identity in (8) is akin to formulae of Heath-Brown for sums involving $\Lambda(n)$, the von Mangoldt function: compare (10), from which (8) may be deduced, with Lemma 1 of [**2**]. The earliest formula of this type is due to Linnik himself in [**6**,**7**].

We shall refer to the case of (3) (or of (4), (5), (6), or (8)), where the function $g(n)$ takes the constant value 1, as the principal case. The main focus of our work has been on the principal case of the identity (5). Indeed, all subsequent sections of this paper are exclusively devoted to matters connected with this single topic, such as (for example) questions concerning certain properties of the $N \times N$ matrix $A = A(N)$ that occurs in the principal case of (5) and has, by (4), elements $a_{mn} = [N^2/(mn)] \in \mathbb{N}$. In Section 2 we discuss matters related to the spectral decomposition of $A = A(N)$. In the third (and final) section we discuss decompositions (spectral and otherwise) of the quadratic form $\mathbf{m}^T A \mathbf{m}$, where $\mathbf{m} = \mathbf{m}(N)$ is the column-matrix $(\mu(1), \ldots, \mu(N))^{\mathrm{T}}$ that occurs in the principal case of (5).

We consider especially the principal case of (5), in the hope that it (modified as necessary) might lead to a new proof of the prime number theorem, or even some new upper bound for the Mertens sum $|M(x)|$. The following parts of this paper report what we have discovered in the search for such an application of (5).

One of our findings is that the matrix $A(N)$, which (clearly) is real and symmetric, has one exceptionally large positive eigenvalue, approximately $N^2\zeta(2)$, with eigenvector approximately $(1, 1/2, 1/3, \ldots, 1/N)^{\mathrm{T}}$. Calculations by the second author show that the second-largest eigenvalue of $A(N)$ lies in an interval of the form $[d_4 N + o(N), c_4 N + o(N)]$, where c_4 and d_4 are constants that are approximately -0.496 and -0.572, respectively: for more details, see (18), (25), (31) and (32) below. Hence, for N sufficiently large, the quadratic form on the right-hand side of (5) is neither positive definite nor negative definite in the principal case.

By the principal case of (6), we have a sequence of formulae through which each of $M(N^2), M(N^3), M(N^4), \ldots$ is expressed in terms of $\mu(1), \ldots, \mu(N)$. Although the first of these formulae, the principal case of (5), may be considered analogous to the sieve of Eratosthenes (1), there seems to be no version of (1) for $\pi(N^3)$, because unwanted numbers of the form pq, where p and q are both primes greater than N, survive the sieve process ("Gnoggensplatts" in Greaves's lectures on *Sieve Methods*).

A connection between Mertens sums and certain symmetric matrices U_n $(n \in \mathbb{N})$, that bear some resemblance to our matrices $A(N)$ $(N \in \mathbb{N})$ has previously been established by Cardinal [**1**]. To define Cardinal's matrix U_n, one first takes $\sigma_1 < \sigma_2 < \cdots < \sigma_s$ to be the elements of the set $\mathcal{S} = \mathcal{R} \cup \{[n/\rho] : \rho \in \mathcal{R}\}$, where $\mathcal{R} = \{\rho \in \mathbb{N} : \rho \leq \sqrt{n}\}$ (it follows that $0 \leq 2[\sqrt{n}] - s \leq 1$). Then U_n is the $s \times s$ matrix with elements $u_{ij} = [n/(\sigma_i \sigma_j)]$. In Propositions 21 and 22 of [**1**], it is shown that one has $T_n U_n^{-1} T_n = V_n$, where T_n and V_n are the $s \times s$ matrices with elements $t_{ij} = |[2, s+1] \cap \{i+j\}|$ and $v_{ij} = M(u_{ij})$, respectively.

In the cases where n is a perfect square, so that $n = N^2$ for some integer N, then $|\mathcal{R}| = N$, and the $N \times N$ principal submatrix of U_n consisting of the array of elements from the first N rows and first N columns of U_n is our matrix $A(N)$: since $2N - 1 \leq s \leq 2N$, we can say that $A(N)$ constitutes (exactly, or approximately) the top left-hand quarter of Cardinal's matrix U_n. In these same cases, Cardinal's identity $T_n U_n^{-1} T_n = V_n$ implies that v_{11}, which is $M(N^2)$, will be equal to the sum of all s^2 of the elements of the inverse of the matrix $U_n = U_{N^2}$: we obtain a formula for $M(N^2)$ thereby that seems quite different from what we see in the principal case of (5).

As Cardinal observes in Theorem 24 and Remark 25 of [**1**], information about small eigenvalues of the matrix $V_n^{-1} = T_n^{-1} U_n T_n^{-1}$ might lead to new upper bounds on $M(x)$. In this respect, the connection that we have found between $M(x)$ and $A(N)$ is quite different from Cardinal's connection between $M(x)$ and U_n, for it is the larger eigenvalues of $A(N)$ and their eigenvectors that matter most in the principal case of (5): see, for example, equation (35), below.

We have scarcely considered non-principal cases of (5), (6), or (8). Certain non-principal cases of (5) may merit further investigation. The first case is when $g(n) = \chi(n)$, a non-principal Dirichlet character to some modulus $q > 1$. The sums $\sum_{\ell \leq x} \chi(\ell)$ that we use to construct the matrix elements $a_{mn}(\chi, N)$ in (4) are periodic step functions of x, whose period is q or some

proper factor of q. In contrast to the principal case, where the set of elements of the matrix $A(N)$ in (5) contains at least N different integers, namely $[N^2/1], [N^2/2], \dots, [N^2/N]$, there is a single finite set, $\{\sum_{0<\ell\le L}\chi(\ell) : L \in (0,q]\cap\mathbb{Z}\}$, that contains all the elements of all the matrices $A(\chi,1), A(\chi,2), A(\chi,3), \dots$. For χ real, $A(\chi,N)$ will, of course, be real and symmetric just like $A(N)$.

A case of (3) known to be related to the prime number theorem is when $g(n) = 1/n$ (see page 248 of [**9**], for example). More generally, when $g(n) = n^{-s}$ for some fixed complex number s, then the sum $M(g,x)$ in (3) becomes a partial sum for the Dirichlet series for $1/\zeta(s)$. If, for some $\sigma_0 \in [1/2,1)$, the only zeros of $\zeta(s)$ with real parts greater than σ_0 are a pair of simple zeros, ρ and $\overline{\rho}$ (say), and if we put $g(n) = n^{-\rho}$ $(n \in \mathbb{N})$, then the sum $M(g,x)$ in (3) will grow logarithmically in x.

Another interesting case of (3) to (5) is when $g(n) = \lambda(n)$, the Liouville function, which is the projection of the Möbius function μ onto the space of totally multiplicative arithmetic functions. In this case $M(g,x)$ grows like $x/\zeta(2)$.

2. Elementary Estimates for Eigenvalues and an Eigenvector

Let N be a given positive integer. Since the matrix $A = A(N)$, in the principal case of (5), is both real and symmetric, it has eigenvalues $\lambda_1 \le \lambda_2 \le \dots \le \lambda_N$ with corresponding eigen-(column-)vectors of unit length $\mathbf{e}_1, \dots, \mathbf{e}_N$ that form an orthonormal basis of $\mathbb{R}^N$. When $\mathbf{v} \in \mathbb{R}^N$, one has

$$\mathbf{v}^T A\mathbf{v} = \sum_{k=1}^{N} \lambda_k \,(\mathbf{e}_k \cdot \mathbf{v})^2 \tag{12}$$

as a consequence of the spectral decomposition $A = \sum_{k=1}^{N} \lambda_k \mathbf{e}_k \mathbf{e}_k^T$, and Parseval's identity gives

$$\sum_{k=1}^{N} (\mathbf{e}_k \cdot \mathbf{v})^2 = \mathbf{v}\cdot\mathbf{v} = \|\mathbf{v}\|^2. \tag{13}$$

In order to study the terms appearing in (12) and (13), we estimate:

(a) $\mathrm{Tr}(A) = \sum a_{nn}$ (the trace of the matrix A),

(b) $\mathrm{Tr}(A^2) = \mathrm{Tr}(A^T A) = \sum\sum a_{mn}^2$,

(c) $\mathbf{f}^T A\mathbf{f}$, where $\mathbf{f} = (1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{N})^T$,

(d) $\mathbf{w}^T A\mathbf{w}$, where $\mathbf{w} = \mathbf{u} - \|\mathbf{f}\|^{-2}(\mathbf{f}\cdot\mathbf{u})\mathbf{f}$, with $\mathbf{u} = (1,1,\dots,1)^T \in \mathbb{R}^N$.

We use the following notation:

$$\zeta_j = \sum_{m=1}^{N} m^{-j}\,, \quad \delta = \sum_{m\le N}\sum_{n\le N} \frac{\{N^2/(mn)\}}{mn} \quad \text{and} \quad \phi = \frac{1}{N^2}\sum_{m\le N}\sum_{n\le N}\left\{\frac{N^2}{mn}\right\}^2\,,$$

where $\{t\} = t - [t]$ (the fractional part of t). Taking (b) first, we simply observe that

$$\mathrm{Tr}\left(A^2\right) = \sum_{m\le N}\sum_{n\le N}\left[\frac{N^2}{mn}\right]^2 = \sum_{m\le N}\sum_{n\le N}\left(\frac{N^2}{mn} - \left\{\frac{N^2}{mn}\right\}\right)^2 = \zeta_2^2 N^4 + (\phi - 2\delta)\,N^2\,. \tag{14}$$

Since $\mathrm{Tr}(A^2) = \lambda_1^2 + \dots + \lambda_N^2$, and since $\delta \ge 0$ and $\phi < 1$, the identity (14) shows already that $\lambda_N < \zeta_2 N^2 + (2\zeta_2)^{-1}$.

Regarding (c), we are content to note that

$$\mathbf{f}^T A\mathbf{f} = \sum_{m\le N}\sum_{n\le N}\frac{\left[N^2/(mn)\right]}{mn} = \sum_{m\le N}\sum_{n\le N}\frac{\left(N^2/(mn) - \left\{N^2/(mn)\right\}\right)}{mn} = \zeta_2^2 N^2 - \delta\ . \tag{15}$$

We have here $\|\mathbf{f}\|^2 = \zeta_2$, so by Rayleigh's Principle it follows from (15) that

$$\zeta_2 N^2 - \frac{\delta}{\zeta_2} \le \lambda_N\ . \tag{16}$$

By (16) and the point noted immediately below (14), we conclude that

$$-\frac{(1+\log N)^2}{\zeta_2} < \lambda_N - \zeta_2 N^2 < \frac{1}{2\zeta_2}\ . \tag{17}$$

As $0 \le \delta < \zeta_1^2 \le \zeta_0\zeta_2 = N\zeta_2 \le N^2\zeta_2^2$, the lower bound on λ_N in (16) is non-negative, and so we may deduce from it that $\lambda_N^2 \ge (\zeta_2 N^2 - \delta\zeta_2^{-1})^2 = \zeta_2^2 N^4 - 2\delta N^2 + \delta^2\zeta_2^{-2}$: this, together with the evaluation of $\mathrm{Tr}(A^2)$ in (14), is enough to show that

$$\lambda_1^2 + \ \cdots\ + \lambda_{N-1}^2 \le \phi N^2 - \delta^2\zeta_2^{-2} < N^2\ . \tag{18}$$

From the way we have ordered the eigenvalues, the bound (18) implies:

$$|\lambda_k| < \frac{N}{\sqrt{\min\{k, N-k\}}} \qquad (k = 1, 2, \dots, N-1). \tag{19}$$

In view of (17) and (19), it is clear that for N large, λ_N will be exceptionally large, compared with all other eigenvalues of A. Accordingly we consider first the corresponding eigenvector $\mathbf{e}_N$, before discussing the estimation (a) of $\mathrm{Tr}(A)$. Putting $F_N = \mathbf{e}_N \cdot \hat{\mathbf{f}}$, where $\hat{\mathbf{f}} = \|\mathbf{f}\|^{-1}\mathbf{f}$, we find by (15) and (17), and (12), (19) and (13), that

$$\lambda_N - \left(\frac{1}{2} + (1+\log N)^2\right) < \hat{\mathbf{f}}^T A\hat{\mathbf{f}} < \lambda_N F_N^2 + N\left(1 - F_N^2\right)\ .$$

For $N > 1$ we have $\lambda_N > N$ (this follows by (17) when $N \ge 3$), and so, by comparison of the upper and lower bounds for $\hat{\mathbf{f}}^T A\hat{\mathbf{f}}$ that were just obtained, we deduce that

$$1 \ge F_N^2 > 1 - \frac{\left(\frac{1}{2} + (1+\log N)^2\right)}{(\lambda_N - N)}\ .$$

Choosing the $\pm$-sign so that $\pm F_N = |F_N|$, we therefore find from (17) that

$$\left\|\mathbf{e}_N - \left(\pm\hat{\mathbf{f}}\right)\right\| = \sqrt{2\left(1 - |F_N|\right)} = \sqrt{\frac{2\left(1-F_N^2\right)}{r1 + |F_N|}} = O\left(\frac{\log N}{rN}\right)\ . \tag{20}$$

We now come to the task mentioned in (a) above, which is the estimation of the sum $S = \mathrm{Tr}(A) = \sum a_{nn}$. We pick a positive integer K, and we divide the original sum S into two parts: S_1, which has the terms with $n^2 \le N^2/(K+1)$, and S_2, which has the terms with $N^2 \ge n^2 > N^2/(K+1)$ (so that $a_{nn} = [N^2/n^2] = k$ for some $k \in \{1, \dots, K\}$). We have

$$\begin{aligned} S_1 = \sum_{n^2 \le N^2/(K+1)} a_{nn} &= \sum_{n \le N/\sqrt{K+1}}\left(\frac{N^2}{n^2} + O(1)\right) \\ &= N^2\left(\zeta_2 - \int_{N/\sqrt{K+1}}^{N} x^{-2}\,\mathrm{d}x + O\left(\frac{K}{N^2}\right)\right) + O\left(\frac{N}{\sqrt{K}}\right) \\ &= \zeta_2 N^2 - N\sqrt{K} + N + O\left(K + \frac{N}{\sqrt{K}}\right). \end{aligned}$$

The sum S_2 is more complicated. We have

$$S_2 = \sum_{k=1}^{K} \sum_{\frac{N}{\sqrt{k+1}}<n\le\frac{N}{\sqrt{k}}} k = \sum_{1\le\ell\le k\le K}\sum \left(\left[\frac{N}{\sqrt{k}}\right] - \left[\frac{N}{\sqrt{k+1}}\right]\right)$$
$$= \sum_{\ell=1}^{K}\left(\left[\frac{N}{r\sqrt{\ell}}\right] - \left[\frac{N}{\sqrt{K+1}}\right]\right) = \sum_{\ell=1}^{K}\frac{N}{\sqrt{\ell}} - \frac{KN}{\sqrt{K+1}} + O(K).$$

Let

$$g(\ell) = 2\sqrt{\ell} - 2\sqrt{\ell-1} - \frac{1}{\sqrt{\ell}} = \frac{1}{\sqrt{\ell}(\sqrt{\ell}+\sqrt{\ell-1})^2} \quad (\ell\in\mathbb{N}) \quad \text{and} \quad \alpha = \sum_{\ell=1}^{\infty} g(\ell).$$

Then

$$\sum_{\ell=1}^{K}\frac{1}{\sqrt{\ell}} = \sum_{\ell=1}^{K}\left(2\sqrt{\ell} - 2\sqrt{\ell-1} - g(\ell)\right) = 2\sqrt{K} - \alpha + O\left(\frac{1}{\sqrt{K}}\right).$$

Hence

$$S_2 = 2N\sqrt{K} - \alpha N - \frac{NK}{\sqrt{K+1}} + O\left(\frac{N}{r\sqrt{K}} + K\right) = N\sqrt{K} - \alpha N + O\left(\frac{N}{\sqrt{K}} + K\right),$$

and so, putting $K = [N^{2/3}]$, we get:

$$\mathrm{Tr}(A) = S_1 + S_2 = \zeta_2 N^2 - (\alpha-1)N + O\left(N^{2/3}\right). \tag{21}$$

By (21) and (17), it follows that

$$\lambda_1 + \cdots + \lambda_{N-1} = -(\alpha-1)N + O\left(N^{2/3}\right). \tag{22}$$

By equations (1.11) to (1.13) of [**4**] and the case $K = 1$ of of equation (B.24) of [**9**] (itself an application of the Euler-Maclaurin summation formula), we find that for $\sigma \in (0,1)\cup(1,\infty)$ and $K\in\mathbb{N}$,

$$\sum_{\ell=1}^{K}\frac{1}{\ell^\sigma} = \frac{K^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + \frac{\theta(K,\sigma)}{K^\sigma} \tag{23}$$
$$= \frac{\theta(K,\sigma)}{K^\sigma} + \frac{K^{1-\sigma}-1}{1-\sigma} + \gamma + \sum_{j=1}^{\infty}\gamma_j(\sigma-1)^j, \tag{24}$$

where $\zeta(s)$ is Riemann's zeta function, each of γ, γ_1, γ_2, ... is a certain (real valued) absolute constant (the first of these, γ, being Euler's constant) and $\theta(K,\sigma)$ is a number lying in the interval $(0,1)$. By (23), we have $\alpha = -\zeta(1/2)$ in (21), and we can calculate that

$$\alpha - 1 = -(\zeta(1/2)+1) = 0.4603545\ldots.$$

Given that $\zeta(2) = \pi^2/6$, we find (similarly) that $\zeta_2 = (\pi^2/6) - N^{-1} + O(N^{-2})$ in (14) to (18). We also note that $\zeta_1 = \log N + \gamma + O(1/N)$ (as follows, for example, by letting $\sigma\to 1$ in (24)).

We remark that, by combining methods similar to those used to obtain (21) with certain applications of the Euler-Maclaurin summation formula, we have been able to determine that the variable $\phi\in[0,1)$ in (14) and (18) satisfies

$$\phi = \beta + O\left(\frac{1+\log N}{N^{1/7}}\right), \tag{25}$$

where $\beta = 1 - \frac{\pi^2}{24} - \frac{1}{2}(\log(2\pi) - 1)^2 + \frac{1}{2}(1-\gamma)^2 = 0.32712\ldots$. We omit our proof of (25), which shows no features that are truly novel (and would require more than just a few pages). By (25), we can sharpen (19) somewhat, for large values of N.

Finally we consider the estimation problem (d), stated earlier. Noting firstly that $\mathbf{w} = \mathbf{u} - -(\zeta_1/\zeta_2)\mathbf{f}$, we are able to deduce that

$$\|\mathbf{w}\|^2 = N - \frac{\zeta_1^2}{\zeta_2} = N + O\left((1+\log N)^2\right) \tag{26}$$

and that

$$\mathbf{w}^T A\mathbf{w} = \mathbf{u}^T A\mathbf{u} - 2\left(\zeta_1/\zeta_2\right)\mathbf{u}^T A\mathbf{f} + \left(\zeta_1/\zeta_2\right)^2 \mathbf{f}^T A\mathbf{f}\ . \tag{27}$$

We have, moreover,

$$\mathbf{u}^T A\mathbf{u} = \sum_{m\le N}\sum_{n\le N}\left[\frac{N^2}{mn}\right] = \sum_m\sum_n\left[\frac{N^2}{mn}\right] - 2\sum_{m>N}\sum_n\left[\frac{N^2}{mn}\right] = D_1 - 2D_2 \quad \text{(say)}. \tag{28}$$

Here

$$D_1 = \sum_{\ell\le N^2}\tau_3(\ell) = \left(\frac{1}{2}\log^2\left(N^2\right) + (3\gamma-1)\log\left(N^2\right) + c_1\right)N^2 + O\left(N^{\varepsilon+43/48}\right)\ , \tag{29}$$

where $c_1 = 3\gamma^2 - 3\gamma + 3\gamma_1 + 1$; see pages 352-4 of [**4**] for the second equality in (29).

Regarding the sum D_2 in (28), we have:

$$\begin{aligned} D_2 = \sum_{m>N}\sum_{\substack{n\\(nk)m\le N^2}}\sum_k 1 &= \sum_{\ell<N}\left(\sum_{n|\ell}1\right)\sum_{N<m\le N^2/\ell}1 \\ &= N^2\sum_{\ell<N}\frac{\tau_2(\ell)}{\ell} - N\sum_{\ell<N}\tau_2(\ell) + O\left(\sum_{\ell<N}\tau_2(\ell)\right)\ . \end{aligned}$$

By partial summation and Huxley's estimate on page 593 of [**3**] for the remainder term in Dirichlet's divisor problem (namely $\Delta(x) = \sum_{\ell\le x}\tau_2(\ell) - (\log x + 2\gamma - 1)x$), we deduce from the above that

$$D_2 = \left(\frac{1}{2}\log^2 N + (2\gamma-1)\log N + c_2\right)N^2 + O\left(N^{547/416}(\log N)^{3.26}\right)\ ,$$

where

$$c_2 = \int_1^\infty \frac{\Delta(x)\mathrm{d}x}{x^2} = \lim_{\sigma\to 2+}\left(\frac{\zeta^2(\sigma-1)}{\sigma-1} - \frac{1}{(\sigma-2)^2} - \frac{2\gamma-1}{\sigma-2}\right) = \gamma^2 - 2\gamma + 2\gamma_1 + 1$$

(with γ and γ_1 as in (24)). Using this, (28), and (19), we have

$$\mathbf{u}^T A\mathbf{u} = \left(\log^2 N + 2\gamma\log N + c_3\right)N^2 + O\left(N^{547/416}(\log N)^{3.26}\right)\ , \tag{30}$$

where $c_3 = c_1 - 2c_2 = \gamma^2 + \gamma - \gamma_1 - 1$. Trivial estimates show that one has

$$\mathbf{u}^T A\mathbf{f} = \zeta_1\zeta_2 N^2 + O((1+\log N)N).$$

Using this, (15), (30), (27), and estimates already obtained for ζ_1 and ζ_2, we find that

$$\begin{aligned} \mathbf{w}^T A\mathbf{w} &= \left(\log^2 N + 2\gamma\log N + c_3 - \zeta_1^2\right)N^2 + O\left(N^{547/416}(\log N)^{3.26}\right) \\ &= c_4 N^2 + O\left(N^{547/416}(\log N)^{3.26}\right)\ , \end{aligned} \tag{31}$$

where $c_4 = c_3 - \gamma^2 = \gamma - \gamma_1 - 1 = 0.57721566\ldots - 0.07281584\ldots - 1 = -0.495600\ldots$ (see [**10**].

Since (26) implies $N > \|\mathbf{w}\|^2 \geq N/10$, we find, using (26), (31), and Rayleigh's principle that:

$$\lambda_1 \leq \frac{\mathbf{w}^T A \mathbf{w}}{\|\mathbf{w}\|^2} < c_4 N + O\left(N^{131/416}(\log N)^{3.26}\right) \quad (N \geq 2). \tag{32}$$

The coefficient of N in this upper bound may well be close to optimal: when $N = 10321$, for example, computations done with the 'GNU Octave' software package returned $-0.493678\ldots$ as an estimate of the value of λ_1/N in this case. By reasoning similar to that which gives (20), we may deduce from (18), (25) and (32) that, as $N \to \infty$, we have $|\lambda_2|/N < (1 + o(1))(\beta - c_4^2)^{1/2} \sim \sim 0.2855539\ldots$ and $(\mathbf{e}_1 \cdot \hat{\mathbf{w}})^2 \geq (0.5 + o(1))(1 + (2c_4^2\beta^{-1} - 1)^{1/2}) \sim 0.8540699\ldots$. Therefore, for N sufficiently large, the lines $\{t\mathbf{w} : t \in \mathbb{R}\}$ and $\{t\mathbf{e}_1 : t \in \mathbb{R}\}$ will meet at an angle of less than $\pi/8$ radians.

We end this section with some speculations driven by certain numerical evidence, gathered with the help of 'GNU Octave'. We omit the detailed evidence, and instead just summarise what it suggests. Let k be any fixed non-zero integer, and let N now be free to vary in the range $N > |k|$. Our numerical evidence suggests that $\lambda_{\{-k/N\}N} \sim \Lambda_k N$ as $N \to \infty$, where Λ_k is a real number that depends only on k, and where each of the two associated sequences, $\Lambda_1, \Lambda_2, \Lambda_3, \ldots$ and $-\Lambda_{-1}, -\Lambda_{-2}, -\Lambda_{-3}, \ldots$, decreases monotonically, and converges to 0. Further numerical evidence suggests that if $\theta \in (0,1)$ is fixed, and if $e_{j,\ell}$ denotes the ℓ-th component of the normalised eigenvector $\mathbf{e}_j$, so that $\mathbf{e}_j = (e_{j,1}, e_{j,2}, \ldots, e_{j,N})^{\mathrm{T}}$ for $j = 1, \ldots, N$, then as $N \to \infty$ we appear to see that

$$e_{\{-k/N\}N,\ell} \sim (-1)^{b(N,k)} N^{-1/2} E_k(\ell/N) \quad \text{for } \ell = [\theta N] + 1, [\theta N] + 2, \ldots, N,$$

with E_k here being a certain real function independent of ℓ and N that is continuous on $(0,1]$, and with an integer exponent $b(N,k)$ independent of ℓ. The occurrence of the functions $E_{\pm 1}, E_{\pm 2}, E_{\pm 3}, \ldots$ in this might be explained if they were eigenfunctions of a suitable linear operator $\mathcal{A} : L^2[0,1] \to L^2[0,1]$.

3. Various Decompositions of $\mathbf{m}^T A\mathbf{m}$ in the principal case

It is our hope (as yet unrealised) that a study of the quadratic form $\mathbf{v}^T A\mathbf{v}$ (particularly when $\mathbf{v}$ is the vector $\mathbf{m} = (\mu(1), \ldots, \mu(N))^T$), in the principal case of (5), might lead to new results about the Mertens function $M(x)$. In this section we briefly describe (and compare) several different approaches to such an investigation, each involving a different decomposition of the quadratic form. We find it convenient to modify the earlier notation $M(g,x)$ in (3): we use $M(s,x)$, where s is a complex number, (rather than a function), to mean $M(g,x)$ for the power function $g(n) = n^{-s}$.

We consider firstly (12) with $\mathbf{v} = \mathbf{m}$. We assume throughout that N is large. As the eigenvalue λ_N is exceptionally large among all the eigenvalues of A, we handle the term $\lambda_N(\mathbf{e}_N \cdot \mathbf{m})^2$ with some care. As substitution of $-\mathbf{e}_N$ for $\mathbf{e}_N$ does not alter this term, we can take the ambiguous sign in (20) to be $+$. We note that

$$(\mathbf{e}_N \cdot \mathbf{m})^2 = \Big((\mathbf{e}_N - \hat{\mathbf{f}}) \cdot \mathbf{m}\Big)^2 + 2\Big((\mathbf{e}_N - \hat{\mathbf{f}}) \cdot \mathbf{m}\Big)(\hat{\mathbf{f}} \cdot \mathbf{m}) + (\hat{\mathbf{f}} \cdot \mathbf{m})^2 \,. \tag{33}$$

Here

$$\hat{\mathbf{f}} \cdot \mathbf{m} = \|\mathbf{f}\|^{-1}\mathbf{f} \cdot \mathbf{m} = \frac{1}{\sqrt{\zeta_2}} \sum_{n \leq N} \frac{\mu(n)}{n} = \frac{M(1,N)}{\sqrt{\zeta_2}} \ll \log N$$

and, by the Cauchy-Schwarz inequality and (20),

$$|(\mathbf{e}_N - \hat{\mathbf{f}}) \cdot \mathbf{m}| \leq \|\mathbf{e}_N - \hat{\mathbf{f}}\| \cdot \|\mathbf{m}\| = O\left(\frac{\log N}{N}\right) \cdot \sqrt{\sum_{n \leq N} \mu^2(n)} \ll \frac{\log N}{\sqrt{N}} \,.$$

By these results, together with (33) and (17), we have:

$$\lambda_N(\mathbf{e}_N \cdot \mathbf{m})^2 = O\left(N \log^2 N\right) + O\left(N^{3/2}(\log N)|M(1,N)|\right) + N^2(M(1,N))^2 \,. \tag{34}$$

Small eigenvalues make a relatively insignificant contribution here, for (13) and (19) imply that if $1 \le K \le N/2$, then

$$\sum_{k=K}^{N-K} |\lambda_k| \, (\mathbf{e}_k \cdot \mathbf{m})^2 < \frac{N}{\sqrt{K}} \sum_{n=1}^{N} (\mathbf{e}_k \cdot \mathbf{m})^2 = \frac{N}{\sqrt{K}} \|\mathbf{m}\|^2 \le \frac{N^2}{\sqrt{K}} \,.$$

By this, and by (34) and (12) (for $\mathbf{v} = \mathbf{m}$), we find that

$$\begin{aligned} \frac{\mathbf{m}^T A \mathbf{m}}{N^2} = (M(1,N))^2 \; + \; \left(\|\mathbf{m}\|^2/N\right) \sum_{\substack{1 \le k < N \\ \min\{k, N-k\} < K}} (\lambda_k/N) \, (\mathbf{e}_k \cdot \hat{\mathbf{m}})^2 \\ + O\left(K^{-1/2} + N^{-1/2}(\log N)|M(1,N)| + N^{-1} \log^2 N\right) \,, \end{aligned} \tag{35}$$

for $K = 1, 2, \ldots, N^2$. We remark that, if the second of the three terms on the right-hand side of (35) is considered in isolation, then we observe trivially from (19) that the absolute value of this term is $O(\sqrt{K}\,)$. Taking account of the context here (the relation (35) and the principal case of (5) and (3)), and noting also that $|M(1,N)| \le \|\mathbf{m}\|^2/N$ (a consequence of (11), the trivial bound $|[y] - y| < 1$, and the fact that $[N/1] - (N/1) = 0$), it is clear that this term is a bounded function of the pair $(N, K) \in \mathbb{N}^2$. This gives some idea of the gap that must be bridged if (35) is to help in the study of $M(x)$.

To reach (35) we have used the work of Section 2, on λ_N and $\mathbf{e}_N$. Our next decomposition of $\mathbf{m}^T A \mathbf{m}$ avoids such results, but nevertheless has much in common with (35).

First we use $[x] = x - \frac{1}{2} - \psi(x)$, where $\psi(x) = \{x\} - \frac{1}{2}$. We have

$$A = N^2 \mathbf{f}\mathbf{f}^T - \frac{1}{2}\mathbf{u}\mathbf{u}^T + Z \,, \tag{36}$$

where Z is the $N \times N$ matrix of elements $z_{mn} = -\psi(N^2/(mn))$, whilst $\mathbf{f}$ and $\mathbf{u}$ are as in Section 2. We have trivially $\mathrm{Tr}(Z^2) < N^2/4$; with the help of (25), (30), and an estimate for ζ_1, we obtain the sharper result that $\mathrm{Tr}(Z^2) \sim c_5 N^2$ as $N \to \infty$, where $c_5 = \beta + \frac{1}{4} + c_3 - \gamma^2 = 0.0815206\ldots$. Reasoning as in the derivation of (35), we see from (36) that, for $K = 1, 2, \ldots, N^2$ (say), one has

$$\frac{\mathbf{m}^T A \mathbf{m}}{N^2} = (\mathbf{m} \cdot \mathbf{f})^2 - \frac{(\mathbf{m} \cdot \mathbf{u})^2}{2N^2} + \frac{\mathbf{m}^T Z \mathbf{m}}{N^2} \tag{37}$$

$$\begin{aligned} &= (M(1,N))^2 \; - \frac{(M(N))^2}{2N^2} \\ &\quad + \; \left(\|\mathbf{m}\|^2/N\right) \sum_{\substack{1 \le k \le N \\ \min\{k, N+1-k\} < K}} \left(\widetilde{\lambda}_k/N\right) (\widetilde{\mathbf{e}}_k \cdot \hat{\mathbf{m}})^2 + O\left(K^{-1/2}\right) \,, \end{aligned} \tag{38}$$

where $\widetilde{\lambda}_1 \le \widetilde{\lambda}_2 \le \; \cdots \; \le \widetilde{\lambda}_N$ are the eigenvalues of Z, while $\widetilde{\mathbf{e}}_1, \ldots, \widetilde{\mathbf{e}}_N$ form the corresponding orthonormal basis of eigenvectors. We note the presence of the term $-\frac{1}{2}N^{-2}(M(N))^2$ in (38), which is not apparent in (35): in view of our results on Problem (d) of Section 2, one may regard this term as being an approximation to the term $(\|\mathbf{m}\|^2/N)(\lambda_1/N)(\mathbf{e}_1 \cdot \hat{\mathbf{m}})^2 = N^{-2}\lambda_1(\mathbf{e}_1 \cdot \mathbf{m})^2$, which is present in (35) for $K > 1$.

We remark that (37) permits an alternative, non-spectral, decomposition of $\mathbf{m}^T A\mathbf{m}$, through substituting the usual truncated Fourier expansion of the function ψ into each element of the matrix Z in (37):

$$-\psi(x) = \sum_{0<h\le H} \frac{\sin(2\pi hx)}{\pi h} + O\left(\frac{\eta}{\eta + \min\{|x-\ell| \,:\, \ell\in\mathbb{Z}\}}\right) \qquad (H = 1/\eta \ge 1).$$

This leads (via estimates from [**11**]) to the decompositions

$$\mathbf{m}^T Z\mathbf{m} = \sum_{h=1}^{H} \frac{\mathbf{m}^T Z(h)\mathbf{m}}{\pi h} + O\left(\frac{N^2(\log N)^2\log H}{H}\right) \qquad (\text{for } H = 1, 2, \dots, N \text{ (say)}),$$

where $Z(h)$ is the $N\times N$ matrix with elements $z_{mn}(h) = \sin(2\pi hN^2/(mn))$. We have yet to explore making proper use of this truncation idea.

One further approach to the decomposition of $\mathbf{m}^T A\mathbf{m}$ uses Perron's formula, Theorem 5.1 of [**9**], equation (A.8) of [**4**]. We apply Perron's formula as in Lemma 3.12 of [**12**], adapting the proof to sharpen certain error terms (parts of the improvement come from results of Shiu [**11**]). We find that if, whenever $\mathrm{Re}(s) > 1$, one has

$$F(s) = \sum_{\ell=1}^{\infty} \frac{a_\ell}{\ell^s} = \left(\sum_{m\le y} \frac{\alpha_m}{m^s}\right)\left(\sum_{n\le z} \frac{\beta_n}{n^s}\right)\zeta(s) = A(s)B(s)\zeta(s) \qquad (\text{say}), \tag{39}$$

where $y, z \ge 1$ and α_m, β_n denote complex constants of modulus less than or equal to 1, then, for any fixed $\varepsilon > 0$, when $x = yz$, in the ranges $1 < c \le 2$ and $3 \le T \le x^{1-\varepsilon}$, we have

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} F(s)x^s\,\frac{\mathrm{d}s}{s} = \sum_{\ell\le x} a_\ell + O\left(\frac{x^c\log^2 x}{(c-1)T}\right) + O_\varepsilon\left(\frac{x(\log x)^2(\log T)}{T}\right). \tag{40}$$

To link this to our matrix A, we observe that (39) implies

$$\sum_{\ell\le x} a_\ell = \sum_{\ell\le x}\sum_{m\le y}\sum_{\substack{n\le z\\ mnk=\ell}}\sum_{k} \alpha_m\beta_n = \sum_{m\le y}\sum_{\substack{n\le z\\ mnk\le x}}\sum_{k} \alpha_m\beta_n = \sum_{m\le y}\sum_{n\le z}\left[\frac{x}{mn}\right]\alpha_m\beta_n\,.$$

Setting $c = 1 + (\log x)^{-1}$ in (40), we shift the contour of integration there until it aligns with the line $\mathrm{Re}(s) = \frac12$: in so doing, we pick up a contribution from the residue of $\zeta(s)$ at its pole, $s = 1$, and also some remainder terms, which are integrals along the line segments joining $\frac12 + iT$ to $c + iT$, and $\frac12 - iT$ to $c - iT$. By Theorem 7.2 (A) of Titchmarsh [**12**], we deduce that these remainder term integrals are of size $O(x(\log x)^2\sqrt{\log T}/T)$ for almost all values of T (in a certain sense) lying in any given 'dyadic interval' $[T_0, 2T_0] \subseteq [3, 2x^{1-\varepsilon}]$. Hence we arrive at the conclusion that, for any given $\varepsilon > 0$ when $x = yz$ and $3 \le T_0 \le x^{1-\varepsilon}$, we have

$$\sum_{m\le y}\sum_{n\le z}\left[\frac{x}{mn}\right]\alpha_m\beta_n = A(1)B(1)x + \frac{1}{2\pi i}\int_{\frac12-iT}^{\frac12+iT} A(s)B(s)\zeta(s)x^s\,\frac{\mathrm{d}s}{s} + O_\varepsilon\left(\frac{x\log^3 x}{T}\right),$$

for some $T \in [T_0, 2T_0]$. We specialise this to the case $\varepsilon = 1/2$, $y = z = N$, where N is a positive integer, so that $x = N^2$, and $\alpha_n = \beta_n = \mu(n)$. We find that when $3 \le T_0 \le N$, there exists some $T \in [T_0, 2T_0]$ such that

$$\begin{aligned}\frac{\mathbf{m}^T A\mathbf{m}}{N^2} = (M(1,N))^2 + \frac{\|\mathbf{m}\|^2}{N}\int_{-T}^{T} \frac{\zeta_1 N^{2it}\zeta\left(\frac12+it\right)}{(\pi + 2\pi it)}\left(\frac{M\left(\frac12+it, N\right)}{\sqrt{\zeta_1}\|\mathbf{m}\|}\right)^2 \mathrm{d}t \\ + O\left(T_0^{-1}\log^3 N\right)\,.\end{aligned} \tag{41}$$

If we put $\mathbf{E}(s) = (1^{-s}, 2^{-s}, \ldots, N^{-s})^T$ for a fixed complex number s, then the factor $M(\frac{1}{2} + it, N)/(\sqrt{\zeta_1}\|\mathbf{m}\|)$ here may be written as $\hat{\mathbf{E}}(\frac{1}{2} + it) \cdot \hat{\mathbf{m}}$: the decomposition in (41) may therefore be considered similar in form to that in (35), although (41) involves an integration over the range $[-T, T]$, instead of the summation over a subset of the (discrete) spectrum of A that we had in (35).

4. Conclusions

Using the principal case of (5), and results such as (35), (38), or (41), we are able to approximate $M(N^2)$ by an expression involving only certain limited data: the numbers $\mu(1), \mu(2), \ldots, \mu(N)$ and either the relevant eigenvalues and eigenvectors, or else values of $\zeta(\frac{1}{2} + it)$ and $g_t(n) = n^{-\frac{1}{2}-it}$. It remains to be seen whether or not such approximations for $M(N^2)$ can be an effective tool in studying the function $M(x)$. With regard to (35) and (38), it would be helpful to find out more about the relevant eigenvalues and eigenvectors, since that might clarify the possible uses of those results. More generally, it may be worthwhile to study the eigenvalues and eigenvectors of certain submatrices of $A = A(N)$, and also (in certain non-principal cases) those of $A(g, N)$ and certain of its submatrices.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. J.-P. Cardinal. Symmetric matrices related to the Mertens function // Linear Algebra Appl. **432** (2010), 161-172.
2. D.R. Heath-Brown. Prime Numbers in Short Intervals and a Generalised Vaughan Identity // Can. J. Math. **34**, no. 6 (1982), 1365-1377.
3. M.N. Huxley. Exponential Sums and Lattice Points III // Proc. London Math. Soc. (3), **87** (2003), 591-609.
4. A. Ivić. The Riemann Zeta-Function / Dover Publications, Mineola, New York (2003).
5. H. Iwaniec and E. Kowalski. Analytic Number Theory / A.M.S. Colloquium Publications 53, American Mathematical Society, Providence RI, 2004.
6. Yu. V. Linnik. All large numbers are sums of a prime and two squares I' // Mat. Sbornik Nov. Ser. **52 (94)** (1960), 561-700.
7. Yu. V. Linnik. All large numbers are sums of a prime and two squares II' // Mat. Sbornik Nov. Ser. **53 (95)** (1961), 3-38.
8. E. Meissel. Observationes quaedam in theoria numerorum // J. Reine Angew. Math., **48** (1854), 301-316.
9. H.L. Montgomery and R.C. Vaughan. Multiplicative Number Theory I. Classical Theory // Cambridge Studies in Advanced Mathematics 97, Cambridge University Press (2007).
10. On-Line Encyclopedia of Integer Sequences // "Sloane's", http://oeis.org
11. P. Shiu. A Brun-Titchmarsh theorem for multiplicative functions // J. Reine Angew. Math., **313** (1980), 161-170.
12. E.C. Titchmarsh (revised by D.R. Heath-Brown). The Theory of the Riemann Zeta-function / Oxford Univ. Press, 1986

13. R.C. Vaughan. An Elementary Method in Prime Number Theory // Recent Progress in Analytic Number Theory, vol. 1 (Durham, 1979), Academic Press, London - New York, 1981, pp. 341-348.

REFERENCES

1. J.-P. Cardinal, 2010 "Symmetric matrices related to the Mertens function", *Linear Algebra Appl.* **432**, 161-172.

2. D.R. Heath-Brown, 1982, "Prime Numbers in Short Intervals and a Generalised Vaughan Identity", *Can. J. Math.*, **34**, no. 6, 1365-1377.

3. M.N. Huxley, 2003, "Exponential Sums and Lattice Points III", *Proc. London Math. Soc.* (3), **87**, 591-609.

4. A. Ivić, 2003, *The Riemann Zeta-Function*, Dover Publications, Mineola, New York.

5. H. Iwaniec and E. Kowalski, 2004, *Analytic Number Theory*, A.M.S. Colloquium Publications 53, American Mathematical Society, Providence RI.

6. Yu. V. Linnik, 1960, "All large numbers are sums of a prime and two squares I", *Mat. Sbornik Nov. Ser.* **52 (94)**, 561-700.

7. Yu. V. Linnik, 1961, "All large numbers are sums of a prime and two squares II", *Mat. Sbornik Nov. Ser.* **53 (95)**, 3-38.

8. E. Meissel, 1854, "Observationes quaedam in theoria numerorum", *J. Reine Angew. Math.*, **48**, 301-316.

9. H.L. Montgomery and R.C. Vaughan, 2007, *Multiplicative Number Theory I. Classical Theory*, Cambridge Studies in Advanced Mathematics 97, Cambridge University Press.

10. *On-Line Encyclopedia of Integer Sequences* ("Sloane's"), http://oeis.org

11. P. Shiu, 1980, "A Brun-Titchmarsh theorem for multiplicative functions", *J. Reine Angew. Math.*, **313**, 161-170.

12. E.C. Titchmarsh (revised by D.R. Heath-Brown), 1986, *The Theory of the Riemann Zeta-function*, Oxford Univ. Press.

13. R.C. Vaughan, 1981, "An Elementary Method in Prime Number Theory", *Recent Progress in Analytic Number Theory, vol.* 1 (Durham, 1979), Academic Press, London - New York, pp. 341-348.

Получено 01.06.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-35-39

К вопросу о теореме Бредихина и Линника

Джон Фридландер[1] — профессор кафедры математики, Университет Торонто.
e-mail: frdlndr@math.toronto.edu
Хенрик Иванец[2] — профессор кафедры математики, Ратгерский университет.
e-mail: iwaniec@math.rutgers.edu

Аннотация

Мы приводим новое доказательство теоремы Б. М. Бредихина, которая изначально была доказана путем адаптации решения проблемы Харди-Литтлвуда, полученного Линником с помощью его дисперсионного метода.

Ключевые слова: простые числа, дисперсия, теорема Бомбьери-Виноградова.

Библиография: 5 названий.

Для цитирования:
Д. Фридландер, Х. Иванец. К вопросу о теореме Бредихина и Линника // Чебышевский сборник, 2018, т. 19, вып. 3, с. 35–39.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-35-39

On a theorem of Bredihin and Linnik

John Friedlander — Professor of Department of Mathematics, University of Toronto.
e-mail: frdlndr@math.toronto.edu
Henryk Iwaniec — Professor of Department of Mathematics, Rutgers University.
e-mail: iwaniec@math.rutgers.edu

Abstract

We give a new proof of a theorem of B. M. Bredihin which was originally proved by extending Linnik's solution, via his dispersion method, of a problem of Hardy and Littlewood.

Keywords: primes, dispersion, Bombieri-Vinogradov theorem.

Bibliography: 5 titles.

For citation:
J. Friedlander, H. Iwaniec, 2018, "On a theorem of Bredihin and Linnik" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 35–39.

[1]Supported in part by NSERC grant A5123.
[2]Supported in part by NSF grant DMS-1406981

Dedicated to the memory of Yu. V. Linnik.

1. Introduction

Among the many beautiful consequences of Linnik's dispersion method is an asymptotic formula for the number of solutions to the equation

$$p = a^2 + b^2 + 1$$

in primes $p \leqslant x$ and integers a and b. This result of 1965, due to Bredihin [2] was a follow-up to Linnik's celebrated work on the Hardy-Littlewood problem, cf. Chapter 7 of [5]. The involved arguments are lengthy and complicated, though very inventive. Due to much progress over the intervening years, much shorter arguments can now be put forward. This of course does not mean that they are shorter ab-initio. Our purpose here is to illustrate how these arguments can be applied.

THEOREM 1. *Let $S(x)$ be the number of solutions to*

$$p = a^2 + b^2 + 1 \tag{1}$$

in integers a and b and primes $p \equiv 3(\mod 8)$, $p \leqslant x$. We have

$$S(x) = c\,\frac{x}{\log x} + O\Big(x\Big(\frac{\log\log x}{\log x}\Big)^2\Big), \tag{2}$$

where the constant c is given by

$$c = \frac{\pi}{2}\prod_p\Big(1 + \frac{\chi(p)}{p(p-1)}\Big), \tag{3}$$

with χ being the Dirichlet character of conductor 4.

The other reduced residue classes modulo 8 can be covered by essentially the same arguments but we do not treat them.

Note that the theorem shows that the integers $p-1$ tend to have about as many representations as the sum of two squares as does a typical integer n. Recall also that, if the number of representable $p-1$ is counted without multiplicity in a and b, then the order of magnitude is given by $x/(\log x)^{3/2}$ by a theorem of the second-named author [4].

2. Dirichlet divisor switching

Let $\lambda = 1 * \chi$ that is

$$\lambda(n) = \sum_{ab=n}\chi(a) \tag{4}$$

This is similiar in many respects to the divisor function $\tau(n)$. The number of representations of n as the sum of two squares is equal to $4\lambda(n)$. If $n \equiv 1(\mod 4)$ then, in (4), $\chi(a)$ can be replaced by $\chi(b)$; therefore we can write

$$\lambda(n) = \sum_{\substack{a|n\\ a\leqslant y}}\chi(a) + \sum_{\substack{b|n\\ b<n/y}}\chi(b) \tag{5}$$

for any $y > 0$. We can refine this partition by integrating over y against a smooth weight function. Let $w(t)$ be a smooth function supported on $1 \leqslant t \leqslant 2$ such that

$$\int_0^\infty w(t)t^{-1}dt = 1. \tag{6}$$

Let $Y \geqslant 1$, multiply (5) by $w(y/Y)$ and integrate with the measure $y^{-1}dy$, getting

$$\lambda(n) = \int_0^\infty \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{n}{yY}\big)\Big]\Big(\sum_{\substack{b|n\\ b<y}} \chi(b)\Big)\frac{dy}{y}\ . \tag{7}$$

Note that if $X < n \leqslant 2X$ we can choose $Y = \sqrt{X}$ so the integration in (7) runs over the segment $\frac{1}{2}\sqrt{X} < y < 2\sqrt{X}$.

3. Primes in arithmetic progressions

The key input which greatly streamlines the proof is the main result of [1] which gives asymptotics of Bombieri-Vinogradov type for the distribution of primes in arithmetic progressions and which treats moduli of the progression which go beyond the range of that which can be sucessfully handled even on the assumption of the Generalized Riemann Hypothesis.

We state this restricted to a range somewhat lesser than that in [1], which is however sufficient for our needs and is conveniently recorded as Theorem 2.2.1 of [3].

$$\sum_{\substack{q\leqslant Q\\ (q,a)=1}} \Big|\pi(x;q,a) - \frac{\pi(x)}{\varphi(q)}\Big| \ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{8}$$

for $Q = \sqrt{x}(\log x)^A$ with any $a \neq 0$, $A \geqslant 0$, $x \geqslant 3$, the implied constant depending only on a and A.

We actually require a slightly modified form of (8) which follows from it in two easy steps. In the first place we have

$$\sum_{\substack{q\leqslant Q\\ (q,a)=1\\ (q,k)=1}} \Big|\sum_{\substack{p\leqslant x\\ p\equiv a(\bmod q)\\ p\equiv \ell(\bmod k)}} 1 - \frac{\pi(x)}{\varphi(qk)}\Big| \ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{9}$$

for $Q = \sqrt{x}(\log x)^A$ with any $a \neq 0$, $k \geqslant 1$, $(\ell, k) = 1$, $A \geqslant 0$, $x \geqslant 3$, the implied constant depending only on a,k and A. To this end one merely splits the indexed variables into classes modulo k, which is harmless for k fixed.

In the second step we modify (9) to a counting of primes with smooth weight.

LEMMA 1. *Let $f(t)$ be a smooth function supported on $1 \leqslant t \leqslant 2$. We have*

$$\sum_{\substack{q\leqslant Q\\ (q,a)=1\\ (q,k)=1}} \Big|\sum_{\substack{p\leqslant x\\ p\equiv a(\bmod q)\\ p\equiv \ell(\bmod k)}} f\big(\frac{p}{X}\big) - \frac{1}{\varphi(qk)}\sum_p f\big(\frac{p}{X}\big)\Big| \ll x\Big(\frac{\log\log x}{\log x}\Big)^2 \tag{10}$$

for $Q = \sqrt{x}(\log x)^A$ with any $a \neq 0$, $k \geqslant 1$, $(\ell, k) = 1$, $A \geqslant 0$, $x \geqslant 3$, the implied constant depending only on a,k, A and f.

Proof. We write

$$f\big(\frac{p}{X}\big) = -\int_{p/X}^\infty f'(t)dt.$$

Given $1 \leqslant t \leqslant 2$ this implies $p \leqslant tX$. Applying (9) with $x = tX$ and integrating the result over t, we derive (10). ∎

4. Proof of the theorem

We have

$$S(x) = 4 \sum_{\substack{p \leqslant x \\ p \equiv 3 (\mod 8)}} \lambda\big(\frac{p-1}{2}\big). \tag{11}$$

We are going to evaluate

$$T(X) = S(2X) - S(X) = 4 \sum_{\substack{X < p \leqslant 2X \\ p \equiv 3 (\mod 8)}} \lambda\big(\frac{p-1}{2}\big) \tag{12}$$

for every $X \geqslant 3$. Applying (7) we write

$$T(X) = 4 \int \sum_{b<y} \chi(b) \sum_{\substack{X < p \leqslant 2X \\ p \equiv 1 (\mod b) \\ p \equiv 3 (\mod 8)}} \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p-1}{2yY}\big) \Big] \frac{dy}{y}$$

where we choose $Y = \sqrt{X}$. Here we can replace $w((p-1)/2yY)$ by $w(p/2yY)$ up to an error term $O(1/yY)$ which contributes to $T(X)$ a bounded amount:

$$T(X) = 4 \int \sum_{b<y} \chi(b) \sum_{\substack{X < p \leqslant 2X \\ p \equiv 1 (\mod b) \\ p \equiv 3 (\mod 8)}} \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p}{2yY}\big) \Big] \frac{dy}{y} + O(1)\,.$$

Note that the integration runs over the segment $\frac{1}{4}\sqrt{X} < y < 2\sqrt{X}$. Now we can apply (9) for the first term and (10) for the second term with $q = b$, $k = 8$, $\ell = 3$, getting

$$T(X) = \int \sum_{b<y} \frac{\chi(b)}{\varphi(b)} \sum_{X < p \leqslant 2X} \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p}{2yY}\big) \Big] \frac{dy}{y} + O\Big(X \Big(\frac{\log\log X}{\log X} \Big)^2 \Big)\,.$$

Next, we replace the sum over $b < y$ by the complete series

$$c_1 = \sum_b \frac{\chi(b)}{\varphi(b)} = L(1,\chi) \prod_p \Big(1 + \frac{\chi(p)}{p(p-1)} \Big) \tag{13}$$

up to an error term $O(1/y)$ which contributes to $T(X)$ at most $O(\sqrt{X}/\log X)$. Now the free integration over y yields (see (6))

$$\int \Big[w\big(\frac{y}{Y}\big) + w\big(\frac{p}{2yY}\big) \Big] \frac{dy}{y} = 2\,.$$

Therefore,

$$T(X) = 2c_1\big(\pi(2X) - \pi(X)\big) + O\Big(X \Big(\frac{\log\log X}{\log X} \Big)^2 \Big)\,.$$

Summing this over $X = 2^{-n}x$, $n = 1, 2, 3, \ldots$, we derive (2).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli III // it J. Amer. Math. Soc. 2, 1989, 215–224.

2. B.M. Bredihin, Binary additive problems of indeterminate type. II. Analogue of the problem of Hardy and Littlewood // Izv. Akad. Nauk SSSR Ser. Mat. 27, 1963, 577–612.

3. J.B. Friedlander and H. Iwaniec, Opera de Cribro, // Amer. Math. Soc. Colloq. Pub. 57 AMS (Providence), 2010.

4. H. Iwaniec, Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form // Acta Arith. 21, 1972, 203–234.

5. Yu. V. Linnik, The Dispersion Method in Binary Additive Problems (translated from the Russian by S. Schuur) / AMS (Providence), 1963.

REFERENCES

1. E. Bombieri, J.B. Friedlander and H. Iwaniec, 1989, Primes in arithmetic progressions to large moduli III, *J. Amer. Math. Soc.* 2, 215–224.

2. B.M. Bredihin, 1963, Binary additive problems of indeterminate type. II. Analogue of the problem of Hardy and Littlewood, *Izv. Akad. Nauk SSSR Ser. Mat.* 27, 577–612.

3. J.B. Friedlander and H. Iwaniec, 2010, Opera de Cribro, *Amer. Math. Soc. Colloq. Pub.* 57 AMS (Providence).

4. H. Iwaniec, 1972, Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form, *Acta Arith.* 21, 203–234.

5. Yu. V. Linnik, 1963, The Dispersion Method in Binary Additive Problems (translated from the Russian by S. Schuur), AMS (Providence).

Получено 27.05.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.334+511.335 DOI 10.22405/2226-8383-2018-19-3-40-45

Об одном свойстве функционалов Маасса и Шинтани[1]

Быковский Виктор Алексеевич — доктор физико-математических наук, профессор, член-корреспондент РАН, Тихоокеанский государственный университет, Хабаровск.
e-mail: vab@iam.khv.ru

Аннотация

Функционалы Маасса и Шинтани играют фундаментальную роль при изучении классических задач аналитической теории чисел: задачи Линника о распределении целых точек на гиперболоидах и задачи о среднем значении функции числа делителей квадратичных полиномов.

В работе доказывается, что эти функционалы на пространствах, состоящих из нечетных функций (нечетных относительно оператора отражения, а для голоморфных форм веса, который не делится на 4) равны нулю.

Ключевые слова: автоморфные формы, функционалы Маасса и Шинтани, спектральная теория автоморфных функций.

Библиография: 5 названий.

Для цитирования:
В. А. Быковский. Об одном свойстве функционалов Маасса и Шинтани // Чебышевский сборник, 2018, т. 19, вып. 3, с. 40–45.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.334+511.335 DOI 10.22405/2226-8383-2018-19-3-40-45

On one property of the Maass and Shintani functionals[2]

Bykovsky Victor Alekseevich — doctor of physical and mathematical Sciences, Professor, corresponing member of RAS, Pacific national University, Khabarovsk.
e-mail: vab@iam.khv.ru

Abstract

Functionals of Maass and Shintani play a fundamental role in the study of classical problems of analytic number theory: the Linnik problem on the distribution of integer points on hyperboloids and the problem of the mean value of the function of the number of divisors of quadratic polynomials.

In the paper it is proved that these functionals on spaces consisting of odd functions (odd with respect to the reflection operator, and for holomorphic forms of weight, which is not divisible by 4) are zero.

Keywords: automorphic forms, Maass and Shintani functionals, spectral theory of automorphic functions.

Bibliography: 5 titles.

[1]Исследование выполнено за счет гранта Российского научного фонда (проект № 18-41-05001).
[2]The study was performed by a grant of Russian scientific Foundation (project No. 18-41-05001).

For citation:
V. A. Bykovskii, 2018, "On one property of the Maass and Shintani functionals", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 40–45.

Посвящается 100-летию Ю. В. Линника.

1. Введение

В работе [1] Маасс определил функционалы на пространствах автоморфных функций, ассоциированные с дискриминантами целочисленных бинарных квадратичных форм. В работе [2] Шинтани определил подобного рода функционалы на пространствах голоморфных параболических форм четного веса. В настоящей работе доказывается, что эти функционалы на пространствах, состоящих из нечетных функций (нечетных относительно оператора отражения, а для голоморфных форм веса, который не делится на 4) равны нулю.

2. Определения и вспомогательные сведения

Мультипликативная группа $SL_2(\mathbb{Z})$, состоящая из матриц

$$M = \begin{pmatrix} m & n \\ l & h \end{pmatrix} \qquad (m,n,l,h \in \mathbb{Z}; \det(M) = 1)$$

действует слева на верхней полуплоскости

$$\mathbb{H} = \{z = x + iy \mid x, y \in \mathbb{R}; y > 0\}$$

посредством дробно-линейных преобразований

$$M(z) = \frac{mz+n}{lz+h}.$$

Так как $M(z) = (-M)(z)$, то M и $-M$ обычно отождествляют и вместо $SL_2(\mathbb{Z})$ работают с факторгруппой

$$\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

На пространстве автоморфных относительно Γ функций $f : \mathbb{H} \to \mathbb{C}$, для которых

$$f(M(z)) = f(z) \qquad \forall M \in \Gamma,$$

действует оператор отражения (инволюция)

$$Tf(z) = f(-\overline{z}).$$

Автоморфная функция f называется четной (относительно T), если $Tf = f$, и нечетной, если $Tf = -f$. Любую f можно записать в виде

$$f = f_+ + f_-,$$

где

$$f_+ = \frac{1}{2}(f + Tf), \qquad f_- = \frac{1}{2}(f - Tf),$$

соответственно, четная и нечетная функции.

Пусть

$$Q(X,Y) = aX^2 + bXY + cY^2$$

— невырожденная бинарная квадратичная форма с целыми коэффициентами и дискриминантом

$$d = b^2 - 4ac \equiv 0, 1 \pmod 4.$$

Положим для $d > 0$

$$\mathbb{K}_{\mathbb{Z}}(d) = \{(a,b,c) \in \mathbb{Z}^3 \mid b^2 - 4ac = d\},$$

а для $d < 0$

$$\mathbb{K}_{\mathbb{Z}}(d) = \{(a,b,c) \in \mathbb{Z}^3 \mid b^2 - 4ac = d; a > 0, c > 0\}.$$

Во втором случае квадратичные формы положительно определены.

Замечание. *В дальнейшем мы будем иметь дело с дискриминантами d, отличными от квадрата.*

Группа действует слева на $\mathbb{K}_{\mathbb{Z}}(d)$ по правилу

$$M : \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \to M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M^t = \begin{pmatrix} a(M) & b(M)/2 \\ b(M)/2 & c(M) \end{pmatrix}.$$

Оно соответствует линейной замене переменных X и Y для квадратичной формы

$$Q(X,Y) = aX^2 + bXY + cY^2 \to$$
$$(MQ)(X,Y) = Q(mX + lY, nX + hY) = a(M)X^2 + b(M)XY + c(M)Y^2.$$

Для $d > 0$ сопоставим каждой точке $(a,b,c) \in \mathbb{K}_{\mathbb{Z}}(d)$ ориентированную полуокружность

$$\{z \in \mathbb{H} \mid a - b\mathrm{Re}z + c|z|^2 = 0\}$$

с параметрическим представлением

$$L(\varphi) = \mathcal{P}_d(a,b,c)(\varphi) = \mathrm{Ce}(L) + \mathrm{Ra}(L)\exp(\mathrm{sign}(c)i\varphi) \qquad (0 < \varphi < \pi),$$

где

$$\mathrm{Ce}(L) = \frac{b}{2c}, \qquad \mathrm{Ra}(L) = \frac{\sqrt{d}}{2c}.$$

Она начинается из точки $x_1 = \mathrm{Ce}(L) + \mathrm{Ra}(L)$ и кончается в $x_2 = \mathrm{Ce}(L) - \mathrm{Ra}(L)$ — корнях квадратного уравнения $a - bx - cx^2 = 0$. Преобразование $(a,b,c) \to (-a,-b,-c)$ меняет ориентацию элементов множества

$$\widehat{\mathbb{H}}_{\mathbb{Z}}(d) = \mathcal{P}_d(\mathbb{K}_{\mathbb{Z}}(d))$$

на противоположную. Для $d < 0$ соответствие

$$(a,b,c) \to \frac{b}{2c} + \frac{\sqrt{d}}{2c}$$

определяет биекцию

$$\mathcal{P}_d : \mathbb{K}_{\mathbb{Z}}(d) \to \mathbb{H} = \mathbb{H}_{\mathbb{Z}}(d)$$

с обратной к ней

$$\mathcal{P}_d^{-1}(z) = \left(\frac{\sqrt{|d|}}{2} \cdot \frac{|z|^2}{\mathrm{Im}z}, \sqrt{|d|}\frac{\mathrm{Re}z}{\mathrm{Im}z}, \frac{\sqrt{|d|}}{2} \cdot \frac{1}{\mathrm{Im}z} \right).$$

При этом для любого элемента M из Γ диаграмма

$$\begin{array}{ccc} \mathbb{K}_{\mathbb{Z}}(d) & \xrightarrow{M} & \mathbb{K}_{\mathbb{Z}}(d) \\ \Big\downarrow{\scriptstyle \mathcal{P}_d} & & \Big\downarrow{\scriptstyle \mathcal{P}_d} \\ \widehat{\mathbb{H}}_{\mathbb{Z}}(d) & \xrightarrow[M]{} & \widehat{\mathbb{H}}_{\mathbb{Z}}(d) \end{array}$$

коммутативна. Стабилизатор Γ_L любого элемента L из $\widehat{\mathbb{H}}_{\mathbb{Z}}(d)$ — бесконечная циклическая группа. Ее образующую M_L выберем так, чтобы переход от точки z по дуге L к $M_L(z)$ соответствовал ориентации L. При этом для любой точки z из L в качестве $\Gamma_L\backslash L$ можно выбрать дугу $(z, M_L(z))$.

Для дискриминантов d на линейном пространстве непрерывных автоморфных функций определим линейный функционал

$$\Omega_d(f) = \frac{1}{2}\left(\frac{\sqrt{d}}{2}\right)^{-1/2} \sum_{L\in\Gamma\backslash\widehat{\mathbb{H}}_{\mathbb{Z}}(d)} \int\limits_{\Gamma_L\backslash L} f(z)\sqrt{d\zeta^2}$$

с Γ-инвариантной метрикой

$$d\zeta^2 = \frac{dx^2+dy^2}{y^2}.$$

Пусть k — натуральное число. Голоморфная на верхней полуплоскости $\mathbb{H}$ функция f называется параболической формой веса $2k$, если для любого элемента M из Γ

$$(f|_{2k}M)(z) = (lz+h)^{-2k} f(M(z)) = f(z)$$

и автоморфная функция $y^k|f(z)|$ ограничена на $\mathbb{H}$. Обозначим через S_{2k} линейное пространство всех параболических форм веса $2k$ со скалярным произведением Петерсона

$$\langle f, g\rangle_{2k} = \iint\limits_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}y^{2k-2}\,dxdy.$$

Оно конечномерно и

$$\dim S_{2k} = \begin{cases} [k/6], \text{ если } k \not\equiv 1 \pmod 6 \\ [k/6]-1, \text{ если } k \equiv 1 \pmod 6. \end{cases}$$

В частности, S_{2k} пусто для $k = 1,2,3,4,5,7$ и одномерно для $k = 6,8,9,10,11,13$.

Функционалы Шинтани (см. [2]) определяются по формуле

$$\Omega_d^{(2k)}(f) = \frac{1}{2}\left(\frac{\sqrt{d}}{2}\right)^{-k-\frac{1}{2}} \sum_{L\in\Gamma\backslash\widehat{\mathbb{H}}_{\mathbb{Z}}(d)} \int\limits_{\Gamma_L\backslash L} g_L(z)\,dz$$

с инвариантной относительно Γ_L дифференциальной формой

$$g_L(z)\,dz = (a(L) - b(L)z + c(L)z^2)^{k-1} f(z)\,dz,$$

где $(a(L), b(L), c(L)) = \mathcal{P}_d^{-1}(L)$.

Для $d < 0$

$$\Omega_d(f) = \left(\frac{|d|}{4}\right)^{-\frac{1}{4}} \left(\sum_{z\in\Gamma\backslash\mathbb{H}_{\mathbb{Z}}(d)} \frac{1}{|\Gamma_z|} f(z)\right).$$

3. Основной результат

Теорема. *Пусть d — любой дискриминант, отличный от квадрата. Тогда*

1) Для любой нечетной автоморфной функции f

$$\Omega_d(f) = 0;$$

2) Для любого нечетного k и любой функции $f \in S_{2k}$

$$\Omega_d^{(2k)}(f) = 0.$$

Доказательство. На $\mathbb{K}_{\mathbb{Z}}(d)$ действует инволюция

$$(a, b, c) \to (a, -b, c).$$

Ей соответсвует инволюция

$$z \to -\overline{z}$$

на верхней полуплоскости $\mathbb{H}$, которая индуцируется биекцией $\mathcal{P}_d$. Принимая во внимание коммутативную диаграмму из предыдущего параграфа, отсюда находим что

$$\Omega_d(f) = -\Omega_d(f).$$

Действуя точно также в случае 2) и принимая во внимание то, что инволюция $z \to -\overline{z}$ меняет ориентацию на противоположную, получим

$$\Omega_d^{(2k)}(f) = -\Omega_d^{(2k)}(f) = 0.$$

4. Заключение

Функционалы Маасса и Шинтани играют фундаментальную роль при изучении классических задач аналитической теории чисел: задачи Линника о распределении целых точек на гиперболоидах и задачи о среднем значении функции числа делителей квадратичных полиномов. По этому поводу см. работы [3–5].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Maass H. Über die räumliche Verteilung der Punkte in Gittern mit indefiniter Metrik. Math. Ann., **138**, 1959. P. 287–315.

2. Shintani T. On construction of holomorphic cusp forms of half–integral weight, Nagoya Math. J. V. 58, 1975. P. 83–126.

3. Быковский В.А. Спектральные разложения некоторых автоморфных функций и их теоретико-числовые приложения. В кн.: Записки научных семинаров. ЛОМИ. Л.: "Наука", 1984, С. 15–33.

4. Duke W. *Hyperbolic distribution problems and half-integral weight*, Invent. Math., **92**, 1988. P. 73–90.

5. Liu S. and Masri R. The average of the divisor function over values of quadratic polynomial, Proc. Amer. Math. Soc., 143, 2015. P. 4143–4160.

REFERENCES

1. Maass H, 1959, "Über die räumliche Verteilung der Punkte in Gittern mit indefiniter Metrik", *Math. Ann.*, **138**. P. 287–315.

2. Shintani T, 1975, "On construction of holomorphic cusp forms of half–integral weight", Nagoya Math. J. V. 58, pp. 83–126.

3. Bykovskij V. A., 1984, "Spektral'nye razlozheniya nekotoryh avtomorfnyh funkcij i ih teoretiko-chislovye prilozheniya", *V kn.: Zapiski nauchnyh seminarov. LOMI.* L.: "Nauka", pp. 15–33.

4. Duke W., 1984, "Hyperbolic distribution problems and half-integral weight", *Invent. Math.*, **92**, X pp. 73–90.

5. Liu S. and Masri R., 2015, "The average of the divisor function over values of quadratic polynomial", *Proc. Amer. Math. Soc.*, 143, pp. 4143–4160.

Получено 17.09.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.313:511.331.1:511.526 DOI 10.22405/2226-8383-2018-19-3-46-60

Гипотеза Римана как чётность специальных биномиальных коэффициентов

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

Аннотация

Гипотеза Римана имеет много эквивалентных переформулировок. Часть из них является арифметическими, то есть утверждениями о свойствах целых или натуральных чисел. Простейшую логическую структуру имеют переформулировки из класса Π_1^0 арифметической иерархии, имеющие вид "для любых $x_1, \ldots, x_m$ имеет место $A(x_1, \ldots, x_m)$", где A – алгоритмически проверяемое отношение. Примером может служить переформулировка гипотезы Римана в виде утверждения о том, что некоторое диофантово уравнение не имеет решений (такое конкретное уравнение может быть явно указано).

Хотя логическая структура такой переформулировки очень проста, известные способы построения такого диофантова уравнения приводят к уравнениям, требующим для своей записи нескольких страниц. С другой стороны, известны весьма краткие по записи переформулировки, также принадлежащие классу Π_1^0. Примерами могут служить три критерия справедливости гипотезы Римана, которые предложили Ж.-Л. Николас, Г. Робин, и Дж. Лагариас. Недостатком этих переформулировок (по сравнению с диофантовым уравнением) является использование более "сложных" констант и функций, чем натуральные числа и сложение и умножение, достаточные для построения диофантова уравнения.

В работе приводится система из 9 условий, налагаемых на 9 переменных. Для формулировки этих условий используются только сложение, умножение, возведение в степень (унарное, с фиксированным основанием 2), функция "остаток от деления", неравенства, сравнения по модулю и биномиальный коэффициент. Вся система может быть явно выписана на одной странице. Доказано, что построеная система условий несовместна в том и только том случае, когда гипотеза Римана верна.

Ключевые слова: гипотеза Римана, биномиальные коэффициенты.

Библиография: 36 названий.

Для цитирования:
Ю. В. Матиясевич. Гипотеза Римана как чётность специальных биномиальных коэффициентов // Чебышевский сборник, 2018, т. 19, вып. 3, с. 46–60.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.313:511.331.1:511.526 DOI 10.22405/2226-8383-2018-19-3-46-60

The Riemann hypothesis as the parity of special binomial coefficients

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

Abstract

The Riemann Hypothesis has many equivalent reformulations. Some of them are arithmetical, that is, thewy are statements about properties of integers or natural numbers. Among them the reformulations with the simplest logical structure are those from the class Π_1^0 from the arithmetical hierachy, that is, having the form "for every $x_1, \ldots, x_m$ relation $A(x_1, \ldots, x_m)$ holds", where A is decidable. As an example one can take the reformulation of the Riemann Hypothsis as the assertion that certain Diophantine equation has no solution (such particular equation can be given explicitly).

While the logical structure of this reformulation is indeed very simple, all known methods for constructing such Diophantine equation produce equations occupying several pages. On the other hand, there are known other reformulation also belonging to class Π_1^0 but having rather short wording. As examples one can mention the criteria of the validity of the Riemann Hypothesis proposed by J.-L. Nicolas, by G. Robin, and by J. Lagarias. The shortcoming of these reformulations (as compared to Diophantine equations) consists in the usage of constants and funtions which are "more complicated" than integers and addition and multiplication sufficient for constructing Diophantine equations.

The paper presents a system of 9 conditions imposed on 9 variables. In order to state these conditions one needs only addition, multiplication, exponentiation (unary, with fixed base 2), congruences and remainders, inequalities, and binomial coefficient. The whole system can be written explicitly on a single sheet of paper. It is proved that the system is inconsistent if and only if the Riemann Hypothesis is true.

Keywords: the Riemann Hypothesis, binomial coefficients.

Bibliography: 36 titles.

For citation:
Yu. V. Matiyasevich, 2018, "The Riemann hypothesis as the parity of special binomial coefficients" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 46–60.

1. Введение

Гипотеза Римана, подобно большинству великих проблем, имеет огромное количество эквивалентных переформулировок. Их обзору посвящено, например, недавно вышедшее двухтомное издание [1, 2]. Такие переформулировки даются в очень разных терминах, но мощная техника *арифметизации*, равитая К. Гёделем [3] позволяет легко превратить их в утверждения о целых или о натуральных числах. В этой работе мы ограничися такими *арифметическими* переформулировками.

А. Тьюринг, внёсший большой вклад в верификацию гипотезы Римана (см., например, [1, 4, 5, 6, 7]), интересовался также вопросом, сколь простой, *с логической точки зрения*, может быть переформулировка гипотезы Римана. Он ввёл в [8] понятие *теоретико-числовой теоремы*:

> By a number-theoretic theorem we shall mean a theorem of the form "$\theta(x)$ vanishes for infinitely many natural numbers x", where $\theta(x)$ is a primitive recursive function. ... An alternative form for number-theoretic theorems is "for each natural number x there exists a natural number y such that $f(x, y)$ vanishes", where $f(x, y)$ is primitive recursive.

Теоретико-числовые теоремы в смысле Тьюринга эквивалентны доказуемым формулам из класса Π_2^0 *арифметической иерархии*. Этот класс может быть описан как класс формул вида

$$\forall x_1 \dots x_m \exists y_1 \dots y_n A(x_1, \dots, x_m, y_1, \dots, y_n), \tag{1}$$

где $A(x_1, \dots, x_m, y_1, \dots, y_n)$ – алгоритмически проверяемое отношение между натуральными числами x_1, ..., x_m, $y_1, \dots, y_n$. Мотивируя свое определение, Тьюринг построил формулу из класса Π_2^0, эквивалентную гипотезе Римана.

Этот результат был усилен Г. Крайзелем [9], который дал переформулировку гипотезы Римана посредством формулы из класса Π_1^0, состоящего из формул вида

$$\forall x_1 \dots x_m A(x_1, \dots, x_m). \tag{2}$$

Такие формулы можно охарактеризовать, как *эффективно опровергаемые*: если формула (2) является ложной, то для установления этого достаточно предъявить один конкретный набор чисел $x_1 \dots x_n$, не находящихся в отношении A. Пользуясь алгоритической разрешимостью этого отношения, можно построить, например, машину Тьюринга (или написать программу на каком-либо языке программирования), которая будет перебирать по очереди всевозможные значения $x_1 \dots x_n$ в поисках требуемого контпримера. Такая машина/программа будет работать неограниченно долго в том и только случае, когда формула (2) истина.

Благодаря результату Крайзеля появилась возможность указать такую машину/программу для гипотезы Римана, и в ряде работ это было сделано. С. Ааронсон и А. Едидиа [10] построили машину Тьюринга с двухбуквенным ленточным алфавитом, которая, начав работу с пустой лентой, никогда не остановится, если и только если гипотеза Римана верна. В [10] машина имеет 5372 состояния; это было в дальнейшем улучшено до 744 состояний (см. [11]). Х. Калуд, Е. Калуд и М. Динин [12, 13] и автор [14] построили разные версии *регистровых машин* с аналогичным свойством.

В 1970 году автор сделал последний шаг в доказательстве того, что сейчас часто называется ДПРМ-теоремой[1]. Этот результат позволяет по произвольной формуле из класса Π_1^0 построить эквивалентную ей формулу из того же класса, имеющую следующий специальный вид:

$$\forall x_1 \dots x_m P(x_1, \dots, x_m) \neq 0, \tag{3}$$

где $P(x_1, \dots, x_m)$ – многочлен с целыми коэффициентами. В частности, можно явно указать многочлен $R(x_1, \dots, x_m)$ такой, что гипотеза Римана эквивалентна утверждению о том, что диофантово уравнение

$$R(x_1, \dots, x_m) = 0 \tag{4}$$

[1] По первым буквам фамилий авторов теоремы – М. Дейвиса, Х. Патнема, Дж. Робинсон и автора этой статьи; детальные доказательства теоремы приведены, например, в [15, 16].

не имеет решений. Способы построения такого многочлена описаны в [17, раздел 2] и [16, параграф 6.4]; больше деталей дано в [18, 19]; см. также [20].

Переформулировка гипотезы Римана в виде (3) имеет, несомненно, чрезвычайно простую *структуру*: используются только кванторы общности, а проверяемое условие сводится к вычислению значения многочлена. С другой стороны, хотя в таком многочлене может быть всего 9 переменных ([21], детали см. в [22]), все ранее известные способы дают многочлены, требующие нескольких страниц для своего явного выписывания.

Известно немало других переформулировок гипотезы Римана в виде (2) со сложнее проверяемыми, но зато коротко записываемыми отношениями A; несколько таких примеров приведено ниже.

Многие классические результаты близки по форме к (2), но используют, например, символ O-большое, содержащий скрытый квантор существования. Такой квантор можно устранить, найдя явное значение соответствующей константы.

Для построения диофантова уравнения (4) в [17] и машины Тьюринга в [10] была использована переформулировка гипотезы Римана, которую предложил Х. Шапиро (см. [17, раздел 2] и [1, раздел 10.2]). Она даётся в терминах *функции Чебышева* $\psi(n)$, которая определяется следующим образом:

$$\psi(n) = \ln(\mathrm{LCM}(1,\ldots,n)) = \ln(2)\log_2(\mathrm{LCM}(1,\ldots,n)), \tag{5}$$

где LCM обозначает наименьшее общее кратное. Гипотеза Римана эквивалентна утверждению, что

$$\psi(n) = n + O\sqrt{n}\ln^2(n). \tag{6}$$

Для устранения неявной константы, подразумеваемой здесь в символе O-большое, Шапиро рассмотрел сумматорную функцию

$$\psi_1(n) = \sum_{1\leqslant m<n} \psi(m) \tag{7}$$

и доказал, что гипотеза Римана эквивалентна следующему неравенству с явной константой:

$$\left|\psi_1(m) - \frac{m^2}{2}\right| < 6m\sqrt{m}. \tag{8}$$

Позднее Л. Шёнфельд ([23], см. также [1, теорема 4.9]) нашёл явное значение константы в (6), а именно, доказал, что гипотеза Римана эквивалентна справедливости неравенства

$$|\psi(n) - n| < \frac{1}{8\pi}\sqrt{n}\ln(n)^2, \tag{9}$$

при $n \geqslant 74$. Как раз использование этого критерия вместо (8) позволило упростить построение многочлена (3) в [16] и уменьшить количество состояний у машины Тьюринга в [11].

Ж.-Л. Николас ([24], см. также [1, теорема 5.31]) установил, что гипотеза Римана эквивалентна неравенству

$$\mathrm{e}^\gamma \log(\log(N_n)) < \frac{N_n}{\phi(N_n)}, \tag{10}$$

где $\mathrm{e} = 2.71828\ldots$, $\gamma = 0.577215\ldots$ – постоянная Эйлера, N_n – произведение n первых простых чисел, $\phi(m)$ – функция Эйлера (количество чисел, которые меньше m и взаимно просты с этим числом).

Г. Робин ([25], см. также [1, теорема 7.16]) установил, что гипотеза Римана эквивалентна справедливости при $n \geqslant 5040$ неравенства

$$\sigma(n) < \mathrm{e}^\gamma n \log(\log(n)), \tag{11}$$

где $\sigma(n)$ – сумма всех делителей n. Это необходимое и достаточное условие известно также как *критерий Раманудджана–Робина*, поскольку С. Рамануджан доказал неравенство (11) для достаточно больших n в предположении гипотезы Римана.

Дж. Лагариас ([26], см. также [1, Теорема 7.18]) заменил правую часть неравенства (11) и получил ещё одно условие, необходимое и достаточное для справедливости гипотезы Римана:

$$\sigma(n) < H_n + \mathrm{e}^{H_n} \log(H_n), \tag{12}$$

где $H_n = 1 + 1/2 + \cdots + 1/n$ и n может быть произвольным.

Условия типа (8)–(12) коротко записываются и алгоритмически проверяюся, однако они содержат константы и функции, такие как $\psi(n)$, N_n, $\phi(n)$, $\sigma(n)$, которые являются "сложными" по сравнению с целыми коэффициентами и операциями сложения и умножения, используемыми в (4). Цель настоящей работы – предложить "компромисную" переформулировку гипотезы Римана. Её преимущество перед диофантовым уравнением состоит в том, что все условия можно явно выписать на одной странице. Недостатком по сравнению с (4), но преимуществом по сравнению с (8)–(12), является набор используемых функции. Наряду со сложением и умножением в нашем необходимом и достаточном условии участвуют лишь возведение в степень (только унарное, с основанием 2), квадратный корень (легко устраняемый), $\mathrm{rem}(a, b)$ (остаток от деления a на b), неравенства и сравнения по модулю, а также биномиальный коэффициент, играющий ключевую роль.

Биномиальные коэффициенты обладают удивительно большой выразительной силой. Х. Манн и Д. Шенкс [27] дали критерий простоты в виде делимости определённых элементов треугольника Паскаля. Л. Шю и Р. Шуе [28] переформулировали Великую теорему Ферма в виде равенства нулю некоторой комбинаторной суммы произведений биномиальных коэффициентов. Автор [29] дал в виде делимости одного биномиального коэффициента критерии того, что

1. число p является простым;
2. числа p и $p + 2$ являются простыми числами-близнецами;
3. число p является простым числом Ферма;
4. p является простым числом Мерсенна.

В [30] автор переформулировал гипотезу (ныне теорему) о четырёх красках в виде неделимости некоторого произведения биномиальных коэффициентов. В аналогичном виде М. Маргенштерн и автор [31] переформулировали известную $3x + 1$ проблему.

Конструкции в [29, 30, 31] основаны на следующем свойстве биномиальных коэффициентов.

Теорема (Э. Куммер [32]). *Пусть числа a и b следующим образом записываются в позиционной системе счисления с простым основанием p:*

$$a = \sum_{k=0}^{m} a_k p^k, \quad b = \sum_{k=0}^{m} b_k p^k, \qquad 0 \leqslant a_k < p, \quad 0 \leqslant b_k < p, \quad k = 0, \ldots, m; \tag{13}$$

тогда степень, с которой p входит в разложение биномиального коэффициента $\binom{a+b}{a}$, равна количеству переносов из разряда в разряд при сложении чисел a и b.

Этот результат Куммера долго оставался малоизвестным и был переоткрыт разными авторами; доказательство теоремы можно найти также, например, в [16, 33].

Мы будем использовать такое следствие теоремы Куммера для случая $p = 2$ в (13). Будем говорить, что a *маскирует* b (и писать $a \succeq b$), если $a_k \geqslant b_k$ для $k = 0, \ldots, m$. Из теоремы Куммера следует такая эквивалентность:

$$\binom{a}{b} \equiv 1 \pmod 2 \iff a \succeq b. \tag{14}$$

Это можно также вывести из частного случая теоремы Люка [34, раздел XXI]:

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \ldots \binom{a_m}{b_m} \pmod p. \tag{15}$$

2. Новая переформулировка гипотезы Римана

Исходным пунктом для нас будет неравенство (9), модифицированное по-разному в необходимом и достаточном условиях:

- *из гипотезы Римана следует, что для всех* $n > 1$

$$\psi(n) > n - \sqrt{n}\log_2^2(n); \tag{16}$$

- *если гипотеза Римана не верна, то существует бесконечно много значений* n*, для которых*

$$\psi(n) < n - 20\sqrt{n}\log_2^2(n). \tag{17}$$

Мы будем использовать тот факт, что правая часть в необходимом условии (16) больше правой части в достаточном условии (17). Неравенство (16) при $n \geqslant 74$ следует из неравества (9), а недостающие случаи $n = 2, \ldots, 73$ проверяются непосредственным вычислением. Достаточность условия (17) следует из $\Omega_\pm$-результата для функции $\psi(n)$, который получил Е. Шмидт ([35], см. также [36, теорема 32], [1, теорема 4.8]).

Теорема 1. *Рассмотрим систему условий*

$$2^l \leqslant n < 2^{l+1}, \tag{18}$$

$$2^m \leqslant 2q < 2^{m+1}, \tag{19}$$

$$s = \frac{B^{(n+1)}\left(B^{(n+1)n} - n - 1\right) + n}{\left(B^{(n+1)} - 1\right)^2}, \tag{20}$$

$$t = \frac{(2^m - 1)\left(B^{n^2} - 1\right)}{B^n - 1}, \tag{21}$$

$$\binom{t}{r} \equiv 1 \pmod 2, \tag{22}$$

$$u = \operatorname{rem}\left(rs, B^{n^2-n}\right), \tag{23}$$

$$rs - u \equiv \frac{B^{n^2-n}\,(B^n - 1)}{B - 1} q \pmod{B^{n^2}}, \tag{24}$$

$$p = \operatorname{rem}(r, B^n + 1), \tag{25}$$

$$mp < nq - 15l^2 q\sqrt{n}, \tag{26}$$

в которой B обозначает 2^{l+m+1}.

(А) Если гипотеза Римана верна, то система (18)–(26) *не имеет решений в положительных целых числах $l, m, n, p, q, r, s, t, u$.*

(Б) Если гипотеза Римана не верна, то система (18)–(26) *имеет бесконечно много таких решений.*

Доказательство части (А) мы проведём "от противного". Предположим, что нашлись числа l, m, n, p, q, r, s, t и u, удовлетворяющие условиям (18)–(26).

Согласно (18),

$$n > 1 \tag{27}$$

и

$$l = \lfloor \log_2(n) \rfloor. \tag{28}$$

Очевидно, что

$$1 \leqslant l, \quad 0 \leqslant \log_2(n) - l < 1. \tag{29}$$

Аналогично согласно (19)

$$m = \lfloor \log_2(q) \rfloor + 1 \tag{30}$$

и

$$0 < m - \log_2(q) \leqslant 1. \tag{31}$$

Рассмотрим записи чисел s, t, r и rs в позиционной системе счисления с основанием B.

Легко проверить, что из (20) следует, что

$$s = \sum_{j=1}^{n} j B^{(n-j)(n+1)}. \tag{32}$$

Это означает, что единственными ненулевыми цифрами числа s являются числа $1, \ldots, n$, и они разделены блоками из n нулей.

Аналогично из (21) следует, что

$$t = \sum_{k=1}^{n} (2^m - 1) B^{(k-1)n}, \tag{33}$$

иными словами, все ненулевые цифры числа t равны $2^m - 1$, и они разделены блоками из $n - 1$ нуля.

Двоичная запись некоторого числа a получается из его записи в системе счисления с основанием B посредством замены каждой B-ичной цифры на её двоичную запись, при необходимости дополненную спереди нулями до длины $l + m + 1$. По этой причине a маскирует b тогда и только тогда, когда каждая B-ичная цифра a маскирует соответствующую цифру числа b.

Согласно (14) из (22) следует, что $t \succeq r$ и, и потому число r имеет вид

$$r = \sum_{k=1}^{n} r_k B^{(k-1)n}, \tag{34}$$

где

$$r_k \leqslant 2^m - 1, \quad k = 1, \ldots, n. \tag{35}$$

Пусть

$$rs = \sum_{i=0}^{2n^2} d_i B^i, \quad 0 \leqslant d_i < B, \quad i = 0, \ldots 2n^2. \tag{36}$$

Согласно (32) и (34)

$$rs = \sum_{j=1}^{n} \sum_{k=1}^{n} j r_k B^{(n-j)(n+1)+(k-1)n}. \tag{37}$$

Легко проверить, что при $1 \leqslant j \leqslant n$, $1 \leqslant k \leqslant n$ среди чисел вида $(n-j)(n+1)+(k-1)n$ нет двух одинаковых. Кроме того, из (18) и (34) следует, что

$$j r_k \leqslant n(2^m - 1) < 2^{l+1}(2^m - 1) < 2^{l+m+1} = B. \tag{38}$$

Таким образом, всевозможные произведения вида jr_k являются единственными ненулевыми цифрами числа rs, точнее,

$$d_i = \begin{cases} j r_k, & \text{если } i = (n-j)(n+1)+(k-1)n \\ 0, & \text{в противном случае.} \end{cases} \tag{39}$$

В частности, при $j = k$ получаем, что

$$d_{n^2-k} = k r_k, \quad k = 1, \ldots, n. \tag{40}$$

Согласно (23) и (36)

$$u = \sum_{i=0}^{n^2-n-1} d_i B^i. \tag{41}$$

Иными словами, число u – это “хвост” записи произведения rs, состоящий из её последних $n^2 - n$ цифр. Соответственно,

$$rs - u = \sum_{i=n^2-n}^{2n^2} d_i B^i \equiv \sum_{i=n^2-n}^{n^2-1} d_i B^m \pmod{B^{n^2}}. \tag{42}$$

Имеет место тождество

$$\sum_{i=n^2-n}^{n^2-1} q B^i = \frac{(B^n - 1)\, B^{n^2-n}}{B-1} q, \tag{43}$$

благодаря которому из (24), (40) и (42) следует, что

$$k r_k = d_{n^2-k} = q, \quad k = 1, \ldots, n. \tag{44}$$

Отсюда мы получаем следующие значения цифр числа r:

$$r_k = \frac{q}{k}, \quad k = 1, \ldots, n. \tag{45}$$

Согласно (44) q делится на $1, \ldots, n$, следовательно,

$$\mathrm{LCM}(1, \ldots, n) \leqslant q. \tag{46}$$

Из очевидного сравнения

$$B^n \equiv -1 \pmod{B^n + 1} \tag{47}$$

и равенства (34) следует, что

$$p \equiv \sum_{k=1}^{n} (-1)^{k-1} r_k \pmod{B^n + 1}. \tag{48}$$

Слагаемые в знакопеременной сумме в (48) по абсолютной величине монотонно убывают, первое слагаемое равно q, следовательно, сумма положительна и не превосходит q. Таким образом, в сравнении (48) левая и правая части не превосходят его модуля, следовательно, они равны. Соответственно,

$$\frac{p}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1} r_k}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \approx \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = \ln(2) \tag{49}$$

и справедливы элементарные неравенства

$$\frac{1}{2} \leqslant \frac{p}{q}, \quad \left| \frac{p}{q} - \ln(2) \right| < \frac{1}{2n}. \tag{50}$$

Из (26) и (50) следует, что

$$m < \frac{n - 15l^2 p\sqrt{n}}{p/q} \leqslant 2n. \tag{51}$$

Далее, согласно (50), (51), (31), (5) и (27), имеем:

$$\begin{aligned} \frac{p}{q} m > \left(\ln(2) - \frac{1}{2n} \right) m = \ln(2) m - \frac{m}{2n} > \ln(2) \log_2(q) - 1 = \\ = \ln(q) - 1 \geqslant \ln\big(\mathrm{LCM}(1, \ldots, n)\big) - 1 = \\ = \psi(n) - 1 > \psi(n) - 2\sqrt{n} \log_2^2(n). \end{aligned} \tag{52}$$

С другой стороны, согласно (26) и (29)

$$\frac{p}{q} m < n - 15l^2\sqrt{n} < n - 3\sqrt{n} \log_2^2(n). \tag{53}$$

Три неравенства, (16), (52) и (53), дают требуемое противоречие. Часть (А) доказана. Доказательство части (Б). В качестве n мы возьмём произвольное из чисел, превосходящих 1 и удовлетворяющих неравенству (17). Из доказательства части (А) видно, что значения остальных переменных почти однозначно определяются значением n.

Выберем l согласно (28), так что условие (18) будет выполнено и будут справедливы неравенства (29).

Положим

$$q = \mathrm{LCM}(1, \ldots, n), \tag{54}$$

и выберем m согласно (30), так что условие (19) будет выполнено и будут справедливы неравенства (31).

Выберем s согласно (32), так что условие (20) будет выполнено.

Определим числа r_k и r согласно (45) и (34), при этом согласно (31) будут справедливы неравенства (35) и (38). Поскольку двоичная запись числа $2^m - 1$ состоит из m единиц, из (38) следует, что

$$2^m - 1 \succeq r_k, \quad k = 1, \ldots, n. \tag{55}$$

Выберем t согласно (33), так что условие (21) будет выполнено. Все ненулевые цифры числа t равны 2^m-1, и согласно (55) они маскируют соответствующие цифры числа r. Отсюда следует, что $t \succeq r$ и, согласно (14), условие (22) выполнено.

Точно так же, как в доказатеьстве части (А) мы заключаем, что в представлении (36) цифры d_i определяются равенством (39) и его частным случаем (40).

Выберем u согласно (41), тогда будут выполнены условие (23) и сравнение (42), в котором согласно (40) во второй сумме все d_i равны q. Поскольку меет место тождество (43), то выполнено и условие (24).

Точно так же, как в доказательстве части (А) мы заключаем, что справедливы неравенства (50).

Согласно (54), (5) и (17)

$$\log_2(q) = \log_2\big(\mathrm{LCM}(1,\ldots,n)\big) = \psi(n)/\ln(2) < 2\psi(n) < 3n. \tag{56}$$

Используя, кроме того, (50), (31), (27), (17) и (29), отсюда получаем, что

$$\frac{p}{q}m < \left(\ln(2)+\frac{1}{2n}\right)(\log_2(q)+1) = \psi(n) + \frac{\log_2(q)}{2n} + \ln(2) + \frac{1}{2n} < \\ < \psi(n) + 3\sqrt{n}\log_2^2(n) < n - 17\sqrt{n}\log_2^2(n) < n - 17\sqrt{n}l^2 \tag{57}$$

и, следовательно, условие (26) выполнено.

Часть (Б) доказана. Теорема доказана.

Замечание. Если разрешить возведение в степень произвольных чисел (а не только числа 2 как в (18)–(26)), то можно избежать использования биномиального коэффициента. А именно,

$$\binom{t}{r} \equiv 1 \pmod 2 \iff \mathrm{rem}((2^t+1)^t, 2^{rt+1}) > 2^{rt}. \tag{58}$$

Заменив условие (22) на правую часть в (58), мы получим систему условий, каждое из которых легко может быть преобразовано в экспоненциально диофантово уравнение за счёт введения дополнительных неизвестных. Все эти уравнения могут быть объединены в одно экспоненциально диофантово уравнение, неразрешимость которого эквивалентна гипотезе Римана. Стандартная техника позволяет преобразовать это экспоненциально диофантово уравнение в эквивалентное ему диофантово уравнение с дополнительными переменными, допускающее сравнительно короткую запись.

Заключение

Мы установили, что гипотеза Римана эквивалентна несовместности условий (18)–(26). Представляется интересным исследовать системы условий, получающиеся из (18)–(26) удалением одного из них или заменой его на более слабое. Например, допускают ли хорошее описание решения системы, получающейся заменой биномиального условия (22) на вытекающее из него неравенство $r \leqslant t$?

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Broughan K. Equivalents of the Riemann hypothesis. Volume 1: Arithmetic equivalents. — Cambridge: Cambridge University Press, 2017. — ISBN 978-1-107-19704-6/hbk.

2. Broughan K. Equivalents of the Riemann hypothesis. Volume 2: Analytic equivalents. — Cambridge: Cambridge University Press, 2017. — P. xx + 491. — ISBN 978-1-107-19712- 1/hbk; 978-1-108-17826-6/ebook. — DOI: 10.1017/9781108178266.

3. Gödel K. Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme. I. // Monatsh. Math. Phys. — 1931. — B. 38. — S. 173–198. — ISSN 0026-9255; 1436-5081/e. — DOI: 10.1007/BF01700692.

4. Booker A. R. Turing and the Riemann hypothesis. // Notices Am. Math. Soc. — 2006. — T. 53, № 10. — P. 1208–1211. — ISSN 0002-9920; 1088-9477/e.

5. Booker A. R. Artin's conjecture, Turing's method, and the Riemann hypothesis. // Exp. Math. — 2006. — V. 15, № 4. — P. 385–407. — ISSN 1058-6458; 1944-950X/e. — DOI: 10.1080/10586458.2006.10128976.

6. Alan Turing – His Work and Impact / под ред. S. B. Cooper, J. van Leeuwen. — Elsevier Science, 2013. — ISBN 978-0-12-386980-7. — DOI: 10.1016/C2010-0-66380-2.

7. Матиясевич Ю. В. Алан Тьюринг и теория чисел // Математика в высшем образовании. — 2012. — Т. 10. — С. 111–134. — URL: `http://www.unn.ru/math/no/10/_nom10_012_matiyasevich.pdf`.

8. Turing A. M. On computable numbers, with an application to the Entscheidungsproblem // Proc. London Math. Soc. — 1936. — V. 42, № 2. — P. 230–265.

9. Kreisel G. Mathematical significance of consistency proofs // Journal of Symbolic Logic. — 1958. — V. 23, № 2. — P. 155–182.

10. Yedidia A., Aaronson S. A Relatively Small Turing Machine Whose Behavior Is Independent of Set Theory // Complex Systems. — 2016. — V. 25. — DOI: 10.25088/ComplexSystems.25.4.297.

11. Aaronson S. The blog. — URL: `https://www.scottaaronson.com/blog/?p=2741`.

12. Calude C. S., Calude E., Dinneen M. J. A new measure of the difficulty of problems // J. Mult.-Val. Log. Soft Comput. — 2006. — V. 12, № 3/4. — P. 285–307. — ISSN 1542-3980; 1542-3999/e.

13. Calude E. The complexity of Riemann's hypothesis. // J. Mult.-Val. Log. Soft Comput. – 2012. — V. 18, № 3/4. — P. 257–265. — ISSN 1542-3980; 1542-3999/e.

14. Yu. V. Matiyasevich. The Riemann Hypothesis in Computer Science // Препринты Санкт-Петербургского отделения Математического ин-та РАН. — 2018. — № 07.

    — DOI: 10.13140/RG.2.2.14041.83041. — URL: `http://www.pdmi.ras.ru/preprint/2018/18-07.html`.

15. Манин Ю. И., Панчишкин А. А. Введение в теорию чисел. — М.:ВИНИТИ, 1990. — P. 5–341. — (Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления. Т. 49.).

16. Матиясевич Ю. В. Десятая проблема Гильберта. — М.:Физматлит, 1993.

17. Davis M., Matijasevič Yu., Robinson J. Hilbert's tenth problem: Diophantine equations: Positive aspects of a negative solution // Proc. Symp. Pure Math. — 1976. — V. 28, P. 323–378.

18. Hernandez Caceres J. M. The Riemann Hypothesis and Diophantine equations. — Master's Thesis in Mathematics, Mathematical Institute, University of Bonn.

19. Мороз Б. З. Гипотеза Римана и диофантовы уравнения // Препринты Санкт-Петербургского математического общества. — 2018. — № 03.

— URL: http://www.mathsoc.spb.ru/preprint/2018/index.html#03.

20. Nayebi A. On the Riemann Hypothesis and Hilbert's Tenth Problem. — Unpublished Manuscript, 2012.

— URL: http://web.stanford.edu/~anayebi/projects/RH_Diophantine.pdf.

21. Matijasevič Yu. V. On recursive unsolvability of Hilbert's tenth problem // Studies in Logic and the Foundations of Mathematics. — V. 74. — P. 89–110.

22. Jones J. P. Universal Diophantine equation. // J. Symb. Log. — 1982. — V. 47. — P. 549– 571. — ISSN 0022-4812; 1943-5886/e. — DOI: 10.2307/2273588.

23. Schoenfeld L. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. // Math. Comput. — 1976. — V. 30. — P. 337–360. — ISSN 0025-5718; 1088-6842/e. — DOI: 10.2307/2005976.

24. Nicolas J.-L. Petites valeurs de la fonction d'Euler // J. Number Theory. — 1983. — V. 17. — P. 375–388. — ISSN 0022-314X; 1096-1658/e. — DOI: 10.1016/0022-314X(83)90055-0.

25. Robin G. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann // J. Math. Pures Appl. (9). — 1984. — V. 63. — P. 187–213. — ISSN 0021-7824.

26. Lagarias J. C. An elementary problem equivalent to the Riemann hypothesis // Am. Math. Mon. — 2002. — V. 109, № 6. — P. 534–543. — ISSN 0002-9890. — DOI: 10.2307/2695443.

27. Mann H. B., Shanks D. A necessary and sufficient condition for primality, and its source. // J. Comb. Theory, Ser. A. — 1972. — V. 13. — P. 131–134. — ISSN 0097-3165. — DOI: 10.1016/0097-3165(72)90016-7.

28. Hsu L., Shiue P. J.-S. On a combinatorial expression concerning Fermat's Last Theorem // Adv. Appl. Math. — 1997. — V. 18, № 2. — P. 216–219. — ISSN 0196-8858. — DOI: 10.1006/aama.1996.0510.

29. Матиясевич Ю. В. Один класс критериев простоты, формулируемых в терминах делимости биномиальных коэффициентов // Зап. научн. сем. ЛОМИ. — 1977. — Т. 67. — P. 167–183. — URL: http://mi.mathnet.ru/znsl2015.

30. Matiyasevich Yu. Some arithmetical restatements of the four color conjecture. // Theor. Comput. Sci. — 2001. — V. 257, № 1/2. — P. 167–183. — ISSN 0304-3975. — DOI: 10.1016/S0304-3975(00)00115-8.

31. Margenstern M., Matiyasevich Yu. A binomial representation of the $3x + 1$ problem. // Acta Arith. — 1999. — V. 91, № 4. — P. 367–378. — ISSN 0065-1036; 1730-6264/e. — DOI: 10.4064/aa-91-4-367-378.

32. Kummer E. E. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen // Journal für die Reine und Angewandte Mathematik. — 1852. — V. 44. — P. 93–146.

33. Singmaster D. Notes on binomial coefficients. I: A generalization of Lucas' congruence. // J. Lond. Math. Soc., II. Ser. — 1974. — V. 8. — P. 545–548. — ISSN 0024-6107; 1469-7750/e. — DOI: 10.1112/jlms/s2-8.3.545.

34. Lucas E. Théorie des Fonctions Numériques Simplement Périodiques // American Journal of Mathematics. — 1878. — V. 1. — P. 184–240. — URL: http://www.jstor.org/stable/2369311.

35. Schmidt E. 1903, Über die Anzahl der Primzahlen unter gegebener Grenze // Math Annalen. — 1932. — V. 57. — P. 195–203.

36. Ингам А. Э. *Распределение простых чисел* (перевод с англ.) — М.:Едиториал УРСС, 2005.

REFERENCES

1. Broughan, K. 2017, *Equivalents of the Riemann hypothesis. Volume 1: Arithmetic equivalents.*, Cambridge University Press, Cambridge.

2. Broughan, K. 2017, *Equivalents of the Riemann hypothesis. Volume 2: Analytic equivalents.*, Cambridge University Press, Cambridge. DOI: 10.1017/9781108178266.

3. Gödel, K. 1931, "Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme. I.", *Monatsh. Math. Phys.* vol. 38, pp 173–198. DOI: 10.1007/BF01700692.

4. Booker, A. R. 2006, "Turing and the Riemann hypothesis", *Notices Am. Math. Soc.* vol. 53, no. 10, pp 1208–1211.

5. Booker, A. R. 2006, "Artin's conjecture, Turing's method, and the Riemann hypothesis", *Exp. Math.* vol. 15, no. 4, pp 385–407. DOI: 10.1080/10586458.2006.10128976.

6. Cooper, S. B. & van Leeuwen, J. (eds) 2013, *Alan Turing – His Work and Impact*, Elsevier Science. ISBN 978-0-12-386980-7. DOI: 10.1016/C2010-0-66380-2.

7. Matiyasevich Yu. V. 2012, "Alan Turing and number theory" (in Russian), *Matematika v vysshem obrazovanii*, vol. 10, pp 111–134. Available at: `http://www.unn.ru/math/no/10/_nom10_012_matiyasevich.pdf`.

8. Turing, A. M. 1936, "On computable numbers, with an application to the Entscheidungsproblem", *Proc. London Math. Soc* vol. 42, no. 2, pp 230–265.

9. Kreisel, G. 1958, "Mathematical significance of consistency proofs", *Journal of Symbolic Logic* vol. 23, no. 2, pp 155–182.

10. Yedidia, A. & Aaronson, S. 2016, "A relatively small Turing machine whose behavior is independent of set theory", *Complex Systems* vol. 25, pp 297–327.

    DOI 10.25088/ComplexSystems.25.4.297.

11. Aaronson, S. 2016, *The blog*. Available at: `https://www.scottaaronson.com/blog/?p=2741`.

12. Calude, C. S., Calude, E. & Dinneen, M. J. 2006, "A new measure of the difficulty of problems", *J. Mult.-Val. Log. Soft Comput.* vol. 12, no. 3–4, pp 285–307.

13. Calude, E. 2012, "The complexity of Riemann's hypothesis", *J. Mult.-Val. Log. Soft Comput.* vol. 18, no. 3–4, pp 257–265.

14. Matiyasevich, Yu. V. 2018, "The Riemann hypothesis in computer science", *Preprints of St.Petersburg Department of Steklov Mathematical Institute*, no. 07.

    DOI: 10.13140/RG.2.2.14041.83041 Available at: `http://www.pdmi.ras.ru/preprint/2018/18-07.html`.

15. Manin Yu. I. & Panchishkin A. A. 2005. *Introduction to modern number theory. Fundamental problems, ideas and theories.* Transl. from the Russian. 2nd revised ed. Springer, Berlin.

16. Matiyasevich Yu. 1993, *Hilbert's Tenth Problem.* Transl. from the Russian. MIT Press, Cambridge (Massachusetts), London.

17. Davis, M., Matijasevič Yu. & Robinson, J. 1976, "Hilbert's tenth problem: Diophantine equations: Positive aspects of a negative solution". *Proc. Symp. Pure Math.* vol. 28, 323–378.

18. Hernandez Caceres, J. M. 2018, *The Riemann Hypothesis and Diophantine equations.* Master's Thesis in Mathematics, Mathematical Institute, University of Bonn, Bonn.

19. Moroz B. Z. 2018, "The Riemann Hypothesis and Diophantine equatons" (in Russian), *St.Petersburg Mathematical Society Preprints*, no. 03. Available at: `http://www.mathsoc.spb.ru/preprint/2018/index.html#03`.

20. Nayebi, A. 2012, *"On the Riemann Hypothesis and Hilbert's tenth problem"*, unpublished manuscript. Available at: `http://web.stanford.edu/~anayebi/projects/RH_Diophantine.pdf`.

21. Matijasevič, Y. V. 1973, "On recursive unsolvability of Hilbert's tenth problem", *Studies in Logic and the Foundations of Mathematics* vol. 74, pp. 89–110.

22. Jones, J. P. 1982, "Universal Diophantine equation", *J. Symb. Log.* vol. 47, pp 549–571. DOI: 10.2307/2273588.

23. Schoenfeld, L. 1976, "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II", *Math. Comput.* vol. 30, pp 337–360. DOI: 10.2307/2005976.

24. Nicolas, J.-L. 1983, "Petites valeurs de la fonction d'Euler", *J. Number Theory* vol. 17, pp 375–388. DOI: 10.1016/0022-314X(83)90055-0.

25. Robin, G. 1984, "Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann", *J. Math. Pures Appl. (9)* vol. 63, pp 187–213.

26. Lagarias, J. C. 2002, "An elementary problem equivalent to the Riemann hypothesis", *Am. Math. Mon.* vol. 109, no. 6, pp 534–543. DOI: 10.2307/2695443.

27. Mann, H. B. & Shanks, D. 1972, "A necessary and sufficient condition for primality, and its source", *J. Comb. Theory, Ser. A* vol. 13, pp 131–134. DOI: 10.1016/0097-3165(72)90016-7.

28. Hsu, L. & Shiue, P. J.-S. 1997, "On a combinatorial expression concerning Fermat's Last Theorem", *Adv. Appl. Math.* vol. 18, no. 2, pp 216–219. DOI: 10.1006/aama.1996.0510.

29. Matiyasevich Yu. V. 1981, "A class of primality criteria formulated in terms of the divisibility of binomial coefficients". Translation from Russian, *Journal of Soviet Mathematics*, vol. 16, no. 1, pp 874–885. DOI: 10.1007/BF01213897.

30. Matiyasevich, Yu. 2001, "Some arithmetical restatements of the four color conjecture", *Theor. Comput. Sci.* vol. 257, no. 1–2, pp 167–183. DOI 10.1016/S0304-3975(00)00115-8.

31. Margenstern, M. & Matiyasevich, Yu. 1999, "A binomial representation of the $3x+1$ problem", *Acta Arith.* vol. 91, no. 4, pp 367–378. DOI: 10.4064/aa-91-4-367-378.

32. Kummer, E. E. 1852, "Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen", *Journal für die Reine und Angewandte Mathematik* vol. 44, pp 93–146.

33. Singmaster, D. 1974, "Notes on binomial coefficients. I: A generalization of Lucas' congruence", *J. Lond. Math. Soc., II. Ser.* vol. 8, pp 545–548. DOI: 10.1112/jlms/s2-8.3.545.

34. Lucas E. 1878. “Théorie des Fonctions Numériques Simplement Périodiques”, *American Journal of Mathematics*, vol. 1, pp 184–240. Available at: `http://www.jstor.org/stable/2369311`.

35. Schmidt, E. 1903, “Über die Anzahl der Primzahlen unter gegebener Grenze”, *Math Annalen*, vol. 57, pp 195–203.

36. Ingham, A. E. 1932, *The distribution of prime numbers*, Cambridge University Press, London (Cambridge Tracts in Mathematics and Mathematical Physics, vol. 30,); reprinted in 1990.

Получено 17.07.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.313:511.331.1:511.526 DOI 10.22405/2226-8383-2018-19-3-61-73

Теория чисел и приложения в криптографии

Востоков Сергей Владимирович — доктор физико-математических наук, профессор, профессор кафедры алгебры и теории чисел Санкт-Петербургского государственного университета, президент фонда им. Л. Эйлера.
e-mail: sergei.vostokov@gmail.com
Востокова Регина Петровна — старший преподаватель, Балтийский государственный технический университет "Военмех".
e-mail: rvostokova@yandex.ru
Беззатеев Сергей Валентинович — доктор технических наук, доцент, заведующий кафедрой «Кафедра технологий защиты информации», Санкт-Петербургский государственный университет аэрокосмического приборостроения.
e-mail: bsv@aanet.ru

Аннотация

В статье рассмотрены некоторые элементы теории чисел и показано каким образом они используются в современных системах защиты информации. В качестве примеров выбраны наиболее известные протоколы и алгоритмы, такие как протокол Диффи-Хэллмана для создания парного ключа, алгоритмы шифрования с открытым ключом RSA и Эль Гамаля. Рассмотрен обобщенный алгоритм Евклида, являющийся одним из наиболее часто встречающихся примитивов из теории чисел, используемом в криптографии. Приведены алгоритмы электронной подписи RSA и Эль Гамаля. В заключение предложен алгоритм электронной подписи, основанный на билинейном преобразовании, использующем упрощенный вид спаривания в явном законе взаимности.

Ключевые слова: теория чисел, криптографические протоколы, несимметричные алгоритмы шифрования, электронное подпись, билинейное преобразование.

Библиография: 21 названий.

Для цитирования:
С. В. Востоков, Р. П. Востокова, С. В. Беззатеев. Теория чисел и приложения в криптографии // Чебышевский сборник, 2018, т. 19, вып. 3, с. 61–73.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.313:511.331.1:511.526 DOI 10.22405/2226-8383-2018-19-3-61-73

Number theory and applications in cryptography

Vostokov Sergey Vladimirovich — doctor of physical and mathematical Sciences, Professor, Professor of algebra and number theory Department of St. Petersburg state University, President of the Foundation. L. Euler.
e-mail: sergei.vostokov@gmail.com

Vostokova Regina Petrovna — senior lecturer, Baltic State Technical University "Voenmech".
e-mail: rvostokova@yandex.ru
Bezzateev Sergei Valentinovich — Doctor of technical sciences, Saint-Petersburg State University of Aerospace Instrumentation.
e-mail: bsv@aanet.ru

Abstract

The paper describes some elements of the number theory and shows how they are used in modern information security systems. As examples, the most famous protocols and algorithms such as the Diffie-Hellman Protocol for pair key generation, RSA and El Gamal public key encryption algorithms. The generalized Euclid algorithm is considered, as a one of the most common element of the number theory used in cryptography. Algorithms are given RSA and El Gamal signature algorithms are given. In conclusion, the algorithm of the electronic signature based on bilinear transformation uses a simplified case of the pairing in the explicit law of reciprocity.

Keywords: number theory, cryptography protocols, public key cryptographic algorithms, signature, bilinear transformation.

Bibliography: 21 titles.

For citation:
S. V. Vostokov, R. P. Vostokova, S. V. Bezzateev, 2018, "Number theory and applications in cryptography" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 61–73.

1. Введение

Один мой друг, который закончил Ленинградский ВУЗ, спросил меня как-то: «Ну что ты делаешь в своей математике, ведь всю Высшую математику мы прошли в институте». В этой работе мы попробуем разъяснить это заблуждение очень многих людей не только в нашей стране. Попытаемся это сделать на примере теории чисел и криптографии.

Теория чисел очень древняя наука, которая сейчас переросла в направление «Арифметическая геометрия». Но даже самые давние фундаментальные результаты этой науки только в наше время находят применения в очень востребованной ныне прикладной науке — криптографии [5]. Мы покажем это на примере теоремы Эйлера из теории чисел, которая была доказана в середине XVIII века и нашла свое применение в созданном в 1978 году первом современном методе криптографии RSA[9].

Во второй части работы будет рассказано, как окончательное решение 9 проблемы Гильберта в 1978 году [2] дало в 2003 году новый способ электронной подписи.

2. Теория чисел

2.1. Функция Эйлера

Определим функцию Эйлера $\varphi(m)$ для целого числа $m > 1$ следующим образом.

Рассмотрим все остатки при делении на число m: $0, 1, 2, \ldots, m-1$ и сосчитаем количество взаимно-простых с m остатков. Это число и будем называть функцией Эйлера.

Рассмотрим два частных случая:

1. Если p — простое число, то нетрудно заметить, что $\varphi(p) = p - 1$.

2. Если p и q — два различных простых числа, то $\varphi(pq) = (p-1)(q-1)$.

2.2. Теорема Эйлера

Теорема 1 (Эйлера). *[1] Пусть a и m — взаимно простые числа, тогда выполнено сравнение*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{1}$$

3. Расширенный Алгоритм Евклида

Для понимания выполняемых операций в криптографических преобразованиях одним из наиболее часто используемых инструментов является расширенный алгоритм Евклида для нахождения мульипликативно обратного по модулю некоторого целого числа. Надо отметить, что в общем случае применение этого алгоритма значительно шире и затрагивает не только криптографические преобразования но и, например, теорию алгебраического кодирования. Однако здесь мы остановимся только на возможностях этого замечательного алгоритма для наших целей, а именно, - вычисление числа x обратного по умножению числу y по модулю целого числа p.

$$x : x \cdot y \equiv 1 \mod p.$$

Необходимым условием для нахождения такого x очевидно является взаимная простота y и p. В расширенном алгоритме Евклида используется вспомогательные элементы u_i связанные рекуррентной формулой $u_{i+1} = q_i \cdot u_i + u_{i-1}$ где $u_{-1} = 0, u_0 = 1$ и q_i - частное, полученное на $i-$ ом шаге алгоритма.
Приведем теперь последовательность шагов алгоритма:

Шаг 1. $p = y \cdot q_1 + r_1, u_1 = q_1 \cdot u_0 + u_{-1}$, где q_1 и r_1 соответственно частное и остаток от деления p на y.

Шаг 2. $y = r_1 \cdot q_2 + r_2, u_2 = q_2 \cdot u_1 + u_0$,

Шаг 3. $r_1 = r_2 \cdot q_3 + r_3, u_3 = q_3 \cdot u_2 + u_1$,

...

Шаг i. $r_{i-2} = r_{i-1} \cdot q_i + r_i, u_i = q_i \cdot u_{i-1} + u_{i-2}$,

...

Шаг (ℓ) $r_{\ell-2} = r_{\ell-1} \cdot q_\ell + 1, u_\ell = q_\ell \cdot u_{\ell-1} + u_{\ell-2}$. Это последний шаг алгоритма, так как остаток, полученный на этом шаге равен 1 - наибольшему общему делителю чисел p и y .

Искомое значение x определяется следующим образом:

$$x \equiv (-1)^\ell \cdot u_\ell \mod p.$$

4. Приложения в криптографии

4.1. Несимметричная криптография

История создания криптографических алгоритмов не менее загадочна и секретна чем сами алгоритмы [7]. Идея передачи секретной информации по незащищенному каналу была первоначально предложена James H. Ellis в 1970 году [12]. Затем Ellis, Cocks и Williamson в 1973 году [11] предложили идею алгоритма RSA, однако результат был засекречен Government Communications Headquarters (Великобритания) и лишь 18 декабря 1997, Clifford Cocks анонсировал его, сделав достоянием широкой общественности. К сожалению James Ellis умер 25

ноября 1997 за месяц до публичного анонсирования этого факта. В 2010 Malcolm Williamson, Clifford Cocks и James Ellis получили престижную награду Milestone Award Института IEEE (IEEE) за развитие криптографии с открытым ключом. Рассмотрим здесь, какой же алгоритм был предложен этими тремя британцами.

4.1.1. Алгоритм WCE

В качестве секретного ключа выбираются два большие простые числа p и q. Открытым ключом является их произведение $N = p \cdot q$. Сообщением m должно удовлетворять следующим ограничениям: это целое положительное число, $m < N$. Для того чтобы зашифровать сообщение, его необходимо возвести в степень открытого ключа N и результат взять по модулю N (то есть вычислить остаток от деления).

$$e = m^N \mod N \tag{2}$$

Таким образом, для зашифрования достаточно знание только открытого ключа. При этом отметим здесь, что открытый ключ в алгоритме WCE представляет собой одно число N являющееся произведением двух секретных простых чисел p и q таких что

$$(p, (q-1)) = 1, \quad (q, (p-1)) = 1.$$

Для того чтобы расшифровать сообщение e необходимо знание секретного ключа. Первоначально находится функция Эйлера $\varphi(N) = (p-1)(q-1)$ и вычисляется вспомогательное число c

$$c = N \mod \varphi(N).$$

Затем вычисляется секретный ключ d

$$d \cdot c = 1 \mod \varphi(N))$$

Для этого используется расширенный алгоритм Евклида. Здесь следует заметить, что автоматически выполняется очень важное свойство для корректной работы расширенного алгоритма Евклида. А именно - наибольший общий делитель чисел N и $\varphi(N)$ равен 1. И, наконец, зашифрованное сообщение e возводится в степень d.

$$m = e^d = m^{c \cdot d} = m^{1 \mod \varphi N} \equiv m \mod N$$

А теперь посмотрим официальную, наиболее часто встречающуюся, версию появления несимметричной криптографии.

4.1.2. Протокол Диффи-Хеллмана

В 1976 году американцы Уитфилд Диффи и Мартин Хеллман опубликовали в журнале IEEE Transaction on Information Theory статью "New directions in cryptography"[8] в которой описали схему шифрования без обмена секретным ключом по открытому каналу. Основной идеей, лежащей в основе предложенного протокола являлось использование проблемы дискретного логарифма. То есть отсутствие эффективного алгоритма вычисления числа x при известных простом числе p, и целых числах a и b.

$$a = b^x \mod p$$

Что же собой представляет этот протокол, опубликованный более 40 лет назад и до сих пор эффективно используемый в огромном числе практических приложений обеспечивающих

безопасный канал для любых двух устройств не имевших до этого никакой информации друг о друге и использующих для выработки секретного ключа канал связи свободно прослушиваемый всеми.

Первым шагом протокола является выбор сторонами в открытом обсуждении пары чисел : большого простого числа p и b -первообразного корня из 1 по модулю p. На втором шаге каждый из участников протокола выбирает свое секретное число . Соответственно x, y , $1 < x < p-1, 1 < y < p-1$. Для обмена по открытому, прослушиваемому каналу участники вычисляют числа , $a = b^x \mod p$ и $c = b^x \mod p$ соответственно. После получения этих значений участники протокола могут вычислить общий парный ключ K.

$$K = a^y = c^x \equiv b^{xy} \mod p. \tag{3}$$

4.1.3. Алгоритм шифрования RSA

В 1978 году Рональд Райвест, Ади Шамир и Леонард Адлеман запатентовали и опубликовали свой алгоритм получивший в дальнейшем название RSA [9]. В этом же номере журнала, известный математик и учёный Мартин Гарднер по согласию авторов алгоритма, опубликовал математическую задачу, получившую название RSA-129. В условии задачи он указал два числа n и e - открытый ключ и зашифрованный текст. Длина числа n составляла 129 десятичных знаков, а число $e = 1007$. За расшифровку текста предполагалась премия в 100 долларов. Шифр удалось взломать через 17 лет — около 600 человек объединились в сеть и усилиями 1600 компьютеров за полгода смогли прочитать фразу в 1995 году:

«The Magic Words are Squesmish Ossifrage»[1]

Основные этапы алгоритма RSA
Выбор секретного ключа и вычисление открытого ключа

Шаг 3. Выбираем большое простые числа p и q с близким количеством цифр, после чего вычисляем $N = pq$.

Шаг 4. Вычисляем $\varphi(N) = (p-1)(q-1)$.

Шаг 5. Случайным образом выбираем число c, взаимно простое с $\varphi(N)$.

Шаг 6. С помощью расширенного алгоритма Евклида вычисляем число d, такое что $c \cdot d \equiv 1 \mod \varphi(N)$.

Определение 1. *Число d — секретный ключ, так же как и числа p и q.*

Определение 2. *Пара (c, N) — открытый ключ, который распространяется открыто .*

Шифрация сообщений с использованием открытого ключа

Сообщение может быть любое целое положительное число m не превосходящее N. При шифрации используется открытый ключ:

$$e \equiv m^c \mod N.$$

Дешифрация с использование секретного ключа

Возводим число e в степень d и ищем остаток числа e^d при делении на N. Это и будет искомое число m, так как

$$e^d = m^{cd} \equiv m^{1+k\cdot\varphi(N)} \equiv m + \ell \cdot N \equiv m \mod N.$$

[1] В переводе с английского: «Волшебные слова — это брезгливая скопа». Скопа — это птица, родственник стервятника.

Замечание 1. *Если число N имеет 100 цифр, то имеется не менее $4 \cdot 10^{42}$ простых числа, которые могут делить число N. Если компьютер выполняет 1 миллион операций в секунду, то ему понадобится примерно 10^{35} лет для вычисления $\varphi(N)$.*

Замечание 2. *В алгоритме RSA, использованном Гарднером для своего конкурса, использовались 64 и 65-значные простые числа.*

Замечание 3. *Сейчас для алгоритма RSA используют 150-значные простые числа.*

4.2. Алгоритм Эль Гамаля

Основные этапы алгоритма Эль Гамаля

В 1985 году в журнале IEEE Transactions on Information Theory [10] Тахером Эль-Гамалем был предложен алгоритм шифрования использующий идеи протокола Диффи-Хеллмана. В отличии предыдущих авторов Эль-Гамаль не патентовал свою схему и во многом именно вследствие этого она была использована как основа для национальных стандартов в большинстве стран(Россия, США, Европа и т.д.).

Выбор секретного ключа и вычисление открытого ключа

Шаг 1. Выбираем большое простое число p и q - примитивный корень из единицы по модулю p.

Шаг 2. Случайным образом выбираем число c, $1 < c < p - 1$.

Шаг 2. Вычисляем $b = q^c \mod p$.

Определение 3. *Число c — секретный ключ.*

Определение 4. *Тройка чисел (p, q, b) — открытый ключ, который распространяется открыто .*

Шифрация сообщений с использованием открытого ключа

Сообщением может быть любое целое положительное число m не превосходящее N. При шифрации используется открытый ключ и случайное число r, $1 < r < p - 1$:

$$e \equiv m \cdot b^r \mod p.$$

Определение 5. *Зашифрованное сообщение представляется парой чисел:*

$$(e, f \equiv q^r \mod p).$$

Дешифрация с использование секретного ключа

Возводим число f в степень c и получаем $b^r \mod p$.

$$f^c = q^{rc} = q^{cr} = b^r \mod p$$

Используя расширенный алгоритм Евклида находим мультипликативно обратное d к b^r по модулю p.

$$d \cdot b^r \equiv 1 \mod p.$$

Теперь осталось умножить первое из пары чисел представленных в зашифрованном сообщении и мы получим исходное сообщение.

$$e \cdot d = m \cdot b^r \cdot d \equiv m \cdot 1 = m \mod p.$$

4.3. Электронная подпись

В предыдущем разделе мы посмотрели каким образом можно создать общий секретный ключ используя для этого открытый прослушиваемый канал связи. Однако шифрация решает лишь одну из трех основных задач информационной безопасности - обеспечение конфиденциальности хранимой, обрабатываемой и передаваемой информации. К сожалению, это не позволяет предотвратить незаметное изменение критически важной информации [5]. Очевидно, что злоумышленник, зная открытый ключ, которым было зашифровано исходное сообщение, может легко заменить его на другое [6]. Для того, чтобы этого нельзя было сделать требуется использовать некоторую секретную информацию - секретный ключ. Когда говорят про электронную подпись, то обязательно упоминается некоторая однонаправленная функция - хэш-функция, позволяющая сообщение любого размера преобразовать в "отпечаток"фиксированной длины (например 256 бит). Такое преобразование и выполняется с помощью хэш-функции. В английском языке одним из значений слова "hash"является "путаница". И действительно при выполнении хэш-преобразования исходная информация "запутывается"так, что распутать(восстановить) ее обратно практически не представляется возможным. Для реализации подписи исходная информация сначала хэшируется, а затем подписывается с помощью секретного ключа. Таким образом возникает первая уязвимость подписи - так называемая коллизия при вычислении хэш-функции. Очевидно, если два разных сообщения имеют один и тот же результат хэш-функции, то и подписи у этих сообщений будут одинаковые. Таким образом, можно просто подставить подпись одного сообщения под другим. Существуют два вида электронной подписи:

- отрицаемая подпись,
- неотрицаемая подпись.

Отрицаемая подпись подразумевает использование одного и того же секретного ключа и при вычислении и при проверке электронной подписи. В этом случае, очевидно, обе стороны могут подписать сообщение и невозможно будет доказать кто же из них на самом деле подписал документ.
Неотрицаемая подпись использует при вычислении секретный ключ пользователя, а при проверке - его открытый ключ. Такой вариант позволяет говорить о том, что подпись может быть сформирована только одним лицом - обладателем секретного ключа, в о время как поверить подпись может любой, кому известен его открытый ключ. Как мы с вами уже видели на примере алгоритмов несимметричного шифрования, знание отрытого ключа не дает возможности вычислить соответствующий ему секретный ключ.
Рассмотрим теперь алгоритмы электронной подписи соответствующие приведенным ранее алгоритмам шифрования RSA и Эль Гамаля.

4.4. Электронная подпись RSA

Используя введенные ранее обозначения опишем этапы вычисления электронной подписи и ее проверки, считая, что для сообщения m значение хэш-функции равно h и $h < N$. Тогда подпись s вычисляется следующим образом:

$$s = h^d \mod N.$$

После вычисления электронной подписи хранимой или передаваемой информацией является пара - сообщение и подпись - (m, s). Не трудно заметить, что алгоритм подписи для RSA совпадает с алгоритмом расшифровки и естественным образом требует секретного ключа.

Для того чтобы проверить правильность электронной подписи s, то есть проверить не искажен ли исходный документ m и действительно ли он подписан конкретным лицом, имеющим открытый ключ (c, N) необходимо выполнить следующие действия:

- вычислить хэш функцию от проверяемого сообщения m' , $h' = Hash(m')$,
- проверить выполняется ли равенство $s^c \equiv h' \mod N$.

Очевидно, что для выполнения этих операций необходим только открытый ключ (c, N).

4.5. Электронная подпись Эль Гамаля

Подпись Эль Гамаля реализуется на много сложнее и главное требует использования случайного числа, что с одной стороны затрудняет ее вычисление, а с другой делает ее более защищенной, так как одно и то же сообщение подписанное тем же пользователем будет иметь каждый раз разную подпись.
При наличии секретного ключа c и открытого (p, q, b) нам понадобится еще случайное целое положительное число r, такое что $1 < r < p-1$ и наибольший общий делитель r и $p-1$ равен 1. Зачем требуется второе ограничение на это случайное число мы увидим немного позже. Электронная подпись s для сообщения m с хэш-функцией h вычисляется из соотношения

$$h \equiv r \cdot s + f \cdot c \mod (p-1).$$

где $f = q^r \mod p$.
Не трудно заметить что здесь опять необходимо найти мультипликативно обратное к r по модулю $p-1$ и это можно сделать только в том случае когда $(r, (p-1)) = 1$. Подписью в системе Эль Гамаля так же как и при шифровании являются два числа (s, f).
Для проверки целостности сообщения и принадлежности подписи требуется сообщение m', подпись (s, f) и открытый ключ пользователя. Если искажений не было, то есть $m' = m, h' = Hash(m') = Hash(m) = h$ и подпись была вычислена пользователем с открытым ключом (p, q, b) и соответствующим ему секретным ключом c то будет выполнено сравнение

$$q^{h'} \equiv f^s \cdot b^f \equiv q^{r \cdot s} \cdot q^{c \cdot f} \equiv q^{r \cdot s + c \cdot f} \equiv q^{h + \ell \cdot (p-1)} = q^h \mod p.$$

4.6. Электронная подпись на билинейном преобразовании

Метод для создания электронной подписи, который сейчас будет предложен, использует упрощенный вид спаривания в явном законе взаимности, полученном С.В.Востоковым в работе [2].
Множество целых чисел, взаимно простых с p:

$$\mathbb{Z}^{(p)} = \left\{ a \in \mathbb{Z} \;\middle|\; \text{н.о.д. } ap = 1 \right\}.$$

Из свойств взаимно-простых чисел ясно, что умножение оставляет числа из $\mathbb{Z}^{(p)}$ в этом же множестве.

Пусть $\mathbb{N}^+$ — множество натуральных чисел с операцией сложения. Зададим спаривание

$$\langle , \rangle_p \colon \quad \mathbb{Z}^{(p)} \times \mathbb{N}^+ \to \mathbb{Z} \mod p$$
$$\langle a, n \rangle = l(a) n \mod p$$
$$l(a) = \frac{\log a^{p-1}}{p}$$

Здесь $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$

Определение 6. *Число a называем числом Виферих, если $a^{p-1} \equiv 1 \pmod{p^2}$. В противном случае будем называть антивифериховым.*

Утверждение 1. *Спаривание $\langle , \rangle_p$ является билинейным, то есть*

$$\langle ab, n\rangle_p = \langle a, n\rangle_p + \langle b, n\rangle_p \qquad \text{для любых } a \text{ и } b \text{ из } \mathbb{Z}^{(p)};$$
$$\langle a, n+m\rangle_p = \langle a, n\rangle_p + \langle a, m\rangle_p \qquad \text{для любых } n \text{ и } m \text{ из } \mathbb{N}^+.$$

Кроме того, это спаривание невырожденно для антивиферихова числа a, то есть для такого a найдется n из $\mathbb{N}^+$ такое, что $\langle a, n\rangle_p = 1 \pmod{p}$.

Доказательство.

1. Билинейность по второму аргументу очевидна, а по первому следует из свойств логарифма.

2. Невырожденность. Пусть число a — антивиферихово. Тогда

$$\frac{a^{p-1}-1}{p} \,|/\, p.$$

Поэтому

$$L(a) = \frac{\log\left(a^{p-1}\right)}{p} = \frac{\log\left(1 + \frac{a^{p-1}-1}{p} \cdot p\right)}{p} = \\ = \frac{\frac{a^{p-1}}{p} \cdot p}{p} - \frac{\left(\frac{a^{p-1}}{p} \cdot p\right)^2}{2p} + \dots = \frac{a^{p-1}-1}{p}$$

не делится на p. Тогда в качестве n можно взять такое число, чтобы спаривание $\langle a, n\rangle_p$ стало бы равно $1 \mod p$.

Действительно, так как н.о.д.$\,l(a)p = 1$, то найдутся целые числа x и y такие, что $l(a)x + py = 1$. Заменяя, если нужно, x на $x' = x + pk$, а y на $y' = y - l(a)k$, получаем, при подходящем k, что x' — натуральное число. □

4.6.1. Формирование подписи

Алиса — доверенное лицо (арбитр). Она выбирает большое простое число p, взаимно простое с ним антивиферихово число a из $\mathbb{Z}^{(p)}$ и натуральное число n из $\mathbb{N}^+$ такое, чтобы было выполнено сравнение

$$\langle a, n\rangle = \frac{a^{p-1}-1}{p} \cdot n \equiv 1 \pmod{p}$$

Пусть x — случайное число такое, что $1 < x < p$,и s — решение сравнения $sx \equiv n \pmod{p}$.

Определение 7. *Набор (a, x, n) является секретным ключом.*

Пусть $M = \{m_1, m_2, \dots m_k\}$ — информация (сообщение). В криптографии определена функция, называемая хэш-функцией, которая однозначно задана информацией M.

Найдем остаток при делении a^{hx} на p^2:

$$r = a^{hx} \pmod{p^2}, \quad 0 < r < p^2.$$

Подписанное сообщение имеет вид $\Pi = (M, r < s < h)$. Получатель Боб должен проверить подпись, то есть проверить справедливость сравнения

$$\frac{r^{p-1}-1}{p} \cdot s \equiv h \mod p, \tag{4}$$

то есть остаток $\frac{r^{p-1}-1}{p} \cdot s$ при делении на p должен быть равен ha.

Утверждение 2. *Если подпись верна, что сравнение* (4) *выполнено.*

Доказательство. Вычислим спаривание $\langle r, s\rangle_p$. Имеем

$$\langle r, s\rangle_p \equiv l(r) \cdot s \equiv \frac{\log\left(1 + \frac{r^{p-1}-1}{p}\right)}{p} \cdot s = \frac{r^{p-1}-1}{p} \cdot s \equiv h \mod p.$$

Действительно, так как $r = a^{hx} \pmod{p^2}$, то

$$\langle r, s\rangle_p = \langle a^{hx}, s\rangle_p \equiv x\langle a^h, s\rangle_p \equiv$$
$$\equiv \langle a^h, sx\rangle_p \equiv h\langle a, n\rangle_p \equiv h \pmod p.$$

□

Утверждение 3. *Подпись* Π *удовлетворяет требованиям к подписи, то есть*

1. *никто, кроме Алисы, не может подписать сообщение с ее подписью;*
2. *в случае конфликта Алиса с Бобом они обращаются к третьим лицам и судья проверяет подлинность подписи после предъявления ему чисел* (a, x, n).

Используя явную формулу закона взаимности [2, 3], а также полученные позднее соответствующие формулы в формальных модулях Любина-Тейта [13, 14, 16] и в формальных модулях Любина-Тейта [19, 20, 21] и явные формулы в многомерных локальных полях [15, 17, 18] можно применить их в алгоритме WCE, протоколе Диффи-Хеллмана и алгоритме Эль-Гамаля, что будет сделано в последующих работах

5. Заключение

В данной работе рассмотрены криптографические примитивы шифрования и подписи, использующие основные понятия теории чисел. Предложен алгоритм электронной подписи, основанный на билинейном преобразовании использующем упрощенный вид спаривания в явном законе взаимности, описанный С. В. Востоковым в работе [2] , где было дано окончательное решение 9-ой проблемы Гильберта.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. А. А. Бухштаб, Теория чисел, Москва, 1960
2. С. В. Востоков, Явная форма закона взаимности, Изв АН СССР, Сер мат, том 42, № 6, 1978
3. С. В. Востоков, Символы на формальных группах Изв. АН СССР, Сер. матем. том 45, № 5, 985-1014, 1981

4. Н. Коблиц, Курс теории чисел и криптографии, Москва, изд ТВП, 2001, 254 с.

5. Б. Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, Москва, изд. Триумф, 2002, 816 с.

6. Б. Шнайер, Секреты и ложь. Безопасность данных в цифровом мире, изд. Питер, 2003, 366 с.

7. Д. Кан, Взломщики кодов, Центрполиграф, 2000, 480 с.

8. W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT-22, pp. 472-492, 1976.

9. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commum. ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

10. T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. Inform. Theory, 31 (4), pp. 469–472, 1985

11. C. C. Cocks, A Note on non-secret encryption, UK Communications Electronics Security Group, November 20, 1973

12. J. H. Ellis, The possibility of secure non-secret digital encryption, CSEG Report 3006, January 1970.

13. С. В. Востоков, В. А. Лецко, Каноническое разложение в группе точек формальной группы Любина–Тэйта, Зап. научн. сем. ЛОМИ, 103 (1980), 52–57

14. С. В. Востоков, Символ Гильберта для формальных групп Любина–Тэйта I, Зап. научн. сем. ЛОМИ, 114 (1982), 77–95

15. С. В. Востоков, А. Н. Кириллов, Норменное спаривание в двумерном локальном поле, Зап. научн. сем. ЛОМИ, 132 (1983), 76–84

16. С. В. Востоков, И. Б. Фесенко, Символ Гильберта для формальных групп Любина–Тэйта II, Зап. научн. сем. ЛОМИ, 132 (1983), 85–96

17. С. В. Востоков, Явная конструкция теории полей классов многомерного локального поля, Изв. АН СССР. Сер. матем., 49:2 (1985), 283–308

18. D. G. Benous and S. V. Vostokov, Sur les represetations p-adiques des corps locaux multidimensionnels attache's aux groups formels, J fuer die reine und angew. Math., 437(1993), 131-166

19. С. В. Востоков, О. В. Демченко, Явная формула спаривания Гильберта для формальных групп Хонды, Зап. научн. сем. ПОМИ, 272 (2000), 86–128

20. Falko Lorenz and Sergei Vostokov, Honda groups and explicit pairing on the module of Cartier curves, Algebraic Number Theory and Algebraic Geometry, Contemporary Methematics 300, Parshin Festschrift,Ed. S. Vostokov and Y. Zarhin, AMS, Providence Rhode Island, 2002, pp. 143-170.

21. С. В. Востоков, Ф. Лоренц, Явная формула символа Гильберта для групп Хонды в многомерном локальном поле, Матем. сб., 194:2 (2003), 3–36

REFERENCES

1. A. A. Buhshtab, 1960, *Teoriya chisel*, Moskva
2. S. V. Vostokov, 1978, "Yavnaya forma zakona vzaimnosti", *Izv AN SSSR, Ser mat*, tom 42, № 6
3. S. V. Vostokov, 1981, "Simvoly na formal'nyh gruppah", *Izv. AN SSSR, Ser. matem.* tom 45, № 5, 985-1014
4. N. Koblic, 2001, *Kurs teorii chisel i kriptografii*, Moskva, izd TVP, 254 P.
5. B. SHnajer, 2002, *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si*, Moskva, izd. Triumf, 816 P.
6. B. SHnajer, 2003, *Sekrety i lozh'. Bezopasnost' dannyh v cifrovom mire*, izd. Piter, 366 P.
7. D. Kan, 2000, *Vzlomshchiki kodov*, Centrpoligraf, 480 P.
8. W. Diffie and M. Hellman, 1976, "New directions in cryptography", *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 472-492.
9. R. Rivest, A. Shamir, and L. Adleman, 1978, "A method for obtaining digital signatures and public key cryptosystems", *Commum. ACM*, vol. 21, no. 2, pp. 120-126, Feb.
10. T. ElGamal, 1985, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. Inform. Theory*, 31 (4), pp. 469–472
11. C. C. Cocks, 1973, "A Note on non-secret encryption", *UK Communications Electronics Security Group*
12. J. H. Ellis, 1970, "The possibility of secure non-secret digital encryption", *CSEG Report 3006.*
13. S. V. Vostokov, V. A. Lecko, 1980, "Kanonicheskoe razlozhenie v gruppe tochek formal'noj gruppy Lyubina–Tehjta", *Zap. nauchn. sem. LOMI*, 103, pp. 52–57
14. S. V. Vostokov, 1982, "Simvol Gil'berta dlya formal'nyh grupp Lyubina–Tehjta I", *Zap. nauchn. sem. LOMI*, 114, pp. 77–95
15. S. V. Vostokov, A. N. Kirillov, 1983, "Normennoe sparivanie v dvumernom lokal'nom pole", *Zap. nauchn. sem. LOMI*, 132, pp. 76–84
16. S. V. Vostokov, I. B. Fesenko, 1983, Simvol Gil'berta dlya formal'nyh grupp Lyubina–Tehjta II, Zap. nauchn. sem. LOMI, 132, pp. 85–96
17. S. V. Vostokov, 1985, "Yavnaya konstrukciya teorii polej klassov mnogomernogo lokal'nogo polya", *Izv. AN SSSR. Ser. matem.*, 49:2, pp. 283–308
18. D. G. Benous and S. V. Vostokov, 1993, "Sur les represetations p-adiques des corps locaux multidimensionnels attache's aux groups formels", *J fuer die reine und angew. Math.*, 437, pp. 131-166
19. S. V. Vostokov, O. V. Demchenko, 2000, "Yavnaya formula sparivaniya Gil'berta dlya formal'nyh grupp Hondy", *Zap. nauchn. sem. POMI*, 272, pp. 86–128

20. Falko Lorenz and Sergei Vostokov, 2002, "Honda groups and explicit pairing on the module of Cartier curves" , *Algebraic Number Theory and Algebraic Geometry, Contemporary Methematics 300*, Parshin Festschrift,Ed. S. Vostokov and Y. Zarhin, AMS, Providence Rhode Island, pp. 143-170.

21. S. V. Vostokov, F. Lorenc, 2003, "Yavnaya formula simvola Gil'berta dlya grupp Hondy v mnogomernom lokal'nom pole" , *Matem. sb.*, 194:2, pp. 3–36

Получено 01.09.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-74-79

О неполных рациональных тригонометрических суммах

Салиба Холем Мансур — кандидат физико-математических наук, доцент факультета естественных и прикладных наук университета Нотр-Дам-Луэз, Ливан.
e-mail: qwe123@rocketmail.com

Аннотация

Приводится версия метода Хуа для оценки неполных рациональных тригонометрических сумм. Эти оценки не являются тривиальными для суммы с длинами, превышающими квадратный корень длины полной суммы.

Ключевые слова: метод Хуа оценки полных рациональных тригонометрических сумм, неполные рациональные тригонометрические суммы, полиномиальные сравнения, цепь показателей и корни сравнений.

Библиография: 10 названий.

Для цитирования:
Х. М. Салиба. О неполных рациональных тригонометрических суммах // Чебышевский сборник, 2018, т. 19, вып. 3, с. 74–79.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-74-79

On non-complete rational trigonometric sums

Saliba Holem Monsour — Ph.D. Assistant Professors of faculty of natural & applied sciences of Notre Dame University Louaize, Lebanon.
e-mail: qwe123@rocketmail.com

Abstract

We give the version of Hua's method for the estimation of non-complete rational trigonometric sums. These estimates are non-trivial one for sums with lengths exceeding a square root of length the complete sum.

Keywords: the Hua's method of complete rational trigonometric sums estimate, non-complete rational trigonometric sums, polynomial congruencies, the chain of exponents and roots of congruencies.

Bibliography: 10 titles.

For citation:
Saliba H. M., 2018, "On non-complete rational trigonometric sums" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 74–79.

To the memory of Academician J. V. Linnik

1. Introduction

The purpose of this article is to give the new demonstration of the estimation of non-complete rational trigonometric sums. Early the deduction of similar estimations are realized with using the Fourier analysis [1],[2]. Here we develop the Hua's method of estimations of complete rational sums ([2], p.101–109). We follow the version of this method, proposed by V. N. Chubarikov [6]-[10].

Let $n \geq 2, p$ is a prime number, $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, $(a_n, \dots a_1, p) = 1, \quad 0 \leq l < k$ and $e(x) = e^{2\pi i x}$,

$$S = S(p^k; k-l, f) = \sum_{x=1}^{p^{k-l}} e(f(x)/p^k) \tag{1}$$

$$S = \sum_{\xi=1}^{p} S(\xi), \quad S(\xi) = \sum_{\substack{x=1 \\ x \equiv \xi \pmod p}}^{p^{k-l}} e(f(x)/p^k), \tag{2}$$

moreover

$$S(\xi) = \sum_{x=1}^{p^{k-l-1}} e(f(\xi + px)/p^k).$$

Let $w = [\ln n / \ln p], \quad p^\tau \| (na_n, \dots, 2a_2, a_1)$, then $\tau \leq w$.

We define, following Hua L.-K. ([2], p. 217), solutions

$$x = \xi_1 + p\xi_2 + \cdots + p^{s-1}\xi_s + \dots \tag{3}$$

of congruence $f'(x) \equiv 0 \pmod{p^k}$ in the next way

$$p^{-\tau_0} f'(\xi_1) \equiv 0 \pmod p, p^{u_1} g_{\xi_1}(x) = f(\xi_1 + px) - f(\xi), \tag{4}$$

where the coefficients of the polynomial $g_{\xi_1}(x)$ and the number p have no common factor excepted 1, and further by the analogy for $s \geq 1$ we put

$$p^{-\tau_{s-1}} g_{(\xi_1,\dots,\xi_{s-1})}(\xi_s) \equiv 0 \pmod p, \tag{5}$$

$$p^{u_r} g_{(\xi_1,\dots,\xi_r)}(x) = g_{(\xi_1,\dots,\xi_{r-1})}(\xi_r + px) - g_{(\xi_1,\dots,\xi_{r-1})}(\xi_r), \tag{6}$$

$$k_s = k_{s-1} - u_s, l_s = l_{s-1} - u_s + 1. \tag{7}$$

Now we formulate statements of following theorems.

THEOREM 1. *Let inequalities $k_{r-1} \geq 2(l_{r-1} + w + 1), k_r < 2(l_r + w + 1)$ be define the number r. Then we have*

$$S(p^k; k-l, f) = \sum_{(\xi_1,\dots,\xi_r)} e\left(\frac{f(\xi_1)}{p^k} + \frac{g_{\xi_1}(\xi_2)}{p^{k_1}} + \cdots + \frac{g_{\xi_1,\dots,\xi_{r-1}}(\xi_r)}{p^{k_{r-1}}}\right) S(p^{k_r}; k_r - l_r, g_{(\xi_1,\dots,\xi_r)}).$$

THEOREM 2. *Let r be the smallest number over all solutions $(\xi_1, \xi_2, \dots, \xi_r)$, defining early, and satisfying inequalities $k_{r-1} \geq 2(l_{r-1} + w + 1), k_r < 2(l_r + w + 1)$. Then*

$$|S(p^k; k-l, f)| \leq (n-1)p^{k-l-r}. \tag{8}$$

2. Lemmas

Further we have the following statement.

LEMMA 1. *Let ξ is not a solution of the congruence $p^{-\tau}f'(x) \equiv 0 \pmod p$, and let $0 \le l < k$. Then for $k \ge l + 2(l + w)$ we get $S(\xi) = 0$.*

PROOF. We put $x = y + p^{k-l-\tau-2}z$, where $1 \le y \le p^{k-l-\tau-2}, 0 \le z \le p^{\tau+1} - 1$. It gives

$$S(\xi) = \sum_{y=1}^{p^{k-l-\tau-2}} \sum_{z=0}^{p^{\tau+1}-1} e(f(\xi + py + p^{k-l-\tau-1}z)/p^k) =$$

$$= \sum_{y=1}^{p^{k-l-\tau-2}} e(e(f(\xi + py)/p^k)) \sum_{z=0}^{p^{\tau+1}-1} e(f'(\xi + py)z/p^{\tau+1}) = 0,$$

as $p^{-\tau}f'(\xi) \not\equiv 0 \pmod p$ and $k \ge 2(l + \tau + 1)$.

Lemma is proved.

LEMMA 2. *Let ξ be a solution of the congruence $p^{-\tau}f'(\xi) \equiv 0 \pmod p$. Let*

$$p^u g(x) = f(\xi + px) - f(\xi), \quad g(x) = g_\xi(x) = b_n x^n + \cdots + b_1 x, \quad (b_n, \ldots b_1, p) = 1.$$

Then we have

$$S(\xi) = e(f(\xi)/p^k) \sum_{x=1}^{p^{k-l-1}} e(g(x)/p^{k-u}).$$

PROOF. We find

$$e(-f(\xi)/p^k)S(\xi) = \sum_{x=1}^{p^{k-l-1}} e((f(\xi + px) - f(\xi))/p^k) = \sum_{x=1}^{p^{k-l-1}} e(g(x)/p^{k-u}).$$

Lemma is proved.

LEMMA 3. *The number of solutions of the congruence $f'(x) \equiv 0 \pmod{p^k}$ in the sense described (3)–(7) is at most $n - 1$.*

PROOF. See ([2], p.217, Lemma 6.1).

LEMMA 4. *We have*

$$n - 1 \ge u_1 \ge u_2 \ge \cdots \ge u_r \ge 2.$$

PROOF. See ([2], p.219, Lemma 7.1).

LEMMA 5. *We have*

$$k - l + r - (u_1 + \cdots + u_r) \le [\ln n / \ln p].$$

PROOF. See ([2], p.220, Lemma 7.2).

3. Proof of theorems

1. For $k \ge 2(l + w + 1)$ we get

$$S(p^k; k - l, f) = \sum_{\xi} e(f(\xi)/p^k) S(p^{k-u}; k - l - 1, g_\xi),$$

where $\xi = \xi_1$ runs all solutions of the congruence $p^{-\tau} f'(\xi) \equiv 0 \pmod p$, and $u = u_1 = u_1(\xi)$ is defined in the statement of the Lemma 2.

Putting $k_1 = k - u_1, l_1 = l + 1 - u_1$, we have

$$S(p^k; k-l, f) = \sum_{\xi} e(f(\xi)/p^k) S(p^{k_1}; k_1 - l_1, g_\xi).$$

Thus if $k_1 \geq 2(l_1 + w + 1)$ then we obtain from Lemmas 1 and 2

$$S(p^k; k-l, f) = \sum_{(\xi_1, \xi_2)} e\left(\frac{f(\xi_1)}{p^k} + \frac{g_{\xi_1}(xi_2)}{p^{k_1}}\right) S(p^{k_1 - u_2}; k_1 - l_1 - 1, g_{(\xi_1,\xi_2)}),$$

where ξ_2 is a solution of the congruence

$$p^{-\tau_1} g'_{\xi_1}(\xi_2) \equiv 0 \pmod p, \quad p^{\tau_1} \| (nb_n, \ldots, 2b_2, b_1), \quad \tau_1 \leq w,$$

and

$$p^{u_2} g_{(\xi_1,\xi_2)}(x) = g_{\xi_1}(\xi_2 + px) - g_{\xi_1}(\xi_2), \quad g_{(\xi_1,\xi_2)}(x) = c_n x^n + \cdots + c_1 x, \quad (c_n, \ldots c_1, p) = 1.$$

We carry on doing this procedure further. For $r \geq 1$ we put

$$k_r = k_{r-1} - u_r, l_r = l_{r-1} + 1 - u_r.$$

$$p^{u_r} g_{(\xi_1,\ldots,\xi_r)}(x) = g_{(\xi_1,\ldots,\xi_{r-1})}(\xi_r + px) - g_{(\xi_1,\ldots,\xi_{r-1})}(\xi_r),$$

$$g_{(\xi_1,\ldots,\xi_r)}(x) = c_n^{(r)} x^n + \cdots + c_1^{(r)} x, \quad (c_n^{(r)}, \ldots c_1^{(r)}, p) = 1.$$

Then finally by Lemma 4 and 5 for some r from conditions

$$k_{r-1} \geq 2(l_{r-1} + w + 1), k_r < 2(l_r + w + 1),$$

we find

$$S(p^k; k-l, f) = \sum_{(\xi_1,\ldots,\xi_r)} e\left(\frac{f(\xi_1)}{p^k} + \frac{g_{\xi_1}(\xi_2)}{p^{k_1}} + \cdots + \frac{g_{\xi_1,\ldots,\xi_{r-1}}(\xi_r)}{p^{k_{r-1}}}\right) \times$$

$$\times S(p^{k_{r-1} - u_r}; k_{r-1} - l_{r-1} - 1, g_{(\xi_1,\ldots,\xi_r)}) =$$

$$= \sum_{(\xi_1,\ldots,\xi_r)} e\left(\frac{f(\xi_1)}{p^k} + \frac{g_{\xi_1}(\xi_2)}{p^{k_1}} + \cdots + \frac{g_{\xi_1,\ldots,\xi_{r-1}}(\xi_r)}{p^{k_{r-1}}}\right) S(p^{k_r}; k_r - l_r, g_{(\xi_1,\ldots,\xi_r)}),$$

where ξ_r is a solution of the congruence

$$p^{-\tau_{r-1}} g'_{(\xi_1,\ldots,\xi_{r-1})}(\xi_r) \equiv 0 \pmod p, \quad p^{\tau_{r-1}} \| (nb_n^{(r-1)}, \ldots, 2b_2^{(r-1)}, b_1^{(r-1)}), \quad \tau_{r-1} \leq w.$$

The theorem 1 is proved.

2. Further we have

$$k_r = k_{r-1} - u_r = k_{r-2} - u_{r-1} - u_r = \cdots = k - u_1 - u_1 - \cdots - u_r,$$

$$l_r = l_{r-1} + 1 - u_r = l_{r-2} + 1 - u_{r-1} + 1 - u_{r-2} = \cdots = l + r - u_1 - \cdots - u_r.$$

Hence

$$k_r - l_r = k - l - r.$$

From here we get

$$S(p^k;k-l,f)=\sum_{(\xi_1,\ldots,\xi_r)} e\left(\frac{f(\xi_1)}{p^k}+\frac{g_{\xi_1}(\xi_2)}{p^{k_1}}+\cdots+\frac{g_{\xi_1,\ldots,\xi_{r-1}}(\xi_r)}{p^{k_{r-1}}}\right) S(p^{k_r};k-l-r,g_{(\xi_1,\ldots,\xi_r)}).$$

Therefore, using the Lemma 3, we find

$$|S(p^k;k-l,f)|\le (n-1)p^{k-l-r}.$$

The theorem 2 is proved.

Conclusive notes. It's interesting to get non-trivial estimations for shorter non-complete rational trigonometric sums.

We continue recent studies of Professor V.N.Chubarikov on complete arithmetical sums. The problem of this paper due to him. I express my gratitude to Professor V.N.Chubarikov for the discussion of this problem.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Vinogradov I. M. Selected works. / New York Inc.: Springer Verlag, 1985, P. 401.
2. Hua L.-K. Selected Papers. / New York Inc.: Springer Verlag, 1983, P. 888.
3. Arkhipov G. I. Selected Papers. / Orjol: Publ. House of Orjol State University, 2013, P. 464.
4. 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, 2004. 554 P.
5. Karatsuba A. A. Distribution of fractional parts of polynomials of special form // Bull. Moscow University, Math., 1962, № 3. pp.34–38.
6. Chubarikov,V.N. Linear arithmetic sums and Gaussian multiplication theorem. // Azerbaijan — Turkey — Ukrainian Int.Conf. "Mathematical Analysis, Differential Equations and their Applications". Abstracts.(September 08-13, 2015, Baku-Azerbaijan). 2015, p.38.
7. Chubarikov V. N. Elementary of the complete rational arithmetical sums. // Chebyshevskii Sbornik. 2015;16(3) pp. 450-459.
8. Chubarikov V. N. Arithmetic sums of polynomial values // Dokl. RAN — 2016. — V.466, № 2. — pp.152-153.
9. Chubarikov V. N. Complete Rational Arithmetic Sums // Bull. Math. of Moscow Univ. Ser.I, 2015, № 1, pp.60-61.
10. Chubarikov V. N. On Complete Rational Arithmetic Sums of Polynomial Values // Proc. of the Steklov Institute of Math., 2017, V. 299, pp.50–55.

REFERENCES

1. Vinogradov I. M., 1985, *Selected works.* New York Inc.: Springer Verlag, P. 401.
2. Hua L.-K., 1983, *Selected Papers.* New York Inc.: Springer Verlag, P. 888.
3. Arkhipov G. I., 2013, *Selected Papers.* Orjol: Publ. House of Orjol State University, P. 464.

4. 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, 554 P.

5. Karatsuba A. A., 1962, "Distribution of fractional parts of polynomials of special form", *Bull. Moscow University, Math.,* № 3. pp. 34–38.

6. Chubarikov,V.N., 2015, "Linear arithmetic sums and Gaussian multiplication theorem", *Azerbaijan-Turkey-Ukrainian Int.Conf. "Mathematical Analysis, Differential Equations and their Applications".* Abstracts.(September 08-13, 2015, Baku-Azerbaijan), p.38.

7. Chubarikov V. N., 2015, "Elementary of the complete rational arithmetical sums", *Chebyshevskii Sbornik*, 16(3) pp. 450-459.

8. Chubarikov V. N., 2016, "Arithmetic sums of polynomial values", *Dokl. RAN* V.466, № 2. pp.152-153.

9. Chubarikov V. N., 2015, "Complete Rational Arithmetic Sums", *Bull. Math. of Moscow Univ. Ser.I,* № 1, pp.60-61.

10. Chubarikov V. N., 2017, "On Complete Rational Arithmetic Sums of Polynomial Values", *Proc. of the Steklov Institute of Math.*, V. 299, pp.50–55.

Получено 16.09.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-80-94

Константа Линника меньше 5

Xylouris Triantafyllos — Франкфурт-на-Майне, Германия.
e-mail: t.xylouris@gmail.com

Аннотация

Пусть a и q — положительные, целые числа. В 1944 г. Ю. В. Линник показал, что наименьшее простое число в арифметической прогрессии $mod q$ меньше Cq^L с положительными константами C и L.

Основываясь на работе Хис-Брауна, мы доказываем, что $L = 5$ допустимо.

Ключевые слова: Константа Линника.

Библиография: 24 названия.

Для цитирования:
T. Xylouris, Linniks Konstante ist kleiner als 5 // Чебышевский сборник, 2018, т. 19, вып. 3, с. 80–94.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-80-94

Linniks Konstante ist kleiner als 5

Xylouris Triantafyllos — Frankfurt am Main, Germany.
e-mail: t.xylouris@gmail.com

Abstract

Seien a und q zwei teilerfremde, positive, ganze Zahlen. In 1944 bewies Y. Linnik, dass die kleinste Primzahl in einer arithmetischen Progression $mod\ q$ kleiner als Cq^L ist mit positiven Konstanten C und L.

Aufbauend auf einer Arbeit von Heath-Brown beweisen wir, dass $L = 5$ zulässig ist.

Keywords: Linniks Konstante.

Bibliography: 24 titles.

For citation:
T. Xylouris, 2018, "Linniks Konstante ist kleiner als 5", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 80–94.

1. Einführung

Seien a und q zwei teilerfremde, positive, ganze Zahlen und

$$P(a,q) := \min\{p \equiv a(\mod q) \,|\, p \text{ Primzahl}\}.$$

In 1944 bewies Y. Linnik [15, 16]

$$P(a,q) < Cq^L$$

mit effektiv berechenbaren, positiven Konstanten C und L. Dies wird als Linniks Theorem und L als Linniks Konstante bezeichnet. Wir verweisen auf [12, §18], [11, S.265-270] und [24, §2.2] für eine weitergehende Einführung und Motivation. Mehrere Autoren haben zulässige Werte für L bewiesen:

Tabelle 1. Zulässige Werte für L

L	Jahr	Autor	Verweis
10000	1957	Pan	[18]
5448	1958	Pan	[19]
777	1965	Chen	[2]
630	1971	Jutila	[20, S.370]
550	1970	Jutila	[13]
168	1977	Chen	[3]
80	1977	Jutila	[14]
36	1977	Graham	[8]
20	1981	Graham	[10]
17	1979	Chen	[4]
16	1986	Wang	[21]
13.5	1989	Chen und Liu	[5]
11.5	1991	Chen und Liu	[6]
8	1991	Wang	[22]
5.5	1992	Heath-Brown	[11]
5.18	2011	Xylouris	[23]
5	2011	Xylouris	[24]

In [23] verwenden wir mehrere Verbesserungspotentiale, die Heath-Brown in [11, S.332f] beschreibt und beweisen Linniks Theorem mit $L = 5.18$. Unsere Arbeit [24] beinhaltet [23], sowie vier weitere technische Verbesserungen:

- Kleinere Anpassungen bei der Herleitung (fast) nullstellenfreier Regionen (§3 der vorliegenden Arbeit)
- Verwendung allgemeinerer Siebgewichte in einem Nullstellendetektor - es folgen bessere Abschätzungen der Nullstellendichte für Nullstellen weit weg von $s = 1$ (§4)
- Verallgemeinerung und Optimierung von Abschätzungen der Nullstellendichte für Nullstellen nahe $s = 1$ (§5)
- Verwendung einer allgemeineren Gewichtsfunktion in jener expliziten Formel, die Ausgangspunkt für unseren Beweis von Linniks Theorem ist (§6)

Die vorliegende Arbeit ist eine Zusammenfassung dieser vier technischen Verbesserungen aus [24]. Unser Hauptresultat lautet:

THEOREM 1. *Seien a und q zwei teilerfremde, positive, ganze Zahlen. Dann ist*

$$P(a,q) < Cq^5$$

mit einer effektiv berechenbaren Konstanten C.

Genauer erhalten wir anstelle von 5 einen Wert, der geringfügig kleiner als 5 ist. Wenn wir unsere Computerberechnungen stark erweitern würden, dann vermuten wir, dass wir Linniks Theorem mit $L = 4.96$ beweisen könnten. Weiterhin erhalten wir nicht nur die Existenz einer Primzahl, sondern von $q^{3.21}$ Primzahlen, welche kleiner als q^5 sind für q groß genug [24, Lemma 6.2]. Ähnliche Aussagen folgen auch aus anderen Arbeiten zu Linniks Theorem.

Ausgangspunkt für den Beweis von Theorem 1 ist eine explizite Formel, welche die Primzahlen in arithmetischen Progressionen mit den Nullstellen Dirichletscher L-Funktionen nahe $s = 1$ in Verbindung bringt. Je weniger Dirichletsche L-Funktionen *mod* q eine Nullstelle nahe $s = 1$ haben, und je weiter weg diese potentiellen Nullstellen von $s = 1$ sind, desto mehr bedingt dies die Existenz kleiner Primzahlen ($< q^L$) in einer arithmetischen Progression *mod* q.

Ähnlich zu [11] verwenden wir Computerberechnungen. Diese haben wir mit der Software Maple und einem handelsüblichen Laptop im Jahr 2011 durchgeführt.

Ich möchte meinem Doktorvater Prof. Dr. B. Z. Moroz für seine konstante Unterstützung eingehend danken.

2. Notation

Für $q \in \mathbb{N} = \{1, 2, 3, \ldots\}$ bezeichne χ einen Dirichlet-Charakter *mod* q, χ_0 den Hauptcharakter *mod* q und $L(s, \chi)$ die zugehörige Dirichletsche L-Funktion. $(\operatorname{ord} \chi)$ bezeichne die Ordnung von χ in der Gruppe der Dirichlet-Charaktere *mod* q, $[x] := \max\{a \in \mathbb{Z} \mid a \leq x\}$ und

$$\mathscr{L} := \log q.$$

Für den Realteil einer komplexen Zahl z schreiben wir $\Re\{z\}$ und für den Imaginärteil $\Im\{z\}$. Die Resultate in dieser Arbeit werden meist für $q \geq q_0$ bewiesen, wobei q_0 eine effektiv berechenbare Konstante ist.

Um Linniks Konstante zu verbessern, genügt es die vorhandenen Abschätzungen zur Lage der Nullstellen Dirichletscher L-Funktionen im Rechteck

$$R := R(l) := \left\{\sigma + it \in \mathbb{C} \mid 1 - \frac{\log\log \mathscr{L}}{3\mathscr{L}} \leq \sigma \leq 1,\ |t| \leq l\right\}$$

zu verbessern. Dabei ist $l \leq \mathscr{L}/10$ die positive Zahl aus [11, Lemma 6.1]. Diese Wahl für l garantiert, dass es keine Nullstellen leicht oberhalb oder unterhalb von R gibt, was die Berechnungen vereinfacht. Für ein festes q betrachten wir alle Nullstellen $\rho \in R$ von

$$P(s) := \prod_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} L(s, \chi). \tag{1}$$

Sei ρ_1 eine Nullstelle von $P(s)$ in R, für die $\Re\{\rho_1\}$ maximal ist und sei χ_1 ein Charakter mit $L(\rho_1, \chi_1) = 0$. Wir führen diesen Prozess weiter, indem wir im k'ten Schritt ($k \geq 2$) die Nullstellen $\rho \in R$ von

$$\frac{P(s)}{L(s, \chi_1)L(s, \overline{\chi_1}) \cdot \ldots \cdot L(s, \chi_{k-1})L(s, \overline{\chi_{k-1}})}$$

betrachten und eine Nullstelle ρ_k wählen mit maximalem Realteil und ein χ_k mit $L(\rho_k, \chi_k) = 0$. Wir führen dies weiter fort bis im betrachteten Produkt keine weiteren Dirichletschen L-Funktionen auftauchen. Es ist

$$\chi_i \neq \chi_j, \overline{\chi_j} \quad \text{für} \quad i \neq j.$$

Wir setzen

$$\rho_k = \beta_k + i\gamma_k, \quad \beta_k = 1 - \mathscr{L}^{-1}\lambda_k, \quad \gamma_k = \mathscr{L}^{-1}\mu_k.$$

Wir benennen noch eine weitere, potentielle Nullstelle ρ' von $L(s, \chi_1)$ wie folgt:

1. Wenn ρ_1 eine mehrfache Nullstelle ist, dann wähle $\rho' = \rho_1$.
2. Wenn χ_1 reell und ρ_1 komplex ist, dann wähle ρ' aus den Nullstellen in $R\backslash\{\rho_1, \overline{\rho_1}\}$, so dass $\Re\{\rho'\}$ maximal ist.
3. Ansonsten wähle ρ' aus den Nullstellen in $R\backslash\{\rho_1\}$, so dass $\Re\{\rho'\}$ maximal ist.

Analog zu vorher schreiben wir

$$\rho' = \beta' + i\gamma', \quad \beta' = 1 - \mathscr{L}^{-1}\lambda', \quad \gamma' = \mathscr{L}^{-1}\mu'.$$

Für Abschätzungen zur Nulstellendichte genügt es nur Nullstellen mit $\Im(\rho) \leq 1$ zu betrachten. Wir definieren

$$N(\lambda) := \#\{\chi \pmod q \mid \chi \neq \chi_0,\, L(s,\chi) \text{ hat eine Nullstelle in } \sigma \geq 1 - \mathscr{L}^{-1}\lambda,\, |t| \leq 1\}$$

und bezeichnen die $N(\lambda)$ dazugehörigen Charaktere durch

$$\chi^{(1)}, \chi^{(2)}, \ldots, \chi^{(N(\lambda))}.$$

Zu jedem der $N(\lambda)$ Charaktere χ wählen wir eine Nullstelle $\rho(\chi) = \rho^{(k)}$ mit maximalem Realteil und schreiben

$$\rho^{(k)} = \beta^{(k)} + i\gamma^{(k)}, \quad \beta^{(k)} = 1 - \mathscr{L}^{-1}\lambda^{(k)}.$$

Wir werden an vielen Stellen die Gewichtsfunktion

$$f(t) = \begin{cases} \int_{t-\gamma}^{\gamma} g(x)g(t-x)\,dx = -\frac{1}{30}t^5 + \frac{2\gamma^2}{3}t^3 - \frac{4\gamma^3}{3}t^2 + \frac{16\gamma^5}{15} & \text{falls } t \in [0, 2\gamma), \\ 0 & \text{falls } t \geq 2\gamma. \end{cases} \tag{2}$$

benutzen, sowie ihre Laplace-Transformierte

$$F(z) = \begin{cases} \frac{16\gamma^5}{15}z^{-1} - \frac{8\gamma^3}{3}z^{-3} + 4\gamma^2(1 + e^{-2\gamma z})z^{-4} \\ \qquad\qquad +4(-1 + e^{-2\gamma z} + 2\gamma z e^{-2\gamma z})z^{-6} & \text{falls } z \neq 0, \\ \frac{8\gamma^6}{9} & \text{falls } z = 0. \end{cases}$$

Die Funktion $f(t)$ ist nicht-negativ und erfüllt zwei Regularitätsbedingungen, die in [24, § 3.1.2] genauer beschrieben werden. Außerdem ist $F(z)$ als Laplace-Transformierte einer nicht-negativen Funktion monoton fallend in z.

3. Kleinere Anpassungen (fast) nullstellenfreier Regionen

Für $\lambda_1 < 0.348$ haben wir Linniks Theorem für $L = 4.9$ [11, Lemma 14.2]. Um Theorem 1 für den verbleibenden Fall $\lambda_1 \geq 0.348$ zu beweisen, benutzen wir eine Ungleichung der Form (vergleiche [23, (4.10), (4.17), (4.18)])

$$\sum_{\substack{p \text{ prim} \\ p \equiv a \pmod q \\ p \leq q^5}} w(p) > g_1(\lambda_1, \lambda_2, \lambda_3, \lambda') \tag{3}$$

wobei g_1 monoton wachsend in λ_1, λ_2, λ_3 und λ' ist. Wir müssen zeigen, dass die rechte Seite von (3) positiv ist. Um diese nach unten abzuschätzen, können wir Abschätzungen der Form (vergleiche [23, Tabellen 1-10])

$$\lambda_1 \in [\lambda_{11}, \lambda_{12}] \Longrightarrow \lambda_1 \geq \widetilde{\lambda_{11}}, \quad \lambda_2 \geq \lambda_{21}, \quad \lambda_3 \geq \lambda_{31}, \quad \lambda' \geq \lambda'_{11}$$

verwenden mit konkreten Werten für λ_{11}, λ_{12}, λ_{21}, λ_{31} und λ'_{11}. Solche Abschätzungen sind äquivalent zu nullstellenfreien Regionen (im Fall von λ_1) oder fast nullstellenfreier Regionen (in den anderen Fällen) der Funktion $P(s)$ aus (1).

In [23] haben wir Abschätzungen für λ' hergeleitet mittels Ungleichungen der Form [23, Lemma 3.1]

$$\lambda' \geq g_2(\min(\lambda', \lambda_2)) \tag{4}$$

wobei g_2 monoton wachsend in $\min(\lambda', \lambda_2)$ ist. Sobald wir also eine untere Abschätzung für λ' beweisen, können wir diese wieder in (4) einsetzen und eventuell die untere Abschätzung für λ' weiter verbessern: Genauer benutzen wir vermöge [23, Table 7] ein größeres $\lambda^\star$ in den Berechnungen, die zu [23, Table 2] führen. Weiterhin benutzen wir $\lambda_1 \geq 0.44$ vermöge [23, Theorem 1.2]. Damit verbessern wir [23, Table 2] zu [24, Tabelle 2'], welche wir weiter unten notieren.

Um darüber hinaus den Beweis der Zulässigkeit von $L = 5$ im Fall von $\lambda_1 \in [0.68, 0.78]$ zu ermöglichen, unterscheiden wir mehrere Fälle in den Berechnungen, die zu [23, Table 9] führen. Damit erhalten wir [24, Tabelle 9]. Die erhöhte Anzahl der Fälle spiegelt sich in der erhöhten Anzahl der Zeilen in letzterer Tabelle wieder. Schlussendlich verändern wir die in [23, Table 10] betrachteten Fälle leicht und reduzieren das $\delta = 0.001$ zu $\delta = 0.0001$ in den entsprechenden Berechnungen. Damit erhalten wir [24, Tabelle 10].

Tabelle 2'. Verbesserte λ'-Abschätzungen.
(χ_1 oder ρ_1 komplex)

$\lambda_1 \leq$	$\lambda' >$	$\lambda^\star$	$C \leq$
0.46	1.85	1.56	0.0797
0.48	1.76	1.45	0.0598
0.50	1.67	1.36	0.0455
0.52	1.59	1.27	0.0332
0.54	1.51	1.19	0.0235
0.56	1.44	1.11	0.0150
0.58	1.36	1.04	0.0084
0.60	1.29	0.97	0.0026
0.62	1.22	0.91	0.0016
0.64	1.15	0.85	0.0010
0.66	1.08	0.79	0.0008
0.68	1.02	0.74	0.0007
0.70	0.96		-
0.72	0.93		-
0.74	0.91		-
0.76	0.89		-
0.78	0.86		-
0.80	0.84		-
0.82	0.83		-
0.827	0.827		-

Tabelle 9. λ_3**-Abschätzungen.**
(χ_1 komplex)

$\lambda_1 \in$	Bedingung	$\lambda_3 >$
$[0.62, 0.64]$	-	0.902
$[0.64, 0.66]$	-	0.898
$[0.66, 0.68]$	-	0.893
$[0.68, 0.70]$	-	0.888
$[0.68, 0.70]$	$\lambda_2 \leq 0.745$	1.054
$[0.70, 0.71]$	-	0.886
$[0.70, 0.71]$	$\lambda_2 \leq 0.745$	1.048
$[0.71, 0.72]$	-	0.883
$[0.71, 0.72]$	$\lambda_2 \leq 0.75$	1.036
$[0.72, 0.74]$	-	0.878
$[0.72, 0.74]$	$\lambda_2 \leq 0.76$	1.012
$[0.74, 0.78]$	-	0.868
$[0.74, 0.78]$	$\lambda_2 \leq 0.78$	0.996

Tabelle 10. λ_3**-Abschätzungen**
(χ_1 und ρ_1 reell)

$\lambda_1 \in$	$\lambda_3 >$
$[0.44, 0.60]$	1.176
$[0.60, 0.70]$	1.055
$[0.70, 0.80]$	0.952

4. Verbesserung der Nullstellendichte-Abschätzung für großes λ

Wir beweisen Linniks Theorem ausgehend von einer Ungleichung vom Typ (3), wobei g_1 von den Nullstellen der Charaktere χ_1, χ_2, χ_3 abhängt. Darüber hinaus hängt g_1 auch von den Nullstellen aller weiteren Dirichletschen L-Funktionen *mod* q ab (siehe [24, (6.31), (6.32)]). Deren Beitrag kann mit Hilfe von Abschätzungen der Nullstellendichte beschränkt werden, die in ihrer klassischen Form die maximale Anzahl aller Nullstellen aller Dirichletschen L-Funktionen modulo einem festen q beschränken.

Um Linniks Konstante zu verbessern, benutzt Heath-Brown eine angepasste Abschätzung, die nur eine Nullstelle (jene, deren Realteil am Nähesten zu $s = 1$ ist) für jede Dirichletsche L-Funktion betrachtet [11, Lemma 11.1]. Um Heath-Browns Abschätzung weiter zu verbessern, benutzen wir allgemeinere 'Siebgewichte' ψ_d im verwendeten 'Nullstellendetektor' [24, (3.28)]

$$1 \leq \left| \sum_{U<n<X\mathscr{L}} (\sum_{d|n} \psi_d)(\sum_{d|n} \theta_d)\chi(n)n^{-\rho(\chi)}e^{-n/X} \right| + O(\mathscr{L}^{-1}).$$

Letztere Abschätzung wird Nullstellendetektor genannt, weil nicht für zu viele, unterschiedliche ρ, diese Ungleichung gültig sein kann. Im Folgenden beschreiben wir kurz unseren Ansatz und das resultierende Lemma. Für mehr Details verweisen wir auf [24, §3.2, §5.1].

Seien $0 < u < v < x$ und $U = q^u$, $V = q^v$, $X = q^x$. Der Nullstellendetektor beinhaltet Gewichte ψ_d ($d \in \mathbb{N}$), die

$$\begin{aligned} &\psi_d = \mu(d) \qquad (1 \leq d \leq U), \\ &\psi_d = 0 \qquad (d \geq V), \\ &\psi_d \ll 1 \end{aligned}$$

erfüllen müssen. Um Linniks Konstante zu verbessern, sind die ψ_d so zu wählen, dass

$$\sum_{U<n\leq X} \Big(\sum_{d|n} \psi_d\Big)^2 n^{-1} \tag{5}$$

möglichst klein ausfällt. Heath-Brown wählt

$$\psi_d = \psi_d^{U,V} := \begin{cases} \mu(d) & \text{falls } 1 \leq d \leq U, \\ \mu(d)\frac{\log(V/d)}{\log(V/U)} & \text{falls } U \leq d \leq V, \\ 0 & \text{falls } V \leq d, \end{cases}$$

was ziemlich optimal wäre, falls $U = V$ (vergleiche [1]). Da aber $U < V$, gibt es hier eventuell die Möglichkeit die Wahl der ψ_d weiter zu optimieren. In der Tat ist dies möglich, indem eine passende Linearkombination

$$\psi_d = \sum_{i=1}^{M} \alpha_i \psi_d^{U_{i-1},U_i}$$

gewählt wird, mit $M \in \mathbb{N}$, $\alpha_i \geq 0$, $\sum_{i=1}^{M} \alpha_i = 1$ und $U_i = q^{u_i}$ für $u_i = u + i \cdot (v-u)/M$.

Für festes M wird der Ausdruck (5) durch

$$\alpha_i := \left(\sum_{1 \leq j \leq M} \frac{C(M)-i}{C(M)-j} \right)^{-1} \qquad (i = 1, \cdots, M)$$

minimiert mit

$$C(M) := \frac{1}{2} + M \frac{x-u_0}{u_M - u_0}.$$

Je größer wir M wählen, desto besser die resultierende Abschätzung. Computerberechnungen lassen vermuten, dass der zusätzliche Gewinn mit wachsendem M sehr schnell fällt. Wir wählen später $M = 10$. Mit diesen neuen Gewichten ψ_d erhalten wir die folgende Verbesserung von [23, Lemma 3.4] (welches selbst eine Verallgemeinerung von [11, Lemma 11.1] ist).

LEMMA 1. *Sei $M \in \mathbb{N}$, ε, c_1, $c_2 > 0$ und $\lambda_0 = \frac{1}{3} \log\log \mathscr{L}$. Sei*

$$u_i := \frac{1}{3} + 2c_1 + \frac{i \cdot c_2}{M} \quad (i \in \{0, \ldots, M\})$$

und

$$x := \frac{2}{3} + 3c_1 + c_2.$$

Sei $w_0 : [u_0, x] \to \mathbb{R}$ eine stetige Funktion, welche stetig differenzierbar ist bis auf endliche viele Stellen. Weiterhin erfülle diese Funktion

$$1 \ll w_0(t) \ll 1 \quad \text{und} \quad w_0'(t) \ll 1$$

mit gewissen absoluten impliziten Konstanten. Dann gibt es ein q_0, welches von allen gewählten Konstanten abhängt, so dass für $q \geq q_0$

$$\sum_{1 \leq k \leq N(\lambda_0)} \left(\int_{u_0}^{x} w_0(t)^2 e^{2\lambda^{(k)} t}\, dt \right)^{-1} \leq \frac{M^2 + \varepsilon}{c_1 c_2^2} \sum_{i=1}^{M} \alpha_i^2 \int_{u_{i-1}}^{x} w_0(t)^{-2} \min\{t - u_{i-1}, u_i - u_{i-1}\}\, dt.$$

Speziell erhalten wir für $w_0(t) \equiv 1$, $c_1 = \frac{1}{10}$, $c_2 = \frac{1}{4}$ und $M = 10$, dass für $q \geq q_0$ und $\lambda \leq \lambda_0$

$$N(\lambda) \leq \frac{10.98}{\lambda} (e^{\frac{73\lambda}{30}} - e^{\frac{16\lambda}{15}}).$$

5. Verbesserung der Nullstellendichte-Abschätzung für kleine λ

Um Linniks Konstante zu verbessern, müssen wir eine Summe über Nullstellen (vergleiche (14))

$$\sum_{c_1 < \lambda^{(k)} \leq c_2} g_3(\lambda^{(k)})$$

nach oben abschätzen, wobei g_3 eine monoton fallende Funktion ist. Lemma 1 liefert eine Abschätzung

$$\sum_{c_1<\lambda^{(k)}\le c_2} g_4(\lambda^{(k)}) \le C$$

für eine fallende Funkiton g_4, womit

$$\sum_{c_1<\lambda^{(k)}\le c_2} g_3(\lambda^{(k)}) \le C\cdot \sup_t \frac{g_3(t)}{g_4(t)}.$$

Eine Alternative zu letzterer Vorgehensweise ist wie folgt: Haben wir hinreichend gute Abschätzungen $N(\lambda)\le N_0(\lambda)$, dann kann die folgende Abschätzung besser sein (setze $\delta=(c_2-c_1)/10$):

$$\begin{aligned}\sum_{c_1<\lambda^{(k)}\le c_2} g_3(\lambda^{(k)}) &\le \sum_{j\ge 0}^{9}(N(c_1+(j+1)\delta)-N(c_1+j\delta))g_3(c_1+j\delta)\\ &\le N_0(c_1)\cdot g_3(c_1)+\sum_{j\ge 0}^{9}(N_0(c_1+(j+1)\delta)-N_0(c_1+j\delta))g_3(c_1+j\delta).\end{aligned}$$

Heath-Brown leitet Abschätzungen $N(\lambda)\le N_0(\lambda)$ her [11, Lemma 12.1], welche für kleine λ (ungefähr $\lambda\le 1.3$) bessere Resultate liefern als Lemma 1. Wir haben Heath-Browns Lemma in [23, Lemma 3.5] leicht verallgemeinert. Darüber hinaus setzen wir jetzt Verbesserungspotential 2 ein (vergleiche [11, S.332]) und führen eine weitere Verallgemeinerung ein, um unsere späteren Berechnungen durch mehrere Fallunterscheidungen weiter zu optimieren. Es folgt [24, Lemma 5.3], welches wir hier notieren:

LEMMA 2. *Seien B_1, D_1 nicht-negative, ganze Zahlen. Seien b, d, λ und $\lambda^\star$ positive Zahlen, $C\ge 0$, $\lambda_{12}\in(0,\infty]$ und f eine Funktion, die Bedingungen 1 und 2 aus [11, S. 280, 286] erfüllt. Sei F die Laplace-Transformierte von f und setze*

$$m(\chi_1):=\begin{cases}0 & \text{falls } \lambda_{12}\ge b,\\ 1 & \text{falls } \lambda_{12}\le b \text{ und } \chi_1 \text{ reell},\\ 2 & \text{falls } \lambda_{12}\le b \text{ und } \chi_1 \text{ komplex},\end{cases}$$

$$E(\chi_1):=\begin{cases}1 & \text{falls } \chi_1 \text{ reell und } \rho_1 \text{ komplex},\\ 0 & \text{sonst}\end{cases}$$

und

$$\begin{aligned}a_0 :=& -D_1F(\lambda-\lambda^\star)+(D_1-B_1)F(d-\lambda^\star)\\ &+(B_1-m(\chi_1))F(b-\lambda^\star)+m(\chi_1)F(\lambda_{12}-\lambda^\star)-E(\chi_1)\cdot C,\\ a_1 :=& F(-\lambda^\star)\frac{f(0)}{6}-\left(F(\lambda-\lambda^\star)-\frac{f(0)}{6}\right)^2,\\ a_2 :=& F(-\lambda^\star)\left(F(-\lambda^\star)-\frac{f(0)}{6}+2C\right)-2a_0\left(F(\lambda-\lambda^\star)-\frac{f(0)}{6}\right),\\ a_3 :=& -a_0^2-2C\cdot F(-\lambda^\star).\end{aligned}$$

Angenommen die benutzten Parameter erfüllen

$$\lambda^\star\le b\le d\le\lambda\le 2,\quad \lambda_1\le\lambda_{12},\quad \lambda^\star\le\min\{\lambda',\lambda_2\},\qquad a_1<0,$$

$$F(\lambda-\lambda^\star) > \frac{f(0)}{6} + E(\chi_1)\cdot C,$$
$$C \geq \sup_{t\in\mathbb{R}}\{-\Re\{F(\lambda_1-\lambda^\star+it)\}\},$$
$$B_1 \leq N(b), \quad D_1 \leq N(d).$$

Dann haben wir für $q \geq q_0$

$$N(\lambda) \leq \max\left\{0, \left[\frac{a_2+\sqrt{|a_2^2-4a_1a_3|}}{-2a_1}\right]\right\}. \tag{6}$$

Proof. Wir führen den Beweis analog zum Beweis von [11, Lemma 12.1]. Sei $l = l(q) \in [1, \mathscr{L}]$ die Zahl aus [11, Lemma 6.1] und

$$N := \widetilde{N}(\lambda) := \#\{\chi \mid \chi(\mod q), L(s,\chi) \text{ hat eine Nullstelle in } \sigma \geq 1-\mathscr{L}^{-1}\lambda,\ |t|\leq l\}.$$

Seien $\chi^{(1)}$, …, $\chi^{(N)}$ die verschiedenen Charaktere aus der Definition von N. Wähle zu jedem Charakter $\chi^{(j)}$ eine entsprechende Nullstelle $\rho^{(j)}$ von $L(s,\chi^{(j)})$ mit

$$\sigma \geq 1-\mathscr{L}^{-1}\lambda, \qquad |t| \leq l.$$

Für $\chi^{(j)} = \chi_1$ wählen wir die Nullstelle ρ_1 und, falls χ_1 komplex ist, so wählen wir für $\chi^{(j')} = \overline{\chi_1}$ die Nullstelle $\overline{\rho_1}$.

Wir erinnern daran, dass die Laplace-Transformierte F monoton fallend ist. Da $b \leq d \leq \lambda$, folgt

$$F(\lambda-\lambda^\star) \leq F(d-\lambda^\star) \leq F(b-\lambda^\star).$$

Mit $\lambda_1 \leq \lambda_{12}$, $B_1 \leq N(b)$, $D_1 \leq N(d)$ folgt

$$\begin{aligned}(N-D_1)F(\lambda-\lambda^\star) &+ (D_1-B_1)F(d-\lambda^\star)\\ &+ (B_1-m(\chi_1))F(b-\lambda^\star) + m(\chi_1)F(\lambda_{12}-\lambda^\star) - N(\frac{f(0)}{6}+\varepsilon) - E(\chi_1)\cdot C \end{aligned}\tag{7}$$

$$\begin{aligned}\leq &(N-\max\{D_1,B_1,m(\chi_1)\})F(\lambda-\lambda^\star) + (\max\{D_1,B_1,m(\chi_1)\}-\max\{B_1,m(\chi_1)\})F(d-\lambda^\star)\\ &+ (\max\{B_1,m(\chi_1)\}-m(\chi_1))F(b-\lambda^\star) + m(\chi_1)F(\lambda_{12}-\lambda^\star) - N(\frac{f(0)}{6}+\varepsilon) - E(\chi_1)\cdot C.\end{aligned}$$

Da F monoton fallend ist, ist Letzteres

$$\leq \sum_{j\leq N} F(\lambda^{(j)}-\lambda^\star) - N(\frac{f(0)}{6}+\varepsilon) - E(\chi_1)\cdot C. \tag{8}$$

Sei

$$K(s,\chi) := \sum_{n=1}^{\infty}\Lambda(n)\Re\left\{\frac{\chi(n)}{n^s}\right\} f(\mathscr{L}^{-1}\log n).$$

Vermöge [23, Lemma 2.1] mit $\beta^\star = 1-\mathscr{L}^{-1}\lambda^\star$ folgt

$$K(\beta^\star+i\gamma^{(j)},\chi^{(j)}) \leq \begin{cases} -\mathscr{L}F(\lambda^{(j)}-\lambda^\star) + \mathscr{L}\cdot E(\chi_1)\cdot C + \mathscr{L}\left(\frac{f(0)}{6}+\varepsilon\right) & \text{falls } \chi^{(j)}=\chi_1,\\ -\mathscr{L}F(\lambda^{(j)}-\lambda^\star) + \mathscr{L}\left(\frac{f(0)}{6}+\varepsilon\right) & \text{sonst.}\end{cases}$$

Also ist (8)

$$\leq \mathscr{L}^{-1}\sum_{n=1}^{\infty}\Lambda(n)n^{-\beta^\star}f(\mathscr{L}^{-1}\log n)\left|\sum_{j\leq N}\frac{\chi^{(j)}(n)}{n^{i\gamma^{(j)}}}\right|. \tag{9}$$

Kombiniert man (7) - (9) und benutzt man Cauchys Ungleichung, so erhält man

$$\mathscr{L}^2\Big((N-D_1)F(\lambda-\lambda^\star)+(D_1-B_1)F(d-\lambda^\star)+(B_1-m(\chi_1))F(b-\lambda^\star) + m(\chi_1)F(\lambda_{12}-\lambda^\star)-N(\frac{f(0)}{6}+\varepsilon)-E(\chi_1)\cdot C\Big)^2 \leq \Sigma_1\Sigma_2 \tag{10}$$

wobei

$$\Sigma_1 := \sum_{n=1}^{\infty}\Lambda(n)\chi_0(n)n^{-\beta^\star}f(\mathscr{L}^{-1}\log n) = K(\beta^\star,\chi_0)$$

und

$$\begin{aligned}\Sigma_2 &= \sum_{n=1}^{\infty}\Lambda(n)n^{-\beta^\star}f(\mathscr{L}^{-1}\log n)\left|\sum_{j\leq N}\frac{\chi^{(j)}(n)}{n^{i\gamma^{(j)}}}\right|^2\\ &= \sum_{n=1}^{\infty}\Lambda(n)n^{-\beta^\star}f(\mathscr{L}^{-1}\log n)\sum_{j,k\leq N}\frac{\chi^{(j)}(n)}{n^{i\gamma^{(j)}}}\frac{\overline{\chi^{(k)}}(n)}{n^{-i\gamma^{(k)}}}\\ &= \sum_{j,k\leq N}K(\beta^\star+i(\gamma^{(j)}-\gamma^{(k)}),\chi^{(j)}\overline{\chi^{(k)}}).\end{aligned}$$

Für Σ_1 und die N Terme in Σ_2 mit $j=k$ haben wir gemäß [11, Lemma 5.3]

$$K(\beta^\star,\chi_0)\leq\mathscr{L}(F(-\lambda^\star)+\varepsilon). \tag{11}$$

Wir benutzen [23, Lemma 2.1] für die verbleibenden Terme. Wir müssen zuerst die Anzahl der Elemente in der Menge

$$\{(j,k)\in\mathbb{N}^2 \quad | \quad 1\leq j\neq k\leq N, \quad \chi^{(j)}\overline{\chi^{(k)}}\in\{\chi_1,\overline{\chi_1}\}\} \tag{12}$$

abschätzen. Gemäß der Definitionen tauchen χ_1 und $\overline{\chi_1}$ beide innerhalb der N Charaktere $\chi^{(j)}$ auf. Außerdem haben wir

$$\chi^{(j)}\overline{\chi^{(k_1)}}=\chi^{(j)}\overline{\chi^{(k_2)}} \quad\Longrightarrow\quad k_1=k_2.$$

Wähle nun ein festes j.

Fall 1: χ_1 ist reell.
Fall 1.1: $\chi^{(j)}=\chi_1$. Dann ist $\chi^{(j)}\overline{\chi^{(k)}}\notin\{\chi_1,\overline{\chi_1}\}$ für jedes $k\neq j$.
Fall 1.2: $\chi^{(j)}\neq\chi_1$. Dann ist $\chi^{(j)}\overline{\chi^{(k)}}\in\{\chi_1,\overline{\chi_1}\}=\{\chi_1\}$ für maximal ein $k\neq j$.
Wenn also χ_1 reell ist, dann gibt es maximal (wir können $N\geq 1$ annehmen)

$$N-1\leq 2N-2$$

Elemente in (12).

Fall 2: χ_1 ist komplex.
Fall 2.1: $\chi^{(j)}=\chi_1$ oder $\chi^{(j)}=\overline{\chi_1}$. Dann ist $\chi^{(j)}\overline{\chi^{(k)}}\in\{\chi_1,\overline{\chi_1}\}$ für maximal ein $k\neq j$.
Fall 2.2: $\chi^{(j)}\neq\chi_1,\overline{\chi_1}$. Dann ist $\chi^{(j)}\overline{\chi^{(k)}}\in\{\chi_1,\overline{\chi_1}\}$ für maximal zwei $k\neq j$.
Wenn also χ_1 komplex ist, so gibt es maximal

$$2\cdot 1+(N-2)\cdot 2=2N-2$$

Elemente in (12).

Die Menge $A_1 = A_1(\chi)$ aus [23, Lemma 2.1] erfüllt offensichtlich

$$A_1 \subseteq \begin{cases} \emptyset & \text{falls } \chi \neq \chi_1, \overline{\chi_1}, \\ \{\rho_1\} & \text{falls } \chi = \chi_1 \text{ und } \chi_1 \text{ reell, } \rho_1 \text{ reell}, \\ \{\rho_1, \overline{\rho_1}\} & \text{falls } \chi = \chi_1 \text{ und } \chi_1 \text{ reell, } \rho_1 \text{ komplex}, \\ \{\rho_1\} & \text{falls } \chi = \chi_1 \text{ und } \chi_1 \text{ komplex}, \\ \{\overline{\rho_1}\} & \text{falls } \chi = \overline{\chi_1} \text{ und } \chi_1 \text{ komplex}. \end{cases}$$

Mit [24, (3.38)]

$$\sup_{t\in\mathbb{R}} \Re(F(\sigma + it)) \geq 0$$

schließen wir

$$\sum_{\substack{j,k\leq N \\ j\neq k}} K(\beta^\star + i(\gamma^{(j)} - \gamma^{(k)}), \chi^{(j)}\overline{\chi^{(k)}})$$

$$\leq \mathscr{L} \cdot (2N-2) \cdot \sup_{t\in\mathbb{R}}\{-\Re\{F(\lambda_1 - \lambda^\star + it)\}\} + \mathscr{L}(N^2 - N)(\frac{f(0)}{6} + \varepsilon). \quad (13)$$

Das Lemma folgt nach der Wahl eines hinreichend kleinen $\varepsilon > 0$ (beachte, dass f und F beschränkt sind, genauso wie N gemäß wohlbekannten Nullstellendichte-Abschätzungen) aus (10), (11), (13) und dem Lösen der sich ergebenden quadratischen Ungleichung. □

Mit $B_1 = D_1 = 0$, $\lambda_{12} = \infty$, $\lambda^\star = \lambda_1$ und $C = 0$ folgt das Ausgangslemma von Heath-Brown [11, Lemma 12.1].

6. Beweis von Theorem 1

Um Linniks Theorem zu beweisen, betrachtet Heath-Brown [11, S.323]

$$\Sigma := \sum_{p\equiv a(\mod q)} \frac{\log p}{p} h(\mathscr{L}^{-1}\log p),$$

wobei

$$h(t) := h_{L,K}(t) := \begin{cases} 0 & \text{falls } t \leq L-2K, \\ t-(L-2K) & \text{falls } L-2K \leq t \leq L-K, \\ L-t & \text{falls } L-K \leq t \leq L, \\ 0 & \text{falls } t \geq L, \end{cases}$$

für gewisse positive Konstanten L, K. Wir optimieren diesen Ansatz, indem wir $h_{L,K}$ durch eine passende Linearkombination $\sum_i \alpha_i h_{L_i,K_i}$ ersetzen. Die Parameter α_i, L_i, K_i müssen sorgfältig gewählt werden, damit der Beweis geführt werden kann. Für Details zur Herleitung unserer Wahl der Parameter verweisen wir auf [24, §3.4, §6.1, §6.2].

Für $L = 5$ und $\beta_1 \geq 0$, $\beta_2 \geq 0$, $K < 1/3$ wählen wir

$$h(t) := h_{L,K}(t) + \beta_1^2 h_{L-2K,K}(t) + \beta_2^2 h_{L-4K,K}(t) + 2\beta_1 h_{L-K,K}(t) + 2\beta_2 h_{L-2K,K}(t) + 2\beta_1\beta_2 h_{L-3K,K}(t).$$

Die Laplace-Transformierte von $h(t)$ ist gegeben durch

$$H(z) = \begin{cases} e^{-(L-2K)z}\left(z^{-1}(1+\beta_1 e^{Kz} + \beta_2 e^{2Kz})(1-e^{-Kz})\right)^2 & \text{falls } z \neq 0, \\ K^2(1+\beta_1+\beta_2)^2 & \text{falls } z = 0. \end{cases}$$

Es folgt (wir lassen die nicht-trivialen Details aus) für festes $\varepsilon > 0$ und $C_0 = C_0(\varepsilon)$, $q \geq q_0 = q_0(\varepsilon)$:

$$\Sigma \geq \frac{\mathscr{L}}{\varphi(q)} \left(H(0) - \sum_{\chi \neq \chi_0} \sum_{\rho \in R_0} |H((1-\rho)\mathscr{L})| - \varepsilon \right)$$

wobei

$$R_0 := \{\sigma + it \in \mathbb{C} \mid 1 - \mathscr{L}^{-1} C_0 \leq \sigma \leq 1,\ |t| \leq \mathscr{L}^{-1} C_0\}.$$

Wir können die Summe über alle Nullstellen abschätzen, indem wir nur jene Nullstelle für jede Funktion $L(s,\chi)$ betrachten, die den kleinsten Abstand zu $s = 1$ hat:

$$H(0)^{-1} \sum_{\chi \neq \chi_0} \sum_{\rho \in R_0} |H((1-\rho)\mathscr{L})| \leq \sum_k e^{-(L-6K)\lambda^{(k)}} B(\lambda^{(k)}) - n(\chi_1) A(\chi_1) + \varepsilon, \tag{14}$$

wobei

$$B(\lambda) := H(0)^{-1} \left(F_1^\lambda(-\lambda) + \frac{f_1^\lambda(0)}{6} \right),$$

$$f_1^C(t) := \begin{cases} \frac{-1}{\lambda} \sinh(|C| - t)\lambda & \text{falls } 0 \leq t \leq |C|, \\ 0 & \text{falls } t \geq |C|, \end{cases}$$

$$F_1^C(z) := \frac{(z-\lambda)e^{|C|\lambda} - (z+\lambda)e^{-|C|\lambda} + 2\lambda e^{-|C|z}}{2\lambda(\lambda^2 - z^2)},$$

$$A(\chi_1) := \begin{cases} \max\{0, (e^{-(L-6K)\lambda_1} - e^{-(L-6K)\lambda'})(B(\lambda_1) - \frac{\alpha(\chi_1) H_2(\lambda_1)}{H(0)})\} & \text{falls } \rho_1 \in R_0, \\ 0 & \text{sonst}, \end{cases}$$

$$H_2(z) := e^{(L-2K-2K_2)z} H(z),$$

$$\alpha(\chi_1) := \begin{cases} 2 & \text{falls } \chi_1 \text{ reell und } \rho_1 \text{ komplex}, \\ 1 & \text{sonst}, \end{cases}$$

$$n(\chi_1) = \begin{cases} 2 & \text{falls } \chi_1 \text{ komplex}, \\ 1 & \text{falls } \chi_1 \text{ reell}. \end{cases}$$

Für den Beweis von Theorem 1 verbleibt zu Zeigen, dass für $L = 5$ die rechte Seite von (14) echt kleiner als 1 ist. Für $\lambda_1 < 0.348$ haben wir bereits Linniks Theorem mit $L = 4.9$ gemäß [11, Lemma 14.2]. Wir können also $\lambda_1 \geq 0.348$ annehmen.

Wir unterscheiden die Fälle χ_1 reell oder komplex, ρ_1 reell oder komplex und unterteilen den Beweis außerdem in verschiedene Fälle (vergleiche [24, §6]):

$$\lambda_1 \in [0.348, 0.44], [0.44, 0.58], \cdots, [0.78, 0.82], [0.82, \infty).$$

Wir wählen $L = 5$, $K = 0.13$, $\beta_1 = 0.65$, $\beta_2 = 0.33$ und schätzen die rechte Seite von (14) wie folgt ab:

Der Beitrag der Nullstellen ρ_1, ρ' und ρ_2 (sowie deren entsprechenden, eventuell existierenden, komplex konjugierten Nullstellen) wird abgeschätzt durch die Tabellen in [23] und [11], welche Abschätzungen der Form

$$\lambda_1 \in [\lambda_{11}, \lambda_{12}] \quad \Longrightarrow \quad \lambda' \geq \lambda'_{11}, \quad \lambda_2 \geq \lambda_{21}$$

beinhalten.

Der Beitrag der Nullstellen mit großem $\lambda (= \lambda^{(k)})$, sagen wir

$$\lambda \geq \Lambda := 1.11 + 0.35 \cdot \lambda^\star \approx 1.3$$

mit $\lambda^\star := \min\{\lambda'_{11}, \lambda_{21}\}$, wird abgeschätzt mit Hilfe von Lemma 1. Dabei wählen wir die Parameter $c_1 = 0.11$, $c_2 = 0.27$, $M = 10$, $\theta = 1.15$ und

$$w_0(t) := e^{-\frac{\theta}{2}t} \min\{t - u + 10^{-7}, v - u + 10^{-7}\}^{\frac{1}{4}}.$$

Sei $\lambda_{31} \leq \lambda_3$ gemäß Tabellen 9 und 10. Für die verbleibenden Nullstellen, also jene mit

$$\lambda_{31} \leq \lambda \leq \Lambda \tag{15}$$

benutzen wir Lemma 2, wobei f aus (2) gewählt wird mit

$$\gamma = 1.62 - 0.55\lambda^\star$$

und

$$\begin{aligned} b =& \lambda_{31} + \frac{\Lambda - \lambda_{31}}{3} - 0.01, \\ d =& \lambda_{31} + 2 \cdot \frac{\Lambda - \lambda_{31}}{3} - 0.01. \end{aligned}$$

Hier führen wir eine weitere Fallunterscheidung ein: Für zwei nicht-negative ganze Zahlen B_1, D_1 und einem $\lambda > 0$, sei

$$N_0(\lambda; B_1, D_1)$$

die resultierende obere Abschätzung aus (6). Wir benutzen die Symbole $\wedge$ für 'logisches UND', $\vee$ für 'logisches ODER', sowie

$$N_b := N_0(b; 0, 0).$$

Dann teilen wir den Ausgangsfall in die folgenden Fälle ein:

$$\begin{aligned} &\Big(N(b) \in [0,4] \quad \wedge \quad \big(N(d) \in [0,4] \ \vee \ N(d) = 5 \ \vee \ \ldots \ \vee \ N(d) = N_0(d; 0, 0)\big)\Big) \\ \vee &\Big(N(b) = 5 \quad \wedge \quad \big(N(d) = 5 \ \vee \ N(d) = 6 \ \vee \ \ldots \ \vee \ N(d) = N_0(d; 5, 0)\big)\Big) \\ &\ \vdots \\ \vee &\Big(N(b) = N_b \quad \wedge \quad \big(N(d) = N_b \ \vee \ N(d) = N_b + 1 \ \vee \ \ldots \ \vee \ N(d) = N_0(d; N_b, 0)\big)\Big). \end{aligned}$$

Wir haben also unsere Ausgangssituation in

$$(N_0(d;0,0)-3)+(N_0(d;5,0)-4)+\ldots+(N_0(d;N_b,0)-N_b+1)$$

verschiedene Fälle aufgeteilt. Jeder Fall wird durch das Tupel $(B_1,B_2,D_1,D_2)\in\mathbb{N}_0^4$ charakterisiert, wobei

$$B_1\le N(b)\le B_2 \quad \text{und} \quad D_1\le N(d)\le D_2$$

(wir haben meist $B_1=B_2$ und $D_1=D_2$). Für jedes Tupel benutzen wir die obere Abschätzung

$$N(\lambda)\le N_0(\lambda):=\begin{cases}\min\{B_2,N_0(\lambda;0,0)\} & \text{falls } \lambda\le b,\\ \min\{D_2,N_0(\lambda;B_1,0)\} & \text{falls } b<\lambda\le d,\\ N_0(\lambda;B_1,D_1) & \text{falls } d<\lambda.\end{cases}$$

Damit schätzen wir den Anteil der Nullstellen in (15) ab.

Mit Hilfe aller oben genannten Abschätzungen, und in allen betrachteten Fällen, berechnen wir, dass die rechte Seite von (14) kleiner als 1 ist. Es folgt Theorem 1. Wir haben viele Details ausgelassen, für die wir auf [24, §6] verweisen.

REFERENCES

1. Barban M.B., Vehov P.P., *On an extremal problem (Russian)*, Trans. Moscow Math. Soc. 18 (1968), 91-99; see also Trudy Moskov. Mat. Obsc. 18 (1968) 83-90.
2. J. Chen, *On the least prime in an arithmetical progression*, Sci. Sinica 14 (1965), 1868-1871.
3. J. Chen, *On the least prime in an arithmetical progression and two theorems concerning the zeros of Dirichlet's L-functions*, Sci. Sinica 20 (1977), no. 5, 529-562.
4. J. Chen, *On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichlet's L-functions II*, Sci. Sinica 22 (1979), no. 8, 859-889.
5. J. Chen, J. M. Liu, *On the least prime in an arithmetical progression (III), (IV)*, Science in China Ser. A 32 (1989) no. 6-7, 654-673 and 792-807.
6. J. Chen, J. M. Liu, *On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichlet's L-functions (V)*, International Symposium in Memory of Hua Loo Keng Vol. I (Beijing, 1988), Springer-Verlag, Berlin (1991), 1942.
7. D. D. Goldston, C. Y. Yıldırım, 'Higher correlations of divisor sums related to primes III: k-Correlations', *arXiv:math/0209102v1 [math.NT] 10 Sep 2002.*
8. S. W. Graham, *Applications of sieve methods*, Ph.D. Thesis, University of Michigan, 1977.
9. S. W. Graham, 'An asymptotic estimate related to Selberg's sieve', *J. Number Theory* 10 (1978) 83–94.
10. S. W. Graham, *On Linnik's constant*, Acta Arith. 39 (1981), no. 2, 163-179.
11. D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64 (1992), no. 2, 265-338.
12. H. Iwaniec, E. Kowalski, *Analytic Number Theory*, 2004, AMS Colloquium Publications, vol. 53.
13. M. Jutila, *A new estimate for Linnik's constant*, Ann. Acad. Sci. Fenn. Ser. A I No. 471, 1970, 8 pp.

14. M. Jutila, *On Linnik's constant*, Math. Scand. 41 (1977), no. 1, 45-62.

15. Yu. V. Linnik, *On the least prime in an arithmetic progression I. The basic theorem*, Rec. Math. (Mat. Sbornik) N.S. 15(57) (1944), 139-178.

16. Yu. V. Linnik, *On the least prime in an arithmetic progression II. The Deuring-Heilbronn phenomenon*, Rec. Math. (Mat. Sbornik) N.S. 15(57) (1944), 347-368.

17. M. C. Liu, T. Wang, *A numerical bound for small prime solutions of some ternary linear equations*, Acta Arith. 86 (1998), no. 4, 343-383.

18. C. D. Pan, *On the least prime in an arithmetical progression*, Sci. Record (N.S.) 1 (1957), 311-313.

19. C. D. Pan, *On the least prime in an arithmetical progression*, Acta Sci. Natur. Univ. Pekinensis 4 (1958), 1-34.

20. P. Turán, *On some recent results in the analytic theory of numbers*, Number Theory Institute, 1969, Proceedings of Symposia in Pure Mathematics 20 (American Mathematical Society, Providence, R.I., 1971), 359-374.

21. W. Wang, *On the least prime in an arithmetic progression*, Acta Math. Sinica 29 (1986), no. 6, 826-836.

22. W. Wang, *On the least prime in an arithmetic progression*, Acta Math. Sinica 7 (1991), no. 3, 279-289.

23. T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, *Acta Arith.* 150, 1 (2011), 65-91.

24. T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, *Bonner Mathematische Schriften* Nr. 404, Bonn, 2011, 1–110.

Получено 18.06.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-95-108

О моноиде квадратичных вычетов[1]

Добровольский Николай Николаевич — кандидат физико-математических наук, ассистент кафедры прикладной математики и информатики, Тульский государственного университет; 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
Калинина Алина Олеговна — студентка механико-математического факультета Московского государственного университета имени М. В. Ломоносова.
e-mail: kalininaalina2008@rambler.ru
Добровольский Михаил Николаевич — кандидат физико-математических наук, старший научный сотрудник Геофизического центр РАН.
e-mail: m.dobrovolsky@gcras.ru
Добровольский Николай Михайлович — профессор, доктор физико-математических наук, заведующий кафедрой алгебры, математического анализа и геометрии, Тульский государственный педагогический университет им. Л. Н. Толстого.
e-mail: dobrovol@tsput.ru

Аннотация

В работе изучается дзета-функция моноида квадратичных вычетов по простому модулю p. Моноид квадратичных вычетов задается равенством

$$M_{p,2} = \left\{ a \in \mathbb{N} \,\middle|\, \left(\frac{a}{p}\right) = 1 \right\} = \bigcup_{\nu=1}^{\frac{p-1}{2}} (r_\nu + p\mathbb{N}_0)\,,$$

где $\mathbb{N}_0 = \{0\} \bigcup \mathbb{N}$ и $r_1 < r_2 < \ldots < r_{\frac{p-1}{2}}$ — наименьшая положительная система квадратичных вычетов по модулю p, соответственно, $r_{\frac{p+1}{2}} < \ldots < r_{p-1}$ — наименьшая положительная система квадратичных невычетов по модулю p.

Множество простых элементов моноида $M_{p,2}$ состоит из множества простых чисел $\mathbb{P}_p^{(1)}$ и множества псевдопростых чисел $\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)}$:

$$P(M_{p,2}) = \mathbb{P}_p^{(1)} \bigcup \left(\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)} \right),$$

где множество простых чисел $\mathbb{P}$ разбивается на два бесконечных подмножества $\mathbb{P}_p^{(\nu)}$ $(\nu = 1, 2)$ и одноэлементное множество $\{p\}$:

$$\mathbb{P} = \mathbb{P}_p^{(1)} \bigcup \mathbb{P}_p^{(2)} \bigcup \{p\}, \quad \mathbb{P}_p^{(\nu)} = \left\{ q \in \mathbb{P} \,\middle|\, \left(\frac{q}{p}\right) = 3 - 2\nu \right\} \quad (\nu = 1, 2).$$

Моноид $M_{p,2}$ разлагается в произведение двух взаимно простых моноидов $M_{p,2} = M_{p,2}^{(1)} \cdot M_{p,2}^{(2)}$, где

$$M_{p,2}^{(\nu)} = \left\{ a \in M_{p,2} \,\middle|\, a = \prod_{j=1}^{n} q_j^{\alpha_j},\ q_j \in \mathbb{P}_p^{(\nu)} \right\}, \quad \nu = 1, 2.$$

[1]Работа подготовлена по гранту РФФИ №16-41-710194_р_центр_а

В статье изучаются свойства функции распределения простых элементов $\pi_{M_{p,2}^{(\nu)}}(x)$ для $\nu = 1, 2$. Отметим, что $\pi_{M_{p,2}}(x) = \pi_{M_{p,2}^{(1)}}(x) + \pi_{M_{p,2}^{(2)}}(x)$. Показано, что

$$\pi_{M_{p,2}^{(1)}}(x) = \frac{1}{2}\operatorname{li} x + O\left(\frac{x^{\beta_1}}{2} + \frac{p-1}{2} x e^{-c_9\sqrt{\ln x}}\right)$$

и

$$\pi_{M_{p,2}^{(2)}}(x) = \frac{x \ln\ln x}{2\ln x} + O\left(\frac{x}{(1-\beta_1)\ln x}\right),$$

где β_1 — исключительный ноль исключительного характера χ_1 по модулю p.

В заключении рассмотрены актуальные задачи с дзета-функциями моноидов натуральных чисел, требующие дальнейшего исследования.

Ключевые слова: дзета-функция Римана, ряд Дирихле, дзета-функция моноида натуральных чисел, эйлерово произведение.

Библиография: 17 названий.

Для цитирования:
Н. Н. Добровольский, А. О. Калинина, М. Н. Добровольский, Н. М. Добровольский. О моноиде квадратичных вычетов // Чебышевский сборник. 2018. Т. 19, вып. 3, С. 95–108.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-95-108

On the monoid of quadratic residues

Dobrovolsky Nikolai Nikolaevich — candidate of physical and mathematical sciences, assistant of the department of applied mathematics and computer science, Tula State University; associate Professor of the Department of algebra, mathematical analysis and geometry of Tula state pedagogical University L. N. Tolstoy.
e-mail: cheb@tspu.tula.ru, nikolai.dobrovolsky@gmail.com
Kalinina Alina Olegovna — student of mechanics and mathematics faculty of Moscow state University named after M. V. Lomonosov.
e-mail: kalininaalina2008@rambler.ru
Dobrovolsky Mikhail Nikolaevich — candidate of candidate of physical and mathematical sciences, senior researcher, Geophysical centre of RAS.
e-mail: m.dobrovolsky@gcras.ru
Dobrovolsky 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.
e-mail: dobrovol@tsput.ru

Abstract

In this paper we study the Zeta function of the monoid of quadratic residues modulo a simple p. The monoid of quadratic residues is given by

$$M_{p,2} = \left\{ a \in \mathbb{N} \,\middle|\, \left(\frac{a}{p}\right) = 1 \right\} = \bigcup_{\nu=1}^{\frac{p-1}{2}} (r_\nu + p\mathbb{N}_0),$$

where $\mathbb{N}_0 = \{0\} \bigcup \mathbb{N}$ and $r_1 < r_2 < \ldots < r_{\frac{p-1}{2}}$ — the smallest positive system of quadratic residues modulo p, respectively, $r_{\frac{p+1}{2}} < \ldots < r_{p-1}$ — the smallest positive system of quadratic residuals modulo p.

The set of simple elements of a monoid $M_{p,2}$ consists of a set of Prime numbers $\mathbb{P}_p^{(1)}$ and a set of pseudo-Prime numbers $\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)}$:

$$P(M_{p,2}) = \mathbb{P}_p^{(1)} \bigcup \left(\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)} \right),$$

where the Prime set $\mathbb{P}$ is split into two infinite subsets $\mathbb{P}_p^{(\nu)}$ $(\nu = 1, 2)$ and the singleton set $\{p\}$:

$$\mathbb{P} = \mathbb{P}_p^{(1)} \bigcup \mathbb{P}_p^{(2)} \bigcup \{p\}, \quad \mathbb{P}_p^{(\nu)} = \left\{ q \in \mathbb{P} \,\middle|\, \left(\frac{q}{p}\right) = 3 - 2\nu \right\} \quad (\nu = 1, 2).$$

The monoid $M_{p,2}$ decomposes into a product of two mutually simple monoids $M_{p,2} = M_{p,2}^{(1)} \cdot M_{p,2}^{(2)}$, where

$$M_{p,2}^{(\nu)} = \left\{ a \in M_{p,2} \,\middle|\, a = \prod_{j=1}^{n} q_j^{\alpha_j},\ q_j \in \mathbb{P}_p^{(\nu)} \right\}, \quad \nu = 1, 2.$$

The paper studies the properties of the distribution function of simple elements $\pi_{M_{p,2}^{(\nu)}}(x)$ for $\nu = 1, 2$. Note that $\pi_{M_{p,2}}(x) = \pi_{M_{p,2}^{(1)}}(x) + \pi_{M_{p,2}^{(2)}}((x)$. It is shown that

$$\pi_{M_{p,2}^{(1)}}(x) = \frac{1}{2} \operatorname{li} x + O\left(\frac{x^{\beta_1}}{2} + \frac{p-1}{2} x e^{-c_9 \sqrt{\ln x}} \right)$$

and

$$\pi_{M_{p,2}^{(2)}}(x) = \frac{x \ln\ln x}{2 \ln x} + O\left(\frac{x}{(1-\beta_1) \ln x} \right),$$

where β_1 — exceptional zero of exceptional character χ_1 modulo p.

In conclusion, the actual problems with Zeta functions of monoids of natural numbers requiring further research are considered.

Keywords: Riemann zeta function, Dirichlet series, zeta function of the monoid of natural numbers, Euler product.

Bibliography: 17 titles.

For citation:
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.

1. Введение

Пусть $p > 2$ — простое число и $\mathbb{Z}_p = \left\{ \overline{\overline{0}}, \ldots, \overline{\overline{p-1}} \right\}$ — простое поле классов вычетов[2] по модулю p. $\mathbb{Z}_p^* = \left\{ \overline{\overline{1}}, \ldots, \overline{\overline{p-1}} \right\}$ — мультипликативная группа поля $\mathbb{Z}_p$ и через $\mathbb{Z}_{p,2}^*$ будем обозначать подгруппу квадратичных вычетов по модулю p, которая, как хорошо известно, имеет индекс $\left[\mathbb{Z}_p^* : \mathbb{Z}_{p,2}^*\right] = 2$. Через $r_1 < r_2 < \ldots < r_{\frac{p-1}{2}}$ будем обозначать наименьшую положительную систему квадратичных вычетов по модулю p, соответственно, через $r_{\frac{p+1}{2}} < \ldots < r_{p-1}$ — наименьшую положительную систему квадратичных невычетов по модулю p.

В работах [6], [7] начато исследование дзета-функций мультипликативных моноидов натуральных чисел. В данной работе нас будет интересовать моноид $M_{p,2}$ всех натуральных чисел,

[2]Здесь и далее через $\overline{\overline{a}}$ обозначается класс вычетов чисел сравнимых с a по модулю p.

являющихся квадратичными вычетами по модулю p. Таким образом[3],

$$M_{p,2} = \left\{ a \in \mathbb{N} \,\middle|\, \left(\frac{a}{p}\right) = 1 \right\} = \bigcup_{\nu=1}^{\frac{p-1}{2}} (r_\nu + p\mathbb{N}_0)\,,$$

где $\mathbb{N}_0 = \{0\} \bigcup \mathbb{N}$.

При изучении моноидов натуральных чисел существенную роль играют простые элементы моноида. Если M — произвольный моноид натуральных чисел, то $P(M)$ — множество его простых элементов состоит из тех элементов моноида M отличных от единицы, которые нельзя представить в виде произведения других неединичных элементов моноида M. Таким образом, если простое число $p \in M$, то $p \in P(M)$, но, вообще говоря, не все элементы из $P(M)$ являются простыми числами. В $P(M)$ могут входить и псевдопростые числа. Элемент q из M, являющийся составным числом, будет псевдопростым числом в M, если ни один его собственный делитель не является элементом из M.

Разобьём множество простых чисел $\mathbb{P}$ на два бесконечных подмножества $\mathbb{P}_p^{(\nu)}$ $(\nu = 1, 2)$ и одноэлементное множество $\{p\}$:

$$\mathbb{P} = \mathbb{P}_p^{(1)} \bigcup \mathbb{P}_p^{(2)} \bigcup \{p\}, \quad \mathbb{P}_p^{(\nu)} = \left\{ q \in \mathbb{P} \,\middle|\, \left(\frac{q}{p}\right) = 3 - 2\nu \right\} \quad (\nu = 1, 2).$$

Нетрудно понять, что множество простых элементов моноида $M_{p,2}$ состоит из множества простых чисел $\mathbb{P}_p^{(1)}$ и множества псевдопростых чисел $\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)}$:

$$P(M_{p,2}) = \mathbb{P}_p^{(1)} \bigcup \left(\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)} \right).$$

Это разбиение соответствует разложению моноида $M_{p,2}$ в произведение двух взаимно простых моноидов $M_{p,2} = M_{p,2}^{(1)} \cdot M_{p,2}^{(2)}$, где

$$M_{p,2}^{(\nu)} = \left\{ a \in M_{p,2} \,\middle|\, a = \prod_{j=1}^{n} q_j^{\alpha_j},\ q_j \in \mathbb{P}_p^{(\nu)} \right\}, \quad \nu = 1, 2.$$

Ясно, что при $\nu = 1$ показатели степени $\alpha_1, \ldots, \alpha_n$ — произвольные натуральные числа, а при $\nu = 2$ они удовлетворяют дополнительному условию четности суммы:

$$\alpha_1 + \ldots + \alpha_n \equiv 0 \pmod 2.$$

В работе [7] дано описание общего вида моноидов натуральных чисел с однозначным разложением на простые элементы. В случае произвольного моноида M натуральных чисел общий вид $P(M)$ множества его простых элементов очень просто описать. А именно, $P(M)$ является максимальным множеством элементов из M таким, что ни один элемент из $P(M)$ не делится ни на какой другой элемент из $P(M)$. Через $\pi_M(x)$ будем обозначать количество простых элементов в моноиде M, не превосходящих x.

Если $\mathbb{P}^*$ — произвольное подмножество простых чисел, то простейшим примером моноида с однозначным разложением на простые множители является моноид $M(\mathbb{P}^*)$, образованный множеством простых $\mathbb{P}^*$:

$$M(\mathbb{P}^*) = \left\{ a \in \mathbb{N} \,\middle|\, a = \prod_{j=1}^{n} p_j^{\alpha_j},\ p_j \in \mathbb{P}^* \right\}.$$

[3]Здесь и далее, как обычно, $\left(\frac{a}{p}\right)$ — символ Лежандра числа a по модулю p.

Так как множество простых элементов $P(M)$ может содержать псевдопростые числа, то можно определить порядок простого элемента $q \in P(M)$ как величину $V(q)$ — общее число простых делителей числа q с учетом их кратности.

Таким образом, простые числа p из $P(M)$ выделяются среди всех простых элементов q, как те, у которых порядок равен 1.

Согласно предыдущему определению все простые элементы в моноиде $M_{p,2}^{(1)}$ имеют порядок 1, то есть являются обычными простыми числам, которые одновременно являются квадратичными вычетами по модулю p, таким образом, $M_{p,2}^{(1)} = M\left(\mathbb{P}_p^{(1)}\right)$. А все простые элементы из моноида $M_{p,2}^{(2)}$ имеют порядок 2 и являются псевдопростыми числами, то есть составными числами, равными произведению двух простых чисел, каждое из которых квадратичный невычет по модулю p. Таким образом, справедливо равенство $M_{p,2}^{(2)} = M\left(\mathbb{P}_p^{(2)} \cdot \mathbb{P}_p^{(2)}\right)$.

Если через A^n обозначать произведение числовых множеств $A \cdot A \cdot \ldots \cdot A$ из n сомножителей, которое состоит из всевозможных произведений $a_1 a_2 \ldots a_n$ чисел из A, то можно записать равенства:

$$M_{p,2}^{(1)} = \{1\} \bigcup \bigcup_{n=1}^{\infty} \left(\mathbb{P}_p^{(1)}\right)^n, \quad M_{p,2}^{(2)} = \{1\} \bigcup \bigcup_{n=1}^{\infty} \left(\mathbb{P}_p^{(2)}\right)^{2n}.$$

Обозначим через $\zeta(M|\alpha)$ дзета-функцию моноида M:

$$\zeta(M|\alpha) = \sum_{n \in M} \frac{1}{n^\alpha} \quad \alpha = \sigma + it, \quad \sigma > \sigma_M,$$

где σ_M — абсцисса абсолютной сходимости дзета-ряда, а через $P(M|\alpha)$ эйлерово произведение:

$$P(M|\alpha) = \prod_{q \in P(M)} \left(1 - \frac{1}{q^\alpha}\right)^{-1},$$

тогда для произвольного моноида M натуральных чисел с однозначным разложением на простые элементы справедливо равенство

$$\zeta(M|\alpha) = P(M|\alpha) \quad \alpha = \sigma + it, \quad \sigma > \sigma_M.$$

В частности,

$$\zeta\left(M_{p,2}^{(1)}\middle|\,\alpha\right) = P\left(M_{p,2}^{(1)}\middle|\,\alpha\right), \quad \sigma_{M_{p,2}^{(1)}} = 1.$$

Будем называть каноническим разложением элемента x из мультипликативного моноида M натуральных чисел представление вида

$$x = q_1^{\alpha_1} \ldots q_k^{\alpha_k}, \quad 1 < q_1 < \ldots < q_k, \quad q_1, \ldots, q_k \in P(M).$$

Через $k(x)$ будем обозначать количество различных канонических представлений числа x, тогда эйлерово произведение $P(M|\alpha)$ будет раскладываться в следующий ряд Дирихле

$$P(M|\alpha) = \sum_{x \in M} \frac{k(x)}{x^\alpha}.$$

Таким образом, равенство эйлерова произведения и дзета-функции моноида M равносильно однозначности разложения на простые элементы в этом моноиде.

Так как в моноиде $M_{p,2}^{(2)}$ нет однозначности разложения на простые элементы, то

$$\zeta\left(M_{p,2}^{(2)}\middle|\,\alpha\right) \neq P\left(M_{p,2}^{(2)}\middle|\,\alpha\right).$$

Из равенства для моноидов $M_{p,2} = M_{p,2}^{(1)} \cdot M_{p,2}^{(2)}$ в силу их взаимной простоты следует равенство для дзета-функций:

$$\zeta(M_{p,2}|\alpha) = \zeta\left(M_{p,2}^{(1)}\middle|\,\alpha\right) \cdot \zeta\left(M_{p,2}^{(2)}\middle|\,\alpha\right).$$

В моноиде $M_{p,2}^{(2)}$ есть подмоноид $M_{p,2}^{(2,2)}$ с однозначным разложение на простые элементы — это моноид, образованный из квадратов простых чисел, квадратичных невычетов по модулю p:

$$M_{p,2}^{(2,2)} = \left\{a \in \mathbb{N}\,\middle|\, a = p_1^{2\alpha_1}\dots p_n^{2\alpha_n}, \quad p_1,\dots,p_n \in \mathbb{P}_p^{(2)}\right\}.$$

Если через $R_{p,2}^{(2)}$ обозначить множество радикалов четного порядка[4], образованное из простых чисел, квадратичных невычетов по модулю p:

$$R_{p,2}^{(2)} = \left\{a \in \mathbb{N}\,\middle|\, a = p_1\dots p_{2n}, \quad p_1 < \dots < p_{2n} \in \mathbb{P}_p^{(2)}\right\},$$

то будут справедливы равенства:

$$M_{p,2}^{(2)} = M_{p,2}^{(2,2)} \cdot R_{p,2}^{(2)}, \quad \zeta\left(M_{p,2}^{(2)}\middle|\,\alpha\right) = \zeta\left(M_{p,2}^{(2,2)}\middle|\,\alpha\right) \cdot \zeta\left(R_{p,2}^{(2)}\middle|\,\alpha\right), \quad \zeta\left(M_{p,2}^{(2,2)}\middle|\,\alpha\right) = P\left(M_{p,2}^{(2,2)}\middle|\,\alpha\right).$$

Заметим, что справедливо интересное равенство эйлеровых произведений:

$$P\left(M_{p,2}^{(2,2)}\middle|\,\alpha\right) = P\left(M\left(\mathbb{P}_p^{(2)}\right)\middle|\,2\alpha\right),$$

из которого следует, что $\zeta\left(M_{p,2}^{(2,2)}\middle|\,\alpha\right)$ не имеет нулей при $\sigma \geqslant \frac{1}{2}$.

Цель данной статьи — изучить свойства функции распределения простых элементов $\pi_{M_{p,2}^{(\nu)}}(x)$ для $\nu = 1, 2$. Отметим, что $\pi_{M_{p,2}}(x) = \pi_{M_{p,2}^{(1)}}(x) + \pi_{M_{p,2}^{(2)}}(x)$.

2. Общие формулы для числа простых и псевдопростых

Пусть, как обычно, $\pi(x, a, p)$ — количество простых чисел q, не превосходящих x, для которых $q \equiv a \pmod p$, тогда с помощью этих обозначений можно легко написать выражение для $\pi_{M_{p,2}^{(1)}}(x)$ и $\pi_{M_{p,2}^{(2)}}(x)$.

Лемма 1. *Справедливо равенство*

$$\pi_{M_{p,2}^{(1)}}(x) = \sum_{j=1}^{\frac{p-1}{2}} \pi(x, r_j, p).$$

[4]Термин радикал мы используем как современный синоним понятия бесквадратное число. Таким образом, число n — радикал, если оно равно своему радикалу, то есть все простые делители числа n входят в него в первой степени.

Доказательство. Действительно, если

$$q \leqslant x, \quad q \equiv r_j \pmod p, \quad j = 1, \ldots, \frac{p-1}{2},$$

то $q \in \mathbb{P}_p^{(1)}$.

Если $q \leqslant x$ и $q \in \mathbb{P}_p^{(1)}$, то найдется единственный квадратичный вычет r_j по модулю p такой, что

$$q \equiv r_j \pmod p.$$

Отсюда следует утверждение леммы.

□

Лемма 2. *Справедливо равенство*

$$\pi_{M_{p,2}^{(2)}}(x) = \sum_{j=\frac{p+1}{2}}^{p-1} \sum_{\substack{q_1 \leqslant \sqrt{x}, \\ q_1 \equiv r_j \pmod p}} \sum_{i=\frac{p+1}{2}}^{p-1} \left(\pi\left(\frac{x}{q_1}, r_i, p\right) - \pi\left(q_1 - 1, r_i, p\right) \right).$$

Доказательство. Действительно, псевдопростое число $q \in P(M_{p,2}^{(2)})$, и непревосходящее x, имеет вид $q = q_1 q_2$, $1 < q_1 \leqslant \sqrt{x}$, $q_1 \leqslant q_2 \leqslant \frac{x}{q_1}$, $q_1 \equiv r_j \pmod p$, $q_2 \equiv r_i \pmod p$, где $\frac{p+1}{2} \leqslant i, j \leqslant p-1$.

Так как количество q_2, удовлетворяющих условиям $q_2 \equiv r_i \pmod p$ и $q_1 \leqslant q_2 \leqslant \frac{x}{q_1}$, равно $\pi\left(\frac{x}{q_1}, r_i, p\right) - \pi(q_1 - 1, r_i, p)$, то лемма доказана. □

3. Вспомогательные утверждения

Прежде всего, сформулируем неравенство Чебышёва. 24 мая 1848 г. П. Л. Чебышёв представил в Санкт-Петербургскую Академию наук мемуар "Об определении числа простых чисел, не превосходящих данной величины" (Полн. собр. соч., т. I, с. 173–190). Таким образом, в этом году исполнилось 170 лет со дня выхода этой принципиальной работы, с которой началась современная теория распределения простых чисел.

Во втором мемуаре он доказал оценки

$$(0,92\ldots)\frac{x}{\ln x} \leqslant \pi(x) \leqslant (1,105\ldots)\frac{x}{\ln x}. \tag{1}$$

Обозначим через $c_1 = 0,92\ldots$ и $c_2 = 1,105\ldots$ константы из неравенств Чебышёва для функции $\pi(x)$.

Заметим, что конечная разность $\Delta\pi(n) = \pi(n) - \pi(n-1)$ является на множестве натуральных чисел характеристической функцией множества простых чисел. Аналогично, конечная разность $\Delta\pi(n, l, p) = \pi(n, l, p) - \pi(n-1, l, p)$ является на множестве натуральных чисел характеристической функцией множества простых чисел q вида $q = l + kp$.

Ещё нам потребуются следующие асимптотические равенства, которые уже стали классическими и получены с помощью дзета-функции Римана и L-функций Дирихле. Пусть β_1 — исключительный ноль исключительного характера χ_1 по модулю k, тогда $\frac{3}{4} \leqslant \beta_1 < 1$ (см. [11], стр. 150–151, 157).

Теорема 1. *Равенство*

$$\pi(x, l, k) = \frac{1}{\varphi(k)} \operatorname{li} x + O\left(\frac{x^{\beta_1}}{\varphi(k)} + x e^{-c_9\sqrt{\ln x}}\right) \tag{2}$$

выполняется равномерно при $k \leqslant \exp(c_{10}\sqrt{\ln x})$.

Доказательство. См. [11], стр. 157. □

Теорема 2. *При постоянном k*

$$\pi(x,l,k)=\frac{1}{\varphi(k)}\operatorname{li}x+O\left(xe^{-c_9\sqrt{\ln x}}\right), \tag{3}$$

в частности,

$$\pi(x,l,k)\sim\frac{x}{\varphi(k)\ln x},\quad x\to\infty. \tag{4}$$

Доказательство. См. [11], стр. 157. □

Теорема 3. *При постоянном k*

$$\pi(x,l,k)=\frac{x}{\varphi(k)\ln x}\left(1+O\left(\frac{1}{\ln x}\right)\right),\quad x\to\infty. \tag{5}$$

Доказательство. См. [11], стр. 158. □

Теорема 4. *При $x\to\infty$ имеют место соотношения*

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+a+O\left(\frac{1}{\ln x}\right), \tag{6}$$

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)^{-1}=B\ln x+O(1). \tag{7}$$

Здесь a и B — некоторые константы, причём $B>0$.

Доказательство. См. [11], стр. 28–30. На стр. 92 дается вариант теоремы с более точным остаточным членом чем в формуле (6):

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+\gamma-\sum_{p}\sum_{m\geqslant 2}\frac{1}{mp^m}+O\left(e^{-c\sqrt{\ln x}}\right).$$

На стр. 94 дается более точное выражение формулы (7) в виде

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{e^{-\gamma}}{\ln x}\left(1+O\left(e^{-c\sqrt{\ln x}}\right)\right).$$

Здесь γ — константа Эйлера,

$$\gamma=\lim_{n\to\infty}\left(\sum_{m=1}^{n}\frac{1}{m}-\ln n\right)=\int\limits_0^1\frac{1-e^{-u}}{u}du-\int\limits_1^\infty\frac{e^{-u}}{u}du.$$

□

Из теорем 3 и 4 докажем следующий результат.

Теорема 5. *При постоянном k и $\frac{3}{4}\leqslant\beta_1<1$ справедливы соотношения:*

$$\sum_{\substack{q\leqslant x,\\ q\equiv l\pmod k}}\frac{1}{q}=\frac{1}{\varphi(k)}\left(\ln\ln x+a_1+O\left(\frac{1}{\ln x}\right)\right),\quad x\to\infty, \tag{8}$$

$$\sum_{l=1,\,(l,k)=1}^{k-1}\ \sum_{\substack{q\leqslant x,\\ q\equiv l\pmod k}}\frac{1}{q^{\beta_1}}=O\left(\frac{x^{1-\beta_1}}{(1-\beta_1)\ln x}\right), \tag{9}$$

где a_1 — некоторая константа.

Доказательство. Действительно, пользуясь теоремой 3, получим:

$$\sum_{\substack{q\leqslant x,\\ q\equiv l \pmod k}} \frac{1}{q} = \sum_{n\leqslant x} \frac{\Delta\pi(n,l,k)}{n} = \frac{\pi([x],l,k)}{[x]} + \sum_{n=2}^{[x]-1} \pi(n,l,k)\left(\frac{1}{n} - \frac{1}{n+1}\right) =$$

$$= \frac{1}{\varphi(k)\ln[x]}\left(1+O\left(\frac{1}{\ln x}\right)\right) + \sum_{n=2}^{[x]-1} \frac{1}{\varphi(k)(n+1)\ln n}\left(1+O\left(\frac{1}{\ln n}\right)\right) =$$

$$= \frac{1}{\varphi(k)}\left(\ln\ln x + a_1 + O\left(\frac{1}{\ln x}\right)\right)$$

и соотношение (8) доказано.

Аналогично, получим

$$\sum_{\substack{q\leqslant x,\\ q\equiv l \pmod k}} \frac{1}{q^{\beta_1}} = \sum_{n\leqslant x} \frac{\Delta\pi(n,l,k)}{n^{\beta_1}} = \frac{\pi([x],l,k)}{[x]^{\beta_1}} + \sum_{n=2}^{[x]-1} \pi(n,l,k)\left(\frac{1}{n^{\beta_1}} - \frac{1}{(n+1)^{\beta_1}}\right) \leqslant$$

$$\leqslant \frac{[x]^{1-\beta_1}}{\varphi(k)\ln[x]}\left(1+O\left(\frac{1}{\ln x}\right)\right) + \sum_{n=2}^{[x]-1} \frac{\beta_1}{\varphi(k)n^{\beta_1}\ln n}\left(1+O\left(\frac{1}{\ln n}\right)\right) = \frac{1}{\varphi(k)} O\left(\frac{x^{1-\beta_1}}{(1-\beta_1)\ln x}\right)$$

и теорема полностью доказана. □

4. Количество простых

Сначала выведем асимптотическую формулу для числа простых в моноиде $M_{p,2}^{(1)}$.

Теорема 6. *Для количества простых чисел в моноиде $M_{p,2}^{(1)}$ при $p < \exp(c_{10}\sqrt{\ln x})$ справедливо асимптотическое равенство*

$$\pi_{M_{p,2}^{(1)}}(x) = \frac{1}{2}\operatorname{li} x + O\left(\frac{x^{\beta_1}}{2} + \frac{p-1}{2} x e^{-c_9\sqrt{\ln x}}\right).$$

Доказательство. Так как $p < \exp(c_{10}\sqrt{\ln x})$, то $r_j < \exp(c_{10}\sqrt{\ln x})$ для $1 \leqslant j \leqslant p-1$. Поэтому по теореме 1 имеем:

$$\pi(x, r_j, p) = \frac{1}{p-1}\operatorname{li} x + O\left(\frac{x^{\beta_1}}{p-1} + x e^{-c_9\sqrt{\ln x}}\right).$$

Применяя лемму 1, получим:

$$\pi_{M_{p,2}^{(1)}}(x) = \sum_{j=\frac{p+1}{2}}^{p-1}\left(\frac{1}{p-1}\operatorname{li} x + O\left(\frac{x^{\beta_1}}{p-1} + x e^{-c_9\sqrt{\ln x}}\right)\right) = \frac{1}{2}\operatorname{li} x + O\left(\frac{x^{\beta_1}}{2} + \frac{p-1}{2} x e^{-c_9\sqrt{\ln x}}\right)$$

и теорема доказана. □

5. Количество псевдопростых

Перейдём к выводу асимптотической формулы для числа псевдопростых чисел в моноиде $M_{p,2}^{(2)}$. Для этого перепишем утверждение леммы 2 в виде

$$\pi_{M_{p,2}^{(2)}}(x) = S_1(x,p) - S_2(x,p),$$

где

$$S_1(x,p)=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\sum_{i=\frac{p+1}{2}}^{p-1}\pi\left(\frac{x}{q_1},r_i,p\right),$$

$$S_2(x,p)=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\sum_{i=\frac{p+1}{2}}^{p-1}\pi\left(q_1-1,r_i,p\right).$$

Сумму $S_2(x,p)$ оценим грубо с помощью неравенства Чебышёва.

Лемма 3. *Справедлива оценка*

$$S_2(x,p)\leqslant 4c_2^2\frac{x}{\ln^2 x}.$$

Доказательство. Действительно, при $q_1\leqslant\sqrt{x}$ имеем:

$$\sum_{i=\frac{p+1}{2}}^{p-1}\pi\left(q_1-1,r_i,p\right)\leqslant\pi\left(\sqrt{x}\right),$$

поэтому

$$S_2(x,p)\leqslant\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\pi\left(\sqrt{x}\right)\leqslant\pi^2\left(\sqrt{x}\right)\leqslant\left(c_2\frac{\sqrt{x}}{\ln\sqrt{x}}\right)^2=4c_2^2\frac{x}{\ln^2 x}.$$

□

Введём обозначения

$$S_3(x,p)=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\sum_{i=\frac{p+1}{2}}^{p-1}\frac{1}{p-1}\operatorname{li}\left(\frac{x}{q_1}\right)=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\frac{1}{2}\operatorname{li}\left(\frac{x}{q_1}\right),$$

$$S_4(x,p)=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\sum_{i=\frac{p+1}{2}}^{p-1}O\left(\frac{\left(\frac{x}{q_1}\right)^{\beta_1}}{p-1}+\left(\frac{x}{q_1}\right)e^{-c_9\sqrt{\ln\left(\frac{x}{q_1}\right)}}\right)=$$

$$=\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}O\left(\frac{\left(\frac{x}{q_1}\right)^{\beta_1}}{2}+\frac{p-1}{2}\left(\frac{x}{q_1}\right)e^{-c_9\sqrt{\ln\left(\frac{x}{q_1}\right)}}\right).$$

Ясно, что в силу теоремы 1

$$S_1(x,p)=S_3(x,p)+S_4(x,p).$$

Лемма 4. *Справедлива оценка*

$$S_4(x,p)=O\left(\frac{x}{(1-\beta_1)\ln x}+\frac{p-1}{4}xe^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}}\ln\ln\sqrt{x}\right).$$

Доказательство. Действительно,

$$e^{-c_9\sqrt{\ln\left(\frac{x}{q_1}\right)}} \leqslant e^{-c_9\sqrt{\ln(\sqrt{x})}} = e^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}}.$$

Поэтому

$$S_4(x,p) = O\left(\frac{x^{\beta_1}}{2}\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\frac{1}{q_1^{\beta_1}} + \frac{p-1}{2}xe^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}}\sum_{j=\frac{p+1}{2}}^{p-1}\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\frac{1}{q_1}\right).$$

Воспользуемся теоремой 5, получим

$$S_4(x,p) = O\left(\frac{x^{\beta_1}}{2}\frac{x^{1-\beta_1}}{(1-\beta_1)\ln x} + \frac{p-1}{2}xe^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}}\frac{1}{2}\left(\ln\ln\sqrt{x} + a_1 + O\left(\frac{1}{\ln\sqrt{x}}\right)\right)\right) =$$
$$= O\left(\frac{x}{(1-\beta_1)\ln x} + \frac{p-1}{4}xe^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}}\ln\ln\sqrt{x}\right).$$

□

Лемма 5. *Справедлива оценка*

$$S_3(x,p) = \frac{x\ln\ln x}{2\ln x} + O\left(\frac{x}{2\ln x}\right).$$

Доказательство. Действительно, имеем:

$$\sum_{\substack{q_1\leqslant\sqrt{x},\\ q_1\equiv r_j \pmod p}}\frac{1}{2}\operatorname{li}\left(\frac{x}{q_1}\right) = \pi(\sqrt{x},r_j,p)\frac{1}{2}\operatorname{li}\left(\sqrt{x}\right) + \int_2^{\sqrt{x}}\frac{\pi(t,r_j,p)x}{t^2\ln\left(\frac{x}{t}\right)}dt =$$

$$= O\left(\frac{x}{2(p-1)\ln^2 x}\right) + \int_2^{\sqrt{x}}\frac{tx}{(p-1)(\ln t)t^2\ln\left(\frac{x}{t}\right)}\left(1+O\left(\frac{1}{\ln t}\right)\right)dt =$$

$$= O\left(\frac{x}{2(p-1)\ln^2 x}\right) + O\left(\int_2^{\sqrt{x}}\frac{x}{(p-1)(\ln^2 t)t\ln\left(\frac{x}{t}\right)}dt\right) + \int_2^{\sqrt{x}}\frac{x}{(p-1)(\ln t)t\ln\left(\frac{x}{t}\right)}dt =$$

$$= O\left(\frac{x}{2(p-1)\ln^2 x}\right) + O\left(\frac{x}{(p-1)\ln x}\right) + \frac{x}{p-1}\int_{\ln 2}^{\ln\sqrt{x}}\frac{du}{u(\ln x-u)} =$$
$$= \frac{x\ln\ln x}{(p-1)\ln x} + O\left(\frac{x}{(p-1)\ln x}\right).$$

Отсюда следует, что

$$S_3(x,p) = \sum_{j=\frac{p+1}{2}}^{p-1}\left(\frac{x\ln\ln x}{(p-1)\ln x} + O\left(\frac{x}{(p-1)\ln x}\right)\right) =$$
$$= \frac{x\ln\ln x}{2\ln x} + O\left(\frac{x}{2\ln x}\right).$$

□

Теорема 7. *Справедливо асимптотическое равенство*

$$\pi_{M_{p,2}^{(2)}}(x) = \frac{x \ln\ln x}{2\ln x} + O\left(\frac{x}{(1-\beta_1)\ln x}\right).$$

Доказательство. Действительно, по леммам 3–5 имеем:

$$\pi_{M_{p,2}^{(2)}}(x) = S_1(x,p) - S_2(x,p) = S_1(x,p) + O\left(\frac{x}{\ln^2 x}\right) = S_3(x,p) +$$
$$+O\left(\frac{x}{(1-\beta_1)\ln x} + \frac{p-1}{4} x e^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}} \ln\ln\sqrt{x}\right) + O\left(\frac{x}{\ln^2 x}\right) =$$
$$= \frac{x\ln\ln x}{2\ln x} + O\left(\frac{x}{2\ln x}\right) + O\left(\frac{x}{(1-\beta_1)\ln x} + \frac{p-1}{4} x e^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}} \ln\ln\sqrt{x}\right) + O\left(\frac{x}{\ln^2 x}\right) =$$
$$= \frac{x\ln\ln x}{2\ln x} + O\left(\frac{x}{(1-\beta_1)\ln x} + \frac{p-1}{4} x e^{-\frac{c_9}{\sqrt{2}}\sqrt{\ln x}} \ln\ln\sqrt{x}\right) = \frac{x\ln\ln x}{2\ln x} + O\left(\frac{x}{(1-\beta_1)\ln x}\right).$$

□

6. Заключение

1. В работе рассмотрен моноид $M_{p,2}$ натуральных чисел, образованный подгруппой всех квадратичных вычетов по заданному простому модулю p. Для такого моноида множество простых элементов очень просто описывается: либо это простое число, которое является квадратичным вычетом по модулю p, либо это псевдопростое число, которое является произведением двух простых квадратичных невычетов. Поэтому для этого моноида оказалось возможным найти асимптотический закон распределения простых элементов.

2. Пусть $1 < g_1 < \ldots < g_{\varphi(p-1)} < p$ — наименьшая положительная система первообразных корней по модулю p. Можно рассмотреть $\varphi(p-1)$ моноидов $M(\mathbb{P}_{p,g})$ с однозначным разложением на простые множители:

$$\mathbb{P}_{p,g} = \{\, q \in \mathbb{P} \,|\, q \equiv g \pmod p \,\},$$

где g — произвольный первообразный корень по модулю p.

Рассмотрим моноид $M_1(\mathbb{P}_{p,g}) = M(\mathbb{P}_{p,g}) \bigcap \overline{\overline{1}}$, который уже не обладает однозначным разложением на простые элементы. Нетрудно понять, что множество его простых элементов $P(M_1(\mathbb{P}_{p,g}))$ задается равенством

$$P(M_1(\mathbb{P}_{p,g})) = (\mathbb{P}_{p,g})^{p-1},$$

то есть состоит из псевдопростых чисел порядка $p-1$. Таким образом, интересная задача нахождения асимптотического закона распределения простых элементов для этого моноида существенно усложняется. Мы надеимся в одной из следующих работ решить эту задачу.

3. Рассмотрим бесконечные множества $A_k(\mathbb{P}_{p,g})$ при $k = 1, \ldots, p-1$, заданные равенствами

$$A_k(\mathbb{P}_{p,g}) = \left\{ a \in M(\mathbb{P}_{p,g}) \,|\, a \equiv g^k \pmod p \right\}.$$

Ясно, что $A_{p-1}(\mathbb{P}_{p,g}) = M_1(\mathbb{P}_{p,g})$.

На наш взгляд очень интересным является вопрос об аналогах теоремы Дэвенпорта–Хейльбронна для каждого из множеств $A_k(\mathbb{P}_{p,g})$ $1 \leqslant k \leqslant p-1$.

В заключении авторы выражают свою благодарность за полезные обсуждения и внимание к работе профессору В. Н. Чубарикову.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Э. Бомбьери, А. Гош Вокруг функции Дэвенпорта–Хейльбронна // УМН, 2011. Т. 66, вып. 2(398). С. 15–66.

2. С. М. Воронин Избранные труды: Математика / Под ред. А. А. Карацубы. — М.: Изд-во МГТУ им. Н. Э. Баумана. 2006. — 480 с.

3. С. М. Воронин, А. А. Карацуба Дзета-функция Римана. — М.: Физ-матлит, 1994. — 376 с.

4. Добровольский М. Н. Функциональное уравнение для гиперболической дзета-функции целочисленных решёток // Доклады академии наук 2007. Т. 412, № 3. С. 302–304.

5. Н. М. Добровольский, Н. Н. Добровольский, В. Н. Соболева, Д. К. Соболев, Л. П. Добровольская, О. Е. Бочарова О гиперболической дзета-функции Гурвица // Чебышевский сб. 2016. Т. 17, вып. 3. С. 72–105.

6. Н. Н. Добровольский Дзета-функция моноидов натуральных чисел с однозначным разложением на простые множители // Чебышевский сб. 2017. Т. 18, вып. 4. С. 187–207.

7. Н. Н. Добровольский О моноидах натуральных чисел с однозначным разложением на простые элементы // Чебышевский сб. 2018. Т. 19, вып. 1. С. 79–105.

8. Н. Н. Добровольский Дзета-функция моноидов с заданной абсциссой абсолютной сходимости // Чебышевский сб. 2018. Т. 19, вып. 2. С. 142–150.

9. Н. Н. Добровольский, М. Н. Добровольский, Н. М. Добровольский, И. Н. Балаба, И. Ю. Реброва Гипотеза о "заградительном ряде" для дзета-функций моноидов с экспоненциальной последовательностью простых // Чебышевский сб. 2018. Т. 19, вып. 1. С. 106–123.

10. Н. Н. Добровольский, А. О. Калинина, М. Н. Добровольский, Н. М. Добровольский. О количестве простых элементов в некоторых моноидах натуральных чисел // Чебышевский сборник. 2018. Т. 19, вып. 2, С. ???–???.

11. К. Прахар Распределение простых чисел. — М.: МИР. 1967, 511 с.

12. И. Ю. Реброва, А. В. Кирилина Н. М. Коробов и теория гиперболической дзета-функции решёток // Чебышевский сб. 2018. Т. 19, вып. 2. С. ???–???.

13. К. Хооли Применение методов решета в теории чисел. — М.: Наука, 1987, 20 с.

14. Чебышёв П. Л. Полное собрание сочинений, т. I–V. — М.-Л.: Изд-во АН СССР, 1944–1951.

15. Чебышёв П. Л. Избранные труды. — М.: Изд-во АН СССР, 1955, 926 с.

16. H. Davenport, H. Heilbronn On the zeros of certain Dirichlet series // J. London Math. Soc. 1936. Vol. 11. P. 181–185.

17. L. P. Dobrovolskaya, M. N. Dobrovolsky, N. M. Dobrovol'skii, N. N. Dobrovolsky. On Hyperbolic Zeta Function of Lattices. In: Continuous and Distributed Systems. Solid Mechanics and Its Applications. Vol. 211. 2014. P. 23–62. DOI:10.1007/978-3-319-03146-0_2.

REFERENCES

1. Bombieria E., Ghoshb A., 2011, “Around the Davenport–Heilbronn function”, *Uspekhi Mat. Nauk*, 66:2(398) pp. 15–66.
2. Voronin S. M., 2006, *Izbrannye trudy: Matematika. Pod red. A. A. Karacuby*, Izd-vo MGTU im. N. Je. Baumana, Moskva, 480 p.
3. Voronin S. M., Karacuba A. A., 1994, *Dzeta-funkcija Rimana*, Izd-vo Fiz-matlit, Moskva, 376 p.
4. Dobrovol'skij M. N., 2007, "Funkcional'noe uravnenie dlja giperbolicheskoj dzeta-funkcii celochislennyh reshetok" , *Doklady akademii nauk*, vol 412, № 3, pp. 302–304.
5. Dobrovolsky N. M., Dobrovolsky N. N., Soboleva V. N., Sobolev D. K., Dobrovol'skaya L. P., Bocharova O. E., 2016, "On hyperbolic Hurwitz zeta function" , *Chebyshevskii Sbornik*, vol 17, № 3 pp. 72–105.
6. Dobrovolsky N. N., 2017, *The zeta-function is the monoid of natural numbers with unique factorization Chebyshevskii Sbornik*, vol. 18, № 4. P. 187–207.
7. Dobrovolsky N. N., 2018, "On monoids of natural numbers with unique factorization into prime elements" , *Chebyshevskii Sbornik*, vol. 19, № 1. P. 79–105.
8. N. N. Dobrovol'skii, 2018, "The zeta function of monoids with a given abscissa of absolute convergence" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 142–150.
9. 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. 3, pp. 106–123.
10. 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. ???–???.
11. Prahar K., 1967, *Raspredelenie prostyh chisel, per. s nem*, Izd-vo Mir, Moskva, 511 p.
12. I. Yu. Rebrova, A. V. Kirilina 2018, "N. M. Korobov and the theory of the hyperbolic zeta function of lattices" , *//Chebyshevskii sbornik*, vol. 19, no. 2. P. ???–???.
13. C. Hooley 1987, "Applications of seive methods to the theory of numbers " ,*M.: Nauka*, 20 p.
14. Chebyshev P. L. 1944–1951 "Complete works, v. I–V. " , *M.-L.: Izd-vo AN SSSR.*
15. Chebyshev P. L. 1955, "Selected works." , *M.: Izd-vo AN SSSR*, 926 p.
16. Davenport H., Heilbronn H., 1936, "On the zeros of certain Dirichlet series" , *J. London Math. Soc.* Vol. 11. pp. 181–185.
17. Dobrovolskaya L. P., Dobrovolsky M. N., Dobrovol'skii N. M., Dobrovolsky 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.

Получено 30.06.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-109-134

О двух асимптотических формулах в теории гиперболической дзета-функции решёток[1]

Добровольский Николай Николаевич — кандидат физико-математических наук, ассистент кафедры прикладной математики и информатики, Тульский государственный университет; 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

Аннотация

В работе рассматриваются новые варианты двух асимптотических формул из теории гиперболической дзета-функции решёток.

Во-первых, получена новая асимптотическая формула для гиперболической дзета-функции алгебраической решётки, полученной растяжением в t раз по каждой координате решётки состоящей из полных наборов алгебраически сопряженных целых алгебраических чисел, пробегающих кольцо целых алгебраических чисел чисто вещественного алгебраического поля степени s для любого натурального $s \geqslant 2$.

Во-вторых, получена новая асимптотическая формула для числа точек произвольной решётки в гиперболическом кресте.

В первом случае показано, что главный член асимптотической формулы для гиперболической дзета-функции алгебраической решётки выражается через детерминант решётки, регулятор поля и значения дзета-функции Дедекинда главных идеалов и её производные до порядка $s-1$. Впервые выписана явная формула остаточного члена и дана его оценка.

Во втором случае главный член асимптотической формулы выражается через объём гиперболического креста и детерминант решётки. Даётся явный вид остаточного члена и уточненная его оценка.

В заключении описана суть метода параметризованных множеств, использованного при выводе асимптотических формул.

Ключевые слова: алгебраическая решётка, гиперболическая дзета-функция алгебраической решётки, дзета-функция Дедекинда главных идеалов, гиперболический крест, точки решётки в гиперболическом кресте.

Библиография: 47 названий.

Для цитирования:
Н. Н. Добровольский. О двух асимптотических формулах в теории гиперболической дзета-функции решёток // Чебышевский сборник. 2018. Т. 19, вып. 3, С. 109–134.

[1]Работа подготовлена по гранту РФФИ №16-41-710194_р_центр_а

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-109-134

On two asymptotic formulas in the theory of hyperbolic Zeta function of lattices[2]

Dobrovolsky Nikolai Nikolaevich — candidate of physical and mathematical sciences, assistant of the department of applied mathematics and computer science, Tula State University; associate Professor of the Department of algebra, mathematical analysis and geometry of Tula state pedagogical University L. N. Tolstoy.
e-mail: cheb@tspu.tula.ru, nikolai.dobrovolsky@gmail.com

Abstract

The paper considers new variants of two asymptotic formulas from the theory of hyperbolic Zeta function of lattices.

First, we obtain a new asymptotic formula for the hyperbolic Zeta function of an algebraic lattice obtained by stretching t times over each coordinate of a lattice consisting of complete sets of algebraically conjugate algebraic integers running through a ring of algebraic integers of a purely real algebraic field of degree s for any natural $s \geqslant 2$.

Second, we obtain a new asymptotic formula for the number of points of an arbitrary lattice in a hyperbolic cross.

In the first case, it is shown that the main term of the asymptotic formula for the hyperbolic Zeta function of an algebraic lattice is expressed in terms of the lattice determinant, the field controller, and the values of the Dedekind Zeta function of the principal ideals and its derivatives up to the order of $s - 1$. For the first time an explicit formula of the residual term is written out and its estimation is given.

In the second case, the principal term of the asymptotic formula is expressed in terms of the volume of the hyperbolic cross and the lattice determinant. An explicit form of the residual term and its refined estimate are given.

In conclusion, the essence of the method of parametrized sets used in the derivation of asymptotic formulas is described.

Keywords: algebraic lattice, hyperbolic Zeta function of algebraic lattice, Dedekind Zeta function of principal ideals, hyperbolic cross, lattice points in hyperbolic cross.

Bibliography: 47 titles.

For citation:
N. N. Dobrovol'skii, 2018, "On two asymptotic formulas in the theory of hyperbolic Zeta function of lattices", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 109–134.

[2]The work has been prepared by the RFBR grant №16-41-710194_r_centr_a

1. Введение

В данной работе продолжаются исследования по теории гиперболической дзета-функции решёток.

Гиперболическая дзета-функция решёток задаётся в правой α-полуплоскости $\sigma > 1$, $\alpha = \sigma + it$ дзета рядом[3]

$$\zeta(\Lambda|\alpha) = \sum_{\vec{x}\in\Lambda}{}' (\overline{x_1}\dots\overline{x_s})^{-\alpha}. \tag{1}$$

Очевидно, что при $s = 1$ гиперболическая дзета-функции решётки выражается через дзета-функцию Римана. В многомерном случае имеются свои существенно новые задачи, не имеющие аналогов в одномерном случае.

Впервые гиперболическая дзета-функция решёток возникла в работах Н. М. Коробова [28], [29] и Н. С. Бахвалова [1] в 1959 году для решёток решений линейного сравнения с несколькими переменными. В наиболее общем виде она появилась в работах К. К. Фролова [35], [36].

Термин *"гиперболическая дзета-функция решётки"* был введен в 1984 году Н. М. Добровольским в работах [11] — [13], в которых начато систематическое изучение функции $\zeta_H(\Lambda|\alpha)$ как самостоятельного объекта исследований.

В частности, для действительных $\alpha > 1$ получены нижние оценки для гиперболической дзета-функции произвольной s-мерной решётки:

$$\begin{array}{rcll} \zeta_H(\Lambda|\alpha) & \geqslant & C_1(\alpha,s)(\det\Lambda)^{-1} & \text{при} \quad 0 < \det\Lambda \leqslant 1, \\ \zeta_H(\Lambda|\alpha) & \geqslant & C_2(\alpha,s)(\det\Lambda)^{-\alpha}\ln^{s-1}\det\Lambda & \text{при} \quad \det\Lambda > 1, \end{array} \tag{2}$$

где $C_1(\alpha,s)$, $C_2(\alpha,s) > 0$ — константы, зависящие только от α и s.

Доказана верхняя оценка для гиперболической дзета-функции s-мерной решётки:

$$\begin{array}{rcll} \zeta_H(\Lambda|\alpha) & \leqslant & C_3(\alpha,s)C_1(\Lambda)^s & \text{при} \quad q(\Lambda) = 1, \\ \zeta_H(\Lambda|\alpha) & \leqslant & C_4(\alpha,s)q^{-\alpha}(\Lambda)(\ln q(\Lambda)+1)^{s-1} & \text{при} \quad q(\Lambda) > 1. \end{array} \tag{3}$$

Этот результат является обобщением теоремы Н. С. Бахвалова [1]. Из оценки (3) получены различные следствия. В частности, из нее автоматически следует результат К. К. Фролова [35], так как гиперболический параметр $q(\Lambda(t,F)) = t^s$ при $t > 1$.

Для гиперболической дзета-функции решётки $\Lambda(t,F)$ в работе [19] Добровольским Н. М., Ваньковой В. С., Козловой С. Л. была получена асимптотическая формула

$$\zeta_H(\Lambda(t,F)|\alpha) = \frac{2\cdot(\det\Lambda(F))^\alpha}{R\cdot(s-1)!}\left(\sum_{(w)}\frac{1}{|N(w)|^\alpha}\right)\frac{\ln^{s-1}\det\Lambda(t,F)}{(\det\Lambda(t,F))^\alpha} + O\left(\frac{\ln^{s-2}\det\Lambda(t,F)}{(\det\Lambda(t,F))^\alpha}\right), \tag{4}$$

где R — регулятор поля F (см. [2]) и в сумме $\sum\limits_{(w)}\dfrac{1}{|N(w)|^\alpha}$ суммирование проводится по всем главным идеалам кольца $\mathbb{Z}_F$.

[3]Символ $\sum'$ означает, что из области суммирования исключается $\vec{x} = \vec{0}$, и для любого вещественного x величина $\overline{x}$ задается равенством $\overline{x} = \max(1,|x|)$.

На первом этапе исследований с 1984 года по 1990 год изучение функции $\zeta_H(\Lambda|\alpha)$ проводилось только для вещественных $\alpha > 1$. Начиная с 1995 года, в совместных работах Добровольского Н. М., Ребровой И. Ю. и Рощени А. Л. ([24], [25], [22]) начался новый этап изучения гиперболической дзета-функции $\zeta_H(\Lambda|\alpha)$ решётки Λ: во-первых, как функции комплексного аргумента α, во-вторых, как функции на метрическом пространстве решёток.

По теореме Абеля ([37], с. 106) гиперболическую дзета-функцию решёток в правой α-полуплоскости $\sigma > 1$, $\alpha = \sigma + it$ можно представить в следующем интегральном виде

$$\zeta_H(\Lambda|\alpha) = \alpha \int\limits_1^\infty \frac{D(t|\Lambda)dt}{t^{\alpha+1}},$$

где $D(T|\Lambda)$ — количество ненулевых точек решётки Λ в гиперболическом кресте $K_s(T)$.

Так как $D(T|\Lambda) = 0$ при $T < q(\Lambda)$, то

$$\zeta_H(\Lambda|\alpha) = \alpha \int\limits_{q(\Lambda)}^\infty \frac{D(t|\Lambda)dt}{t^{\alpha+1}}.$$

Возникает естественный вопрос о продолжении для произвольной решётки Λ гиперболической дзета-функции решётки $\zeta_H(\Lambda|\alpha)$ на всю комплексную плоскость. В работах Добровольского Н. М., Ребровой И. Ю. и Рощени А. Л. ([25], [22]) эти вопросы исследовались для PZ_s — множества всех целочисленных решёток, PQ_s — множества всех рациональных решёток, PD_s — множества всех решёток с диагональными матрицами. Доказано, что *для любой целочисленной решётки $\Lambda \in PZ_s$ гиперболическая дзета-функция $\zeta_H(\Lambda|\alpha)$ является регулярной функцией во всей α-плоскости, за исключением точки $\alpha = 1$, в которой она имеет полюс порядка s.*

Для любой решётки $\Lambda \in PQ_s$ гиперболическая дзета-функция $\zeta_H(\Lambda|\alpha)$ также является регулярной аналитической функцией во всей α-плоскости, за исключением точки $\alpha = 1$, в которой она имеет полюс порядка s.

Изучено поведение гиперболической дзета-функции решёток на пространстве решёток. В частности, установлено, что

если последовательность решёток $\{\Lambda_n\}$ сходится к решётке Λ, то последовательность гиперболических дзета-функций решёток $\zeta_H(\Lambda_n|\alpha)$ равномерно сходится к гиперболической дзета-функции решётки $\zeta_H(\Lambda|\alpha)$ в любой полуплоскости $\sigma \geqslant \sigma_0 > 1$.

Другой результат такого типа формулируется следующим образом.

Для любой точки α из α-плоскости, кроме точки $\alpha = 1$, найдется окрестность $|\alpha - \beta| < \delta$ такая, что для любой решётки $\Lambda = \Lambda(d_1, \ldots, d_s) \in PD_s$

$$\lim_{M \to \Lambda, M \in PD_s} \zeta_H(M|\beta) = \zeta_H(\Lambda|\beta),$$

причем эта сходимость равномерна в окрестности точки α.

Вывод этих результатов существенно опирается на асимптотическую формулу для числа точек произвольной решётки в гиперболическом кресте как функции от параметра гиперболического креста, полученную Н. М. Добровольским и А. Л. Рощеней ([26]):

$$D(T \mid \Lambda) = \frac{2^s T \ln^{s-1} T}{(s-1)! \det \Lambda} + \Theta \cdot C(\Lambda) \frac{2^s \cdot T \ln^{s-2} T}{\det \Lambda}, \tag{5}$$

где $C(\Lambda)$ – эффективная константа, вычисляемая через базис решётки, и $|\Theta| \leqslant 1$.

В работах [3]–[36], [38], [39] освящены различные аспекты теории гиперболической дзета-функции решёток. В работах [40]–[47] используется асимптотическая формула (5).

Цель данной статьи — дать новые варианты формул (4) и (5).

2. Асимптотическая формула для алгебраической решётки

Вывод нашей новой асимптотической формулы для дзета-функции алгебраической решётки будет опираться на доказательства из монографии [34], поэтому приведем ряд лемм из этой работы без доказательства, модифицируя где необходимо формулировки.

2.1. Вычисление вспомогательных интегралов

Обозначим через $Sim_k(A)$ k-мерный симплекс заданный равенством

$$Sim_k(A) = \{\vec{x} | x_1, \ldots, x_k \geqslant 0,\ x_1 + \ldots + x_k \leqslant A\}.$$

Лемма 1. *Пусть* $A \geqslant 0, k \geqslant 1$ *и*

$$I_k(A) = \int\limits_{Sim_k(A)} \ldots \int dx_1 \ldots dx_k.$$

Тогда справедливо равенство

$$I_k(A) = \frac{A^k}{k!}.$$

Доказательство. См. [34], стр. 66. □

Лемма 2. *Пусть* $B \geqslant 1, 1 \leqslant k \leqslant s-1, \alpha > 0$ *и*

$$Y_k(B) = \int\limits_{\substack{x_j \geqslant 0 (j=1,\ldots,k-1) \\ x_j \leqslant 0 (j=k,\ldots,s-1) \\ B \geqslant x_1 + \ldots + x_{s-1}}} \ldots \int e^{\alpha(x_k + \ldots + x_{s-1})} dx_1 \ldots dx_{s-1}.$$

Тогда справедливо равенство

$$Y_k(B) = \sum_{m=0}^{k-1} C_{k-1}^m \frac{(s-m)!}{(k-1)!(s-k-1)!\alpha^{s-m+1}} \cdot B^m.$$

Доказательство. См. [34], стр. 66–67. □

2.2. Интегральное представление для гиперболической дзета-функции алгебраической решётки

Пусть F_s — чисто вещественное алгебраическое поле степени s, $F_s^{(1)} = F_s, F_s^{(2)}, \ldots, \ldots, F_s^{(s)}$ — набор его сопряженных полей и для любого алгебраического числа Θ из F_s $\Theta^{(1)} = \Theta, \Theta^{(2)}, \ldots, \Theta^{(s)}$ — набор его алгебраически сопряженных чисел. Через $\mathbb{Z}_{F_s}$ обозначим кольцо целых алгебраических чисел поля F_s.

Рассмотрим алгебраическую решётку $\Lambda = \left\{ \left(\Theta^{(1)}, \Theta^{(2)}, \ldots, \Theta^{(s)}\right) \middle| \Theta \in \mathbb{Z}_{F_s} \right\}$.

Так как для любого ненулевого целого алгебраического числа Θ из $\mathbb{Z}_{F_s}$ имеем $|\Theta^{(1)}\Theta^{(2)} \ldots \Theta^{(s)}| = |N(\Theta)| \geqslant 1$, то $q(\Lambda) = 1$.

Для произвольного $t > 1$ рассмотрим алгебраическую решётку

$$\Lambda(t) = \left\{ \left(\Theta^{(1)}t, \Theta^{(2)}t, \ldots, \Theta^{(s)}t\right) \middle| \Theta \in \mathbb{Z}_{F_s} \right\}.$$

Ясно, что $q(\Lambda(t)) = t^s$. Так как $\det \Lambda(t) = t^s \det \Lambda$, то

$$q(\Lambda(t)) = \frac{\det \Lambda(t)}{\det \Lambda}. \tag{6}$$

Согласно (2), (3), (6) для гиперболической дзета–функции $\zeta_H(\Lambda(t)|\alpha)$

$$\zeta_H(\Lambda(t)|\alpha) = \sum_{\Theta\in\mathbb{Z}_{F_s}}{}' \left(\overline{t\Theta^{(1)}}\dots\overline{t\Theta^{(s)}}\right)^{-\alpha} \tag{7}$$

алгебраической решётки $\Lambda(t)$ справедливы оценки

$$C(\alpha,s,\Lambda)\frac{\ln^{s-1}\det\Lambda(t)}{(\det\Lambda(t))^{\alpha}} \leqslant \zeta_H(\Lambda(t)|\alpha) \leqslant C_1(\alpha,s,\Lambda)\frac{\ln^{s-1}\det\Lambda(t)}{(\det\Lambda(t))^{\alpha}}.$$

Для вывода асимптотической формулы для гиперболической дзета – функции алгебраической решётки $\Lambda(t)$ нам потребуются следующие обозначения.

Через $\varepsilon_1,\dots,\varepsilon_{s-1}$ обозначим набор фундаментальных единиц кольца $\mathbb{Z}_{F_s}$, а через $\varepsilon_j^{(1)} = \varepsilon_j,\dots,\varepsilon_j^{(s)}$ $(j=1,\dots,s-1)$ — их алгебраические сопряженные единицы.

Пусть далее везде $\sum\limits_{(\omega)}$ обозначает суммирование по всем главным идеалам кольца $\mathbb{Z}_{F_s}$, а $\sum\limits_{\varepsilon}$ обозначает суммирование по всем единицам кольца $\mathbb{Z}_{F_s}$. Как обычно,через R обозначим регулятор поля F_s, т. е.

$$R = \left|\begin{array}{ccc} \ln|\varepsilon_1^{(1)}| & \dots & \ln|\varepsilon_1^{(s-1)}| \\ \dots & \dots & \dots \\ \ln|\varepsilon_{s-1}^{(1)}| & \dots & \ln|\varepsilon_{s-1}^{(s-1)}| \end{array}\right|.$$

Обозначения для различных областей суммирования и интегрирования будут вводиться по мере необходимости.

Лемма 3. *Справедливо равенство*

$$\zeta(\Lambda(t)|\alpha) = 2\sum_{(\omega)}\sum_{k_1,\dots,k_{s-1}=-\infty}^{\infty}\left(\prod_{j=1}^{s}\overline{t\omega^{(j)}\varepsilon_1^{(j)k_1}\dots\varepsilon_{s-1}^{(j)k_{s-1}}}\right)^{-\alpha}.$$

Доказательство. См. [34], стр. 68. □

Пусть ω — произвольное целое ненулевое алгебраическое число и вектор $\vec{j}$ — произвольный вектор из области $D(p)$ целочисленных векторов, заданной равенством

$$D(p) = \left\{(j_1,\dots,j_s)\;\middle|\;\begin{array}{c} 1\leqslant j_1<\dots<j_p\leqslant s,\ 1\leqslant j_{p+1}<\dots<j_s<s, \\ \{j_1,\dots,j_s\}=\{1,\dots,s\}\end{array}\right\}.$$

Через $B(\vec{j},p) = B(\vec{j},p,\omega)$ обозначим множество целочисленных векторов, удовлетворяющих условиям:

$$\begin{cases} \left|t\omega^{(j_\nu)}\varepsilon_1^{(j_\nu)k_1}\dots\varepsilon_{s-1}^{(j_\nu)k_{s-1}}\right| \geqslant 1, & \text{при } \nu=1,\dots,p, \\ \left|t\omega^{(j_\nu)}\varepsilon_1^{(j_\nu)k_1}\dots\varepsilon_{s-1}^{(j_\nu)k_{s-1}}\right| < 1, & \text{при } \nu=p+1,\dots,s. \end{cases}$$

Пусть далее

$$A(\vec{j},p) = A(\vec{j},p,\omega) = \sum_{\vec{k}\in B(\vec{j},p)}\prod_{\nu=p+1}^{s}\left|t\omega^{(j_\nu)}\varepsilon_1^{(j_\nu)k_1}\dots\varepsilon_{s-1}^{(j_\nu)k_{s-1}}\right|^{\alpha} \tag{8}$$

и

$$A(\omega) = \sum_{p=1}^{s}\sum_{\vec{j}\in D(p)}A(\vec{j},p). \tag{9}$$

Имеет место следующее утверждение.

Лемма 4. *Справедливо равенство*

$$\zeta_H(\Lambda(t)|\alpha) = 2\sum_{(\omega)} \frac{A(\omega)}{(t^s|N(\omega)|)^\alpha}.$$

Доказательство. См. [34], стр. 69–70. □

Пусть

$$Y(\vec{j},p,\vec{k}) = \prod_{\nu=p+1}^{s} \left| t\omega^{(j_\nu)} \prod_{j=1}^{s-1} \varepsilon_j^{(j_\nu)k_j} \right|^\alpha, \tag{10}$$

$$C(\vec{j},p,m) = \begin{cases} 1 & \text{при } \sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}| = 0, \\ \dfrac{\alpha \sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}|}{2\operatorname{sh}\left(\dfrac{\alpha}{2}\sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}|\right)} & \text{при } \sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}| \neq 0, \end{cases}$$

$$C(\vec{j},p) = \prod_{m=1}^{s-1} C(\vec{j},p,m),$$

$$L_n(x_1,\dots,x_{s-1}) = \ln t + \ln|\omega^{(n)}| + \sum_{j=1}^{s-1} x_j \ln|\varepsilon_j^{(n)}| \quad (n=1,\dots,s),(t>1).$$

Заметим, что для любых $x_1,\dots,x_{s-1}$

$$\sum_{n=1}^{s} L_n(x_1,\dots,x_{s-1}) = \ln t^s + \ln|N(\omega)|.$$

Так как

$$\lim_{b\to 0} \frac{b}{2\operatorname{sh}\left(\frac{b}{2}\right)} = \lim_{b\to 0} \frac{b}{e^{\frac{b}{2}} - e^{-\frac{b}{2}}} = \lim_{b\to 0} \frac{1}{\frac{1}{2}e^{\frac{b}{2}} + \frac{1}{2}e^{-\frac{b}{2}}} = 1,$$

то можно всегда писать

$$C(\vec{j},p,m) = \frac{\alpha \sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}|}{2\operatorname{sh}\left(\dfrac{\alpha}{2}\sum\limits_{\nu=p+1}^{s} \ln|\varepsilon_m^{(j_\nu)}|\right)}.$$

Лемма 5. *Справедливо равенство*

$$Y(\vec{j},p,\vec{k}) = C(\vec{j},p) \int_{k_1-\frac{1}{2}}^{k_1+\frac{1}{2}} \dots \int_{k_{s-1}-\frac{1}{2}}^{k_{s-1}+\frac{1}{2}} e^{\alpha \sum\limits_{\nu=p+1}^{s} L_{j_\nu}(x_1,\dots,x_{s-1})} dx_1 \dots dx_{s-1}.$$

Доказательство. См. [34], стр. 71–72. □

Определим область $\Omega(\vec{j},p) \subset \mathbb{R}^{s-1}$, как множество всех точек $(x_1,\dots,x_{s-1})$, удовлетворяющих соотношениям

$$L_{j_\nu}(x_1,\dots,x_{s-1}) \geqslant \sum_{j=1}^{s-1}\left(\left\{x_j+\frac{1}{2}\right\}-\frac{1}{2}\right)\ln|\varepsilon_j^{(j_\nu)}| \quad (\nu=1,\dots,p),$$

$$L_{j_\nu}(x_1,\dots,x_{s-1}) \leqslant \sum_{j=1}^{s-1}\left(\left\{x_j+\frac{1}{2}\right\}-\frac{1}{2}\right)\ln|\varepsilon_j^{(j_\nu)}| \quad (\nu=p+1,\dots,s).$$

Лемма 6. *Справедливо следующее интегральное представление*

$$A(\vec{j},p)=C(\vec{j},p)\int\limits_{\Omega(\vec{j},p)}\dots\int e^{\alpha\sum\limits_{\nu=p+1}^{s}L_{j_\nu}(x_1,\dots,x_{s-1})}dx_1\dots dx_{s-1}.$$

Доказательство. См. [34], стр. 72–73. □

Пусть далее везде

$$a=\frac{s-1}{2}\max_{\substack{1\leqslant m\leqslant s-1,\\ 1\leqslant n\leqslant s}}|\ln|\varepsilon_m^{(n)}||.$$

Определим область $\Omega_\lambda(\vec{j},p)\subset\mathbb{R}^{s-1}$ $(\lambda=1,2)$ следующими соотношениями

$$L_{j\nu}(x_1,\dots,x_{s-1}) \geqslant (-1)^{\lambda-1}a \qquad (1\leqslant\nu\leqslant p),$$

$$L_{j\nu}(x_1,\dots,x_{s-1}) \leqslant (-1)^{\lambda}a \qquad (p+1\leqslant\nu\leqslant s),$$

а величины $A_\lambda(\vec{j},p)$ $(\lambda=1,2)$ зададим равенствами

$$A_\lambda(\vec{j},p)=C(\vec{j},p)\int\limits_{\Omega_\lambda(\vec{j},p)}\dots\int e^{\alpha\sum\limits_{\nu=p+1}^{s}L_{j_\nu}(x_1,\dots,x_{s-1})}dx_1\dots dx_{s-1} \quad (\lambda=1,2).$$

Кроме указанных областей и величин из монографии [34], введем для параметра θ с $-1\leqslant\theta\leqslant 1$ новую область $\Omega(\vec{j},p,\theta)\subset\mathbb{R}^{s-1}$ следующими соотношениями

$$L_{j\nu}(x_1,\dots,x_{s-1}) \geqslant -\theta a \qquad (1\leqslant\nu\leqslant p),$$

$$L_{j\nu}(x_1,\dots,x_{s-1}) \leqslant \theta a \qquad (p+1\leqslant\nu\leqslant s),$$

а величины $A(\vec{j},p,\theta)$ зададим равенствами

$$A(\vec{j},p,\theta)=C(\vec{j},p)\int\limits_{\Omega(\vec{j},p,\theta)}\dots\int e^{\alpha\sum\limits_{\nu=p+1}^{s}L_{j_\nu}(x_1,\dots,x_{s-1})}dx_1\dots dx_{s-1}.$$

Для дальнейшего важно, что новые области и величины обладают следующими принципиальными свойствами:

$$\Omega_1(\vec{j},p)=\Omega(\vec{j},p,-1),\quad \Omega_2(\vec{j},p)=\Omega(\vec{j},p,1),\quad \Omega(\vec{j},p,\theta_1)\subset\Omega(\vec{j},p,\theta_2)\text{ при }\theta_1<\theta_2$$

и величина $A(\vec{j},p,\theta)$ непрерывно, монотонно возрастает при изменении θ от -1 до 1.

Лемма 7. *Справедливы неравенства*

$$A(\vec{j},p,-1)=A_1(\vec{j},p)\leqslant A(\vec{j},p)\leqslant A_2(\vec{j},p)=A(\vec{j},p,1).$$

Доказательство. См. [34], стр. 73–74. □

Введем для параметра θ с $-1\leqslant\theta\leqslant 1$ новую область $\Omega'(\vec{j},p,\theta)\subset\mathbb{R}^{s-1}$ следующим образом: пусть для произвольной точки $(y_1,\ldots,y_{s-1})$ величина

$$y_s=\ln t^s+\ln|N(\omega)|-(y_1+y_2+\ldots+y_{s-1}).$$

Тогда точка $(y_1,\ldots,y_{s-1})$ принадлежит $\Omega'(\vec{j},p,\theta)$, если выполнены неравенства

$$\begin{cases} y_{j_\nu}\geqslant -\theta a & \text{при} \quad 1\leqslant\nu\leqslant p,\\ y_{j_\nu}<\theta a & \text{при} \quad p+1\leqslant\nu\leqslant s.\end{cases}$$

Лемма 8. *Справедливо равенство*

$$A(\vec{j},p,\theta)=\frac{C(\vec{j},p)}{R}\int\limits_{\Omega'(\vec{j},p,\theta)}\ldots\int e^{\alpha(y_{j_{p+1}}+\ldots+y_{j_s})}dy_1\ldots dy_{s-1}\quad(-1\leqslant\theta\leqslant 1),$$

где R — регулятор поля.

Доказательство. Сделаем линейную замену в интеграле по области $\Omega(\vec{j},p,\theta)$

$$y_j=L_j(x_1,\ldots,x_{s-1})\quad(j=1,\ldots,s-1).$$

Так как

$$\sum_{j=1}^{s}L_j(x_1,\ldots,x_{s-1})=\sum_{j=1}^{s}\left(\ln t+\ln|\omega^{(j)}|+\sum_{m=1}^{s-1}x_m\ln|\varepsilon_m^{(j)}|\right)=$$

$$=\ln t^s+\ln|N(\omega)|+\sum_{m=1}^{s-1}x_m\ln|N\varepsilon_m|=\ln t^s+\ln|N(\omega)|,$$

то $y_s=L_s(x_1,\ldots,x_{s-1})$.

Поэтому область $\Omega(\vec{j},p,\theta)$, заданная соотношениями

$$\begin{cases} L_{j_\nu}(x_1,\ldots,x_{s-1})\geqslant -\theta a & \text{при} \quad 1\leqslant\nu\leqslant p,\\ L_{j_\nu}(x_1,\ldots,x_{s-1}<\theta a & \text{при} \quad p+1\leqslant\nu\leqslant s,\end{cases}$$

перейдет в область $\Omega'(\vec{j},p,\theta)$, заданную соотношениями

$$\begin{cases} y_{j_\nu}\geqslant -\theta a & \text{при} \quad 1\leqslant\nu\leqslant p,\\ y_{j_\nu}<\theta a & \text{при} \quad p+1\leqslant\nu\leqslant s,\end{cases}$$

а так как якобиан линейного преобразования имеет модуль, равный регулятору поля, то лемма доказана. □

2.3. Асимптотическая формула для гиперболической дзета-функции алгебраической решётки

Пусть для $-1 \leqslant \theta \leqslant 1$ величины $I(\vec{j}; p, \theta)$ определены равенствами

$$I(\vec{j}, p, \theta) = \int\limits_{\Omega'(\vec{j},p,\theta)} \dots \int e^{\alpha(y_{j_{p+1}}+\dots+y_{j_{s-1}})} dy_1 \dots dy_{s-1}$$

и

$$C_p(\theta) = e^{\theta(s-p)a\alpha},$$
$$B_p(\theta) = \ln t^s + \ln|N(\omega)| + \theta(2p-s)a.$$

Лемма 9. *Справедливы равенства:*
при $1 \leqslant p \leqslant s-1$

$$I(\vec{j}, p, \theta) = e^{\theta(s-p)\alpha a} \sum_{m=0}^{p-1} C_{p-1}^m \frac{(s-m)!}{(p-1)!(s-p-1)!\alpha^{s-m+1}} \cdot (\ln t^s + \ln|N(\omega)| + \theta(2p-s)a)^m$$

и

$$I(\vec{j}, s, \theta) = \frac{(\ln t^s + \ln|N(\omega)|)^{s-1}}{(s-1)!} + \sum_{\nu=1}^{s-1} \frac{C_{s-1}^\nu s^\nu a^\nu \theta^\nu (\ln t^s + \ln|N(\omega)|)^{s-1-\nu}}{(s-1)!}.$$

Доказательство. При $p = s$ имеем $D(p) = \{(1, 2, \dots, s)\}$ и, следовательно, $\vec{j} = (1, 2, \dots, s) \in D(p)$.

Поэтому

$$I(\vec{j}, s, \theta) = \int\limits_{\Omega'(\vec{j},s,\theta)} \dots \int dy_1 \dots dy_{s-1}$$

и $\Omega'(\vec{j}, s, \theta)$ задано соотношениями

$$\begin{cases} y_\nu \geqslant -\theta a \qquad (\nu = 1, \dots, s-1), \\ y_1 + y_2 + \dots + y_s = \ln t^s + \ln|N(\omega)|. \end{cases}$$

Сделаем линейную замену переменных

$$z_\nu = y_\nu + \theta a \qquad (\nu = 1, \dots, s-1),$$

тогда область $\Omega'(\vec{j}, s, \theta)$ перейдет в область $\Omega''(\theta)$, заданную соотношениями

$$\begin{cases} z_\nu \geqslant 0 \qquad (\nu = 1, \dots, s-1), \\ \ln t^s + \ln|N(\omega)| - \sum_{\nu=1}^{s-1}(z_\nu - \theta a) \geqslant -\theta a. \end{cases} \tag{11}$$

Неравенство (11) можно записать в виде

$$\sum_{\nu=1}^{s-1} z_\nu \leqslant \ln t^s + \ln|N(\omega)| + s \cdot \theta a.$$

Из последнего неравенства следует, что

$$I(\vec{j}, s, \theta) = I_{s-1}(A(\theta)),$$

где величина $I_s(A)$ определена в лемме 1 и

$$A(\theta) = \ln t^s + \ln|N(\omega)| + s \cdot \theta a = B_s(\theta).$$

Отсюда следует, что

$$I(\vec{j},s,\theta)=\frac{(\ln t^s+\ln|N(\omega)|+s\cdot\theta a)^{s-1}}{(s-1)!}=$$
$$=\frac{(\ln t^s+\ln|N(\omega)|)^{s-1}}{(s-1)!}+\sum_{\nu=1}^{s-1}\frac{C_{s-1}^{\nu}s^{\nu}a^{\nu}\theta^{\nu}(\ln t^s+\ln|N(\omega)|)^{s-1-\nu}}{(s-1)!}.$$

Пусть теперь $1\leqslant p\leqslant s-1$. Сделаем линейную замену переменных

$$z_{\nu}=\begin{cases}y_{j_{\nu+1}}+\theta a & \text{при} \quad \nu=1,\dots,p-1,\\ y_{j_{\nu+1}}-\theta a & \text{при} \quad \nu=p,\dots,s-1,\\ y_{j_1}+\theta a & \text{при} \quad \nu=s.\end{cases}$$

Тогда область $\Omega'(\vec{j},p,\theta)$ перейдет в область $\Omega''(\theta)$ точек $(z_1,\dots,z_{s-1})$, удовлетворяющих условиям

$$z_{\nu}\geqslant 0\ (\nu=1,\dots,p-1),\quad z_{\nu}<0\ (\nu=p,\dots,s-1),\quad z_s\geqslant 0.$$

При этом

$$z_1+\ldots+z_s=\sum_{\nu=1}^{p}(y_{j_\nu}+\theta a)+\sum_{\nu=p+1}^{s}(y_{j_\nu}-\theta a)=\ln t^s+\ln|N(\omega)|+\theta(2p-s)a.$$

Отсюда следует, что

$$I(\vec{j},p,\theta)=\int\limits_{\Omega_p''(\theta)}\dots\int e^{\alpha(z_p+\ldots+z_{s-1}+\theta(s-p)a)}dz_1\dots dz_{s-1}=Y_p(B_p(\theta))\cdot e^{\theta(s-p)\alpha a},$$

где величина $Y_p(B)$ определена в лемме 2 и

$$B_p(\theta)=\ln t^s+\ln|N(\omega)|+\theta(2p-s)a.$$

Отсюда следует, что

$$I(\vec{j},p,\theta)=e^{\theta(s-p)\alpha a}\sum_{m=0}^{p-1}C_{p-1}^{m}\frac{(s-m)!}{(p-1)!(s-p-1)!\alpha^{s-m+1}}\cdot(\ln t^s+\ln|N(\omega)|+\theta(2p-s)a)^m.$$

Лемма полностью доказана. □

Обозначим через $\zeta_{D_0}(\alpha|F)$ дзета-функцию Дедекинда главных идеалов чисто-вещественного поля F:

$$\zeta_{D_0}(\alpha|F)=\sum_{(\omega)}|N(\omega)|^{-\alpha},$$

тогда

$$\zeta_{D_0}^{(\nu)}(\alpha|F)=(-1)^{\nu}\sum_{(\omega)}\ln^{\nu}|N(\omega)||N(\omega)|^{-\alpha},\quad \nu\geqslant 1.$$

Теорема 1. *При $t>e^a$ справедливо асимптотическое равенство*

$$\zeta_H(\Lambda(t)|\alpha)=\frac{2(\det\Lambda)^{\alpha}}{R(s-1)!}\sum_{\nu=0}^{s-1}C_{s-1}^{\nu}\frac{(\ln\det\Lambda(t)-\ln\det\Lambda)^{s-1-\nu}(-1)^{\nu}\zeta_{D_0}^{(\nu)}(\alpha|F)}{(\det\Lambda(t))^{\alpha}}+R(\Lambda,\alpha,\theta),\quad(12)$$

где

$$R(\Lambda,\alpha,\theta)=O\left(\frac{\ln^{s-2}(\det\Lambda(t))}{(\det\Lambda(t))^{\alpha}}\right)\quad u\quad R\ -\textit{регулятор поля.}$$

Доказательство. Согласно лемме 4 имеем

$$\zeta_H(\Lambda(t)|\alpha)=2\sum_{(\omega)}\frac{1}{(t^s|N(\omega)|)^\alpha}A(\omega)\quad\text{и}\quad A(\omega)=\sum_{p=1}^{s}\sum_{\vec{j}\in D(p)}A(\vec{j},p).$$

По лемме 7

$$A(\vec{j},p,-1)\leqslant A(\vec{j},p)\leqslant A(\vec{j},p,1).$$

Отсюда следует, что справедливы неравенства

$$2\sum_{(\omega)}\frac{1}{(t^s|N(\omega)|)^\alpha}\sum_{p=1}^{s}\sum_{\vec{j}\in D(p)}A(\vec{j},p,-1)\leqslant\zeta_H(\Lambda(t)|\alpha)\leqslant 2\sum_{(\omega)}\frac{1}{(t^s|N(\omega)|)^\alpha}\sum_{p=1}^{s}\sum_{\vec{j}\in D(p)}A(\vec{j},p,1).$$

Так как величины $A(\vec{j},p,\theta)$ непрерывно, монотонно возрастают при изменении θ от -1 до 1, то найдётся значение $\theta=\theta(\Lambda(t),\alpha)$ с $-1\leqslant\theta\leqslant 1$, такое что

$$\zeta_H(\Lambda(t)|\alpha)=2\sum_{(\omega)}\frac{1}{(t^s|N(\omega)|)^\alpha}\sum_{p=1}^{s}\sum_{\vec{j}\in D(p)}A(\vec{j},p,\theta).$$

Из лемм 8, 9, 1 следует, что при $t>e^a$

$$A(\vec{j},s,\theta)=\frac{1}{R}I_{s-1}(\ln t^s+\ln|N(\omega)|+s\cdot\theta a)=\frac{(\ln t^s+\ln|N(\omega)|+s\cdot\theta a)^{s-1}}{R\cdot(s-1)!}=$$

$$=\frac{(\ln t^s+\ln|N(\omega)|)^{s-1}}{R\cdot(s-1)!}+\frac{1}{R\cdot(s-1)!}\sum_{\nu=0}^{s-2}C_{s-1}^{\nu}(\ln t^s+\ln|N(\omega)|)^\nu(s\cdot\theta a)^{s-1-\nu}.\qquad(13)$$

Из лемм 8, 9, 2 следует, что при $1\leqslant p\leqslant s-1$

$$A(\vec{j},p,\theta)=\frac{C(\vec{j},p)e^{\theta(s-p)\alpha a}}{R}\sum_{m=0}^{p-1}\frac{(s-m)!C_{p-1}^{m}\cdot(\ln t^s+\ln|N(\omega)|+\theta(2p-s)a)^m}{(p-1)!(s-p-1)!\alpha^{s-m+1}}.\qquad(14)$$

Объединяя оценки (13) и (14), получим

$$\zeta(\Lambda(t)|\alpha)=2\sum_{(\omega)}\frac{1}{(t^s|N(\omega)|)^\alpha}\frac{(\ln t^s+\ln|N(\omega)|)^{s-1}}{R\cdot(s-1)!}+R(\Lambda,\alpha,\theta),$$

где

$$R(\Lambda,\alpha,\theta)=\frac{1}{R\cdot(s-1)!}\sum_{\nu=0}^{s-2}C_{s-1}^{\nu}(\ln t^s+\ln|N(\omega)|)^\nu(s\cdot\theta a)^{s-1-\nu}+$$

$$+\sum_{(\omega)}\frac{2}{(t^s|N(\omega)|)^\alpha}\sum_{p=1}^{s-1}\sum_{\vec{j}\in D(p)}\frac{C(\vec{j},p)e^{\theta(s-p)\alpha a}}{R}\sum_{m=0}^{p-1}\frac{(s-m)!C_{p-1}^{m}\cdot(\ln t^s+\ln|N(\omega)|+\theta(2p-s)a)^m}{(p-1)!(s-p-1)!\alpha^{s-m+1}},$$

$$R(\Lambda,\alpha,\theta)=O\left(\frac{\ln^{s-2}(\det\Lambda(t))}{(\det\Lambda(t))^\alpha}\right).$$

Преобразуя главный член по t, окончательно находим

$$\zeta_H(\Lambda(t)|\alpha)=\frac{2}{R(s-1)!}\sum_{\nu=0}^{s-1}C_{s-1}^{\nu}\frac{\ln^{s-1-\nu}t^s}{t^{s\alpha}}\sum_{(\omega)}\frac{\ln^\nu|N(\omega)|}{|N(\omega)|^\alpha}+R(\Lambda,\alpha,\theta)=$$

$$=\frac{2(\det\Lambda)^\alpha}{R(s-1)!}\sum_{\nu=0}^{s-1}C_{s-1}^{\nu}\frac{(\ln\det\Lambda(t)-\ln\det\Lambda)^{s-1-\nu}(-1)^\nu\zeta_{D_0}^{(\nu)}(\alpha|F)}{(\det\Lambda(t))^\alpha}+R(\Lambda,\alpha,\theta),$$

что и требовалось доказать. □

3. Асимптотическая формула для числа точек решётки

Вывод нового варианта асимптотической формулы для числа точек решётки в гиперболическом кресте мы будем проводить тем же методом, что и получение асимптотической формулы для гиперболической дзета-функции алгебраической решётки. Далее везде предполагаем, что размерность $s \geqslant 2$.

3.1. Вспомогательные леммы о многомерных областях и интегралах

Пусть $\vec{\lambda_j} = (\lambda_{j1}, ..., \lambda_{js})$ $(j = 1, ..., s)$ — произвольный фиксированный базис решетки Λ и

$$A = A(\vec{\lambda_1}, ..., \vec{\lambda_s}) = \max_{1 \leqslant j \leqslant s} 1/2 \sum_{\nu=1}^{s} |\lambda_{\nu j}|; \tag{15}$$

$\vec{\lambda_j^*} = (\lambda_{j1}^*, ..., \lambda_{js}^*)$ $(j = 1, ..., s)$ — взаимный базис взаимной решетки Λ^* (как известно, взаимный базис задается соотношениями

$$(\vec{\lambda_i}, \vec{\lambda_j^*}) = \sum_{\nu=1}^{s} \lambda_{i\nu} \lambda_{j\nu}^* = \delta_{ij} = \begin{cases} 1 & \text{при} \quad i = j \\ 0 & \text{при} \quad i \neq j \end{cases}, \tag{16}$$

а взаимная решетка Λ^* однозначно определяется решеткой Λ).

Определим следующие области

$$\Pi(T \mid \Lambda) = \left\{ \vec{t} \left| \prod_{j=1}^{s} \overline{\sum_{\nu=1}^{s} \lambda_{\nu j} t_\nu + \sum_{\nu=1}^{s} \lambda_{\nu j} (1/2 - \{t_\nu + 1/2\})} \leqslant T \right. \right\}, \tag{17}$$

для целого вектора $\vec{m}$

$$\Pi(\vec{m}) = \{\vec{t} \mid [t_\nu + 1/2] = m_\nu \, (\nu = 1, ..., s)\}, \tag{18}$$

$$\Pi^*(T \mid \Lambda) = \left\{ \vec{y} \mid \prod_{j=1}^{s} \overline{y_j + \sum_{\nu=1}^{s} \lambda_{\nu j} (1/2 - \{1/2 + \sum_{k=1}^{s} y_k \lambda_{\nu k}^*\})} \leqslant T \right\}, \tag{19}$$

при $a \geqslant 0$, $-1 \leqslant \theta \leqslant 1$ положим

$$u(y, \theta a) = \begin{cases} 1 & \text{при} \quad |y| + \theta a \leqslant 1, \\ |y| + \theta a & \text{при} \quad |y| + \theta a \geqslant 1 \end{cases} \tag{20}$$

и области

$$\Pi_1(T, a) = \left\{ \vec{y} \mid \prod_{j=1}^{s} \overline{|y_j| + a} \leqslant T \right\}, \tag{21}$$

$$\Pi_2(T, a) = \left\{ \vec{y} \mid \prod_{j=1}^{s} u(y_j, -a) \leqslant T \right\}, \tag{22}$$

$$\Pi(T, \theta a) = \left\{ \vec{y} \mid \prod_{j=1}^{s} u(y_j, \theta a) \leqslant T \right\}. \tag{23}$$

Ясно, что

$$\Pi_1(T, a) = \Pi(T, a) \subset \Pi_2(T, a) = \Pi(T, -a).$$

Заметим, что $\Pi_1(T,0)=\Pi_2(T,0)=K(T)$.
Пусть при $a\geqslant 0$, $T\geqslant 0$, $-1\leqslant\theta\leqslant 1$

$$I_s(a,T)=\int\limits_{\substack{\prod_{j=1}^{s}(y_j+a)\leqslant T\\ y_1,\cdots,y_s\geqslant 0}} d\vec{y}, \tag{24}$$

$$J_s(a,T)=\int\limits_{\substack{\prod_{j=1}^{s}u(y_j,-a)\leqslant T\\ y_1,\cdots,y_s\geqslant 0}} d\vec{y}, \tag{25}$$

$$I_s(a,T,\theta)=\int\limits_{\substack{\prod_{j=1}^{s}u(y_j,a\theta)\leqslant T\\ y_1,\cdots,y_s\geqslant 0}} d\vec{y}. \tag{26}$$

Лемма 10. *Справедливо равенство*

$$\sum_{\prod_{j=1}^{s}\overline{\lambda_{1j}m_1+\cdots+\lambda_{sj}m_s}\leqslant T}\int\limits_{\Pi(\vec{m})} d\vec{t}=\int\limits_{\Pi(T|\Lambda)} d\vec{t}. \tag{27}$$

Доказательство. См. [26]. □

Лемма 11. *Справедливы равенства*

$$\int\limits_{\Pi(T|\Lambda)} d\vec{t}=\frac{1}{\det\Lambda}\int\limits_{\Pi^*(T|\Lambda)} d\vec{y}, \tag{28}$$

$$\int\limits_{\Pi_1(T,a)} d\vec{y}=2^sI_s(a,T)\qquad \textit{при } a\geqslant 1, \tag{29}$$

$$\int\limits_{\Pi_2(T,a)} d\vec{y}=2^sJ_s(a,T)\qquad \textit{при } a\geqslant 0. \tag{30}$$

Доказательство. См. [26]. □

Лемма 12. *При $a>0$, $T\geqslant a^s$ справедливо равенство*

$$I_s(a,T)=(-1)^{s+1}(T-a^s)+T\sum_{n=1}^{s-1}\frac{(\ln T-s\ln a)^n(-1)^{s-1-n}}{n!}. \tag{31}$$

Доказательство. См. [26]. □

Лемма 13. *При $a\geqslant 0$, $T\geqslant 1$, $s\geqslant 1$ справедливо равенство*

$$J_s(a,T)=a^s+\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}\sum_{k=0}^{s-1-n}C_s^kC_{s-k-1}^n a^k. \tag{32}$$

Доказательство. См. [26]. □

Следствие 1. *При $a>1$, $T\geqslant 3$ справедливо неравенство*

$$I_s(a,T)\geqslant\frac{T\ln^{s-1}T}{(s-1)!}-ea^sT\ln^{s-2}T-a^s. \tag{33}$$

Доказательство. См. [26]. □

Следствие 2. *Справедливо неравенство*

$$J_s(a,T) \leqslant \frac{T\ln^{s-1}T}{(s-1)!} + (a+2)^s T\ln^{s-2}T + a^s. \tag{34}$$

Доказательство. См. [26]. □

Лемма 14. *При $a>0$, $T \geqslant a^s$, $-1 \leqslant \theta \leqslant 1$ справедливо равенство*

$$I_s(a,T,\theta) = \begin{cases} (-1)^{s+1}(T-(\theta a)^s) + T\sum\limits_{n=1}^{s-1} \frac{(\ln T - s\ln(\theta a))^n (-1)^{s-1-n}}{n!}, & \text{при } \theta a \geqslant 1, \\ (-\theta a)^s + \sum\limits_{n=0}^{s-1} \frac{T\ln^n T}{n!} \sum\limits_{k=0}^{s-1-n} C_s^k C_{s-k-1}^n (-\theta a)^k, & \text{при } \theta a \leqslant 1. \end{cases} \tag{35}$$

Доказательство. Из определения $I_s(a,T,\theta)$ имеем:
при $a\theta \geqslant 1$ будет $I_s(a,T,\theta) = I_s(a\theta,T$ и в силу леммы 12

$$I_s(a,T,\theta) = (-1)^{s+1}(T-(a\theta)^s) + T\sum_{n=1}^{s-1}\frac{(\ln T - s\ln(a\theta))^n(-1)^{s-1-n}}{n!};$$

при $a\theta \leqslant 1$

$$I_s(a,T,\theta) = \int\limits_0^{1-a\theta} dy_s \int\limits_{\substack{y_1,\cdots,y_{s-1}\geqslant 0 \\ u(y_1,a)\cdot\ldots\cdot u(y_{s-1},a)\leqslant T}} dy_1\cdots dy_{s-1} +$$

$$+ \int\limits_{1-a\theta}^{T-a\theta} dy_s \int\limits_{\substack{y_1,\cdots,y_{s-1}\geqslant 0 \\ u(y_1,a)\cdot\ldots\cdot u(y_{s-1},a)\leqslant \frac{T}{y+a\theta}}} dy_1\cdots dy_{s-1} =$$

$$= (1-a\theta)I_{s-1}(a,T,\theta) + \int\limits_1^T I_{s-1}\left(a,\frac{T}{y},\theta\right)dy. \tag{36}$$

Далее проведем индукцию по s, используя рекуррентное равенство (36).

При $s=1$

$$I_1(a,T,\theta) = \int\limits_{\substack{y\geqslant 0 \\ u(y,a\theta)\leqslant T}} dy = \int\limits_0^{1-a\theta} dy + \int\limits_{1-a\theta}^{T-a\theta} dy = 1-a\theta+T-1 = T-a\theta$$

и равенство (35) выполнено.

Пусть

$$Q_{s,n}(a\theta) = \sum_{k=0}^{s-1-n} C_s^k C_{s-k-1}^n (-a\theta)^k$$

и

$$I_s(a,T,\theta)=(-a\theta)^s+\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}Q_{s,n}(a\theta),$$

тогда

$$I_{s+1}(a,T,\theta)=(1-a\theta)I_s(a,T,\theta)+\int\limits_1^T I_s\left(a,\frac{T}{y},\theta\right)dy=$$

$$=(1-a\theta)(-a\theta)^s+\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}Q_{s,n}(a)(1-a\theta)+\int\limits_1^T\left((-a\theta)^s+\sum_{n=0}^{s-1}\frac{T/y\ln^n(T/y)}{n!}Q_{s,n}(a\theta)\right)dy=$$

$$=(-a\theta)^{s+1}+(-a\theta)^s+T(-a\theta)^s-(-a\theta)^s+\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}Q_{s,n}(a)(1-a\theta)+$$

$$+\sum_{n=0}^{s-1}\frac{T}{n!}Q_{s,n}(a\theta)\frac{\ln^{n+1}T}{n+1}=(-a\theta)^{s+1}+T((-a\theta)^s+Q_{s,0}(a\theta)(1-a\theta))+$$

$$+\sum_{n=1}^{s-1}\frac{T\ln^n T}{n!}\left(Q_{s,n}(a\theta)(1-a\theta)+Q_{s,n-1}(a\theta)\right)+\frac{T\ln^s T}{s!}Q_{s,s-1}(a\theta)=$$

$$=(-a\theta)^{s+1}+\sum_{n=0}^{s}\frac{T\ln^n T}{n!}Q_{s+1,n}(a\theta),$$

где

$$Q_{s+1,0}(a\theta)=(-a\theta)^s+(1-a\theta)\sum_{k=0}^{s-1}C_s^k(-a\theta)^k=\sum_{k=1}^{s}C_s^{k-1}(-a\theta)^k+\sum_{k=0}^{s-1}C_s^k(-a\theta)^k+(-a\theta)^s=$$

$$=s(-a\theta)^s+\sum_{k=1}^{s-1}(C_s^{k-1}+C_s^k)(-a\theta)^k+1=\sum_{k=0}^{s}C_{s+1}^k(-a\theta)^k=\sum_{k=0}^{(s+1)-1-0}C_{s+1}^kC_{s+1-k-1}^0(-a\theta)^k;$$

$$Q_{s+1,s}(a\theta)=Q_{s,s-1}(a\theta)=1=\sum_{k=0}^{(s+1)-1-s}C_{s+1}^kC_{s+1-k-1}^s(-a\theta)^k;$$

и при $1\leqslant n\leqslant s-1$

$$Q_{s+1,n}(a\theta)=Q_{s,n}(a\theta)(1-a\theta)+Q_{s,n-1}(a\theta)=$$

$$=(1-a\theta)\sum_{k=0}^{s-1-n}C_s^kC_{s-k-1}^n(-a\theta)^k+\sum_{k=0}^{s-1-(n-1)}C_s^kC_{s-k-1}^{n-1}(-a\theta)^k=$$

$$=\sum_{k=1}^{s-n}C_s^{k-1}C_{s-(k-1)-1}^n(-a\theta)^k+\sum_{k=0}^{s-1-n}C_s^k(C_{s-k-1}^n+C_{s-k-1}^{n-1})(-a\theta)^k+C_s^{s-n}C_{n-1}^{n-1}(-a\theta)^{s-n}=$$

$$=\sum_{k=1}^{s-n}C_s^{k-1}C_{s-k}^n(-a\theta)^k+\sum_{k=0}^{s-n}C_s^kC_{s-k}^n(-a\theta)^k=$$

$$=\sum_{k=1}^{s-n}(C_s^{k-1}+C_s^k)C_{s-k}^n(-a\theta)^k+C_s^0C_{s-0}^n(-a\theta)^0=\sum_{k=0}^{s-n}(C_{s+1}^kC_{(s+1)-1-k}^n)(-a\theta)^k$$

и, значит, $I_{s+1}(a,T,\theta)$ удовлетворяет равенству (35).

Для полноты изложения покажем что при $a\theta = 1$ обе формулы в (35) задают одно и тоже значение

$$I_s(a,T,\theta) = (-1)^s + T\sum_{n=0}^{s-1}\frac{(-1)^{s-1-n}\ln^n T}{n!}.$$

Действительно, в этом случае имеем:

$$I_{s+1}(a,T,\theta) = \int\limits_1^T I_s\left(a,\frac{T}{y},\theta\right)dy = \int\limits_1^T\left((-1)^s + \frac{T}{y}\sum_{n=0}^{s-1}\frac{(-1)^{s-1-n}\ln^n\frac{T}{y}}{n!}\right) =$$

$$= (-1)^s(T-1) + \sum_{n=0}^{s-1}\frac{T}{n!}(-1)^{s-1-n}\frac{\ln^{n+1}T}{n+1} = (-1)^{s+1} + T\sum_{n=0}^{s}\frac{(-1)^{s-n}\ln^n T}{n!},$$

что и и завершает доказательство леммы. □

Следствие 3. *Объем гиперболического креста задается равенством*

$$V(K(T)) = 2^s\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}C_{s-1}^n.$$

Доказательство. Действительно, $\Pi_1(T,0) = \Pi_2(T,0) = K(T)$. По леммам 11, 13 имеем:

$$V(K(T)) = 2^s J_s(0,T) = 2^s\sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}C_{s-1}^n$$

и следствие доказано. □

Лемма 15. *При $-1 \leqslant \theta \leqslant 1$ справедливо неравенство*

$$|2^s I_s(a,T,\theta) - V(K(T))| \leqslant \begin{cases} \max\left(T(2+2\ln a) - a^2, 2(\ln a)T + a^2\right) & \text{при } s = 2, \\ T\frac{c_1(a,s)\ln^{s-2}T}{(s-2)!} + c_2(a,s)T\ln^{s-3}T + a^s, & \text{при } s > 2 \end{cases},$$

где

$$c_1(a,s) = \max\left(2 + s\ln a, s - 2 + s\ln a\right), \quad c_2(a,s) = \max\left(e(a^s+1), (a+2)^s\right).$$

Доказательство. Действительно, $V(K(T)) = 2^s I_s(a,T,0)$ и

$$I_s(a,T) = I_s(a,T,1) \leqslant I_s(a,T,\theta) \leqslant I_s(a,T,-1) = J_s(a,T),$$

поэтому

$$\left|I_s(a,T,\theta) - 2^{-s}V(K(T))\right| \leqslant \max\left(2^{-s}V(K(T)) - I_s(a,T), J_s(a,T) - 2^{-s}V(K(T))\right),$$

в силу монотонного убывания величины $I_s(a,T,\theta)$ при изменении θ от -1 до 1.

Для первой разности под знаком максимума, которую обозначим через M_1, имеем:

$$M_1 = 2^{-s}V(K(T)) - I_s(a,T) = \sum_{n=0}^{s-1}\frac{T\ln^n T}{n!} - (-1)^{s+1}(T-a^s) - T\sum_{n=1}^{s-1}\frac{(\ln T - s\ln a)^n(-1)^{s-1-n}}{n!} =$$

$$= (-1)^{s+1}a^s + T(1+(-1)^s) + \sum_{n=1}^{s-1}\frac{T\ln^n T(1+(-1)^{s-n})}{n!} +$$

$$+ T\sum_{n=1}^{s-1}\frac{(-1)^{s-n}}{n!}\sum_{k=0}^{n-1}C_n^k(-1)^{n-k}(s\ln a)^{n-k}\ln^k T.$$

Располагая по степеням $\ln^k T$, получим:

$$M_1 = (-1)^{s+1}a^s + T\left(1+(-1)^s\left(1+\sum_{n=1}^{s-1}\frac{1}{n!}(s\ln a)^n\right)\right) + \sum_{n=1}^{s-2}\frac{T\ln^n T(1+(-1)^{s-n})}{n!} +$$
$$+T\sum_{k=1}^{s-2}(-1)^{s-k}\ln^k T\sum_{n=k+1}^{s-1}\frac{C_n^k(s\ln a)^{n-k}}{n!} = (-1)^{s+1}a^s + T\left(1+(-1)^s\left(1+\sum_{n=1}^{s-1}\frac{1}{n!}(s\ln a)^n\right)\right) +$$
$$+T\sum_{n=1}^{s-2}\frac{\ln^n T}{n!}\left(1+(-1)^{s-n}\left(1+\sum_{k=1}^{s-1-n}\frac{(s\ln a)^k}{k!}\right)\right) = (-1)^{s+1}a^s + T\frac{(2+s\ln a)\ln^{s-2}T}{(s-2)!} +$$
$$+T\sum_{n=0}^{s-3}\frac{\ln^n T}{n!}\left(1+(-1)^{s-n}\left(1+\sum_{k=1}^{s-1-n}\frac{(s\ln a)^k}{k!}\right)\right) \leqslant T\frac{(2+s\ln a)\ln^{s-2}T}{(s-2)!} + e(a^s+1)T\ln^{s-3}T + a^s.$$

При $s=2$ справедливо более точное утверждение:

$$M_1 = T(2+2\ln a) - a^2.$$

Перейдём ко второй разности под знаком максимума, которую обозначим через M_2, имеем:

$$M_2 = J_s(a,T) - 2^{-s}V(K(T)) = a^s + \sum_{n=0}^{s-1}\frac{T\ln^n T}{n!}\sum_{k=0}^{s-1-n}C_s^k C_{s-k-1}^n a^k - \sum_{n=0}^{s-1}\frac{T\ln^n T}{n!} =$$
$$= a^s + \sum_{n=0}^{s-2}\frac{T\ln^n T}{n!}\left(\sum_{k=0}^{s-1-n}C_s^k C_{s-k-1}^n a^k - 1\right) = a^s + T\frac{(s-2+s\ln a)\ln^{s-2}T}{(s-2)!} +$$
$$+\sum_{n=0}^{s-3}\frac{T\ln^n T}{n!}\left(\sum_{k=0}^{s-1-n}\frac{s!(s-k-1)!}{k!(s-k)!n!(s-k-n-1)!}a^k - 1\right) = a^s + T\frac{(s-2+s\ln a)\ln^{s-2}T}{(s-2)!} +$$
$$+T\sum_{n=0}^{s-3}\frac{\ln^n T}{n!}\left(C_s^n\sum_{k=0}^{s-1-n}\frac{s-n}{s-k}C_{s-n-1}^k a^k - 1\right) \leqslant a^s + T\frac{(s-2+s\ln a)\ln^{s-2}T}{(s-2)!} +$$
$$+T\sum_{n=0}^{s-3}\frac{\ln^n T}{n!}C_s^n\frac{s-n}{n+1}(a+1)^{s-n-1} \leqslant a^s + T\frac{(s-2+s\ln a)\ln^{s-2}T}{(s-2)!} + (a+2)^s T\ln^{s-3}T.$$

При $s=2$ справедливо более точное утверждение:

$$M_2 = 2\ln aT + a^2.$$

Объединяя рассмотренные случаи, получаем утверждение леммы. □

3.2. Асимптотическая формула для числа точек в гиперболическом кресте

Рассмотрим произвольный базис решетки Λ:

$$\overrightarrow{\lambda}_j = (\lambda_{j1},...,\lambda_{js}) \quad (j=1,...,s)$$

и величину

$$A(\overrightarrow{\lambda}_1,...,\overrightarrow{\lambda}_s) = \frac{1}{2}\max_{1\leqslant j\leqslant s}\sum_{\nu=1}^{s}|\lambda_{\nu j}|. \tag{1}$$

Определим величину —

$$a(\Lambda) = \min_{\overrightarrow{\lambda}_1,...,\overrightarrow{\lambda}_s}\max(1, A(\overrightarrow{\lambda}_1,...,\overrightarrow{\lambda}_s)), \tag{2}$$

где минимум берется по всем базисам $\vec{\lambda}_1, ..., \vec{\lambda}_s$ решетки Λ.

Далее до конца параграфа зафиксируем базис $\vec{\lambda}_1, \dots, \vec{\lambda}_s$ решетки Λ, для которого величина $A(\vec{\lambda}_1, \dots, \vec{\lambda}_s)$ — минимальна, то есть $a(\Lambda) = \max(1, A(\vec{\lambda}_1, ..., \vec{\lambda}_s))$.

Для величины $D(T|\Lambda)$—количества ненулевых точек решетки Λ, лежащих в гиперболическом кресте $K(T)$, докажем следующую теорему.

Теорема 2. *Для любой решетки Λ справедливо асимптотическое равенство при $T \geqslant 3$*

$$D(T \mid \Lambda) = 2^s \sum_{n=0}^{s-1} \frac{T \ln^n T}{n!} C_{s-1}^n - 1 + \Theta C_1(\Lambda, T), \quad |\Theta| \leqslant 1, \tag{37}$$

где

$$C_1(\Lambda, T) = \begin{cases} \max\left(T(2 + 2\ln a) - a^2, 2(\ln a)T + a^2\right) & \text{при } s = 2, \\ T\frac{c_1(a,s)\ln^{s-2} T}{(s-2)!} + c_2(a,s) T \ln^{s-3} T + a^s, & \text{при } s > 2 \end{cases} \tag{38}$$

и

$$c_1(a,s) = \max\left(2 + s\ln a, s - 2 + s\ln a\right), \quad c_2(a,s) = \max\left(e(a^s+1), (a+2)^s\right).$$

Доказательство. Из определения величины $D(T \mid \Lambda)$ следует, что

$$D(T \mid \Lambda) + 1 = \sum_{\substack{\vec{x} \in \Lambda \\ \bar{x_1} \cdots \bar{x_s} \leqslant T}} 1 = \sum_{\prod_{j=1}^s \overline{\lambda_{1j} m_1 + \cdots + \lambda_{sj} m_s} \leqslant T} 1 = \int\limits_{\Pi(T|\Lambda)} d\vec{t} \tag{39}$$

в силу леммы 10.

Применяя лемму 11, получим

$$D(T \mid \Lambda) + 1 = \frac{1}{\det \Lambda} \int\limits_{\Pi^*(T|\Lambda)} d\vec{t} \tag{40}$$

Пусть $a = a(\Lambda)$, тогда справедливы включения

$$\Pi_1(T, a) \subseteq \Pi^*(T \mid \Lambda) \subseteq \Pi_2(T, a), \tag{41}$$

так как

$$\prod_{j=1}^s u(|y_j|, a) \leqslant \prod_{j=1}^s \overline{y_j + \sum_{\nu=1}^s \lambda_{\nu j}(1/2 - \{1/2 + \sum_{k=1}^s y_k \lambda^*_{\nu k}\})} \leqslant \prod_{j=1}^s (|y_j| + a).$$

Из этого включения и леммы 11 следуют неравенства

$$\frac{2^s I_s(a, T, 1)}{\det \Lambda} = \frac{2^s I_s(a, T)}{\det \Lambda} \leqslant D(T \mid \Lambda) + 1 \leqslant \frac{2^s J_s(a, T)}{\det \Lambda} = \frac{2^s I_s(a, T, -1)}{\det \Lambda}. \tag{42}$$

Так как $I_s(a, T, \theta)$ непрерывно зависит от θ при $-1 \leqslant \theta \leqslant 1$, то найдется θ с $-1 \leqslant \theta \leqslant 1$ такое, что

$$D(T \mid \Lambda) + 1 = \frac{2^s I_s(a, T, \theta)}{\det \Lambda}.$$

Применяя оценку из леммы 15, получим

$$|D(T \mid \Lambda) + 1 - V(K(T))| \leqslant \begin{cases} \max\left(T(2 + 2\ln a) - a^2, 2(\ln a)T + a^2\right) & \text{при } s = 2, \\ T\frac{c_1(a,s)\ln^{s-2} T}{(s-2)!} + c_2(a,s) T \ln^{s-3} T + a^s, & \text{при } s > 2 \end{cases},$$

где

$$c_1(a,s) = \max\left(2 + s\ln a, s - 2 + s\ln a\right), \quad c_2(a,s) = \max\left(e(a^s+1), (a+2)^s\right).$$

Отсюда вытекает утверждение теоремы. □

4. Заключение

В данной работе методом, который можно назвать методом параметрических множеств, получены две новые асимптотические формулы из теории гиперболической дзета-функции решёток.

Суть метода состоит в том, что для оценки числа точек решётки в некоторой области находится система вложенных множеств, параметризованная параметром, изменяющимся от -1 до 0, при этом при нулевом значении параметра имеем исходное множество. Так как при крайних значениях параметра имеем оценки сверху и снизу, то объем одного из множеств в точности равен искому числу точек, а объем исходного множества задает главный член.

Данный метод позволил найти новые формы для главного члена асимптотических формул, отличный от работ [19] и [26] с более точной оценкой остаточного члена.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бахвалов Н. С. О приближенном вычислении кратных интегралов // Вестн. Моск. ун-та, 1959. № 4. С. 3–18.

2. Боревич З.И., Шафаревич И.Р. Теория чисел. М.: Наука, 1985.

3. С. С. Демидов, Е. А. Морозова, В. Н. Чубариков, И. Ю. Реброва, И. Н. Балаба, Н. Н. Добровольский, Н. М. Добровольский, Л. П. Добровольская, А. В. Родионов, О. А. Пихтилькова Теоретико-числовой метод в приближенном анализе // Чебышевский сборник 2017 Т. 18, вып. 4(64). С. 6–85.

4. Л. П. Добровольская, М. Н. Добровольский, Н. М. Добровольский, Н. Н. Добровольский Многомерные теоретико-числовые сетки и решётки и алгоритмы поиска оптимальных коэффициентов / Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2012. — 283 с. http://elibrary.ru/item.asp? id=20905960

5. Л. П. Добровольская, М. Н. Добровольский, Н. М. Добровольский, Н. Н. Добровольский Гиперболические дзета-функции сеток и решёток и вычисление оптимальных коэффициентов // Чебышевский сборник 2012. Т. 13, вып. 4(44). С. 4–107.

6. Добровольская Л. П., Добровольский Н. М., Добровольский Н. Н., Огородничук Н. К., Ребров Е. Д., Реброва И. Ю. Некоторые вопросы теоретико-числового метода в приближенном анализе // Труды X международной конференции «Алгебра и теория чисел: современные проблемы и приложения» Ученые записки Орловского государственного университета. 2012. № 6. Часть 2. С. 90–98.

7. Л. П. Добровольская, М. Н. Добровольский, Н. М. Добровольский, Н. Н. Добровольский, И. Ю. Реброва Некоторые вопросы теоретико-числового метода в приближенном анализе // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика, 13:4(2) (2013), 47–52.

8. Добровольский М. Н. Ряды Дирихле с периодическими коэффициентами и функциональное уравнение для гиперболической дзета-функции целочисленных решёток. // Чебышевский сборник 2006. Т. 3, вып. 2(4). С. 43–59.

9. Добровольский М. Н. Функциональное уравнение для гиперболической дзета-функции целочисленных решёток. // ДАН. Т. 412, № 3, Январь 2007. С. 302–304.

10. Добровольский М. Н. Функциональное уравнение для гиперболической дзета-функции целочисленных решёток // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. 2007. № 3. С. 18–23.

11. Добровольский Н. М. Гиперболическая дзета функция решёток. / Деп. в ВИНИТИ 24.08.84, N 6090–84.

12. Добровольский Н. М. О квадратурных формулах на классах $E_s^\alpha(c)$ и $H_s^\alpha(c)$. / Деп. в ВИНИТИ 24.08.84, N 6091–84.

13. Добровольский Н. М. Теоретико–числовые сетки и их приложения. / Дис. ... канд. физ.–мат. наук. Тула, 1984.

14. Добровольский Н. М. Теоретико–числовые сетки и их приложения: / Автореф. дис. ... канд. физ.–мат. наук. Москва, 1985.

15. Добровольский Н. М. Теоретико–числовые сетки и их приложения // Теория чисел и ее приложения: Тез. докл. Всесоюз. конф. Тбилиси, 1985. С. 67–70.

16. Добровольский Н. М. Многомерные теоретико-числовые сетки и решётки и их приложения / Н. М. Добровольский. — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2005.

17. Н. М. Добровольский О современных проблемах теории гиперболической дзета-функции решёток // Чебышевский сб. 2015. Т. 16, вып. 1. С. 176–190.

18. Добровольский Н. М., Ванькова В. С. О гиперболической дзета-функции алгебраических решёток. // Теория чисел и ее приложения: Тез. докл. республик. конф. Ташкент, 1990. С. 22.

19. Добровольский Н. М., Ванькова В. С., Козлова С. Л. Гиперболическая дзета-функция алгебраических решёток. / Деп. в ВИНИТИ 12.04.90, N 2327–В90.

20. Н. М. Добровольский, Н. Н. Добровольский, В. Н. Соболева, Д. К. Соболев, Л. П. Добровольская, О. Е. Бочарова О гиперболической дзета-функции Гурвица // Чебышевский сб., 2016. Т. 17, вып. 3. С. 72–105.

21. Н. М. Добровольский, Н. Н. Добровольский, В. Н. Соболева, Д. К. Соболев, Е. И. Юшина Гиперболическая дзета-функция решётки квадратичного поля // Чебышевский сб., 2015. Т. 16, вып. 4. С. 100–149.

22. Добровольский Н. М., Реброва И. Ю., Рощеня А. Л. Непрерывность гиперболической дзета-функции решеток // Мат. заметки. Т. 63, вып. 4. 1998. С. 522–526.

23. Добровольский Н. М., Рощеня А. Л. О числе точек решётки в гиперболическом кресте // Алгебраические, вероятностные, геометрические, комбинаторные и функциональные методы в теории чисел: Сб. тез. докл. II Междунар. конф. Воронеж, 1995. С. 53.

24. Добровольский Н. М., Рощеня А. Л. Об аналитическом продолжении гиперболической дзета-функции рациональных решёток // Современные проблемы теории чисел и ее приложения: Сб. тез. докл. III Междунар. конф. Тула, 1996. С. 49.

25. Добровольский Н. М., Рощеня А. Л. О непрерывности гиперболической дзета-функции решёток // Изв. Тул. гос. ун-та. Сер. Математика. Механика. Информатика. Т. 2, вып. 1. Тула: Изд–во ТулГУ, 1996. С. 77–87.

26. Добровольский Н. М., Рощеня А. Л. О числе точек решётки в гиперболическом кресте // Мат. заметки. Т. 63. Вып. 3. 1998. С. 363–369.

27. Добровольский Н. Н. О числе целых точек в гиперболическом кресте при значениях параметра $1 \leqslant t < 21$ // Известия ТулГУ. Сер. Математика. Механика. Информатика. 2003. Т. 9, вып.1. С. 91–95.

28. Коробов Н. М. О приближенном вычислении кратных интегралов // ДАН СССР. 1959. Т. 124, № 6. С. 1207–1210.

29. Коробов Н. М. Вычисление кратных интегралов методом оптимальных коэффициентов // Вестн. Моск. ун-та, 1959. № 4. С. 19–25.

30. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. / М.: Физмат-гиз, 1963.

31. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. (второе издание) / М.: МЦНМО, 2004.

32. Реброва И. Ю. Непрерывность гиперболической дзета-функции решёток Тез. докл. III Междунар. конф. // Современные проблемы теории чисел: Тула: Изд-во ТГПУ, 1996. С. 119.

33. Реброва И. Ю. Непрерывность обобщенной гиперболической дзета-функции решёток и ее аналитическое продолжение // Изв. ТулГУ. Сер. Механика. Математика. Информатика. Тула, 1998. Т.4. Вып.3. С. 99–108.

34. Реброва И. Ю., Добровольский Н. М., Добровольский Н. Н., Балаба И. Н., Есаян А. Р., Басалов Ю. А. Теоретико-числовой метод в приближённом анализе и его реализация в ПОИВС «ТМК»: Моногр. В 2 ч. / Под. ред. Н. М. Добровольского. — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2016. – Ч. I. – 232 с.

35. Фролов К. К. Оценки сверху погрешности квадратурных формул на классах функций // ДАН СССР. 231. 1976. № 4. С. 818 — 821.

36. Фролов К. К. Квадратурные формулы на классах функций. / Дис. ... канд. физ.-мат. наук. М.: ВЦ АН СССР. 1979.

37. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974. 188 с.

38. L. P. Dobrovolskaya, M. N. Dobrovolsky, N. M. Dobrovol'skii, N. N. Dobrovolsky. On Hyperbolic Zeta Function of Lattices. In: Continuous and Distributed Systems. Solid Mechanics and Its Applications. Vol. 211. 2014. P. 23–62. DOI:10.1007/978-3-319-03146-0_2.

39. Hua Loo Keng, Wang Yuan Applications of Number Theory to Numerical Analysis, – Springer–Verlag Berlin, 1981.

40. Griebel, M, "Sparse grids for the Schrodinger equation", ESAIM-Mathematical Modelling and Numerical Analysis-Modelisation Mathematique et Analyse Numerique, 41:2 (2007), 215

41. Adcock B., "Multivariate Modified Fourier Series and Application to Boundary Value Problems", Numer. Math., 115:4 (2010), 511–552

42. Shen J., Wang L.-L., "Sparse Spectral Approximations of High-Dimensional Problems Based on Hyperbolic Cross", SIAM J. Numer. Anal., 48:3 (2010), 1087–1109

43. Huybrechs D., Iserles A., Norsett S.P., “From High Oscillation to Rapid Approximation IV: Accelerating Convergence”, IMA J. Numer. Anal., 31:2 (2011), 442–468

44. Shen J., Wang L.-L., Yu H., “Approximations By Orthonormal Mapped Chebyshev Functions For Higher-Dimensional Problems in Unbounded Domains”, J. Comput. Appl. Math., 265 (2014), 264–275

45. Chernov A., Duong Pham, “Sparse Tensor Product Spectral Galerkin Bem For Elliptic Problems With Random Input Data on a Spheroid”, Adv. Comput. Math., 41:1 (2015), 77–104

46. Chernov A., Dung D., “New Explicit-in-Dimension Estimates For the Cardinality of High-Dimensional Hyperbolic Crosses and Approximation of Functions Having Mixed Smoothness”, J. Complex., 32:1 (2016), 92–121

47. Luo X., Xu X., Rabitz H., “On the fundamental conjecture of HDMR: a Fourier analysis approach”, J. Math. Chem., 55:2 (2017), 632–660

REFERENCES

1. Bakhvalov, N.S. 1959, “On approximate computation of multiple integrals”, Vestnik Moskovskogo universiteta, no. 4, pp. 3–18.

2. Боревич З.И., Шафаревич И.Р. Теория чисел. М.: Наука, 1985.

3. С. С. Демидов, Е. А. Морозова, В. Н. Чубариков, И. Ю. Реброва, И. Н. Балаба, Н. Н. Добровольский, Н. М. Добровольский, Л. П. Добровольская, А. В. Родионов, О. А. Пихтилькова Теоретико-числовой метод в приближенном анализе // Чебышевский сборник 2017 Т. 18, вып. 4(64). С. 6–85.

4. Л. П. Добровольская, М. Н. Добровольский, Н. М. Добровольский, Н. Н. Добровольский Многомерные теоретико-числовые сетки и решётки и алгоритмы поиска оптимальных коэффициентов / Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2012. — 283 с. http://elibrary.ru/item.asp? id=20905960

5. Dobrovol’skaja L. P., Dobrovol’skij M. N., Dobrovol’skij N. M., Dobrovol’skij N. N., 2012, "Giperbolicheskie dzeta-funkcii setok i reshjotok i vychislenie optimal’nyh kojefficientov" *Chebyshevskii Sbornik* vol 13, №4(44) pp. 4–107.

6. Добровольская Л. П., Добровольский Н. М., Добровольский Н. Н., Огородничук Н. К., Ребров Е. Д., Реброва И. Ю. Некоторые вопросы теоретико-числового метода в приближенном анализе // Труды X международной конференции «Алгебра и теория чисел: современные проблемы и приложения» Ученые записки Орловского государственного университета. 2012. № 6. Часть 2. С. 90–98.

7. Л. П. Добровольская, М. Н. Добровольский, Н. М. Добровольский, Н. Н. Добровольский, И. Ю. Реброва Некоторые вопросы теоретико-числового метода в приближенном анализе // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика, 13:4(2) (2013), 47–52.

8. Добровольский М. Н. Ряды Дирихле с периодическими коэффициентами и функциональное уравнение для гиперболической дзета-функции целочисленных решёток. // Чебышевский сборник 2006. Т. 3, вып. 2(4). С. 43–59.

9. Dobrovol'skij M. N., 2007, "Funkcional'noe uravnenie dlja giperbolicheskoj dzeta-funkcii celochislennyh reshetok" , *Doklady akademii nauk*, vol 412, № 3, pp. 302–304.

10. Добровольский М. Н. Функциональное уравнение для гиперболической дзета-функции целочисленных решёток // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. 2007. № 3. С. 18–23.

11. Добровольский Н. М. Гиперболическая дзета функция решёток. / Деп. в ВИНИТИ 24.08.84, N 6090–84.

12. Добровольский Н. М. О квадратурных формулах на классах $E_s^\alpha(c)$ и $H_s^\alpha(c)$. / Деп. в ВИНИТИ 24.08.84, N 6091–84.

13. Добровольский Н. М. Теоретико–числовые сетки и их приложения. / Дис. ... канд. физ.–мат. наук. Тула, 1984.

14. Добровольский Н. М. Теоретико–числовые сетки и их приложения: / Автореф. дис. ... канд. физ.–мат. наук. Москва, 1985.

15. Добровольский Н. М. Теоретико–числовые сетки и их приложения // Теория чисел и ее приложения: Тез. докл. Всесоюз. конф. Тбилиси, 1985. С. 67–70.

16. Добровольский Н. М. Многомерные теоретико-числовые сетки и решётки и их приложения / Н. М. Добровольский. — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2005.

17. Н. М. Добровольский О современных проблемах теории гиперболической дзета-функции решёток // Чебышевский сб. 2015. Т. 16, вып. 1. С. 176–190.

18. Добровольский Н. М., Ванькова В. С. О гиперболической дзета-функции алгебраических решёток. // Теория чисел и ее приложения: Тез. докл. республик. конф. Ташкент, 1990. С. 22.

19. Добровольский Н. М., Ванькова В. С., Козлова С. Л. Гиперболическая дзета-функция алгебраических решёток. / Деп. в ВИНИТИ 12.04.90, N 2327–В90.

20. Dobrovolsky N. M., Dobrovolsky N. N., Soboleva V. N., Sobolev D. K., Dobrovol'skaya L. P., Bocharova O. E., 2016, "On hyperbolic Hurwitz zeta function" , *Chebyshevskii Sbornik*, vol 17, № 3 pp. 72–105.

21. Н. М. Добровольский, Н. Н. Добровольский, В. Н. Соболева, Д. К. Соболев, Е. И. Юшина Гиперболическая дзета-функция решётки квадратичного поля // Чебышевский сб., 2015. Т. 16, вып. 4. С. 100–149.

22. Добровольский Н. М., Реброва И. Ю., Рощеня А. Л. Непрерывность гиперболической дзета-функции решеток // Мат. заметки. Т. 63, вып. 4. 1998. С. 522–526.

23. Добровольский Н. М., Рощеня А. Л. О числе точек решётки в гиперболическом кресте // Алгебраические, вероятностные, геометрические, комбинаторные и функциональные методы в теории чисел: Сб. тез. докл. II Междунар. конф. Воронеж, 1995. С. 53.

24. Добровольский Н. М., Рощеня А. Л. Об аналитическом продолжении гиперболической дзета-функции рациональных решёток // Современные проблемы теории чисел и ее приложения: Сб. тез. докл. III Междунар. конф. Тула, 1996. С. 49.

25. Добровольский Н. М., Рощеня А. Л. О непрерывности гиперболической дзета-функции решёток // Изв. Тул. гос. ун-та. Сер. Математика. Механика. Информатика. Т. 2, вып. 1. Тула: Изд–во ТулГУ, 1996. С. 77–87.

26. Добровольский Н. М., Рощеня А. Л. О числе точек решётки в гиперболическом кресте // Мат. заметки. Т. 63. Вып. 3. 1998. С. 363–369.

27. Добровольский Н. Н. О числе целых точек в гиперболическом кресте при значениях параметра $1 \leqslant t < 21$ // Известия ТулГУ. Сер. Математика. Механика. Информатика. 2003. Т. 9, вып.1. С. 91–95.

28. Коробов Н. М. О приближенном вычислении кратных интегралов // ДАН СССР. 1959. Т. 124, № 6. С. 1207–1210.

29. Коробов Н. М. Вычисление кратных интегралов методом оптимальных коэффициентов // Вестн. Моск. ун-та, 1959. № 4. С. 19–25.

30. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. / М.: Физмат-гиз, 1963.

31. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. (второе издание) / М.: МЦНМО, 2004.

32. Реброва И. Ю. Непрерывность гиперболической дзета-функции решёток Тез. докл. III Междунар. конф. // Современные проблемы теории чисел: Тула: Изд-во ТГПУ, 1996. С. 119.

33. Реброва И. Ю. Непрерывность обобщенной гиперболической дзета-функции решёток и ее аналитическое продолжение // Изв. ТулГУ. Сер. Механика. Математика. Информатика. Тула, 1998. Т.4. Вып.3. С. 99–108.

34. Реброва И. Ю., Добровольский Н. М., Добровольский Н. Н., Балаба И. Н., Есаян А. Р., Басалов Ю. А. Теоретико-числовой метод в приближённом анализе и его реализация в ПОИВС «ТМК»: Моногр. В 2 ч. / Под. ред. Н. М. Добровольского. — Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2016. – Ч. I. – 232 с.

35. Фролов К. К. Оценки сверху погрешности квадратурных формул на классах функций // ДАН СССР. 231. 1976. № 4. С. 818 — 821.

36. Фролов К. К. Квадратурные формулы на классах функций. / Дис. ... канд. физ.-мат. наук. М.: ВЦ АН СССР. 1979.

37. Chandrasekharan K., 1974, *Vvedenie v analiticheskuju teoriju chisel*, Izd-vo Mir, Moskva, 188 p.

38. Dobrovolskaya L. P., Dobrovolsky M. N., Dobrovol'skii N. M., Dobrovolsky 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.

39. Hua Loo Keng, Wang Yuan Applications of Number Theory to Numerical Analysis, – Springer–Verlag Berlin, 1981.

40. Griebel, M, "Sparse grids for the Schrodinger equation", ESAIM-Mathematical Modelling and Numerical Analysis-Modelisation Mathematique et Analyse Numerique, 41:2 (2007), 215

41. Adcock B., "Multivariate Modified Fourier Series and Application to Boundary Value Problems", Numer. Math., 115:4 (2010), 511–552

42. Shen J., Wang L.-L., “Sparse Spectral Approximations of High-Dimensional Problems Based on Hyperbolic Cross”, SIAM J. Numer. Anal., 48:3 (2010), 1087–1109

43. Huybrechs D., Iserles A., Norsett S.P., “From High Oscillation to Rapid Approximation IV: Accelerating Convergence”, IMA J. Numer. Anal., 31:2 (2011), 442–468

44. Shen J., Wang L.-L., Yu H., “Approximations By Orthonormal Mapped Chebyshev Functions For Higher-Dimensional Problems in Unbounded Domains”, J. Comput. Appl. Math., 265 (2014), 264–275

45. Chernov A., Duong Pham, “Sparse Tensor Product Spectral Galerkin Bem For Elliptic Problems With Random Input Data on a Spheroid”, Adv. Comput. Math., 41:1 (2015), 77–104

46. Chernov A., Dung D., “New Explicit-in-Dimension Estimates For the Cardinality of High-Dimensional Hyperbolic Crosses and Approximation of Functions Having Mixed Smoothness”, J. Complex., 32:1 (2016), 92–121

47. Luo X., Xu X., Rabitz H., “On the fundamental conjecture of HDMR: a Fourier analysis approach”, J. Math. Chem., 55:2 (2017), 632–660

Получено 04.07.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 512.54 DOI 10.22405/2226-8383-2018-19-3-135-147

О проблеме обобщённой сопряжённости слов в обобщённых древесных структурах групп Кокстера

Безверхний Владимир Николаевич — доктор физико-математических наук, профессор, профессор кафедры высшей математики Академии гражданской защиты МЧС России.
e-mail: Vnbezv@rambler.ru

Добрынина Ирина Васильевна — доктор физико-математических наук, доцент, профессор кафедры алгебры, математического анализа и геометрии Тульского государственного педагогического университета имени Л. Н. Толстого.
e-mail: dobrynirina@yandex.ru

Аннотация

Основными алгоритмическими проблемами теории групп являются проблемы равенства, сопряжённости слов и проблема изоморфизма групп.

В силу неразрешимости данных проблем в классе конечно определенных групп, основные алгоритмические проблемы и их различные обобщения исследуются в конкретных группах.

Группы Кокстера изучаются с 1934 года, а в алгебраическом аспекте – с 1962 года. В них алгоритмически разрешимы проблемы равенства и сопряжённости слов, однако неразрешима проблема вхождения.

В 1983 году К. Аппель и П. Шупп определили класс групп Кокстера экстрабольшого типа. В 2003 году В. Н. Безверхний ввел в рассмотрение группы Кокстера с древесной структурой.

В статье рассматриваются обобщённые древесные структуры групп Кокстера, представляющие собой древесные произведения групп Кокстера экстрабольшого типа и групп Кокстера с древесной структурой.

Обобщённые древесные структуры групп Кокстера, также как группы Кокстера экстрабольшого типа и группы Кокстера с древесной структурой, относятся к гиперболическим группам, поэтому в них решено большинство алгоритмических проблем, в частности, алгоритмически разрешима проблема обобщённой сопряжённости слов.

Авторами статьи предлагается оригинальный метод доказательства алгоритмической разрешимости проблемы обобщённой сопряжённости слов в обобщённых древесных структурах групп Кокстера. Данный метод использует подход Г. С. Маканина, примененный им для доказательства конечной порождённости нормализатора элемента в группах кос. Кроме того, в данной работе показывается, что централизатор конечно порождённой подгруппы в обобщённой древесной структуре групп Кокстера конечно порождён и существует алгоритм, выписывающий его образующие.

Ключевые слова: алгоритмические проблемы, группа Кокстера, обобщённая сопряжённость, древесное произведение групп, централизатор.

Библиография: 21 название.

Для цитирования:
В. Н. Безверхний, И. В. Добрынина О проблеме обобщённой сопряжённости слов в обобщённых древесных структурах групп Кокстера // Чебышевский сборник, 2018, т. 19, вып. 3, с. 135–147.

CHEBYSHEVSKII SBORNIK

Vol. 19. No. 3.

UDC 512.54 DOI 10.22405/2226-8383-2018-19-3-135-147

On problem of generalized conjugation of words in a generalized tree structures of Coxeter groups

Bezverkhnii Vladimir Nikolaevich — doctor of physico-mathematical Sciences, Professor, Professor of the Department of mathematics of civil defence Academy EMERCOM of Russia.
e-mail: Vnbezv@rambler.ru

Dobrynina Irina Vasiljevna — doctor of physico-mathematical Sciences, associate professor, Professor of the Department of algebra, mathematical analysis and geometry of Tula State Lev Tolstoy University.
e-mail: dobrynirina@yandex.ru

Abstract

The main algorithmic problems of group theory are the problems of words, conjugacy of words and the problem of isomorphism of groups.

This algorithmic problems in the class of finitely presented groups are unsolvable. So the main algorithmic problems and their various generalizations are studied in certain classes of groups.

Coxeter groups have been studied since 1934, and in the algebraic aspect - since 1962.

The problems of words and conjugacy of words are algorithmically solvable in these groupss but the problem of occurrence is unsolvable. K. Appel and P. Schupp defined the class of Coxeter groups extra- large type in 1983. V. N. Bezverhny defined the Coxeter groups with a tree structure in 2003.

The article discusses the generalized tree structures of Coxeter groups, which are the tree product of Coxeter groups of extra large type and Coxeter groups with a tree structure.

The generalized tree structure of Coxeter groups, as well as the Coxeter group of extra large type, and a Coxeter group with a tree structure, refer to hyperbolic groups, so most of algorithmic problems algorithmically solvable, in particular, the problem of generalized conjugacy of words.

The authors propose In this paper an original method for proving algorithmic solvable of the problem of generalized conjugacy of words in tree structures of Coxeter groups. This method uses G. S. Makanin's approach applied by Him to prove the finite generation of the normalizer of an element in braid groups. In addition, in this paper we show that the centralizer of a finitely generated subgroup in a generalized wood structure of Coxeter groups is finitely generated and there is an algorithm writing out its generators.

Keywords: algorithmic problems, Coxeter group, generalized conjugation, tree product of groups, centralizer.

Bibliography: 21 titles.

For citation:
V. N. Bezverkhnii, I. V. Dobrynina, 2018, "On problem of generalized conjugation of words in a generalized tree structures of Coxeter groups" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 135–147.

1. Введение

М. Дэном [1] в начале прошлого века сформулировал основные алгоритмические проблемы теории групп: проблемы равенства, сопряжённости слов и проблему изоморфизма групп в конечно определенных группах.

Доказательство П. С. Новиковым [2] неразрешимости основных алгоритмических проблем в классе конечно определенных групп привело к изучению алгоритмических проблем в конкретных группах.

Пусть G – конечно порождённая группа Кокстера с копредставлением

$$G = \langle a_1, \ldots, a_n;\ (a_i a_j)^{m_{ij}}, i, j = \overline{1,n} \rangle,$$

где m_{ij} – элементы симметрической матрицы Кокстера:

$$m_{ii} = 1,\ m_{ij} \in \mathbb{N} \setminus \{1\} \cup \{\infty\}, i, j = \overline{1,n},\ i \neq j.$$

Если $m_{ij} = \infty$, то определяющее соотношение между образующими a_i, a_j отсутствует. Данное определение дает $a_i^2 = 1$ для всех $i \in J$.

Известно [3], что всякая группа отражений является группой Кокстера, если в качестве образующих взять отражения относительно гиперплоскостей, ограничивающих ее фундаментальный многогранник.

Ж. Титс [4] доказал алгоритмическую разрешимость проблемы равенства слов в группах Кокстера.

П. Шуппом [5] показана неразрешимость проблемы вхождения в группах Кокстера.

К. Аппель и П. Шупп [6] в 1983 году решили проблему сопряжённости слов в классе групп Кокстера экстрабольшого типа.

В настоящее время проблема сопряжённости слов решена в классе групп Кокстера [7].

В. Н. Безверхний ввел в расмотрение группы Кокстера с древесной структурой. Очевидно, что в графе, соответствующем группе Кокстера, всегда выделяется максимальный подграф, соответствующий группе Кокстера с древесной структурой [8].

В статье рассматриваются обобщённые древесные структуры групп Кокстера, представляющие собой древесные произведения групп Кокстера экстрабольшого типа и групп Кокстера с древесной структурой.

Обобщённые древесные структуры групп Кокстера, также как группы Кокстера экстрабольшого типа и группы Кокстера с древесной структурой, относятся к гиперболическим группам, поэтому в них решено большинство алгоритмических проблем (например, [9]), в частности, алгоритмически разрешима проблема обобщённой сопряжённости слов [10].

Авторами статьи предлагается оригинальный метод доказательства алгоритмической разрешимости проблемы обобщённой сопряжённости слов в обобщённых древесных структурах групп Кокстера. Данный метод использует подход Г. С. Маканина [11], примененный им для доказательства конечной порождённости нормализатора элемента в группах кос, и технику В. Н. Безверхнего [12]. Кроме того, в данной работе показывается, что централизатор конечно порождённой подгруппы в обобщённой древесной структуре групп Кокстера конечно порождён и существует алгоритм, выписывающий его образующие.

2. Централизатор конечно порождённой подгруппы

Рассмотрим конечно порождённую группу Кокстера, заданную копредставлением

$$G = \langle a_1, \ldots, a_n;\ (a_i a_j)^{m_{ij}}, i, j = \overline{1,n} \rangle,$$

где m_{ij} – элементы симметрической матрицы Кокстера:

$$m_{ii} = 1,\ m_{ij} \in \mathbb{N} \setminus \{1\} \cup \{\infty\}, i, j = \overline{1,n},\ i \neq j.$$

В случае $m_{ij} = \infty$ определяющего соотношения между образующими a_i, a_j нет.

Известно, что в группах Кокстера разрешима проблемы равенства и сопряжённости слов. Обобщением проблемы сопряжённости слов является проблема обобщённой сопряжённости слов.

Определение 1. *Будем говорить, что в группе G разрешима проблема обобщённой сопряжённости слов, если существует алгоритм, позволяющий для любых двух конечных множеств слов $\{w_i\}_{i=\overline{1,n}}$, $\{v_i\}_{i=\overline{1,n}}$ из G установить, существует ли такое $z \in G$, что $\&_{i=1}^{n}(z^{-1}w_iz = v_i)$.*

Группа Кокстера называется группой Кокстера экстрабольшого типа, если $m_{ij} > 3$ для любых $i \neq j$. Данный класс групп в 1983 году выделен К. Аппелем и П. Шуппом.

Для всякой группы Кокстера G можно построить граф Γ такой, что образующим a_i соответствуют вершины графа Γ, а каждому определяющему соотношению $(a_ia_j)^{m_{ij}} = 1$ – ребро, соединяющее a_i и a_j, $i \neq j$. Если при этом получится дерево-граф Γ, то группа G называется группой Кокстера с древесной структурой.

Данный класс групп введен в рассмотрение В. Н. Безверхним в 2003 году.

Группа Кокстера с древесной структурой может быть представлена как свободное произведение двупорождённых групп Кокстера, объединенных по конечным циклическим подгруппам: от графа Γ группы G перейдем к графу $\overline{\Gamma}$ так, что вершинам графа $\overline{\Gamma}$ поставим в соответствие группы Кокстера на двух образующих $G_{ij} = \langle a_i, a_j; a_i^2, a_j^2, (a_ia_j)^{m_{ij}}\rangle$, а всякому ребру $\overline{e}$, соединяющему вершины, соответствующие G_{ij} и G_{jk} – циклическую подгруппу $\langle a_j; a_j^2\rangle$.

Рассмотрим группу Кокстера

$$G = \langle \prod_{s=1}^{t} * G_s; a_{i_m} = a_{j_l}, i \neq j, i, j \in \{\overline{1,t}\}\rangle,$$

представляющую собой древесное произведение групп Кокстера G_s, где G_s либо группа Кокстера с древесной структурой, либо группа Кокстера экстрабольшого типа, запись $a_{i_m} = a_{j_l}$ означает, что объединение групп Кокстера G_i и G_j ведется по циклической подгруппе второго порядка $\langle a_{i_m}; a_{i_m}^2\rangle$ ($\langle a_{j_l}; a_{j_l}^2\rangle$), где a_{i_m} – некоторый образующий группы G_i, a_{j_l} – некоторый образующий группы G_j.

Такую группу Кокстера G будем называть обобщённой древесной структурой групп Кокстера.

Введем ряд понятий, следуя работе [13].

Пусть $F_i = \langle a_i; a_i^2\rangle$, $F = \prod_{i=1}^{n} * F_i$ – свободное произведение циклических групп порядка 2. Отождествим каждый образующий a_i группы F с его обратным a_i^{-1}. Слово $w = a_{i_1} \dots a_{i_n}$ группы F является приведенным, если индексы рядом стоящих букв a_{i_j} и $a_{i_{j+1}}$ записи w различны, длина w равна n. Далее считаем, что $i \neq j$, $m_{ij} < \infty$. Обозначим через F_{ij} группу $F_{ij} = F_i * F_j$.

Обозначим через R_{ij} множество всех нетривиальных слов, циклически приведенных в свободном произвдении F_{ij} и равных 1 в группе G_{ij}.

В дальнейшем под R будем понимать $R = \bigcup\limits_{i,j\in\{\overline{1,n}\}} R_{ij}$ – симметризованное подмножество свободного произведения F.

Пусть w – нетривиальное циклически приведенное в F слово, равное 1 в G, то есть $w \in \langle R\rangle^F$, где $\langle R\rangle^F$ – нормальное замыкание симметризованного множества R в свободном произведении F. Тогда из теоремы ван Кампена [14] следует, что существует R-диаграмма M с граничным циклом $\gamma = \partial M$, меткой которого является слово w, $\varphi(\gamma) = w$, и с метками областей $D \subset M$ из R_{ij}. Будем называть такую R-диаграмму M R-диаграммой M над G, а ее области – R_{ij}-диаграммами.

Подвергнем R-диаграмму M следующему преобразованию.

Если две области D_1, D_2 являются одновременно R_{ij}-диаграммами, пересекаются по ребру с меткой $\varphi(\partial D_1 \cap \partial D_2)$, то, стирая это ребро, объединим D_1, D_2 в одну область D. Допустим, что каждая из областей D_1, D_2 есть R_{ij}-диаграмма, D_1, D_2 пересекаются по вершине. Тогда объединяем D_1, D_2 в одну область D. Если в том или другом случае метка границы полученной области равна единице в свободном произведении F, то, удалив эту область, склеиваем ее границу. Таким образом, через конечное число шагов мы получим приведенную в F односвязную R-диаграмму M, инвариантную относительного рассмотренного преобразования с граничной меткой, равной w, причем если две области D', D'' из M пересекаются по ребру, то длина метки этого ребра равна единице.

Аналогично рассматриваются кольцевые R-диаграммы над G.

Область $D \subset M$ назовем граничной, если $\partial M \cap \partial D \neq \emptyset$. Символами $i(D)$ будем обозначать число внутренних ребер в граничном цикле D, $d(D)$ – число ребер в граничном цикле D.

Область D с граничным циклом $\partial D = e\gamma e^{-1}\delta$, расположенная по обе стороны относительно ребра e, в которой склеенные ребра e и e^{-1} пересекают граничный цикл D, называется $(s-i)$-областью.

Будем говорить, что $\partial D \cap \partial M$ – правильная часть M, если $\partial D \cap \partial M$ есть объединение последовательности $l_1, l_2, \ldots, l_n$ замкнутых ребер, где $l_1, \ldots, l_n$ встречаются в данном порядке в некотором граничном цикле для D и в некотором граничном цикле для M.

Граничную область D R-диаграммы M назовем простой или правильной, если $\partial D \cap \partial M$ есть правильная часть.

Определение 2. *Простая область D R-диаграммы M называется деновской, если $i(D) < d(D)/2$.*

Определение 3. *Удаление деновской области R-диаграммы M, то есть удаление ее граничного пути, называется деновским сокращением R-диаграммы M или R - сокращением.*

R-диаграмма M является R-приведенной, если в M выполнены все деновские сокращения.

Слово $w \in G$ назовем R-приводимым (R-сократимым), если w приведено в F и содержит подслово s, являющееся подсловом некоторого соотношения $r \in R$, $r = sb$, где $|b| < |s|$.

Определение 4. *Поддиаграмма $\Pi = \bigcup\limits_{i=1}^{n} D_i$ образует полосу в R-приведенной R-диаграмме M с граничным циклом $\partial M = \gamma \cup \delta$, если*

1. $\partial D_i \cap \partial D_{i+1} = e_i$, $i = \overline{1, n-1}$, *где e_i – ребро ;*
2. $\partial D_i \cap \gamma = \gamma_i$, $i = \overline{1, n}$, *где γ_i – связный путь, причем $|\gamma_i| \geqslant 1$;*
3. $|\partial D_1 \cap \gamma| = |\partial D_1 \backslash (\partial D_1 \cap \gamma)|$ *и* $|\partial D_n \cap \gamma| = |\partial D_n \backslash (\partial D_n \cap \gamma)|$;
4. $|\partial D_j \cap \gamma| + 2 = |\partial D_j \backslash (\partial D_j \cap \gamma)|$, $j = \overline{2, n-1}$.

Определение 5. *Пусть Π – полоса R-диаграммы M. Замену R-диаграммы M на R-диаграмму M_1, полученную из M удалением полосы Π, назовем $\overline{R}$-сокращением.*

R-приведенное слово w группы G назовем $\overline{R}$-приводимым ($\overline{R}$-сократимым), если в нем можно выделить подслово $s_1 s_2 \cdots s_n$, где каждое s_t содержится в некоторой группе G_{ij} и является подсловом соотношения $s_t^{-1} d_t^{-1} b_t d_{t+1} \in R$, причем при $1 \le t \le n \quad |d_t| = |d_{t+1}| = 1$, $|s_t| = |b_t| + 2$ и для t, $1 < t < n$, $|b_t| = |s_t|$.

Теорема 1. *Существует алгоритм, позволяющий для любого циклически приведенного слова w группы Кокстера G выяснить, является ли w R-приведенным.*

Существует алгоритм, позволяющий для любого циклически приведенного слова w группы Кокстера G выяснить, является ли w $\overline{R}$-приведенным.

Доказательство очевидно.

Определение 6. *Приведенную связную кольцевую R-диаграмму M с границей $\partial M = \sigma \cup \tau$ будем называть однослойной, если*

1) M состоит из областей $D_1, D_2, \ldots, D_m$, где $D_j \cap D_{j+1} = e_j$, $j = \overline{1, m-1}$, $D_1 \cap D_m = e_m$, $D_j \cap \sigma \ne \emptyset$, $D_j \cap \tau \ne \emptyset$, $j = \overline{1, m}$, e_j – ребро,

или

2) $M = (\bigcup\limits_{i=1}^{p} N_i) \cup (\bigcup\limits_{j=1}^{p} \gamma_j)$, N_i – поддиаграммы (диски) в M с границами

$$\partial N_i = \sigma_i \cup \tau_i, \sigma_i \cap \tau_i = \{A_i, B_i\}$$

– вершины, $i = \overline{1, p}$, γ_i – простые пути с концами $B_{i-1}, A_i, i = \overline{2, p}$, простой путь γ_1 имеет начало B_p, а конец – A_1, где каждое N_i из состоит из областей $D_{i_1}, D_{i_2}, \ldots, D_{i_{m_i}}$, причем $D_{i_j} \cap D_{i_{j+1}} = e_{i_j}, j = \overline{1, m_i - 1}, D_{i_j} \cap \sigma \ne \emptyset, D_{i_j} \cap \tau \ne \emptyset, j = \overline{1, m_i}$, e_{i_j} – ребро.

Из данного определения имеем, что в случае 1) все области M граничные, каждая пара соседних областей, взятых в циклической последовательности, пересекается по ребру, каждая область пересекает и σ, и τ (пересечением может быть вершина, одно или несколько ребер). В случае 2) имеем простую кольцевую R-диаграмму, то есть R-диаграмму, в которой $\sigma \cap \tau \ne \emptyset$. Пути γ_i, по которым пересекаются σ, τ, отделяют поддиаграммы (диски), причем заметим, что эти пути, в том числе, могут иметь нулевую длину (быть вершиной).

Аналогично определяются односвязные однослойные R-диаграммы:

Определение 7. *Приведенную односвязную R-диаграмму M с границей $\partial M = \sigma \cup \tau$ будем называть однослойной, если*

1) M состоит из областей $D_1, D_2, \ldots, D_m$, где $D_j \cap D_{j+1} = e_j$, $j = \overline{1, m-1}$, $D_j \cap \sigma \ne \emptyset$, $D_j \cap \tau \ne \emptyset$, $j = \overline{1, m}$, e_j – ребро,

или

2) $M = (\bigcup\limits_{i=1}^{p} N_i) \cup (\bigcup\limits_{j=1}^{p-1} \gamma_j)$, N_i – поддиаграммы (диски) в M с границами

$$\partial N_i = \sigma_i \cup \tau_i, \sigma_i \cap \tau_i = \{A_i, B_i\}$$

– вершины, $i = \overline{1, p}$, γ_i – простые пути с концами $B_{i-1}, A_i, i = \overline{2, p}$, где каждое N_i из состоит из областей $D_{i_1}, D_{i_2}, \ldots, D_{i_{m_i}}$, причем $D_{i_j} \cap D_{i_{j+1}} = e_{i_j}$, $j = \overline{1, m_i - 1}$, $D_{i_j} \cap \sigma \ne \emptyset$, $D_{i_j} \cap \tau \ne \emptyset$, $j = \overline{1, m_i}$, e_{i_j} – ребро.

Лемма 1. *[13] Пусть M – приведенная односвязная R-диаграмма равенства R и $\overline{R}$-несократимых слов $w, v \in G$ над группой Кокстера G. Тогда M является однослойной.*

Пусть M – приведенная связная кольцевая R-диаграмма сопряжённости слов $\varphi(\sigma)$, $\varphi(\tau) \in G$ над группой Кокстера G, не содержащая $(s-i)$-областей; σ, τ – соответственно внешний и внутренний граничный циклы M, слова $\varphi(\sigma)$, $\varphi(\tau)$ циклически R и $\overline{R}$-несократимы. Тогда M является однослойной.

Определение 8. *Кольцевую связную приведенную однослойную R-диаграмму M с граничными циклами σ, τ обобщённой древесной структуры групп Кокстера G, метки которой $\varphi(\sigma)$, $\varphi(\tau)$ приведены в F, $\varphi(\sigma)$ – R-приведено и $\overline{R}$-приведено, назовем особо специальной R-диаграммой, если в M существует одна область D такая, что*

$$|\varphi(\partial D \setminus (\partial D \bigcap \sigma))| + 2 = |\varphi(\partial D \setminus (\partial D \bigcap \tau))| (|\varphi(\partial D \setminus (\partial D \bigcap \sigma))| = |\varphi(\partial D \setminus (\partial D \bigcap \tau))| + 2),$$

а для остальных областей D' $|\varphi(\partial D' \setminus (\partial D' \bigcap \sigma))| = |\varphi(\partial D' \setminus (\partial D' \bigcap \tau))|$.

Замену слова $\varphi(\sigma)(\varphi(\tau))$ на слово $\varphi(\tau)(\varphi(\sigma))$ назовем специальным кольцевым R-сокращением.

Определение 9. *Будем говорить, что циклически несократимое слово w обобщённой древесной структуры групп Кокстера G является тупиковым, если w циклически R-несократимо, циклически $\overline{R}$-несократимо и к нему неприменимо специальное кольцевое R-сокращение.*

Лемма 2. *Пусть M – связная приведенная минимальная R - диаграмма над обобщённой древесной структурой групп Кокстера G с граничными циклами σ, τ; $\varphi(\sigma)$, $\varphi(\tau)$ являются тупиковыми. Тогда если $\varphi(\sigma) = x$, то $\varphi(\tau) = y$, где $x, y \in \{a_1, \ldots, a_n\}$, $\{a_i\}_{i=\overline{1,n}}$ – множество образующих группы G.*

Доказательство следует из работ [16] и [15], где также показано, что такие диаграммы состоят из $(s-i)$-областей.

Теорема 2. *Централизатор конечно порождённой подгруппы H обобщённой древесной структуры групп Кокстера G есть конечно порождённая подгруппа и существует алгоритм, выписывающий образующие централизатора.*

Доказательство. Пусть M – кольцевая R-диаграмма, v – произвольная точка, принадлежащая некоторому замкнутому ребру $e \in M$, $e = e'e''$, $e' \bigcap e'' = v$. Тогда замкнутый путь $l \in M$ с начальной и конечной точкой v: $l = e'^{-1}e_1 \ldots e_n t$, где $t = e'$ либо $t = e''^{-1}$, либо $l = e''e'_1 \ldots e'_n t'$, где $t' = e'$ либо $t' = e''^{-1}$, назовем циклическим в M, если l гомотопен τ, соответственно σ. Кратчайший из всех циклических путей кольцевой R-диаграммы M, проходящих через некоторую точку v, принадлежащую ребру e, $e \in M$, назовем циклическим геодезическим путем с началом и концом в v.

Пусть u, v – слова, принадлежащие обобщённой древесной структуре групп Кокстера G. Допустим, что слова u, v являются тупиковыми и сопряжёны в G. Тогда существует кольцевая связная приведенная R-диаграмма с граничными циклами σ, τ, метками которых являются соответственно слова u, v.

Пусть $u = x$, $x \in \{a_i\}_{i=\overline{1,n}}$, $\{a_i\}_{i=\overline{1,n}}$ – множество образующих группы G, тогда из леммы 2 следует, что $v = y$, $y \in \{a_i\}$ $i = \overline{1,n}$ и диаграмма сопряжённости этих слов состоит из $(s-i)$-областей. Пусть $\sigma_0 = \sigma, \sigma_1, \ldots, \sigma_k = \tau$ – граничные циклы R-диаграмм, полученных из $M = M_0$ последовательным удалением $(s-i)$-областей. Но тогда $\varphi(\sigma_i) = x_i$, $x_i \in \{a_i\}_{i=\overline{1,n}}$ и любые два элемента x_{i-1}, x_i, $i = \overline{1,n}$, где $x = x_0$, $x_n = y$ сопряжёны в $G_{x_{i-1}x_i}$ максимальным куском определяющего соотношения группы $G_{x_{i-1}x_i}$. Пусть $m = \max\{m_{ij} < \infty|$, m_{ij} – элементы матрицы Кокстера. Тогда, очевидно, длина любого циклического геодезического пути из M заключена в пределах $|u| \leqslant d \leqslant |u| + 2m$.

Пусть слова u, v не являются образующими G. В этом случае u, v будут метками граничных циклов кольцевой R-диаграммы. По лемме 1 M – однослойная диаграмма, то, используя формулу Р. Линдона [3] о числе площадей в односвязной R-диаграмме, получим что длина d циклического геодезического пути заключена в пределах $|u| \leqslant d \leqslant (|u| + |v|)m + 2$.

Пусть теперь $w_1, w_2, \ldots, w_n$ – образующие H, $H < G$; считаем, что $w_1 = w_{10}$ – тупиковое слово и $\forall i$, $i = \overline{2,n}$, $w_i = c_i w_{i0} c_i^{-1}$, где w_{i0} является тупиковым; $\Delta(w_{i0}, w_{i0})$ – кольцевая связная приведенная R-диаграмма сопряжённости слова w_{i0} слову w_{i0}. Введем обозначения: $c = \max\{|c_1|, \ldots, |c_n|\}$, где $|c_1| = 0$, $L = 2(m_0 + 1)$ и $S(w_i, w_i)$, $i = \overline{1,n}$ – множество слов, длины d_i которых заключены в пределах $|w_{i0}| \leqslant d_i \leqslant 2(|w_{i0}|m + |c| + 1)$.

Рассмотрим следующую последовательность:

$$w_1^{(0)}, \ldots, w_n^{(0)}, H_1, w_1^{(1)}, \ldots, w_n^{(1)}, H_2, \ldots, H_p, w_1^{(p)}, \ldots, w_n^{(p)}, \ldots \tag{1}$$

где $\forall i$, $i = \overline{1,p}$, $H_i^{-1} w_1^{(i-1)} H_i = w_1^{(i)}, \ldots, H_i^{-1} w_n^{(i-1)} H_i = w_n^{(i)}, H_i \in \{a_i\}, w_j^{(s)} \in S(w_j, w_j)$ и является меткой циклического геодезического диаграммы $\Delta(w_{j0}, w_{j0})$, $j = \overline{1,n}, s = \overline{0,p}$, $w_j^{(0)} = c_j w_{j0} c_j^{-1}$.

Последовательность (1) называется базисной. Базисную последовательность (1) назовем фундаментальной, если для $\forall j, s, 0 \leqslant j < s < p$, наборы $(w_1^{(j)}, \ldots, w_n^{(j)})$, $(w_1^{(s)}, \ldots, w_n^{(s)})$ различны и существует целое v, $0 \leqslant v < p$, такое что $w_1^{(v)} = w_1^{(p)}, \ldots, w_n^{(v)} = w_n^{(p)}$.

Лемма 3. *Если последовательность фундаментальная, то слово $H_1 H_2 \ldots H_p H_v^{-1} \ldots H_1^{-1}$ принадлежит централизатору подгруппы H.*

Доказательство очевидно.

Слово $H_1 H_2 \ldots H_p H_v^{-1} \ldots H_1^{-1}$, связанное с фундаментальной последовательностью (1), назовем базисным словом.

Лемма 4. *Если последовательность (1) является фундаментальной базисной последовательностью, то*

$$p \leqslant |S| = |S(w_1, w_1)| \ldots |S(w_n, w_n)|$$

Лемма 5. *Число фундаментальных базисных последовательностей конечно.*

Доказательство очевидно.

Лемма 6. *Пусть $F \in \mathbb{C}_G(H)$, $\mathbb{C}_G(H)$ – централизатор H в G. Тогда существует разбиение F в произведение образующих $F = H_1 H_2 \ldots H_m$, $H_i \in \{a_i\}$ $i = \overline{1,m}$ и базисная последовательность, связанная с данными разбиением F, то есть*

$$w_1^{(0)}, \ldots, w_n^{(0)}, H_1, w_1^{(1)}, \ldots, w_n^{(1)}, H_2, \ldots, H_m, w_1^{(m)}, \ldots, w_n^{(m)}$$

Доказательство. Пусть $F \in \mathbb{C}_G(H)$, $F \neq 1$, тогда имеет место следующая система соотношений
$F^{-1} w_1 F = w_1$, $c_2 F^{-1} c_2^{-1} w_{20} c_2 F c_2^{-1} = w_{20}, \ldots, c_n F^{-1} c_n^{-1} w_{n0} c_n F c_n^{-1} = w_{n0}$.

Пусть $\forall i, i = \overline{2,n}$, $\exists X_i, Y_i, F_i$ такие, что $F \equiv X_i F_i Y_i$ ($\equiv$ – графическое равенство), $c_i = c_i' X_i^{-1} = c_i'' Y_i$. В результате имеем следующие равенства

$$F^{-1} w_1 F = w_1, c_i'' F_i^{-1} c_i'^{-1} w_{i0} c_i' F_i c_i''^{-1} = w_{i0}, i = \overline{2,n},$$

где каждое из слов $c_i' F_i c_i''^{-1}$ несократимо.

Рассмотрим кольцевые приведенные R — приведенные, $\overline{R}$-приведенные R-диаграммы $\Delta(w_{i0}, w_{i0})$ с граничными циклами $\sigma^{(i0)}$, $\tau^{(i0)}$, где $\varphi(\sigma^{(i0)}) = w_{i0}, \varphi(\tau^{(i0)}) = w_{i0}^{-1}$, $i = \overline{2,n}$ (при $i = 1, w_{10} = w_1$), каждая из которых, соответственно, является диаграммой сопряжённости для i-го соотношения.

Обозначим через $O^{(i0)}$ начальную точку на $\sigma^{(i0)}$ и через $O'^{(i0)}$ – начальную точку на $\tau^{(i0)}$, $i = \overline{1,n}$. Тогда в диаграмме $\Delta(w_{i0}, w_{i0})$, $i = \overline{1,n}$, содержится путь η_i, $\alpha(\eta_i) = O^{(i0)}$,

$\omega(\eta_i) = O'^{(i0)}$ с $\varphi(\eta_1) = F$, $\varphi(\eta_i) = c'_i F_i c''^{-1}_i$, $i = \overline{2,n}$, где $\alpha(\eta)$, $\omega(\eta)$ – соответственно начало и конец пути η. Пусть $\varphi(\eta_1) = F = H_1^{(1)} H_2^{(1)} \dots H_{m(1)}^{(1)}$ – разбиение F в диаграмме $\Delta(w_{10}, w_{10})$ на образующие. Тогда $F \equiv X_i F_i Y_i = H_1^{(1)} \dots H_{\alpha_{(i)}^{(1)}}^{(1)} H_{\alpha_{(i)+1}^{(1)}}^{(1)} \dots H_{\beta_{(i)}^{(1)}}^{(1)} H_{\beta_{(i)+1}^{(1)}}^{(1)} \dots H_{m(1)}^{(1)}$, где $X_i = H_1^{(1)} \dots H_{\alpha_{(i)}^{(1)}}^{(1)}$, $F_i = H_{\alpha_{(i)+1}^{(1)}}^{(1)} \dots H_{\beta_{(i)}^{(1)}}^{(1)}$, $Y_i = H_{\beta_{(i)+1}^{(1)}}^{(1)} \dots H_{m(1)}^{(1)}$. С другой стороны, каждое $\varphi(\eta_i) = c'_i F_i c''^{-1}_i$ в соответствующей диаграмме $\Delta(w_{i0}, w_{i0})$ разбивается на образующие $\varphi(\eta_i) = H_1^{(i)} \dots H_{\alpha_{(i)}^{(1)}}^{(i)} H_{\alpha_{(i)+1}^{(i)}}^{(i)} \dots H_{\beta_{(i)}^{(i)}}^{(i)} H_{\beta_{(i)+1}^{(i)}}^{(i)} \dots H_{m(i)}^{(i)}$, где $c'_i = H_1^{(i)} \dots H_{\alpha_{(i)}^{(i)}}^{(i)}$, $F_i = H_{\alpha_{(i)+1}^{(i)}}^{(i)} \dots H_{\beta_{(i)}^{(i)}}^{(i)}$, $c''^{-1}_i = H_{\beta_{(i)+1}^{(i)}}^{(i)} \dots H_{m(i)}^{(i)}$. Отсюда следуют соотношения $F_i = H_{\alpha_{(i)+1}^{(1)}}^{(1)} \dots H_{\beta_{(i)}^{(1)}}^{(1)} = H_{\alpha_{(i)+1}^{(i)}}^{(i)} \dots H_{\beta_{(i)}^{(i)}}^{(i)}$. Заметим, что разбиение X_i определяется разбиением F. Аналогично, разбиение Y_j, также определяется разбиением F. Следовательно, X_i, Y_j на искомое разбиение F не влияют. В качестве искомого возьмем разбиение $\varphi(\eta_1) = F$ в диаграмме $\Delta(w_{10}, w_{10})$. Получим разбиение F: $F = H_1 H_2 \dots H_m$ и последовательность

$$w_1^{(0)}, \dots, w_n^{(0)}, H_1, w_1^{(1)}, \dots, w_n^{(1)}, H_2, \dots, H_m, w_1^{(m)}, \dots, w_n^{(m)},$$

связанную с полученным разбиением, удовлетворяющую условиям:

$$\forall i, i = \overline{1,m}, H_i^{-1} w_1^{(i-1)} H_i = w_1^{(i)}, \dots, H_i^{-1} w_n^{(i-1)} H_i = w_n^{(i)}, H_i \in \{a_i\},$$

$$w_j^{(s)} \in S(w_j, w_j), j = \overline{1,n}, s = \overline{1,m}.$$

Лемма 7. *Множество всех базисных слов порождает централизатор подгруппы H.*

Доказательство очевидно.

Из лемм 3-7 следует справедливость теоремы 1.

Централизатор произвольного элемента $w \in G$ есть конечно порождённая подгруппа в G и существует алгоритм, выписывающий образующие этого централизатора.

3. обобщённая сопряжённость слов

Теорема 3. *В обобщённой древесной структуре групп Кокстера разрешима проблема обобщённой сопряжённости слов.*

Доказательство. Пусть даны множества слов $w_1, w_2, \dots, w_n$ и $v_1, v_2, \dots, v_n$. Необходимо установить: $\exists z$, $z \in G$, $\&_{i=1}^n (z^{-1} w_i z = v_i)$.

Пусть слова $w_1 = w_{10}$, $v_1 = v_{10}$ являются тупиковыми. Пусть $w_i = a_i w_{i0} a_i^{-1}$, $v_i = b_i v_{i0} b_i^{-1}$, $i = \overline{2,n}$ где w_{i0}, v_{i0} являются тупиковыми. Если предположить, что эти множества сопряжёны, то $\forall i$, $i = \overline{1,n}$, $|w_{i0}| = |v_{i0}|$ и если какое-то из w_{i0} есть образующий x, то сопряжённое ему слово v_{i0} тоже образующий y. Пусть $\Delta(w_{i0}, v_{i0})$ – кольцевая связная приведенная R-диаграмма сопряжённости слов w_{i0}, v_{i0}

$$|a| = \max\{|a_1|, |a_2|, \dots, |a_n|\},$$
$$|b| = \max\{|b_1|, |b_2|, \dots, |b_n|\},$$

где $|a_1| = |b_1| = 0$.

Обозначим через $S(w_i, v_i)$, $i = \overline{1,n}$, множество всех слов длина d_i которых заключена в пределах $|w_{i0}| \leqslant d_i \leqslant (|w_{i0}| + |v_{i0}|)m + 2 + |a| + |b|$.

Введем обозначения $\forall i$, $i = \overline{1,n}$, $w_i = w_i^{(0)}$ и рассмотрим базисные последовательности, соответствующие множеству слов $w_1^{(0)}, \dots, w_n^{(0)}$:

$$w_1^{(0)}, \dots, w_n^{(0)}, H_1, w_1^{(1)}, \dots, w_n^{(1)}, H_2, \dots, H_k, w_1^{(k)}, \dots, w_n^{(k)}, \qquad (2)$$

где $\forall i,\ i = \overline{1,n}$, $\forall j,\ j = \overline{0,k}$, $w_i^{(j)} \in S(w_i, v_i)$ и является меткой циклического геодезического диаграммы $\Delta(w_{i0}, v_{i0})$.

Базисная последовательность (2) называется особой, если она не содержит фундаментальную последовательность либо является пустой, то есть все $H_i = 1$. Слово $H_1 H_2 \dots H_k$, соответствующее особой базисной последовательности, назовем особым базисным словом.

Если в базисной последовательности (2) $w_1^{(k)} = v_1, \dots, w_n^{(k)} = v_n$, то слова $w_1, \dots, w_n$ обобщённо сопряжёны словам $v_1, \dots, v_n$.

Лемма 8. *Если последовательность (2) является особой базисной последовательностью, то* $k \leqslant |S| = |S(w_1, v_1)| \dots |S(w_n, v_n)|$.

Доказательство очевидно.

Лемма 9. *Число особых базисных последовательностей конечно.*

Доказательство очевидно.

Лемма 10. *Пусть F – какое-то решение системы $\&_{i=1}^n (z^{-1} w_i z = v_i)$, тогда существует разбиение F в произведение кусков $H_1 H_2 \dots H_m$, $H_i \in \{a_i\}$, $i = \overline{1,m}$, и базисная последовательность, связанная с данным разбиением F:*

$$w_1^{(0)}, \dots, w_n^{(0)}, H_1, w_1^{(1)}, \dots, w_n^{(1)}, H_2, \dots, H_m, w_1^{(m)}, \dots, w_n^{(m)}, \tag{3}$$

где $w_1^{(m)} = v_1, \dots, w_n^{(m)} = v_n$.

Доказательство аналогично доказательству леммы 6.

Лемма 11. *Пусть F – какое-то решение системы $\&_{i=1}^n (z^{-1} w_i z = v_i)$ и (3) – базисная последовательность, соответствующая данному разбиению F. Тогда из последовательности (3) можно выделить особую подпоследовательность, такую, что соответствующее ей базисное слово F является решением системы.*

Доказательство. Если система

$$\&_{i=1}^n (z^{-1} w_i z = v_i)$$

такова, что $\forall i,\ i = \overline{1,n}$, $w_i \equiv v_i$, то в качестве особой базисной подпоследовательности возьмем пустую подпоследовательность с $F \equiv 1$. Если последовательность (3) не содержит фундаментальных подпоследовательностей то $F' = F$. Если (3) не особая и $\exists j,\ j = \overline{1,n}$, то существуют целые числа $v, k, 0 \leqslant v < k < m$ такие, что подпоследовательность $w_1^{(0)}, \dots, w_n^{(0)}, H_1, \dots, H_v, w_1^{(v)}, \dots, w_n^{(v)}, H_{v+1}, \dots, H_k, w_1^{(k)}, \dots, w_n^{(k)}$ является фундаментальной. Вычеркнув из (3) подпоследовательность $H_{v+1}, w_1^{(v+1)}, \dots, w_n^{(v+1)} H_{v+2}, \dots, H_k, w_1^{(k)}, \dots, w_n^{(k)}$, получим базисную последовательность слов, являющуюся решением системы. Если полученная базисная последовательность не является особой, то применим к ней указанный выше процесс.

Из лемм 8-11 следует доказательство теоремы 2.

Теорема 4. *Пусть G – обобщённая древесная структура групп Кокстера и $\{w_i\}_{i=\overline{1,m}}$, $\{v_i\}_{i=\overline{1,m}}$ – слова из G. Если F – какое-то решение системы $\&_{i=1}^n (z^{-1} w_i z = v_i)$, то множество слов $\mathbb{C}_G(H) \cdot F$, где $\mathbb{C}_G(H)$ – централизатор подгруппы H порождённой словами $\{w_i\}_{i=\overline{1,m}}$ является множеством всех решений системы.*

Доказательство очевидно.

Теорема 5. *Существует алгоритм, позволяющий для любого конечного множества слов из обобщённой древесной структурой групп Кокстера G выписать образующие их нормализатора.*

Доказательство очевидно.

4. Заключение

Проблема обобщённой сопряжённости слов является обобщением проблемы сопряжённости слов, относящейся к основным алгоритмическим проблемам теории групп.

В работе рассмотрены проблемы обобщённой сопряжённости слов и построения централизатора конечно порождённой подгруппы в обобщённых древесных структурах групп Кокстера. Данный класс групп важен для изучения алгоритмических проблем в группах Кокстера, которые могут либо быть представлены как обобщённые древесные структуры групп Кокстера, образованные из групп Кокстера с древесной структурой заменой некоторых вершин соответствующего дерева-графа группами Кокстера большого или экстрабольшого типов, а также группами Кокстера с n-угольной структурой, либо непосредственно принадлежат к перечисленным классам [8]. Данная работа продолжает изучение алгоритмических свойств групп Кокстера [15] – [21].

Несмотря на то, что данный класс групп относится к гиперболическим группам и в нем алгоритмически разрешима проблема обобщённой сопряжённости слов, авторами предложен довольно простой и оригинальный метод решения указанных выше проблем.

Результаты исследования докладывались на Тульском научном алгебраическом семинаре «Алгоритмические проблемы теории групп и полугрупп» и международной алгебраической конференции, посвященной 110-летию со дня рождения А. Г. Куроша.

Для решения проблем обобщённой сопряжённости слов и построения централизатора конечно порождённой подгруппы в обобщённых древесных структурах групп Кокстера применялись современные комбинаторные и геометрические методы исследования, в частности, метод диаграмм, введенный ван Кампеном, переоткрытый Р. Линдоном и усовершенствованный В. Н. Безверхним в части введения $\overline{R}$-сокращений, и подход Г. С. Маканина.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Dehn M. Uber unendliche diskontinuierliche Gruppen // Math. Annal. 1912. Vol. 71. P. 116-144.

2. Новиков П. С. Об алгоритмической неразрешимости проблемы тождества в теории групп // Труды МИАН СССР. 1955. Т. 44. С. 3-143.

3. Coxeter H. S. M. Discrete groups generated by reflections // Ann. Math. 1934. Vol. 35. P. 588-621.

4. Tits J. Groupes simples et geometries associees // Proc. Int. Congress Math. Stocholm. 1962. P. 197-221.

5. Schupp P. Coxeter Groups, 2-Completion, Perimeter Reduction and Subgroup Separability // arXiv math. GR/0203020. 2002. Vol. 1. P. 1-21.

6. Appel K., Schupp P. Artins groups and infinite Coxter groups // Ivent. Math. 1983. Vol. 72. P. 201-220.

7. Bahls P. The isomorphism problem in Coxeter groups. London: Imperial College Press, 2005.

8. Безверхний В. Н., Безверхняя Н. Б., Добрынина И. В., Инченко О. В., Устян А. Е. Об алгоритмических проблемах в группах Кокстера // Чебышевский сборник. 2016. Т. 17, №4. С. 23-50.

9. Лысенок И. Г. О некоторых алгоритмических свойствах гиперболических групп // Известия АН СССР. Сер. матем. 1989. Т. 53. №4. С. 814-832.

10. Buckley D. J., Derek F. Holt. The conjugacy problem in hyperbolic groups for finite lists of group elements // Int. J. of Algebra and Comput. 2013. Vol. 23, №5. P. 1127–1150.

11. Маканин Г. С. О нормализаторах группы кос // Математический сборник. 1971. Т. 86, №2. С. 171-179.

12. Безверхний В. Н. Решение проблемы обобщённой сопряжённости слов в $C(p)\&T(q)$ - группах // Известия Тульского государственного университета. Сер. Математика. Механика. Информатика. 1998. Т. 4. С. 5-13.

13. Добрынина И. В. Об алгоритмических проблемах в обобщённых древесных структурах групп Кокстера // Чебышевский сборник. 2018. Т. 19, №2. С. 10-33.

14. Линдон Р., Шуп П. Комбинаторная теория групп. М.: Мир, 1980.

15. Инченко О. В. Проблемы равенства и сопряжённости слов в группах Кокстера с древесной структурой // Чебышевский сборник. 2005. Т. 6, №2. С. 81-90.

16. Безверхний В. Н., Добрынина И. В. Решение проблемы степенной сопряжённости слов в группах Кокстера экстрабольшого типа // Дискретная математика. 2008. Т. 20, №3. С. 101-110.

17. Безверхний В. Н., Добрынина И. В. Об элементах конечного порядка в группах Кокстера большого типа // Известия Тульского государственного университета. Сер. Математика. Механика. Информатика. 2003. Т. 9, №1. С. 13-22.

18. Безверхний В. Н., Инченко О. В. О кручении в группах Кокстера с древесной структурой // Чебышевский сборник. 2005. Т. 6, №1. С. 5-12.

19. Безверхний В. Н., Добрынина И. В. Решение проблемы сопряжённости слов в группах Кокстера большого типа // Чебышевский сборник. 2003. Т. 4, №1. С. 10-33.

20. Безверхний В. Н., Инченко О. В. Проблема степенной сопряжённости слов в группах Кокстера с древесной структурой // Известия Тульского государственного университета. Сер. Математика. Механика. Информатика. 2005. Т.11. С.63-75.

21. Безверхний В. Н., Добрынина И. В. Решение проблемы обобщённой сопряжённости слов в группах Кокстера большого типа // Дискретная математика. 2005. Т. 17, №3. С. 123-145.

REFERENCES

1. Dehn, M., 1912, “Uber unendliche diskontinuierliche Gruppen“, *Math. Annal.*, vol. 71, pp. 116-144.

2. Novikov, P. S., 1955, “On the algorithmic unsolvability of the word problem in group theory“, *Trudy Mat. Inst. Steklov.*, vol. 44, pp. 3–143.

3. Coxeter, H. S. M., 1934, “Discrete groups generated by reflections“, *Ann. Math.*, vol. 35, pp. 588-621.

4. Tits, J., 1962, “Groupes simples et geometries associees“, *Proc. Int. Congress Math. Stocholm*, pp. 197-221.

5. Schupp, P., 2002, “Coxeter Groups, 2-Completion, Perimeter Reduction and Subgroup Separability“, *arXiv math. GR/0203020*, vol. 1, pp. 1–21.

6. Appel, K. & Schupp, P., 1983, "Artins groups and infinite Coxter groups", *Ivent. Math.*, , vol. 72, pp. 201-220.

7. Bahls, P., 2005, *The isomorphism problem in Coxeter groups*, Imperial College Press, London.

8. Bezverkhnii, V. N., Bezverkhnyaya, N. B., Dobrynina, I. V., Inchenko O. V., Ustyan A. E, 2016, "On algorithmic problems in Coxeter groups", *Chebyshevskii Sb.*, vol. 17, no. 4, pp. 23–50.

9. Lysenok, I. G. 1990, "On some algorithmic properties of hyperbolic groups," *Math. USSR-Izv.*, vol. 35, no. 1, pp. 145-163.

10. Buckley, D. J. & Derek, F. Holt, 2013, "The conjugacy problem in hyperbolic groups for finite lists of group elements", *Int. J. of Algebra and Comput.*, vol. 23, no.5. pp. 1127–1150.

11. Makanin, G. S., 1971, "On normalizers in the braid group", *Math. USSR-Sb.*, vol. 15, no. 2, pp. 167–175.

12. Bezverkhnii, V. N., 1998, "Solution of the problem of generalized conjugacy of words in $C(p)\&T(q)$ – groups", *Izvestia of Tula state University. Ser. Math. Mechanics. Informatics*, vol. 4, pp. 5-13.

13. Dobrynina, I. V., 2018, "On algorithmic problems in generalized tree structures of Coxeter groups", textitChebyshevskii Sb., vol. 19, no. 2, pp. 10–33.

14. Lyndon, R.& Schupp, P., 1980, *Combinatorial group theory*, Mir, Moscow.

15. Inchenko, O. V., 2005, "Problems of words and conjugacy of words in Coxeter groups with a tree structure", *Chebyshevskii Sb.*, vol. 6, no. 2, pp. 81-90.

16. Bezverkhnii, V. N. & Dobrynina, I. V., 2008, "A solution of the power conjugacy problem for words in the Coxeter groups of extra large type", *Diskr. Mat.*, vol. 20, no. 3, pp. 101–110.

17. Bezverkhnii, V. N. & Dobrynina, I. V., 2003, "On elements of finite order in Coxeter groups of large type", *Izvestia of Tula state University. Ser. Math. Mechanics. Informatics*, vol. 9, no. 1, pp. 13-22.

18. Bezverkhnii, V. N. & Inchenko, O. V., 2005, "On torsion in Coxeter groups with tree structure", *Chebyshevskii Sb.*, vol. 6, no. 1, pp. 5-12.

19. Bezverkhnii, V. N. & Dobrynina, I. V., 2003,"Solution of the conjugacy problem for words in Coxeter groups of large type", *Chebyshevskii Sb.*, , vol. 4, no. 1, pp. 10–33.

20. Bezverkhnii, V. N. & Inchenko, O. V., 2005, "Power conjugacy problem for words in Coxeter groups with tree structure", *Izvestia of Tula state University. Ser. Math. Mechanics. Informatics*, vol. 11, pp. 63-75.

21. Bezverkhnii, V. N. & Dobrynina, I. V., 2005, "Solution of the generalized conjugacy problem for words in Coxeter groups of large type", *Diskr. Mat.*, vol. 17, no. 3, pp. 123–145.

Получено 16.04.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 512.54 DOI 10.22405/2226-8383-2018-19-3-148-163

Новое применение дисперсионного метода Линника

Étienne Fouvry — Laboratoire de Mathématiques d'Orsay, Univ. Paris–Sud, CNRS, Université Paris–Saclay, 91405 Orsay, France.
e-mail: Etienne.Fouvry@u-psud.fr
Maksym Radziwiłł — Department of Mathematics, McGill University, Burnside Hall, Room 1005, 805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A 0B9
e-mail: maksym.radziwill@gmail.com

Аннотация

Пусть α_m и β_n — две последовательности вещественных чисел с носителями на отрезках $[M, 2M]$ и $[N, 2N]$, где $M = X^{1/2-\delta}$ и $N = X^{1/2+\delta}$. Мы доказываем существование такой постоянной δ_0, что мультипликативная свертка α_m и β_n имеет уровень распределения $1/2+\delta-\varepsilon$ (в слабом смысле), если только $0 \leqslant \delta < \delta_0$, последовательность β_n является последовательностью Зигеля-Вальфиша, и обе последовательности α_m и β_n ограничены сверху функцией делителей. Наш результат, таким образом, представляет собой общую дисперсионную оценку для "коротких" сумм II типа. Доказательство существенно использует дисперсионный метод Линника и недавние оценки трилинейных сумм с дробями Клоостермана, принадлежащие Беттин и Чанди. Также мы остановимся на применении полученного результата к проблеме делителей Титчмарша.

Ключевые слова: равнораспределение в арифметических прогрессиях, метод дисперсии.

Библиография: 10 названий.

Для цитирования:
Étienne Fouvry, Maksym Radziwiłł, Another application of Linnik dispersion method // Чебышевский сборник, 2018, т. 19, вып. 3, с. 148–163.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 512.54 DOI 10.22405/2226-8383-2018-19-3-148-163

Another application of Linnik dispersion method

Étienne Fouvry — Laboratoire de Mathématiques d'Orsay, Univ. Paris–Sud, CNRS, Université Paris–Saclay, 91405 Orsay, France.
e-mail: Etienne.Fouvry@u-psud.fr
Maksym Radziwiłł — Department of Mathematics, McGill University, Burnside Hall, Room 1005, 805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A 0B9
e-mail: maksym.radziwill@gmail.com

Abstract

Let α_m and β_n be two sequences of real numbers supported on $[M, 2M]$ and $[N, 2N]$ with $M = X^{1/2-\delta}$ and $N = X^{1/2+\delta}$. We show that there exists a $\delta_0 > 0$ such that the multiplicative convolution of α_m and β_n has exponent of distribution $\frac{1}{2} + \delta - \varepsilon$ (in a weak sense) as long as $0 \leq \delta < \delta_0$, the sequence β_n is Siegel-Walfisz and both sequences α_m and β_n are bounded above by divisor functions. Our result is thus a general dispersion estimate for "narrow" type-II sums. The proof relies crucially on Linnik's dispersion method and recent bounds for trilinear forms in Kloosterman fractions due to Bettin-Chandee. We highlight an application related to the Titchmarsh divisor problem.

Keywords: equidistribution in arithmetic progressions, dispersion method.

Bibliography: 10 titles.

For citation:
Étienne Fouvry, Maksym Radziwiłł, 2018, "Another application of Linnik dispersion method", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 148–163.

In memoriam Professor Yu. V. Linnik (1915-1972)

1. Introduction

An important theme in analytic number theory is the study of the distribution of sequences in arithmetic progressions. A representative result in this field is the Bombieri-Vinogradov theorem [2], according to which for any $A > 0$,

$$\sum_{q \leq Q} \max_{(a,q)=1} \Big| \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} 1 - \frac{1}{\varphi(q)} \sum_{p \leq x} 1 \Big| \ll_A x(\log x)^{-A} \tag{1}$$

provided that $Q \leq \sqrt{x}(\log x)^{-B}$ for some constant $B = B(A)$ depending on $A > 0$.

Nothing of the strength of (1) is known in the range $Q > x^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and already establishing for any fixed integer $a \neq 0$ and for all $A > 0$ the weaker estimate,

$$\sum_{q \leq Q} \Big| \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} 1 - \frac{1}{\varphi(q)} \sum_{p \leq x} 1 \Big| \ll_{a,A} x(\log x)^{-A} \tag{2}$$

with $Q = x^{1/2+\delta}$ and some $\delta > 0$ is a major open problem. If we could show (2) then we would say that *the primes have exponent of distribution* $\frac{1}{2} + \delta$ *in a weak sense*. However we note that there are results of this type if one allows to restrict the sum over $q \leq Q$ in (2) to integers that are x^{ε} smooth, for a sufficiently small $\varepsilon > 0$ (see [16, 5]).

Any known approach to (2) goes through combinatorial formulas which decompose the sequence of prime numbers as a linear combination of multiplicative convolutions of other sequences (see for example [13, Chapter 13]). If one attempts to establish (2) by using such a combinatorial formula then one is led to the problem of showing that for any $A > 0$,

$$\sum_{q \leq Q} \Big| \sum_{\substack{M \leq m \leq 2M \\ N \leq n \leq 2N \\ mn \equiv a \pmod q}} \alpha_m \beta_n - \sum_{\substack{M \leq m \leq 2M \\ N \leq n \leq 2N \\ (mn,q)=1}} \alpha_m \beta_n \Big| \ll X(\log X)^{-A}\ ,\ X := MN \tag{3}$$

with $Q > X^{1/2+\varepsilon}$ for some $\varepsilon > 0$. In [14] Linnik developed his "dispersion method" to tackle such expressions. The method relies crucially on the bilinearity of the problem, followed by the use of various estimates for Kloosterman sums of analytic or algebraic origins. For a bound such as (3) to hold one needs to impose a "Siegel-Walfisz condition" on at least one of the sequences α_m or β_n.

Definition 1. *We say that a sequence $\boldsymbol{\beta} = (\beta_n)$ satisfies a Siegel-Walfisz condition (alternatively we also say that $\boldsymbol{\beta}$ is Siegel-Walfisz), if there exists an integer $k > 0$ such that for any fixed $A > 0$, uniformly in $x \geq 2$, $q > |a| \geq 1, r \geq 1$ and $(a, q) = 1$, we have,*

$$\sum_{\substack{x<n\leq 2x\\ n\equiv a \pmod q\\ (n,r)=1}} \beta_n - \frac{1}{\varphi(q)} \sum_{\substack{x<n\leq 2x\\ (n,qr)=1}} \beta_n = O_A(\tau_k(r) \cdot x(\log x)^{-A}).$$

where $\tau_k(n) := \sum_{n_1 \dots n_k = n} 1$ is the kth divisor function.

It is widely expected (see e.g [3, Conjecture 1]) that (3) should hold as soon as $\min(M, N) > X^{\varepsilon}$ provided that at least one of the sequences α_n, β_m is Siegel-Walfisz, and that there exists an integer $k > 0$ such that $|\alpha_m| \leq \tau_k(m)$ and $|\beta_n| \leq \tau_k(n)$ for all integers m, $n \geq 1$. We are however very far from proving a result of this type.

When $Q > X^{1/2+\varepsilon}$ for some $\varepsilon > 0$, there are only a few results establishing (3) unconditionally in specific ranges of M and N (precisely [9, Théorème 1], [3, Theorem 3], [11, Corollaire 1], [12, Corollary 1.1 (i)]). All the results that establish (3) unconditionally place a restriction on one of the variable N or M being much smaller than the other. We call such cases "unbalanced convolutions" and this forms the topic of our previous paper [12].

In applications a recurring range is one where M and N are roughly of the same size. This often corresponds to the case of "type II sums" in which one is permitted to exploit bilinearity but not much else. This is the range to which we contribute in this paper.

Theorem 1. *Let $k \geq 1$ be an integer and $M, N \geq 1$ be given. Set $X = MN$. Let α_m and β_n be two sequences of real numbers supported respectively on $[M, 2M]$ and $[N, 2N]$. Suppose that $\boldsymbol{\beta} = (\beta_n)$ is Siegel–Walfisz and suppose that $|\alpha_m| \leq \tau_k(m)$ and $|\beta_n| \leq \tau_k(n)$ for all integers $m, n \geq 1$. Then, for every $\varepsilon > 0$ and every $A > 0$,*

$$\sum_{\substack{Q\leq q\leq 2Q\\ (q,a)=1}} \Big| \sum_{mn\equiv a \pmod q} \alpha_m\beta_n - \frac{1}{\varphi(q)} \sum_{(mn,q)=1} \alpha_m\beta_n \Big| \ll_A X(\log X)^{-A} \tag{4}$$

uniformly in $N^{56/23}X^{-17/23+\varepsilon} \leq Q \leq NX^{-\varepsilon}$ and $1 \leq |a| \leq X$.

Setting $N = X^{1/2+\delta}$ and $M = X^{1/2-\delta}$ in Theorem 1 it follows from Theorem 1 and the Bombieri-Vinogradov theorem that (4) holds for all $Q \leq NX^{-\varepsilon}$ with $0 \leq \delta < \delta_0 := \frac{1}{112}$. Previously the existence of such a $\delta_0 > 0$ was established conditionally on Hooley's $R^{\star}$ conjecture on cancellations in short incomplete Kloosterman sums in [8, Théorème 1] and in that case one can take $\delta_0 = \frac{1}{14}$. Similarly to our previous paper, we use the work of Bettin-Chandee [1] and Duke-Friedlander-Iwaniec [7] as an unconditional substitute for Hooley's $R^{\star}$ conjecture. In fact the proof of Theorem 1 follows closely the proof of the conditional result in [8, Théorème 1] up to the point where Hooley's $R^{\star}$ conjecture is applied. Incidentally we notice that the largest Q that Theorem 1 allows to take is $Q = X^{17/33-5\varepsilon}$ provided that one chooses $N = X^{17/33-4\varepsilon}$.

Unfortunately the type-II sums that our Theorem 1 allows to estimate are too narrow to make Theorem 1 widely applicable in many problems (however see [15] for an interesting connection with cancellations in character sums). We record nonetheless below one corollary, which is related to Titchmarsh's divisor problem concerning the estimation of $\sum_{p\leq x} \tau_2(p-1)$ (for the best results on this problem see [10, Corollaire 2], [3, Corollary 1] and [6]). The proof of the Corollary below will be given in §5.

Corollary 1. *Let $k \geq 1$ and let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be two sequences of real numbers as in Theorem 1.* Let δ be a constant satisfying

$$0 < \delta < \frac{1}{112},$$

and let

$$X \geq 2,\ M = X^{1/2-\delta},\ \text{and}\ N = X^{1/2+\delta}.$$

Then for every $A > 0$ we have the equality

$$\sum_{m\sim M}\sum_{n\sim N}\alpha_m\beta_n\tau_2(mn-1) = 2\sum_{q\geq 1}\frac{1}{\varphi(q)}\sum_{\substack{m\sim M,\ n\sim N,\ mn>q^2\\(mn,q)=1}}\sum\alpha_m\beta_n + O\big(X(\log X)^{-A}\big).$$

2. Conventions and lemmas

2.1. Conventions

For M and $N \geq 1$, we put $X = MN$ and $\mathcal{L} = \log 2X$. Whenever it appears in the subscript of a sum the notation $n \sim N$ will means $N \leq n < 2N$. Given an integer $a \neq 0$ and two sequences $\boldsymbol{\alpha} = (\alpha_m)_{M\leq m<2M}$ and $\boldsymbol{\beta} = (\beta_n)_{N\leq n<2N}$ supported respectively on $[M, 2M]$ and $[N, 2N]$ we define the discrepancy

$$E(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,q,a) := \sum_{\substack{m\sim M\\ mn\equiv a \bmod q}}\sum_{n\sim N}\alpha_m\beta_n - \frac{1}{\varphi(q)}\sum_{\substack{m\sim M\\(mn,q)=1}}\sum_{n\sim N}\alpha_m\beta_n,$$

and we also define the mean-discrepancy,

$$\Delta(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,q,a) := \sum_{\substack{q\sim Q\\(q,a)=1}}|E(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,q,a)|. \tag{5}$$

Throughout η will denote any positive number the value of which may change at each occurence. The dependency on η will not be recalled in the O or $\ll$–symbols. Typical examples are $\tau_k(n) = O(n^\eta)$ or $(\log x)^{10} = O(x^\eta)$, uniformly for $x \geq 1$.

If f is a smooth real function, its Fourier transform is defined by

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(t)e(-\xi t)\,\mathrm{d}t,$$

where $e(\cdot) = \exp(2\pi i\cdot)$.

2.2. Lemmas

Our first lemma is a classical finite version of the Poisson summation formula in arithmetic progressions, with a good error term.

Lemma 1. *There exists a smooth function $\psi : \mathbb{R} \longrightarrow \mathbb{R}^+$, with compact support equal to $[1/2, 5/2]$, larger than the characteristic function of the interval $[1, 2]$, equal to 1 on this interval such that, uniformly for integers a and $q \geq 1$, for $M \geq 1$ and $H \geq (q/M)\log^4 2M$ one has the equality*

$$\sum_{m\equiv a \bmod q}\psi\Big(\frac{m}{M}\Big) = \hat{\psi}(0)\frac{M}{q} + \frac{M}{q}\sum_{0<|h|\leq H}e\Big(\frac{ah}{q}\Big)\hat{\psi}\Big(\frac{h}{q/M}\Big) + O(M^{-1}). \tag{6}$$

Furthermore, uniformly for $q \geq 1$ and $M \geq 1$ one has the equality

$$\sum_{(m,q)=1}\psi\Big(\frac{m}{M}\Big) = \frac{\varphi(q)}{q}\hat{\psi}(0)M + O\big(\tau_2(q)\log^4 2M\big). \tag{7}$$

Доказательство. See Lemma 2.1 of [12], inspired by [4, Lemma 7]. □ We now recall a classical lemma on the average behavior of the τ_k-function in arithmetic progressions (see [14, Lemma 1.1.5], for instance).

Lemma 2. *For every $k \geq 1$, for every $\varepsilon > 0$, there exists $C(k,\varepsilon)$ such that, for every $x \geq 2$, for every $x^{\varepsilon} < y < x$, for every $1 \leq q \leq yx^{-\varepsilon}$, for every integer a coprime with q, one has the inequality*

$$\sum_{\substack{x-y<n\leq x\\ n\equiv a \bmod q}} \tau_k(n) \leq C(k,\varepsilon)\frac{y}{\varphi(q)}(\log 2x)^{k-1}.$$

The following lemma is one of the various forms of the so–called Barban–Davenport–Halberstam Theorem (for a proof see for instance [3, Theorem 0 (a)].

Lemma 3. *Let $k > 0$ be an integer. Let $\boldsymbol{\beta} = (\beta_n)$ be a Siegel–Walfisz sequence such that $|\beta_n| \leq \tau_k(n)$ for all integer $n \geq 1$. Then for every $A > 0$ there exists $B = B(A)$ such that, uniformly for $N \geq 1$ one has the equality*

$$\sum_{q\leq N(\log 2N)^{-B}} \sum_{a,\,(a,q)=1} \Big| \sum_{\substack{n\sim N\\ n\equiv a \bmod q}} \beta_n - \frac{1}{\varphi(q)} \sum_{\substack{n\sim N\\ (n,q)=1}} \beta_n \Big|^2 = O_A\big(N(\log 2N)^{-A}\big).$$

We now recall an easy consequence of Weil's bound for Kloosterman sums.

Lemma 4. *Let a and b two integers ≥ 1. Let $\mathcal{I}$ an interval included in $[1,a]$. Then for every integer ℓ for every $\varepsilon > 0$ we have the inequality*

$$\sum_{\substack{n\in\mathcal{I}\\ (n,ab)=1}} \frac{n}{\varphi(n)} e\Big(\ell\frac{\overline{n}}{a}\Big) = O_{\varepsilon}\Big((\ell,a)^{\frac{1}{2}}(ab)^{\varepsilon}a^{\frac{1}{2}}\Big).$$

Доказательство. We begin we the case $b = 1$. We write the factor $\frac{n}{\varphi(n)}$ as

$$\frac{n}{\varphi(n)} = \sum_{\nu|n^{\infty}} \nu^{-1} = \sum_{\kappa(\nu)|n} \nu^{-1},$$

where $\kappa(\nu)$ is the largest squarefree integer dividing ν (sometimes $\kappa(\nu)$ is called the *kernel* of ν). This gives the equality

$$\Big| \sum_{\substack{n\in\mathcal{I}\\ (n,a)=1}} \frac{n}{\varphi(n)} e\Big(\ell\frac{\overline{n}}{a}\Big) \Big| \leq \sum_{\nu\geq 1} \nu^{-1} \Big| \sum_{\substack{n\in\mathcal{I}\\ \kappa(\nu)|n\\ (n,a)=1}} e\Big(\ell\frac{\overline{n}}{a}\Big) \Big| = \sum_{\substack{\nu\geq 1\\ (\nu,a)=1}} \nu^{-1} \Big| \sum_{\substack{m\in\mathcal{I}/\kappa(\nu)\\ (m,a)=1}} e\Big(\ell\frac{\overline{\kappa(\nu)}\,\overline{m}}{a}\Big) \Big|.$$

In the summation we can restrict to the ν such that $\kappa(\nu) \leq a$. Applying the classical bound for short Kloosterman sums, we deduce that

$$\Big| \sum_{\substack{n\in\mathcal{I}\\ (n,a)=1}} \frac{n}{\varphi(n)} e\Big(\ell\frac{\overline{n}}{a}\Big) \Big| \ll_{\varepsilon} (\ell,a)^{\frac{1}{2}}a^{\frac{1}{2}+\varepsilon} \prod_{p\leq a}\Big(1-\frac{1}{p}\Big)^{-1} \ll_{\varepsilon} (\ell,a)^{\frac{1}{2}}a^{\frac{1}{2}+2\varepsilon}.$$

This proves Lemma 4 in the case where $b = 1$. When $b \neq 1$, we use the Möbius inversion formula to detect the condition $(n,b) = 1$. □

Our central tool is a bound for trilinear forms for Kloosterman fractions, due to Bettin and Chandee [1, Theorem 1]. The result of Bettin-Chandee builds on work of Duke-Friedlander-Iwaniec [7, Theorem 2] who considered the case of bilinear forms. These two papers show cancellations in exponential sums involving Kloosterman fractions $e(a\overline{m}/n)$ with $m \asymp n$. We state below the main theorem of Bettin-Chandee.

LEMMA 5. *For every $\epsilon > 0$ there exists $C(\varepsilon)$ such that for every non zero integer ϑ, for every sequences let $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ and $\boldsymbol{\nu}$ be of complex numbers, for every A, M and $N \geq 1$, one has the inequality*

$$\Big|\sum_{a\sim A}\sum_{m\sim M}\sum_{n\sim N}\alpha(m)\beta(n)\nu(a)e\Big(\vartheta\frac{a\overline{m}}{n}\Big)\Big| \leq C(\varepsilon)\|\boldsymbol{\alpha}\|_{2,M}\,\|\boldsymbol{\beta}\|_{2,N}\,\|\boldsymbol{\nu}\|_{2,A}$$
$$\times\Big(1+\frac{|\vartheta|A}{MN}\Big)^{\frac12}\Big((AMN)^{\frac{7}{20}+\varepsilon}\,(M+N)^{\frac14}+(AMN)^{\frac38+\varepsilon}(AM+AN)^{\frac18}\Big).$$

3. Proof of Theorem 1

All along the proof we will suppose that the inequality $1 \leq |a| \leq X$ holds and that we also have

$$X^{\frac38} \leq M \leq X^{\frac12} \leq N \text{ and } Q \leq N. \tag{8}$$

3.1. Beginning of the dispersion

Without loss of generality we can suppose that the sequence $\boldsymbol{\beta}$ satisfies the following property

$$n \mid a \Rightarrow \beta_n = 0. \tag{9}$$

Such an assumption is justified because the contribution to $\Delta(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,Q,a)$ of the (q,m,n) such that $n \mid a$ is

$$\ll QX^{\eta} + X^{\eta}\sum_{n|a}\sum_{\substack{m\sim M\\ mn\neq a}}\tau_2(|mn-a|) + MX^{\varepsilon} \ll (M+Q)X^{\eta}.$$

By (5), we have the inequality

$$\Delta(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,Q,a) \leq \sum_{q\sim Q}\sum_{\substack{m\sim M\\(m,q)=1}}|\alpha_m|\Big|\sum_{\substack{n\sim N\\ n\equiv a\overline{m} \bmod q}}\beta_n - \frac{1}{\varphi(q)}\sum_{\substack{n\sim N\\(n,q)=1}}\beta_n\Big|.$$

Let ψ be the smooth function constructed in Lemma 1. By the Cauchy–Schwarz inequality, the inequality $|\alpha_m| \leq \tau_k(m)$ and by Lemma 2 we deduce

$$\Delta^2(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,Q,a) \ll MQ\mathcal{L}^{k^2-1}\Big\{W(Q)-2V(Q)+U(Q)\Big\}, \tag{10}$$

with

$$U(Q) = \sum_{(q,a)=1}\frac{\psi(q/Q)}{\varphi^2(q)}\Big(\sum_{\substack{n\sim N\\(n,q)=1}}\beta_n\Big)^2\sum_{(m,q)=1}\psi\Big(\frac{m}{M}\Big), \tag{11}$$

$$V(Q) = \sum_{(q,a)=1}\frac{\psi(q/Q)}{\varphi(q)}\Big(\sum_{\substack{n_1\sim N\\(n_1,q)=1}}\beta_{n_1}\Big)\Big(\sum_{\substack{n_2\sim N\\(n_2,q)=1}}\beta_{n_2}\Big)\sum_{m\equiv a\overline{n_1} \bmod q}\psi\Big(\frac{m}{M}\Big),$$

$$W(Q) = \sum_{(q,a)=1}\psi(q/Q)\Big(\sum_{\substack{n_1\sim N\\(n_1,q)=1}}\beta_{n_1}\Big)\Big(\sum_{\substack{n_2\sim N\\(n_2,q)=1}}\beta_{n_2}\Big)\sum_{\substack{m\equiv a\overline{n_1} \bmod q\\ m\equiv a\overline{n_2} \bmod q}}\psi\Big(\frac{m}{M}\Big). \tag{12}$$

3.2. Study of $U(Q)$

A direct application of (7) of Lemma 1 in the definition (11) gives the equality

$$U(Q) = \hat{\psi}(0)M\sum_{(q,a)=1}\frac{\psi(q/Q)}{q\varphi(q)}\Big(\sum_{\substack{n\sim N\\(n,q)=1}}\beta_n\Big)^2 + O\big(N^2Q^{-1}X^{\eta}\big)$$
$$= U^{\mathrm{MT}}(Q) + O\big(N^2Q^{-1}X^{\eta}\big), \tag{13}$$

by definition.

3.3. Study of $V(Q)$

Let ε be a fixed positive number. We now apply (6) of Lemma 1 with

$$H = M^{-1}QX^{\varepsilon}. \tag{14}$$

This leads to the equality

$$V(Q) = V^{\mathrm{MT}}(Q) + V^{\mathrm{Err1}}(Q) + V^{\mathrm{Err2}}(Q), \tag{15}$$

where each of the three terms corresponds to the contribution of the three terms on the right hand–side of (6). We directly have the equality

$$V^{\mathrm{Err2}}(Q) = O\big(M^{-1}N^2X^{\eta}\big). \tag{16}$$

For the main term we get

$$V^{\mathrm{MT}}(Q) = \hat{\psi}(0)M \sum_{(q,a)=1} \frac{\psi(q/Q)}{q\varphi(q)} \Big(\sum_{\substack{n\sim N\\(n,q)=1}} \beta_n \Big)^2. \tag{17}$$

By the definition of $V^{\mathrm{Err1}}(Q)$ we have the equality

$$V^{\mathrm{Err1}}(Q) = M \sum_{(q,a)=1} \frac{\psi(q/Q)}{q\varphi(q)} \Big(\sum_{\substack{n_2\sim N\\(n_2,q)=1}} \beta_{n_2} \Big) \Big(\sum_{\substack{n_1\sim N\\(n_1,q)=1}} \beta_{n_1} \sum_{0<|h|\leq H} \hat{\psi}\Big(\frac{h}{q/M}\Big) e\Big(\frac{ah\overline{n_1}}{q}\Big)\Big),$$

from which we deduce the inequality

$$\big|\, V^{\mathrm{Err1}}(Q) \,\big| \leq MQ^{-2} \sum_{n_1\sim N} |\beta_{n_1}| \sum_{n_2\sim N} |\beta_{n_2}| \sum_{0<|h|\leq H} \big|\, \mathcal{V}(n_1,n_2,h) \,\big| \tag{18}$$

with

$$\mathcal{V}(n_1,n_2,h) = \sum_{(q,an_1n_2)=1} \psi(q/Q) \frac{Q^2}{q\varphi(q)} \hat{\psi}\Big(\frac{h}{q/M}\Big) e\Big(\frac{ah\overline{n_1}}{q}\Big).$$

Since $(q,n_1)=1$ Bézout's relation gives the equality

$$\frac{ah\overline{n_1}}{q} = -ah\frac{\overline{q}}{n_1} + \frac{ah}{n_1q} \mod 1.$$

By the inequality $1 \leq |a| \leq X$ and by the definition of H, the derivative of the bounded function

$$t \mapsto \psi(t/Q)\frac{Q^2}{t^2}\hat{\psi}\Big(\frac{h}{t/M}\Big)e\Big(\frac{ah}{n_1t}\Big)$$

is $\ll X^{\varepsilon}t^{-1}$ when $t \asymp Q$. This allows to make a partial summation over the variable q with the loss of a factor X^{ε}. After all these considerations, we see that there exists a subinterval $\mathcal{J} \subset [Q/2, 5Q/2]$ such that we have the inequality

$$\big|\, \mathcal{V}(n_1,n_2,h) \,\big| \ll X^{\varepsilon} \Big| \sum_{\substack{q\in\mathcal{J}\\(q,n_1n_2)=1}} \frac{q}{\varphi(q)} e\Big(ah\frac{\overline{q}}{n_1}\Big) \Big|.$$

Lemma 4 leads to the bound

$$\big|\,\mathcal{V}(n_1,n_2,h)\,\big| \ll X^{\varepsilon}(ah,n_1)^{\frac12}(n_1n_2)^{\eta}n_1^{\frac12}.$$

Inserting this into (18), we obtain

$$V^{\mathrm{Err1}}(Q) \ll MN^{\frac32}Q^{-2}X^{\varepsilon+\eta}\sum_{n_1\sim N}|\beta_{n_1}|\sum_{0<|h|\le H}(h,n_1)^{\frac12},$$

which finally gives

$$V^{\mathrm{Err1}}(Q) \ll N^{\frac52}Q^{-1}X^{2\varepsilon+\eta} \tag{19}$$

using the inequality $|\beta_n| \le \tau_k(n)$ and the definition of H. Combining (15), (16), (17) and (19) we obtain the equality

$$V(Q) = V^{\mathrm{MT}}(Q) + O_{\varepsilon}\big((M^{-1}N^2 + N^{\frac52}Q^{-1})X^{2\varepsilon+\eta}\big). \tag{20}$$

where $V^{\mathrm{MT}}(Q)$ is defined in (17) and where the constant implicit in the O_{ε}–symbol is uniform for a satisfying $1 \le |a| \le X$.

4. Study of $W(Q)$

4.1. The preparation of the variables

The conditions of the last summation in (12) imply the congruence restriction

$$n_1 \equiv n_2 \bmod q \text{ and } (n_1n_2,q) = 1. \tag{21}$$

In order to control the mutual multiplicative properties of n_1 and n_2 we decompose these variables as

$$\begin{cases} (n_1,n_2) = d, \\ n_1 = d\nu_1,\ n_2 = d\nu_2,\ (\nu_1,\nu_2) = 1, \\ \nu_1 = d_1\nu_1' \text{ with } d_1 \mid d^{\infty} \text{ and } (\nu_1',d) = 1. \end{cases} \tag{22}$$

Thanks to $|\beta_n| \le \tau_k(n)$ and to (9) the contribution of the pairs (n_1,n_2) with $d > X^{\varepsilon}$ to the right–hand side of (12) is negligible since it is

$$\begin{aligned} &\ll X^{\eta}\sum_{X^{\varepsilon}<d\le 2N}\sum_{m\sim M}\sum_{\substack{\nu_1\sim N/d\\ dm\nu_1-a\neq 0}}\sum_{\substack{q\sim Q\\ q\mid d\nu_1m-a}}\sum_{\substack{\nu_2\sim N/d\\ \nu_2\equiv\nu_1 \bmod q}} 1 \\ &\ll X^{\eta}\sum_{X^{\varepsilon}<d\le 2N}\sum_{m\sim M}\sum_{\substack{\nu_1\sim N/d\\ dm\nu_1-a\neq 0}}\tau_2(|d\nu_1m-a|)\Big(\frac{N}{dQ}+1\Big) \\ &\ll MN^2Q^{-1}X^{\eta-\varepsilon} + X^{1+\eta}. \end{aligned} \tag{23}$$

Now consider the contribution of the pairs (n_1,n_2) with $d \le X^{\varepsilon}$ and $d_1 > X^{\varepsilon}$ to the right–hand side of (12). It is

$$\ll X^{\eta} \sum_{d\leq X^{\varepsilon}} \sum_{\substack{X^{\varepsilon}<d_1<2N\\ d_1|d^{\infty}}} \sum_{m\sim M} \sum_{\substack{\nu_1'\sim N/(dd_1)\\ dd_1m\nu_1'-a\neq 0}} \sum_{\substack{q\sim Q\\ q|dd_1\nu_1'm-a}} \sum_{\substack{\nu_2\sim N/d\\ \nu_2\equiv d_1\nu_1' \bmod q}} 1$$

$$\ll X^{\eta} \sum_{d\leq X^{\varepsilon}} \sum_{\substack{X^{\varepsilon}<d_1<2N\\ d_1|d^{\infty}}} \sum_{m\sim M} \sum_{\substack{\nu_1'\sim N/(dd_1)\\ dd_1m\nu_1'-a\neq 0}} \tau_2(|dd_1\nu_1'm-a|)\Big(\frac{N}{dQ}+1\Big)$$

$$\ll X^{\eta}MN^2Q^{-1} \sum_{d\leq X^{\varepsilon}} \frac{1}{d^2} \sum_{\substack{d_1>X^{\varepsilon}\\ d_1|d^{\infty}}} \frac{1}{d_1} + X^{\eta}MN \sum_{d\leq X^{\varepsilon}} \frac{1}{d} \sum_{\substack{d_1>X^{\varepsilon}\\ d_1|d^{\infty}}} \frac{1}{d_1}$$

$$\ll MN^2Q^{-1}X^{\eta-\frac{\varepsilon}{2}} + X^{1+\eta-\frac{\varepsilon}{2}}. \tag{24}$$

Consider the conditions

$$d < X^{\varepsilon} \text{ and } d_1 < X^{\varepsilon}, \tag{25}$$

and the subsum $\widetilde{W}(Q)$ of $W(Q)$ where the variables n_1 and n_2 satisfy the condition (25). By (23) and (24) we have the equality

$$W(Q) = \widetilde{W}(Q) + O\big(MN^2Q^{-1}X^{\eta-\frac{\varepsilon}{2}} + X^{1+\eta}\big). \tag{26}$$

4.2. Expansion in Fourier series

We apply Lemma 1 to the last sum over m in (12) with H defined in (14). This decomposes $\widetilde{W}(Q)$ into the sum

$$\widetilde{W}(Q) = \widetilde{W}^{\mathrm{MT}}(Q) + \widetilde{W}^{\mathrm{Err1}}(Q) + \widetilde{W}^{\mathrm{Err2}}(Q), \tag{27}$$

where each of the three terms corresponds to the contribution of each term on the right–hand side of (6).

The easiest term is $\widetilde{W}^{\mathrm{Err2}}(Q)$ since, by $|\beta_n| \leq \tau_k(n)$ and (8), it satisfies the inequality

$$\begin{aligned}\widetilde{W}^{\mathrm{Err2}}(Q) &\ll M^{-1} \sum_{Q/2\leq q\leq 5Q/2} \sum_{\substack{n_1,\ n_1\sim N\\ n_1\equiv n_2 \bmod q}} \sum \tau_k(n_1)\tau_k(n_2)\\ &\ll M^{-1}N^2X^{\eta}\end{aligned} \tag{28}$$

According to the restriction (21), we see that the main term is

$$\widetilde{W}^{\mathrm{MT}}(Q) = \hat{\psi}(0)M \sum_{(q,a)=1} \frac{\psi(q/Q)}{q} \sum_{(\delta,q)=1} \Big(\sum_{\substack{n_1,\ n_2\sim N\\ n_1\equiv n_2\equiv\delta \bmod q}} \sum \beta_{n_1}\beta_{n_2}\Big), \tag{29}$$

where the variables n_1 and n_2 satisfy the conditions (25). By a similar computation leading to (23) and (24) we can drop these conditions at the cost of the same error term. In other words the equality (29) can be written as

$$\widetilde{W}^{\mathrm{MT}}(Q) = W^{\mathrm{MT}}(Q) + O\big(MN^2Q^{-1}X^{\eta-\frac{\varepsilon}{2}} + X^{1+\eta}\big), \tag{30}$$

where $W^{\mathrm{MT}}(Q)$ is the new main term, which is defined by

$$W^{\mathrm{MT}}(Q) = \hat{\psi}(0)M \sum_{(q,a)=1} \frac{\psi(q/Q)}{q} \sum_{(\delta,q)=1} \Big(\sum_{\substack{n\sim N\\ n\equiv\delta \bmod q}} \beta_n\Big)^2. \tag{31}$$

4.3. Dealing with the main terms

We now gather the main terms appearing in (13), (17), (26), (27), (30), and in (31). The main term of $W(Q)-2V(Q)+U(Q)$ is

$$W^{\mathrm{MT}}(Q)-2V^{\mathrm{MT}}(Q)+U^{\mathrm{MT}}(Q)$$
$$=\hat{\psi}(0)M\sum_{(q,a)=1}\frac{\psi(q/Q)}{q}\sum_{(\delta,q)=1}\Big(\sum_{\substack{n\sim N\\ n\equiv\delta \bmod q}}\beta_n-\frac{1}{\varphi(q)}\sum_{\substack{n\sim N\\ (n,q)=1}}\beta_n\Big)^2.$$

Appealing to Lemma 3 we deduce that, for any A, we have the equality

$$W^{\mathrm{MT}}(Q)-2V^{\mathrm{MT}}(Q)+U^{\mathrm{MT}}(Q)=O\Big(M\cdot Q^{-1}\cdot N^2(\log 2N)^{-A}\Big) \tag{32}$$

provided that

$$Q\le N(\log 2N)^{-B}, \tag{33}$$

for some $B=B(A)$.

4.4. Preparation of the exponential sums

By the definition (27), we have the equality

$$\widetilde{W}^{\mathrm{Err1}}(Q)=M\sum_q\frac{\psi(q/Q)}{q}\sum_{\substack{n_1,\ n_2\sim N\\ n_1\equiv n_2 \bmod q}}\sum\beta_{n_1}\beta_{n_2}\sum_{0<|h|\le H}\hat{\psi}\Big(\frac{h}{q/M}\Big)e\Big(\frac{ah\overline{n_1}}{q}\Big),$$

where the variables (n_1,n_2) are such the associated d and d_1 satisfy (25).

This implies that any pair (n_1,n_2) satisfies $n_1-n_2\neq 0$ and since we have $n_1\equiv n_2 \bmod q$ (see (21)) these integers cannot be near to each other, indeed they satisfy the inequality

$$|n_1-n_2|\ge Q/2.$$

Since we have $(n_1n_2,q)=1$, we can equivalently write the congruence $n_1-n_2\equiv 0 \bmod q$ as

$$\nu_1-\nu_2=d_1\nu_1'-\nu_2=qr, \tag{34}$$

and instead of summing over q, we will sum over r. Note that $1\le|r|\le R/d$, where

$$R=2NQ^{-1}. \tag{35}$$

In the summations, the pair of variables (n_1,n_2) is replaced by the quadruple (d,d_1,ν_1',ν_2) (see (22)). The variables d and d_1 are small, so we expect no substantial cancellations when summing over them. Hence for some

$$d,\,d_1\le X^{\varepsilon},\ d_1\mid d^{\infty},$$

we have the inequality

$$\widetilde{W}^{\mathrm{Err1}}(Q)\ll X^{2\varepsilon}MQ^{-1}\big|\mathcal{W}\big|, \tag{36}$$

where $\mathcal{W}=\mathcal{W}(d,d_1)$ is the quadrilinear form in the four variables r, ν_1', ν_2 and h defined by

$$\mathcal{W}=\sum_{1\le|r|\le R/d}\sum_{\substack{dd_1\nu_1',\ d\nu_2\sim N\\ d_1\nu_1'\equiv\nu_2 \bmod r}}\sum\beta_{dd_1\nu_1'}\beta_{d\nu_2}\frac{\psi\big((d_1\nu_1'-\nu_2)/(rQ)\big)}{(d_1\nu_1'-\nu_2)/(rQ)}$$
$$\sum_{0<|h|\le H}\hat{\psi}\Big(\frac{h}{(d_1\nu_1'-\nu_2)/(rM)}\Big)e(\cdot), \tag{37}$$

where $e(\cdot)$ is the oscillating factor

$$e(\cdot) = e\Big(\frac{ah\,\overline{dd_1\nu_1'}}{(d_1\nu_1'-\nu_2)/r}\Big),$$

and where the variables satisfy the following divisibility conditions:

$$(d_1\nu_1', \nu_2) = 1,\ (\nu_1', d) = 1 \text{ and } (dd_1\nu_1' r, d_1\nu_1' - \nu_2) = r.$$

Using Bézout's reciprocity formula we transform the factor $e(\cdot)$ as follows:

$$\frac{ah\,\overline{dd_1\nu_1'}}{(d_1\nu_1'-\nu_2)/r} = -ah\frac{\overline{(d_1\nu_1'-\nu_2)/r}}{dd_1\nu_1'} + \frac{ahr}{dd_1\nu_1'(d_1\nu_1'-\nu_2)} \bmod 1.$$

Since $(dd_1, \nu_1') = (r, \nu_1') = 1$ we can apply Bézout formula again, giving the equalities

$$\begin{aligned} ah\frac{\overline{(d_1\nu_1'-\nu_2)/r}}{dd_1\nu_1'} &= ah\frac{\overline{\nu_1'}\,\overline{(d_1\nu_1'-\nu_2)/r}}{dd_1} + ah\frac{\overline{dd_1}\,\overline{(d_1\nu_1'-\nu_2)/r}}{\nu_1'} \bmod 1 \\ &= ah\frac{\overline{\nu_1'}\,\overline{(d_1\nu_1'-\nu_2)/r}}{dd_1} - ah\frac{r\overline{dd_1\nu_2}}{\nu_1'} \bmod 1 \end{aligned}$$

The first term on the right–hand side of the above equality depends only on the congruences classes of a, h, r, ν_1' and ν_2 modulo dd_1. As a consequence of the above discussion, we see that there exists a coefficient $\xi = \xi(a, h, r, \nu_1', \nu_2)$ of modulus 1, depending only on the congruence classes of a, h, r, ν_1' and ν_2 modulo dd_1 such that we have the equality

$$e(\cdot) = \xi \cdot e\Big(\frac{ahr}{dd_1\nu_1'(d_1\nu_1'-\nu_2)}\Big) \cdot e\Big(\frac{ahr\overline{dd_1\nu_2}}{\nu_1'}\Big).$$

Returning to (37), and fixing the congruences classes modulo dd_1 of the variables h, r, ν_1' and ν_2, we see that there exists

$$0 \leq a_1, a_2, a_3, a_4 < dd_1$$

such that $\mathcal{W}$ satisfies the inequality,

$$|\mathcal{W}| \leq X^{6\varepsilon} \sum_{\substack{1\leq|r|\leq R/d \\ r\equiv a_1 \bmod dd_1}} \Big| \sum_{\substack{dd_1\nu_1',\, d\nu_2\sim N \\ d_1\nu_1'\equiv\nu_2 \bmod r \\ \nu_1'\equiv a_2 \bmod dd_1 \\ \nu_2\equiv a_3 \bmod dd_1}} \beta_{dd_1\nu_1'}\beta_{d\nu_2} \sum_{\substack{1\leq|h|\leq H \\ h\equiv a_4 \bmod dd_1}} \Psi_r(h, \nu_1', \nu_2) e\Big(\frac{ahr\overline{dd_1\nu_2}}{\nu_1'}\Big)\Big|, \quad (38)$$

where Ψ_r is the differentiable function

$$\Psi_r(h, \nu_1', \nu_2) = \frac{\psi\big((d_1\nu_1'-\nu_2)/(rQ)\big)}{(d_1\nu_1'-\nu_2)/(rQ)}\,\hat{\psi}\Big(\frac{h}{(d_1\nu_1'-\nu_2)/(rM)}\Big)\,e\Big(\frac{ahr}{dd_1\nu_1'(d_1\nu_1'-\nu_2)}\Big),$$

In order to perform the Abel summation over the variables ν_1', ν_2 and h (see for instance [9, Lemme 5]) we must have information on the partial derivatives of the Ψ_r–function. Indeed for $0 \leq \epsilon_0,\, \epsilon_1, \epsilon_2 \leq 1$, we have the inequality

$$\frac{\partial^{\epsilon_0+\epsilon_1+\epsilon_2}}{\partial h^{\epsilon_0}\partial {\nu_1'}^{\epsilon_1}\partial \nu_2^{\epsilon_2}}\Psi_r(h, \nu_1', \nu_2) \ll X^{50\varepsilon}|h|^{-\epsilon_0}\,{\nu_1'}^{-\epsilon_1}\,\nu_2^{-\epsilon_2}\big(N/(rQ)\big)^{\epsilon_1+\epsilon_2}, \quad (39)$$

as a consequence of the inequality $|d_1\nu_1' - \nu_2| \geq rQ/2$ (see(34)), of the definition of H (see (14)) and of the inequality $1 \leq |a| \leq X$.

Since $(d_1\nu_1'\nu_2, r) = 1$ we detect the congruence $d_1\nu_1' \equiv \nu_2 \bmod r$ by the $\varphi(r)$ Dirichlet characters χ modulo r. By (39) we eliminate the function Ψ_r in the inequality (38) which becomes

$$|\mathcal{W}| \leq X^{60\varepsilon} N^2 Q^{-2} \sum_{\substack{1\leq|r|\leq R/d \\ r\equiv a_1 \bmod dd_1}} \frac{1}{\varphi(r)\, r^2} \sum_{\chi \bmod r} \Big| \sum_{\substack{dd_1\nu_1'\in\mathcal{N}_1 \\ \nu_1'\equiv a_2 \bmod dd_1 \\ \nu_2\equiv a_3 \bmod dd_1}} \sum_{d\nu_2\in\mathcal{N}_2} \chi(d\nu_1')\overline{\chi}(\nu_2)\beta_{dd_1\nu_1'}\beta_{d\nu_2} \sum_{\substack{h\in\mathcal{H} \\ h\equiv a_4 \bmod dd_1}} e\Big(\frac{ahr\overline{dd_1\nu_2}}{\nu_1'}\Big)\Big|, \quad (40)$$

- where $\mathcal{N}_1$ and $\mathcal{N}_2$ are two intervals included in $[N, 2N]$,
- and where $\mathcal{H}$ is the union of two intervals included in $[-H, -1]$ and $[1, H]$ respectively.

Denote by $\mathcal{W}_1(r,\chi)$ the inner sum over ν_1', ν_2 and h in (40). Remark that the trivial bound for $\mathcal{W}_1(r,\chi)$ is $O(X^\eta HN^2/(d^2d_1))$. We now can apply Lemma 5 to the sum $\mathcal{W}_1(r,\chi)$, with the choice of parameters

$$\vartheta \to ar,\ A \to H, M \to N \text{ and } N \to N.$$

We obtain the bound

$$\mathcal{W}_1(r,\chi) \ll H^{\frac12}N^{\frac12}N^{\frac12}X^{\varepsilon+\eta}\Big(1+\frac{|a|\,|r|H}{N^2}\Big)\Big((HN^2)^{\frac{7}{20}+\varepsilon}N^{\frac14}+(HN^2)^{\frac38+\varepsilon}(HN)^{\frac18}\Big).$$

By the definition (35), (14) and the inequality $1 \leq |a| \leq X$ we deduce the inequality

$$\mathcal{W}_1(r,\chi) \ll X^{4\varepsilon+\eta}\big(H^{\frac{17}{20}}N^{\frac{39}{20}}+HN^{\frac{15}{8}}\big),$$

and using (14) we finally deduce

$$\mathcal{W}_1(r,\chi) \ll X^{5\varepsilon+\eta}\big(M^{-\frac{17}{20}}N^{\frac{39}{20}}Q^{\frac{17}{20}}+M^{-1}N^{\frac{15}{8}}Q\big).$$

Returning to (40), summing over χ and r and inserting into (36) we obtain the bound

$$\widetilde{W}^{\mathrm{Err1}}(Q) \ll X^{67\varepsilon+\eta}\big(M^{\frac{3}{20}}N^{\frac{79}{20}}Q^{-\frac{43}{20}}+N^{\frac{31}{8}}Q^{-2}\big). \quad (41)$$

4.5. Conclusion

We have now all the elements to bound $\Delta(\boldsymbol{\alpha},\boldsymbol{\beta},M,N,Q,a)$. By (10), (13), (20), (26), (27), (28), (30) and (41) we have the inequality

$$\begin{aligned}\Delta^2 \ll MQ\mathcal{L}^{k^2-1}\Big\{&\Big(W^{\mathrm{MT}}(Q)-2V^{\mathrm{MT}}(Q)+U^{\mathrm{MT}}(Q)\Big)+N^2Q^{-1}X^\eta\\ &+(M^{-1}N^2+N^{\frac52}Q^{-1})X^{2\varepsilon+\eta}\\ &+\big(MN^2Q^{-1}X^{\eta-\frac{\varepsilon}{2}}+X^{1+\eta}\big)+X^{67\varepsilon+\eta}\big(M^{\frac{3}{20}}N^{\frac{79}{20}}Q^{-\frac{43}{20}}+N^{\frac{31}{8}}Q^{-2}\big)\Big\},\end{aligned}$$

which is shortened in (recall (8))

$$\begin{aligned}\Delta^2 \ll MQ\mathcal{L}^{k^2-1}\Big\{&MN^2Q^{-1}(\log 2N)^{-A}+\\ &+MN^2Q^{-1}X^{\eta-\frac{\varepsilon}{2}}+X^{67\varepsilon+\eta}\big(M^{\frac{3}{20}}N^{\frac{79}{20}}Q^{-\frac{43}{20}}+N^{\frac{31}{8}}Q^{-2}\big)\Big\},\end{aligned}$$

by (32) and (33) if one assumes

$$Q \leq NX^{-\varepsilon}. \tag{42}$$

To finish the proof of Theorem 1, it remains to find sufficient conditions over M, N and Q to ensure the bound $\Delta^2 \ll M^2N^2\mathcal{L}^{-A}$. Choosing $\eta = \varepsilon/5$, we have to study the following three inequalities hold

$$\begin{cases} MQ \cdot MN^2Q^{-1}X^{-\frac{\varepsilon}{4}} & \ll M^2N^2X^{-\frac{\varepsilon}{4}}, \\ MQ \cdot M^{\frac{3}{20}}N^{\frac{79}{20}}Q^{-\frac{43}{20}}X^{68\varepsilon} & \ll M^2N^2X^{-\frac{\varepsilon}{4}}, \\ MQ \cdot N^{\frac{31}{8}}Q^{-2}X^{68\varepsilon} & \ll M^2N^2X^{-\frac{\varepsilon}{4}}. \end{cases} \tag{43}$$

The first inequality is trivially satisfied. The second inequality of (43) is satisfied as soon as

$$Q > N^{\frac{56}{23}}X^{-\frac{17}{23}+65\varepsilon}. \tag{44}$$

This inequality combined with (42) implies that $N < X^{\frac{17}{33}}$. The last condition of (43) is satisfied as soon as

$$Q > N^{\frac{23}{8}}X^{-1+69\varepsilon}.$$

We can drop this condition since it is a consequence of (44) and of the inequality $N < X^{\frac{17}{33}}$. The proof of Theorem 1 is now complete.

5. Proof of Corollary 1

Let $S(M,N)$ be the sum we are studying in this corollary. We use Dirichlet's hyperbola argument to write

$$mn - 1 = qr, \tag{45}$$

and by symmetry we can impose the condition $q < r$. This symmetry creates a factor 2 unless $mn-1$ is a perfect square. The contribution to $S(M,N)$ of the (m,n) such that $mn-1$ is a square is bounded by $O(X^{\frac{1}{2}+\eta})$ with $\eta > 0$ arbitrary. This is a consequence of $|\beta_n| \leq \tau_k(n)$.

The decomposition (45), the constraint $q < r$ and the inequalities $X - 1 \leq mn - 1 < 4X$ imply that $q \leq 2X^{\frac{1}{2}}$. In counterpart, if $q < X^{\frac{1}{2}}$ we are sure that $q < r$. Thus we have the equality

$$\begin{aligned} S(M,N) &= 2\sum_{q\leq X^{1/2}}\sum_{\substack{m\sim M\\ mn\equiv 1 \bmod q}}\sum_{n\sim N}\alpha_m\beta_n + 2\sum_{\substack{m\sim M,\ n\sim N, X^{1/2}<q\leq 2X^{1/2}}}\sum\sum\sum\sum_{mn-1=qr,\, q<r}\alpha_m\beta_n + O(X^{\frac{1}{2}+\eta}) \\ &= 2S_0(M,N) + 2S_1(M,N) + O(X^{\frac{1}{2}+\eta}), \end{aligned} \tag{46}$$

by definition. A direct application of Theorem 1 with $Q = X^{\frac{1}{2}}$ gives the equality

$$S_0(M,N) = \sum_{q\leq X^{1/2}}\frac{1}{\varphi(q)}\sum_{\substack{m\sim M\\ (mn,q)=1}}\sum_{n\sim N}\alpha_m\beta_n + O(X\mathcal{L}^{-C}), \tag{47}$$

for any C.

For the second term $S_1(M,N)$, we must get rid of the constraint $q < r$. A technique among others is to precisely control the size of the variables m, n and q. If it is so, then $r = (mn-1)/q$ is also controlled and one can check if it satisfies $r > q$. We introduce the following factor of dissection:

$$\Delta = 2^{\frac{1}{[\mathcal{L}^B]}},$$

where $B = B(A)$ is a parameter to be fixed later, and where $[y]$ is the largest integer $\leq y$. If we denote by $L_0 = [\mathcal{L}^B]$ we see that $\Delta^{L_0} = 2$ and that $\Delta = 1 + O(\mathcal{L}^{-B})$. We denote by M_0, N_0 and Q_0 any numbers in the sets

$$\mathcal{M}_0 := \{M, \Delta M, \Delta^2 M, \Delta^3 M, \cdots, \Delta^{L_0-1} M\}$$
$$\mathcal{N}_0 := \{N, \Delta N, \Delta^2 N, \Delta^3 N, \cdots, \Delta^{L_0-1} N\}$$
$$\mathcal{Q}_0 := \{X^{\frac{1}{2}}, \Delta X^{\frac{1}{2}}, \Delta^2 X^{\frac{1}{2}}, \Delta^3 X^{\frac{1}{2}}, \cdots, \Delta^{L_0-1} X^{\frac{1}{2}}\},$$

respectively. We split $S_1(M, N)$ into

$$S_1(M, N) = \sum_{M_0 \in \mathcal{M}_0} \sum_{N_0 \in \mathcal{N}_0} \sum_{Q_0 \in \mathcal{Q}_0} S_1(M_0, N_0, Q_0), \tag{48}$$

where $S_1(M_0, N_0, Q_0)$ is defined by

$$S_1(M_0, N_0, Q_0) = \sum_{q \simeq Q_0} \sum_{\substack{m \simeq M_0, \\ mn \equiv 1 \bmod q}} \sum_{n \simeq N_0} \alpha_m \beta_n.$$

- where the notation $y \simeq Y_0$ means that the integer y satisfies the inequalities $Y_0 \leq y < \Delta Y_0$,
- where the variables m, n and q satisfy the extra condition

$$mn - 1 > q^2. \tag{49}$$

Note that the decomposition (48) contains

$$O(\mathcal{L}^{3B}), \tag{50}$$

terms.

Since $mn - 1 \geq M_0 N_0 - 1$ and $q^2 < Q_0^2 \Delta^2$ in each sum $S_1(M_0, N_0, Q_0)$, we can drop the condition (49) in the definition of this sum as soon as we have

$$M_0 N_0 - 1 > Q_0^2 \Delta^2. \tag{51}$$

When (51) is satisfied, the variables m, n and q are independent and a direct application of Theorem 1 gives for each sum $S_1(M_0, N_0, Q_0)$, the equality

$$S_1(M_0, N_0, Q_0) = \sum_{q \simeq Q_0} \frac{1}{\varphi(q)} \sum_{\substack{m \simeq M_0, \\ (mn,q)=1}} \sum_{n \simeq N_0} \alpha_m \beta_n + O_C(X \mathcal{L}^{-C}), \tag{52}$$

where C is arbitrary.

It remains to consider the case where (51) is not satisfied, which means that $(M_0, N_0, Q_0) \in \mathcal{E}_0$ where

$$\mathcal{E}_0 := \left\{(M_0, N_0, Q_0)\,;\ M_0 N_0 - 1 \leq Q_0^2 \Delta^2\right\}. \tag{53}$$

We now show that the variable n considered in such a $S_1(M_0, N_0, Q_0)$ varies in a rather short interval. More precisely, since $M_0 \Delta > m, N_0 \Delta > n$ and $Q_0 < q$ we deduce from the definition (53) that $q^2 \geq mn\Delta^{-4} - \Delta^{-2}$ which implies the inequality $q \geq (mn)^{\frac{1}{2}} \Delta^{-2} - 1$. Combining with (49), we get the inequality

$$(mn)^{\frac{1}{2}} \Delta^{-2} - 1 < q < (mn)^{\frac{1}{2}}$$

which implies

$$(q^2/m) < n < ((q+1)^2/m)\Delta^4.$$

Using the inequality

$$X^{1/2} \leq q \leq 2X^{1/2} \ll (Q^2/M)(\Delta^4-1)X^{-\frac{\delta}{2}},$$

and $|\beta_n| \leq \tau_k(n)$ we apply Lemma 2 to see that

$$\begin{aligned}
&\sum_{(M_0,N_0,Q_0)\in\mathcal{E}_0}\sum\sum S_1(M_0,N_0,Q_0)\\
&\ll \sum_{m\sim M}\tau_k(m)\sum_{\substack{q\sim X^{1/2}\\(q,m)=1}}\sum_{(q^2/m)<n<((q+1)^2/m)\Delta^4}\tau_k(n)\\
&\ll (\Delta^4-1)\mathcal{L}^{k-1}\sum_{m\sim M}\tau_k(m)\sum_{q\sim X^{1/2}}\frac{1}{\varphi(q)}\cdot\frac{q^2}{m}\\
&\ll \mathcal{L}^{2k-2-B}X.
\end{aligned}$$

Actually, by introducing a main term back, which is less than the error term, we can also write this bound as an equality

$$\begin{aligned}
&\sum_{(M_0,N_0,Q_0)\in\mathcal{E}_0}\sum\sum S_1(M_0,N_0,Q_0)\\
&\qquad=\sum_{(M_0,N_0,Q_0)\in\mathcal{E}_0}\sum\sum_{q\simeq Q_0}\frac{1}{\varphi(q)}\sum_{\substack{m\simeq M_0,\ n\simeq N_0\\(mn,q)=1}}\sum\alpha_m\beta_n+O(\mathcal{L}^{2k-2-B}),
\end{aligned}\tag{54}$$

where the variables (m,n,q) continue to satisfy (49).

Gathering (46), (47), (48), (50), (52), (54) we obtain

$$\begin{aligned}
S(M,N)=2\sum_{q\leq X^{1/2}}\frac{1}{\varphi(q)}\sum_{\substack{m\sim M\\(mn,q)=1}}\sum_{n\sim N}\alpha_m\beta_n\\
+2\sum_{M_0\in\mathcal{M}_0}\sum_{N_0\in\mathcal{N}_0}\sum_{Q_0\in\mathcal{Q}_0}\sum_{q\simeq Q_0}\frac{1}{\varphi(q)}\sum_{\substack{m\simeq M_0,\ n\simeq N_0\\(mn,q)=1}}\sum\alpha_m\beta_n\\
+O(\mathcal{L}^{3B-C}X)+O(\mathcal{L}^{2k-2-B}X)+O(X^{\frac{1}{2}+\eta}),
\end{aligned}$$

where the variables (m,n,q) continue to satisfy (49). Putting the different summations back together, we complete the proof of Corollary 1 by choosing B and C in order to satisfy the equalities $-A=3B-C=2k-2-B$.

REFERENCES

1. S. Bettin and V. Chandee. Trilinear forms with Kloosterman fractions. *Adv. Math.*, 328:1234–1262, 2018.

2. E. Bombieri. *Le grand crible dans la théorie analytique des nombres.* Société Mathématique de France, Paris, 1974. Avec une sommaire en anglais, Astérisque, No. 18.

3. E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Math.*, 156(3-4):203–251, 1986.

4. E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. II. *Math. Ann.*, 277(3):361–393, 1987.

5. W. Castryck, É. Fouvry, G. Harcos, E. Kowalski, P. Michel, P. Nelson, E. Paldi, J. Pintz, A. V. Sutherland, T. Tao, and X-F. Xie. New equidistribution estimates of Zhang type. *Algebra Number Theory*, 8(9):2067–2199, 2014.

6. S. Drappeau. Sums of Kloosterman sums in arithmetic progressions, and the error term in the dispersion method. *Proc. Lond. Math. Soc. (3)*, 114(4):684–732, 2017.

7. W. Duke, J. Friedlander, and H. Iwaniec. Bilinear forms with Kloosterman fractions. *Invent. Math.*, 128(1):23–43, 1997.

8. É. Fouvry. Répartition des suites dans les progressions arithmétiques. *Acta Arith.*, 41(4):359–382, 1982.

9. É. Fouvry. Autour du théorème de Bombieri-Vinogradov. *Acta Math.*, 152(3-4):219–244, 1984.

10. É. Fouvry. Sur le problème des diviseurs de Titchmarsh. *J. Reine Angew. Math.*, 357:51–76, 1985.

11. É. Fouvry. Autour du théorème de Bombieri-Vinogradov. II. *Ann. Sci. École Norm. Sup. (4)*, 20(4):617–640, 1987.

12. É. Fouvry and M. Radziwiłł. Level of distribution of unbalanced sequences. *pre-print*, 2018.

13. H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

14. Ju. V. Linnik. *The dispersion method in binary additive problems*. Translated by S. Schuur. American Mathematical Society, Providence, R.I., 1963.

15. T. Tao. The Elliott-Halberstam conjecture implies the Vinogradov least quadratic nonresidue conjecture. *Algebra Number Theory*, 9(4):1005–1034, 2015.

16. Y. Zhang. Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014.

Получено 22.06.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 517.957 DOI 10.22405/2226-8383-2018-19-3-164-182

О разрешимости вариационной задачи Дирихле для одного класса вырождающихся эллиптических операторов

Исхоков Сулаймон Абунасрович — доктор физико-математических наук, профессор, член-корреспондент АН РТ, Зам. директора Института математики им. А. Джураева АН Республики Таджикистан.
e-mail: sulaimon@mail.ru
Якушев Илья Анатольевич — кандидат физико-математических наук, доцент кафедры фундаментальной и прикладной математики Политехнического института (филиала) Северо-Восточного федерального университета им. М. К. Аммосова в г. Мирном.
e-mail: Yakushevilya@mail.ru

Аннотация

В работе исследуется однозначная разрешимость вариационной задачи Дирихле, связанной с интегро-дифференциальной полуторалинейной формой

$$B[u,\,v]=\sum_{j\in J}B_j[u,\,v], \qquad (*)$$

где

$$B_j[u,\,v]=\sum_{|k|=|l|=j}\int_\Omega \rho(x)^{2\tau_j}b_{kl}(x)u^{(k)}(x)\,\overline{v^{(l)}(x)}dx,$$

Ω — ограниченная область в евклидовом пространстве R^n с замкнутой $(n-1)$-мерной границей $\partial\Omega$, $\rho(x)$, $x\in\Omega$, — регуляризованное расстояние от точки $x\in\Omega$ до $\partial\Omega$, k — мультииндекс, $u^{(k)}(x)$ — обобщенная производная мультииндекса k функции $u(x)$, $x\in\Omega$, $b_{kl}(x)$ — ограниченные в Ω комплекснозначные функции, $J\subset\{1,\,2,\,\ldots,\,r\}$ и τ_j, $j\in J$, — вещественные числа. Предполагается, что $r\in J$. Вырождение коэффициентов дифференциального оператора, ассоциированного с формой (*), называется согласованным, если существует число α такое, что $\tau_j=\alpha+j-r$ при всех $j\in J$. В противном случае оно называется несогласованным.

Вариационная задача Дирихле, связанная с формой (*), в случае согласованного вырождения коэффициентов хорошо исследована во многих работах, где также предполагается, что форма (*) удовлетворяет условию коэрцитивности. Следует отметить, что случай несогласованного вырождения коэффициентов сопряжен с некоторыми техническими сложностями и рассмотрен лишь в некоторых отдельных работах. В этом случае с помощью теорем вложения пространств дифференцируемых функций со степенными весами выделяются старшие формы $B_j[u,\,v]$, $j\in J_2\subset J$ и доказывается, что разрешимость вариационной задачи Дирихле в основном зависит от старших форм.

В работе рассматривается случай несогласованного вырождения коэффициентов исследуемого оператора и, в отличие от ранее опубликованных работ по этому направлению, допускается случай, когда основная форма (*) может не удовлетворять условию коэрцитивности.

Ключевые слова: Вариационная задача Дирихле, эллиптический оператор, несогласованное вырождение, некоэрцитивная форма.

Библиография: 16 названий.

Для цитирования:
С. А. Исхоков, И. А. Якушев. О разрешимости вариационной задачи Дирихле для одного класса вырождающихся эллиптических операторов // Чебышевский сборник, 2018, т. 19, вып. 3, с. 164–182.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 517.957 DOI 10.22405/2226-8383-2018-19-3-164-182

On solvability of variational Dirichlet problem for a class of degenerate elliptic operators

Iskhokov Sulaimon Abuzarovich — doctor of physical and mathematical sciences, professor, corresponding member of the Academy of Sciences RT, deputy director of the Dzhuraev Institute of Mathematics, Academy of Sciences of the Republic of Tajikistan.
e-mail: sulaimon@mail.ru
Yakushev Ilya Anatolyevich — kandidat of physical and mathematical sciences, associate professor of the department of fundamental and applied mathematics, Mirny Polytechnic Institute, the branch of Ammosov North-Eastern Federal University.
e-mail: Yakushevilya@mail.ru

Abstract

The paper is devoted to investigation of unique solvability of the Dirichlet variational problem associated with integro-differential sesquilinear form

$$B[u,\,v]=\sum_{j\in J}B_j[u,\,v], \tag{*}$$

where

$$B_j[u,\,v]=\sum_{|k|=|l|=j}\int_\Omega \rho(x)^{2\tau_j}b_{kl}(x)u^{(k)}(x)\,\overline{v^{(l)}(x)}dx,$$

Ω — a bounded domain in the euclidian space R^n with a closed $(n-1)$-dimensional boundary $\partial\Omega$, $\rho(x)$, $x\in\Omega$, — a regularized distance from a point $x\in\Omega$ to $\partial\Omega$, k — a multi-index, $u^{(k)}(x)$ — a generalized derivative of multi-index k of a function $u(x)$, $x\in\Omega$, $b_{kl}(x)$ — bounded in Ω complex-valued functions, $J\subset\{1,\,2,\,\ldots,\,r\}$ and τ_j, $j\in J$, — real numbers. It is assumed that $r\in J$. A degeneracy of coefficients of the differential operator associated with the form (*), is said to be coordinated if there exist a number α such that $\tau_j=\alpha+j-r$ for all $j\in J$. Otherwise it is called uncoordinated.

The variational Dirichlet problem associated with the form (*) in the case of coordinated degeneracy of coefficients is well studied in many papers, where it is also assumed that the form (*) satisfies a coercivness condition. It should be mentioned that the case of uncoordinated degeneracy of the coefficients is fraught with some technical complexities and it was only considered in some separate papers. In this case with the aid of embedding theorems for spaces of differentiable functions with power weights leading forms $B_j[u,\,v]$, $j\in J_2\subset J$, are separated and it is proved that solvability of the variational Dirichlet problem is generally depends on the leading forms.

We consider the case of uncoordinated degeneracy of coefficients of the operator under investigation and, in contrast to previously published works on this direction, it is allowed that the main form (*) does not obey coerciveness condition.

Keywords: Variational Dirichlet problem, elliptic operator, uncoordinated degeneration, noncoercive form

Bibliography: 16 titles.

For citation:
S. A. Iskhokov, I. A. Yakushev. 2018, "On solvability of variational Dirichlet problem for a class of degenerate elliptic operators", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 164–182.

1. Введение

Работа посвящена исследованию разрешимости вариационной задачи Дирихле с однородными граничными условиями для эллиптических операторов в ограниченной области со степенным вырождением на границе области.

Пусть R^n — n-мерное евклидово пространство точек $x = (x_1, \ldots, x_n)$ и Ω — ограниченная область в R^n с замкнутой $(n-1)$-мерной границей $\partial\Omega$. Символом $\rho(x)$ обозначим положительную функцию класса $C^\infty(\Omega)$ со следующими свойствами

$$\rho(x) \le \operatorname{dist}\{x, \partial\Omega\} \le M\rho(x), \quad |\rho^{(k)}(x)| \le M_k \rho^{1-|k|}(x),$$

для любого $x \in \Omega$ и любого мультииндекса $k = (k_1, k_2, \cdots, k_n)$; M, M_k — некоторые положительные постоянные и $|k| = k_1 + k_2 + \cdots + k_n$ — длина мультииндекса k.

Пусть r — натуральное число и J — некоторое подмножество множества $\{0, 1, \ldots, r\}$, причем $r \in J$. Пусть τ_j, $j \in J$, — вещественные числа. Рассмотрим дифференциальный оператор

$$L[u] = \sum_{|k|=|l|=j\in J} (-1)^j \left(\rho(x)^{2\tau_j} b_{kl}(x) u^{(k)}(x)\right)^{(l)}, \tag{1}$$

который понимается в смысле теории распределений на Ω. Предполагается, что коэффициенты $b_{kl}(x)$, $x \in \Omega$, являются ограниченными комплекснозначными функциями.

Определение 1. Вырождение коэффициентов оператора (1) называется **согласованным**, если существует число α такое, что $\tau_j = \alpha + j - r$ при всех $j \in J$. В противном случае оно называется **несогласованным**.

Вариационная задача Дирихле для оператора (1) в случае согласованного вырождения коэффициентов хорошо исследована в работах [1] - [13]. Случай несогласованного вырождения коэффициентов рассмотрен только в работе [14].

При этом только в работах [9, 10, 11, 12] рассмотрен случай, когда связанная с оператором (1) интегро-дифференциальная полуторалинейная форма

$$B[u, v] = \sum_{|k|=|l|=j\in J} \int_\Omega \rho(x)^{2\tau_j} b_{kl}(x) u^{(k)}(x)\, \overline{v^{(l)}(x)} dx \tag{2}$$

не является коэрцитивной. Здесь и далее понятие коэрцитивности формы понимается в смысле определения 2.0.1 работы [7]: если H_0 — гильбертово пространство со скалярным произведением $(\cdot,\cdot)_0$ и нормой $\|\cdot\|_0$, H_+ — другое гильбертово пространство с нормой $\|\cdot\|_+$, плотно вложенное в H_0, то определенная в H_+ полуторалинейная форма $P[u, v]$ называется H_+-коэрцитивной относительно H_0, если найдутся числа $\mu_0 \in R$, $\delta_0 > 0$ такие, что

$$\operatorname{Re} P[u, u] + \mu_0 \|u\|_0^2 \ge \delta_0 \|u\|_+^2$$

для всех $u \in H_+$.

В настоящей работе исследуется разрешимость вариационной задачи Дирихле, связанной с оператором (1) в случае несогласованности вырождения его коэффициентов и некоэрцитивности формы (2).

2. Формулировка основных результатов

Пусть j — натуральное, α_j, p_j — вещественные числа и $1 \le p_j < \infty$. Символом $W^j_{p_j;\,\alpha_j}(\Omega)$ обозначим пространство функций $u(x)$, определенных на Ω, имеющих все обобщенные в смысле С.Л.Соболева производные $u^{(k)}(x)$ порядка j с конечной нормой

$$\|u; W^j_{p_j;\,\alpha_j}(\Omega)\| = \left\{ \sum_{|k|=j} \int_\Omega \rho^{p_j\alpha_j}(x)|u^{(k)}(x)|^{p_j}dx + \int_\Omega |u(x)|^{p_j}dx \right\}^{1/p_j}.$$

Полуторалинейную форму (2) представим в виде

$$B[u,\,v] = \sum_{j\in J} B_j[u,\,v], \quad B_j[u,\,v] = \sum_{|k|=|l|=j} \int_\Omega \rho(x)^{2\tau_j} b_{kl}(x) u^{(k)}(x)\,\overline{v^{(l)}(x)}dx.$$

Определение 2. Пусть i_0 — наименьший ненулевой элемент множества J. Если $\tau_{i_0} > i_0$, то через j_0 обозначим наибольшее число из множества J такое, что $j_0 - \tau_{j_0} > i_0 - \tau_{i_0}$. В случае $\tau_{i_0} \le i_0$ через j_0 обозначим наибольшее число из множества J такое, что $\tau_{i_0} > \tau_{j_0} i_0/j_0$. Если же такое число $j_0 \in J$ не существует, то обозначим i_0 через j_0. Пусть i_1 — наименьший ненулевой элемент множества $J \setminus \{i_0,\,j_0\}$. Если $\tau_{i_1} > i_1$, то через j_1 обозначим наибольшее число из множества J такое, что $j_1 - \tau_{j_1} > i_1 - \tau_{i_1}$. В случае $\tau_{i_1} \le i_1$ через j_1 обозначим наибольшее число из множества J такое, что $\tau_{i_1} > \tau_{j_1} i_1/j_1$. Если же такое число $j_1 \in J \setminus \{i_0,\,j_0\}$ не существует, то обозначим i_1 через j_1. Продолжая этот процесс до завершения, представим множество индексов J в виде $J = J_1 \cup J_2$, $J_1 \cap J_2 = \emptyset$, где $J_1 = \{i_0,\,i_1,\,\ldots,\,i_t\}$, $J_2 = \{j_0,\,j_1,\,\ldots,\,j_s\}$. Полуторалинейные формы $B_j[u,\,v]$ с индексами из множества J_2 назовем **старшими**.

Вводим пространство $\mathbb{H}_+$ комплекснозначных функций $u(x)$, $x \in \Omega$ с конечной нормой

$$\|u;\,\mathbb{H}_+\| = \left\{ \sum_{m=0}^{s} \left\| u;\, W^{j_m}_{2;\tau_{j_m}}(\Omega) \right\|^2 \right\}^{1/2}. \tag{3}$$

Символом $\mathbb{H}'_+$ обозначим замыкание $C_0^\infty(\Omega)$ в метрике пространства $\mathbb{H}_+$, а через $\mathbb{H}'_-$ обозначим пространство антилинейных непрерывных функционалов, определенных на $\mathbb{H}'_+$ со следующей нормой

$$\|F;\,\mathbb{H}'_-\| = \sup \frac{|<F,\,u>|}{\|u;\,\mathbb{H}_+\|},$$

где верхняя грань берется по всем ненулевым функциям $u \in \mathbb{H}'_+$. Здесь и далее символом $<F,\,u>$ обозначено значение функционала F на функцию u.

Обозначим через $(\cdot,\,\cdot)_0$ скалярное произведение в $L_2(\Omega)$.

Задача D_λ. Для заданного функционала $F \in \mathbb{H}'_-$ требуется найти решение $U(x)$ уравнения

$$B[U,\,v] + \lambda(U,\,v)_0 = <F, v> \quad \forall v \in C_0^\infty(\Omega), \tag{4}$$

принадлежащее пространству $\mathbb{H}'_+$.

Для каждого $m \in \{0,\,1,\ldots,\,s\}$ вводим функцию

$$L_{j_m}(x,\,\zeta) = \sum_{|k|=|l|=j_m} a_{kl}(x)\zeta_k\overline{\zeta_l},$$

где $x \in \Omega$ и $\zeta = \{\zeta_k\}_{|k|=j_m}$ — набор комплексных чисел.

Далее будем считать, что функция $\arg z$ принимает значения на отрезке $(-\pi,\,\pi]$.

Теорема 1. *Пусть числа τ_j, $j \in J$, такие, что*

$$\tau_j \geq -1/2; \quad \max_{j\in J}(j - \tau_j) > 0. \tag{5}$$

Пусть $m \in \{0, 1, \ldots, s\}$ и найдутся числа $\varphi_m \in (0, \pi)$, $M > 0$ и отличная от нуля в $\overline{\Omega}$ функция $\gamma_m(x) \in C(\overline{\Omega})$ такие, что выполняются следующие неравенства

$$|\arg L_{j_m}(x, \zeta)| < \varphi_m, \tag{6}$$

$$\sum_{|k|=j_m} |\zeta_k|^2 \leq M \mathrm{Re}\,\{\gamma_m(x) L_{j_m}(x, \zeta)\} \tag{7}$$

для всех $x \in \Omega$ и любого набора комплексных чисел $\zeta = \{\zeta_k\}_{|k|=j_m}$.

Тогда найдется число $\lambda_0 \geq 0$ такое, что при $\lambda \geq \lambda_0$ для любого заданного функционала $F \in \mathbb{H}'_-$ существует единственное решение $U(x)$ задачи D_λ и при этом справедлива оценка

$$\|U; \mathbb{H}'_+\| \leq M_0 \left\|F; \mathbb{H}'_-\right\|, \tag{8}$$

где число M_0 не зависит от $\lambda \in [\lambda_0, \infty)$ и от функционала F.

Решение задачи D_λ принадлежит пространству $\mathbb{H}'_+$, в котором плотно множество финитных функций. Поэтому, формально, можно считать, что решение задачи D_λ удовлетворяет однородным граничным условиям. Далее мы исследуем разрешимость следующей задачи с неоднородными граничными условиями.

Задача $\mathbb{D}_\lambda$. Для заданного функционала $F \in \mathbb{H}'_-$ и заданной функции $U_1(x) \in \mathbb{H}_+$ требуется найти решение $U(x)$ уравнения (4), принадлежащее пространству $\mathbb{H}_+$ и удовлетворяющее условию

$$U(x) - U_1(x) \in \mathbb{H}'_+. \tag{9}$$

Условие (9) означает, что решение $U(x)$ задачи $\mathbb{D}_\lambda$ принимает на границе $\partial\Omega$ области Ω те же значения, что и заданная функция $U_1(x)$.

Теорема 2. *Пусть выполнены все условия теоремы 1. Тогда существует число $\lambda_0 \geq 0$ такое, что при $\lambda \geq \lambda_0$ для любого заданного функционала $F \in \mathbb{H}'_-$ и любой заданной функции $U_1(x) \in \mathbb{H}_+$ задачи $\mathbb{D}_\lambda$ имеет единственное решение $U(x)$. Это решение удовлетворяет оценке*

$$\|U; \mathbb{H}'_+\| \leq (M_1 + \lambda) \|U_1; \mathbb{H}_+\| + M_1 \left\|F; \mathbb{H}'_-\right\|, \tag{10}$$

где число M_1 не зависит от $\lambda \in [\lambda_0, \infty)$ и от выбора функционала F и функции $U_1(x)$.

3. Доказательство теоремы 1

Далее нам понадобится следующая вспомогательная лемма.

Лемма 1. *Пусть $p \in [1, \infty)$, $r_1 > r_2 \geq 0$, α_1, α_2 — действительные числа, больше (-1/p). Пусть $r_1 - \alpha_1 > r_2 - \alpha_2$ при $\alpha_2 > r_2$ и $\alpha_2 > \alpha_1 r_2/r_1$, $r_2 > 0$ при $\alpha_2 \leq r_2$. Тогда для любого числа ε найдется постоянная $C = C(\varepsilon)$ такая, что для всех $u \in W^{r_1}_{p;\alpha_1}(\Omega)$ справедлива оценка*

$$\|u; W^{r_2}_{p;\alpha_2}(\Omega)\| \leq \varepsilon \|u; W^{r_1}_{p;\alpha_1}(\Omega)\| + C(\varepsilon)\|u; L_p(\Omega)\|. \tag{11}$$

Доказательство. Если выполняется одно из следующих условий:

1) $r_1 - \alpha_1 > r_2 - \alpha_2$;

2) $\alpha_2 > \alpha_1 r_2/r_1$, $r_2 > 0$,

то неравенство (11) имеет место в силу [7, теорема 1.1.7]. Далее для доказательства леммы 1 достаточно заметить, что в случае $\alpha_2 > r_2$ условие 2) слабее условия 1), а в случае $\alpha_2 \le r_2$ условие 1) слабее условия 2).

Согласно определения 2 для любого индекса $i_n, n \in \{0, 1, \dots, t\}$ найдется индекс $j_m, m \in \{0, 1, \dots, s\}$ такой, что $j_m - \tau_{j_m} > i_n - \tau_{i_n}$ при $\tau_{i_n} > i_n$ или $\tau_{i_n} > \tau_{j_m} i_n / j_m$ при $\tau_{i_n} > i_n$. Поэтому применяя лемму 1, имеем

$$\left\| u;\, W^{i_n}_{2;\,\tau_{i_n}}(\Omega) \right\| \le \varepsilon \left\| u;\, W^{j_m}_{2;\,\tau_{j_m}}(\Omega) \right\| + C(\varepsilon) \left\| u;\, L_2(\Omega) \right\|. \tag{12}$$

Замечание 1. Не ограничивая общности, можно считать, что числа φ_m и функции $\gamma_m(x)$ в условиях (6), (7) не зависят от m. Поэтому далее будем считать, что

$$\varphi_0 = \varphi_1 = \dots = \varphi_s = \varphi, \qquad \gamma_0(x) = \gamma_1(x) = \dots = \gamma_s(x) = \gamma(x),\ x \in \Omega.$$

Пусть ν — достаточно малое положительное число и пусть $\psi_r(x),\ \eta_r(x) \in C^\infty(\Omega)\ (r = \overline{1, N})$ такие, что:

а) $\psi_1^2(x) + \psi_2^2(x) + \dots + \psi_N^2(x) \equiv 1 \quad (x \in \overline{\Omega})$;

б) функция $\eta_r(x)$ обращается в единицу в некоторой окрестности множества $\operatorname{supp} \psi_r(x)$ и $0 \le \eta_r \le 1$ для всех $x \in \overline{\Omega}$;

в) $|\gamma(x) - \gamma(y)| < \nu$ для всех $x,\ y \in \operatorname{supp} \eta_r\ (r = \overline{1, N})$.

Рассмотрим полуторалинейную форму

$$B_r^{(0)}[u, v] = \sum_{j \in J} B_{r;j}^{(0)}[u, v], \quad B_{r;j}^{(0)}[u, v] = \sum_{|k|=|l|=j} \int_\Omega \rho^{2\tau_j}(x) b_{klr}^{(0)}(x) u^{(k)}(x) \overline{v^{(l)}(x)} dx, \tag{13}$$

где

$$b_{klr}^{(0)}(x) = (1 - \eta_r(x))\gamma(x_r) b_{kl}(x_r) + \eta_r(x)\gamma(x) b_{kl}(x). \tag{14}$$

Учитывая ограниченность коэффициентов $b_{kl}(x),\ |k| = |l| = j \in J,\ x \in \Omega$, и применяя неравенство Коши-Буняковского, имеем

$$\left| B_r^{(0)}[u, v] \right| \le$$

$$\le M_2 \sum_{m=0}^{s} \| u; W^{j_m}_{2;\tau_{j_m}}(\Omega) \| \cdot \| v; W^{j_m}_{2;\tau_{j_m}}(\Omega) \| + M_2 \sum_{m=0}^{t} \| u; W^{i_m}_{2;\tau_{i_m}}(\Omega) \| \cdot \| v; W^{i_m}_{2;\tau_{i_m}}(\Omega) \|$$

для всех $u, v \in C_0^\infty(\Omega)$. Отсюда в силу неравенства (12) и определения пространства $\mathbb{H}'_+$ (см. (3)) следует, что

$$\left| B_r^{(0)}[u, v] \right| \le M_3 \| u; \mathbb{H}_+ \| \, \| v; \mathbb{H}_+ \| \tag{15}$$

для всех $u, v \in \mathbb{H}'_+$.

Из условия (7) (см. замечание 1) следует, что

$$\operatorname{Re} \left\{ \gamma(x_r) \sum_{|k|=|l|=j_m} b_{kl}(x_r) \zeta_k \overline{\zeta_l} \right\} \ge c \sum_{|k|=j_m} |\zeta_k|^2,$$

$$\operatorname{Re} \left\{ \gamma(x) \sum_{|k|=|l|=j_m} b_{kl}(x) \zeta_k \overline{\zeta_l} \right\} \ge c \sum_{|k|=j_m} |\zeta_k|^2,$$

для всех $r = \overline{1,N}$, $x \in \Omega$ и любого набора комплексных чисел $\{\zeta_k\}_{|k|=j_m}$. Умножая эти неравенства на $(1-\eta_r(x))$ и $\eta_r(x)$, соответственно, и подставляя $\zeta_k = \rho^{\tau_{j_m}}(x)u^{(k)}(x)$, где $u \in C_0^\infty(\Omega)$, после интегрирования по $x \in \Omega$ имеем

$$\mathrm{Re}B^{(0)}_{r,\,j_m}[u,u] \geq c_{j_m} \left\| u;\, L_2^{j_m}(\Omega) \right\|^2. \tag{16}$$

Здесь c_{j_m} — некоторое положительное число,

$$\left\| u;\, L_2^{j_m}(\Omega) \right\| = \left\{ \sum_{|k|=j_m} \int_\Omega |u^{(k)}(x)|^2 dx \right\}^{1/2}. \tag{17}$$

Далее учитывая ограниченность коэффициентов формы (13), в силу неравенства (16) получим

$$\mathrm{Re}B^{(0)}_r[u,u] \geq \mathrm{Re}\sum_{m=0}^{s} B^{(0)}_{r,\,j_m}[u,u] - \sum_{m=0}^{t} \left| B^{(0)}_{r,\,i_m}[u,u] \right| \geq$$
$$\sum_{m=0}^{s} c_{j_m} \left\| u;\, L_2^{j_m}(\Omega) \right\|^2 - \sum_{m=0}^{t} M_{i_m} \left\| u;\, L_2^{i_m}(\Omega) \right\|^2 \quad (u \in C_0^\infty(\Omega)). \tag{18}$$

Неравенство (12) можно записать в виде

$$\left\| u;\, L^{i_n}_{2;\,\tau_{i_n}}(\Omega) \right\|^2 \leq \varepsilon \left\| u;\, L^{j_m}_{2;\,\tau_{j_m}}(\Omega) \right\|^2 + C(\varepsilon) \left\| u;\, L_2(\Omega) \right\|^2.$$

В силу этого неравенства из (18) следует, что

$$\mathrm{Re}B^{(0)}_r[u,\,u] \geq \sum_{m=0}^{s} \left(c_{j_m} - M'_{j_m}\varepsilon \right) \left\| u;\, L_2^{j_m}(\Omega) \right\|^2 - C(\varepsilon) \left\| u;\, L_2(\Omega) \right\|^2.$$

Подбирая в этом неравенстве число $\varepsilon > 0$ достаточно малым, получим

$$\mathrm{Re}B^{(0)}_r[u,u] + \lambda_0 \left\| u;\, L_2(\Omega) \right\|^2 \geq \sum_{m=0}^{s} \delta_{j_m} \left\| u;\, W_2^{j_m}(\Omega) \right\|^2 \geq \varkappa_0 \left\| u;\, \mathbb{H}_+ \right\|^2, \tag{19}$$

где λ_0, $\varkappa_0$ — некоторые положительные числа.

Теперь рассмотрим полуторалинейную форму

$$\mathcal{B}^{(0)}_r[u,v] = \sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) \widehat{b}_{klr}(x) u^{(k)}(x) \overline{v^{(l)}(x)} dx,$$

где $\widehat{b}_{klr}(x) = [(1-\eta_r(x))b_{kl}(x_r) + \eta_r(x)b_{kl}(x)]\gamma(x_r)$.

Так как $b^{(0)}_{klr}(x) - \widehat{b}_{klr}(x) = \eta_r(x)(\gamma(x) - \gamma(x_r))b_{kl}(x)$ и коэффициенты $b_{kl}(x)$ ограничены, то, действуя так же как в доказательстве неравенства (15), с помощью неравенства Коши-Буняков-ского получим

$$|B^{(0)}_r[u,\,v] - \mathcal{B}^{(0)}_r[u,\,v]| \leq M_4\,\Lambda \left\| u;\, \mathbb{H}_+ \right\| \left\| v;\, \mathbb{H}_+ \right\|$$

для всех $u, v \in \mathbb{H}'_+$. Здесь $\Lambda = \sup |\eta_r(x)(\gamma_r(x) - \gamma(x_r))|$, где супремум берется по всем $x \in \Omega$ и всем $r = \overline{1,N}$. В силу этого неравенства из (19) следует, что

$$\varkappa_0 \left\| u;\, \mathbb{H}_+ \right\|^2 \leq \mathrm{Re}\mathcal{B}^{(0)}_r[u,\,u] + \lambda_0 \left\| u;\, L_2(\Omega) \right\|^2 + \Lambda \left\| u;\, \mathbb{H}_+ \right\|^2.$$

Так как $|\eta_r(x)(\gamma(x)-\gamma(x_r))| < \nu \qquad \forall r \in \{1, 2, \ldots, N\}$ и ν — достаточно малое положительное число, то, фиксируя некоторое значение ν, имеем

$$\mathrm{Re}\mathcal{B}_r^{(0)}[u,\, u] + \lambda_0 \|u;\, L_2(\Omega)\|^2 \geq \varkappa_1 \|u;\, \mathbb{H}_+\|^2 \tag{20}$$

для всех $u \in \mathbb{H}'_+$; $\varkappa_1$ — некоторое положительное число.

Вводим следующую полуторалинейную форму

$$\mathcal{B}_r[u,\, v] = \sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) u^{(k)}(x) \overline{v^{(l)}(x)} dx, \tag{21}$$

где $b_{klr}(x) = (1 - \eta_r(x))b_{kl}(x_r) + \eta_r(x) b_{kl}(x)$.

Заметим, что $\mathcal{B}_r^{(0)}[u,\, v] = \gamma(x_r)\mathcal{B}_r[u, v]$. Поэтому из неравенства (20) следует, что

$$\mathrm{Re}\left\{\gamma(x_r)\mathcal{B}_r[u,\, u]\right\} + \lambda_0 \|u;\, L_2(\Omega)\|^2 \geq \varkappa_1 \|u;\, \mathbb{H}_+\|^2 \tag{22}$$

для всех $u \in \mathbb{H}'_+$.

Не нарушая общности, можно считать, что число $\varphi = \varphi_m$ (см. замечание 1) в условии (6) такое, что $\varphi > \pi/2$.

В силу (6) неравенство (7) будет выполняться также и в том случае, если $\gamma(x) = \gamma_m(x)$ (см. замечание 1) заменить на $\exp(i\theta(x))$, где $\theta(x) = \min\{\varphi - \pi/2,\, |\arg\gamma(x)|\}\,(\mathrm{sign\ arg}\ \gamma(x))$. Поэтому из неравенства (22) следует, что

$$\mathrm{Re}\left\{\exp(i\theta_r)\mathcal{B}_r[u,\, u]\right\} + \lambda_0 \|u;\, L_2(\Omega)\|^2 \geq \varkappa_2 \|u;\, \mathbb{H}_+\|^2 \tag{23}$$

для всех $u \in \mathbb{H}'_+$; $\varkappa_2$ — некоторое положительное число.

Здесь и далее $\theta_r = \theta(x_r)$, $r \in \{1, 2, \ldots, N\}$.

Поступая также, как в доказательстве неравенства (15), ввиду ограниченности коэффициентов b_{klr} доказывается неравенство

$$|\mathcal{B}_r[u,\, v]| \leq M_5 \|u;\, \mathbb{H}_+\| \|v;\, \mathbb{H}_+\|$$

для всех $u, v \in \mathbb{H}'_+$. Так как

$$|(u,\, v)_0| \leq \|u;\, L_2(\Omega)\| \|v;\, L_2(\Omega)\| \leq \|u;\, \mathbb{H}_+\| \|v;\, \mathbb{H}_+\|,$$

то отсюда следует, что

$$|\mathcal{B}_r[u,\, v] + \lambda_0(u,\, v)_0| \leq (M_5 + \lambda_0) \|u;\, \mathbb{H}_+\| \|v;\, \mathbb{H}_+\| \tag{24}$$

для всех $u, v \in \mathbb{H}'_+$; M_5 — некоторое положительное число.

Неравенства (23), (24) позволяют нам применить теорему Лакса-Мильграма [7, теорема 2.0.1]. Согласно этой теореме существует оператор $\mathcal{R}_r(\lambda) : \mathbb{H}'_- \to \mathbb{H}'_+$ такой, что:

$$\exp(i\theta_r)\mathcal{B}_r[\mathcal{R}_r(\lambda)F, v] + (\mathcal{R}_r(\lambda)F, v)_0 = \langle F, v\rangle \tag{25}$$

для всех $F \in \mathbb{H}'_-$ и всех $v \in \mathbb{H}'_+$;

$$\|\mathcal{R}_r(\lambda)F; \mathbb{H}'_+\| \leq M_6 \left\|F; \mathbb{H}'_-\right\| \tag{26}$$

для всех $F \in \mathbb{H}'_-$. Здесь $\lambda \geq \lambda_0$ и число M_6 не зависит от F и от λ.

Символом Ψ_r обозначим оператор умножения на функцию $\psi_r(x)$ и введем оператор

$$\mathcal{R}(\lambda) = \sum_{r=1}^{N} \exp(i\theta_r)\Psi_r\mathcal{R}_r(\lambda)\Psi_r. \tag{27}$$

Из (26) следует, что $\mathcal{R}(\lambda)$ является ограниченным оператором, действующим из $\mathbb{H}'_-$ в $\mathbb{H}'_+$.

Аналогично неравенству (15) доказывается, что

$$|B[u,\,v]| \le M_7 \sum_{j\in J} \left\| u;\, W^j_{2;\,\tau_j}(\Omega)\right\| \left\| v;\, W^j_{2;\,\tau_j}(\Omega)\right\| \le M_8 \left\| u;\, \mathbb{H}_+\right\| \left\| v;\, \mathbb{H}_+\right\|.$$

Отсюда и из ограниченности оператора $\mathcal{R}(\lambda) : \mathbb{H}'_- \to \mathbb{H}'_+$ следует, что оператор $\mathbb{R}(\lambda)$, $\lambda \ge \lambda_0$, определенный равенством

$$\langle \mathbb{R}(\lambda)F, v\rangle = B[\mathcal{R}(\lambda)F,\, v] + \lambda\,(\mathcal{R}(\lambda)F,\, v)_0 \quad (\forall v \in \mathbb{H}'_+), \tag{28}$$

есть ограниченный оператор, действующий из $\mathbb{H}'_-$ в $\mathbb{H}'_-$.

Согласно нашим построениям функции $\psi_r^2(x)$, $r = \overline{1,N}$, образуют разбиение единицы области Ω. Поэтому для всех $F \in L_2(\Omega)$ и всех $v \in \mathbb{H}'_+$ выполняются следующие равенства

$$\langle F,\, v\rangle = (F,\, v)_0 = \int_\Omega F(x)\overline{v(x)}dx = \sum_{r=1}^N \int_\Omega \psi_r^2(x)F(x)\overline{v(x)}dx = \sum_{r=1}^N (\psi_r F,\, \psi_r)_0. \tag{29}$$

Так как $b_{klr}(x) = (1-\eta_j(x))b_{kl}(x_r) + \eta_r(x)b_{kl}(x)$ и функция $\eta_r(x)$ обращается в единицу в некоторой окрестности множества $\operatorname{supp}\psi_r$, то функции $b_{klr}(x)$ и $b_{kl}(x)$ на множестве $\operatorname{supp}\psi_r$ совпадают. Поэтому из (2), (27) и (28) следует, что

$$\begin{aligned}\langle \mathbb{R}(\lambda)F, v\rangle = \\ = \sum_{r=1}^N \exp(i\theta_r) \Bigg\{ \sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) D^k(\psi_r \mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{v^{(l)}(x)}dx \\ + \lambda \int_\Omega (\mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{\psi_r(x)v(x)}dx\Bigg\}\end{aligned} \tag{30}$$

Здесь и далее символ D^k обозначает дифференцирование мультииндекса k.

Пусть $F \in L_2(\Omega)$. В равенстве (25) заменим F на $\psi_r F$, а v — на $\psi_r v$:

$$\exp(i\theta_r)\mathcal{B}_r[\mathcal{R}_r(\lambda)\Psi_r F, \psi_r v] + \lambda\,(\mathcal{R}_r(\lambda)\Psi_r F, \psi_r v)_0 = (\psi_r F, \psi_r v)_0.$$

Отсюда в силу равенства (18) следует, что

$$\begin{aligned}(\psi_r F, \psi_r v)_0 = \\ = \exp(i\theta_r) \Bigg\{ \sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) D^k(\mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{D^l(\psi_r(x)v(x))}dx + \\ + \lambda \int_\Omega (\mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{\psi_r(x)v(x)}dx\Bigg\}.\end{aligned}$$

Суммируя это равенство по r от 1 до N и применяя равенство (29) имеем

$$\begin{aligned}\langle F,\, v\rangle = (F,\, v)_0 = \\ = \sum_{r=1}^N \exp(i\theta_r) \Bigg\{ \sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) D^k(\mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{D^l(\psi_r(x)v(x))}dx + \\ + \lambda \int_\Omega (\mathcal{R}_r(\lambda)\Psi_r F)(x)\overline{\psi_r(x)v(x)}dx\Bigg\}.\end{aligned}$$

Отсюда и из (30) следует, что

$$\langle \mathbb{R}(\lambda)F, v\rangle - \langle F,\, v\rangle = \mathbb{S}_\lambda[F,\, v] + \mathbb{T}_\lambda[F,\, v], \tag{31}$$

где

$$\mathbb{S}_\lambda[F,\, v] = \sum_{j\in J}\sum_{r=1}^{N} \exp(i\theta_r) \sum\nolimits_j^{(1)} C_{k'}^{k''} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) \psi_r^{(k')}(x) U_{r,\lambda}^{(k'')}(x) \overline{v^{(l)}(x)}\, dx, \tag{32}$$

$$\mathbb{T}_\lambda[F,\, v] = \sum_{j\in J}\sum_{r=1}^{N} \exp(i\theta_r) \sum\nolimits_j^{(2)} C_{l'}^{l''} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) U_{r,\lambda}^{(k)}(x) \overline{\psi_r^{(l')}(x) v^{(l'')}(x)}\, dx, \tag{33}$$

$$U_{r,\lambda}(x) = (\mathcal{R}_r(\lambda)\Psi_r F)(x), \quad r \in \{1, 2, \ldots,\, N\}.$$

Здесь символ $\sum_j^{(1)}$ обозначает суммирование по мультииндексам $k,\, l,\, k',\, k''$ таким, что $k = k' + k''$, $k' \neq 0$, $|k| = |l| = j$, а символ $\sum_j^{(2)}$ обозначает суммирование по мультииндексам $k,\, l,\, l',\, l''$ таким, что $l = l' + l''$, $l' \neq 0$, $|k| = |l| = j$.

Ниже доказывается, что при $\lambda \geq \lambda_0$, где λ_0 — некоторое большое число, для всех $F \in L_2(\Omega)$, $v \in \mathbb{H}'_+$ выполняются следующие неравенства

$$|\mathbb{S}_\lambda[F,\, v]| \leq \delta_1(\lambda) \left\|F;\, \mathbb{H}'_-\right\| \|v;\, \mathbb{H}_+\|\,, \tag{34}$$

$$|\mathbb{T}_\lambda[F,\, v]| \leq \delta_2(\lambda) \left\|F;\, \mathbb{H}'_-\right\| \|v;\, \mathbb{H}_+\|\,, \tag{35}$$

где положительные функции $\delta_i(\lambda)$, $i = 1,\, 2$, такие, что $\delta_i(\lambda) \to 0$ при $\lambda \to \infty$.

Доказательство неравенства (34). Далее нам понадобится следующая

Лемма 2. *Пусть $B_{\lambda r}$ — самосопряженный оператор в пространстве $L_2(\Omega)$, порожденный симметричной формой*

$$\widetilde{\mathcal{B}_{\lambda r}}[u, v] = \frac{1}{2}\left\{\exp(i\theta_r)\mathcal{B}_r[u, v] + \exp(-i\theta_r)\overline{\mathcal{B}_r[v, u]}\right\} + \lambda \cos\theta_r\, (u,\, v)_0, \tag{36}$$
$$D(\widetilde{\mathcal{B}_{\lambda r}}) = \mathbb{H}'_+.$$

Тогда при $\lambda \geq \lambda_0$, где λ_0 — некоторое положительное число, для любого мультииндекса k такого, что $|k| = j \in J$, и любого $r = \overline{1, N}$ оператор $\rho^{\tau_j} D^k B_{\lambda r}^{-1/2}$ является ограниченным оператором в $L_2(\Omega)$, а если мультииндекс $\widetilde{k}$ такой, что $|\widetilde{k}| < j \in J$, то существует положительная функция $q(\lambda)$ такая, что $q(\lambda) \to 0$ при $\lambda \to \infty$ и

$$\left\|\rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega)\right\| \leq q(\lambda) \|B_{\lambda r}^{1/2} u; L_2(\Omega)\| \tag{37}$$

для всех $u \in \mathbb{H}'_+$

Доказательство. По определению оператора $B_{\lambda r}$ для всех $u, v \in \mathbb{H}'_+$ выполняется равенство

$$\left(B_{\lambda r}^{1/2} u, B_{\lambda r}^{1/2} v\right)_0 = \widetilde{\mathcal{B}}_{\lambda r}[u, v]. \tag{38}$$

Следовательно,

$$\|B_{\lambda r}^{1/2} u; L_2(\Omega)\|^2 = Re\left\{\exp(i\theta_r)\mathcal{B}_r[u, u]\right\} + \lambda \|u; L_2(\Omega)\|^2 \tag{39}$$

и в силу неравенства (23)

$$\|B_{\lambda r}^{1/2} u; L_2(\Omega)\| \geq c_0 \|u; \mathbb{H}_+\| \qquad (\lambda \geq \lambda_0) \tag{40}$$

для всех $u \in \mathbb{H}'_+$. Отсюда следует, что

$$\left\|\rho_j^\tau D^k u;\, L_2(\Omega)\right\| \leq M_9 \|B_{\lambda r}^{1/2} u; L_2(\Omega)\|, (|k| = j, \quad r = \overline{1, N},\ u \in \mathbb{H}'_+).$$

Отсюда следует ограниченность оператора $\rho^{\tau_j} D^k B_{\lambda r}^{-1/2}$.

Рассмотрим случай $|\widetilde{k}| < j \in J$. Применяя лемму 1 имеем

$$\left\| \rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega) \right\| \le \varepsilon \| u; W^j_{2;\tau_j}(\Omega) \| + C(\varepsilon) \left\| u;\, L_2(\Omega) \right\|,$$

где ε — произвольное положительное число и величина $C(\varepsilon)$ неограниченно растет при $\varepsilon \to 0$. Поэтому в силу (40) для всех $u \in \mathbb{H}'_+$ имеет место неравенство

$$\left\| \rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega) \right\| \le \varepsilon \| B_{\lambda r}^{1/2} u; L_2(\Omega) \| + C(\varepsilon) \left\| u;\, L_2(\Omega) \right\|.$$

Применяя равенство (39) имеем

$$\left\| \rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega) \right\|^2 \le \varepsilon^2 Re \left\{ \exp(i\theta_r) \mathcal{B}_r[u,u] \right\} + (\lambda^2 + C_1(\varepsilon)) \| u; L_2(\Omega) \|^2.$$

Отсюда и из (21) при $\lambda = 1/\varepsilon$ следует, что

$$\left\| \rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega) \right\|^2 \le$$
$$\le \varepsilon^2 Re \left\{ \exp(i\theta_r) \left(\sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) u^{(k)}(x) \overline{u^{(l)}(x)} dx \right) \right\} +$$
$$+ p(\varepsilon) \int_\Omega |u(x)|^2 dx,$$

где непрерывная положительная функция $p(\varepsilon)$ такова, что $p(\varepsilon) \to \infty$ при $\varepsilon \to 0$. Обратную относительно $p(\varepsilon)$ функцию обозначим через q, и положив $\varepsilon = q(\lambda)$ в последнем неравенстве, получим

$$\left\| \rho^{\tau_j} D^{\widetilde{k}} u;\, L_2(\Omega) \right\|^2 \le$$
$$\le q(\lambda)^2 Re \left\{ \exp(i\theta_r) \left(\sum_{|k|=|l|=j\in J} \int_\Omega \rho^{2\tau_j}(x) b_{klr}(x) u^{(k)}(x) \overline{u^{(l)}(x)} dx \right) \right\} +$$
$$+ \lambda \int_\Omega |u(x)|^2 dx,$$

где непрерывная положительная функция $q(\lambda)$ такая, что $q(\lambda) \to 0$ при $\lambda \to \infty$. Отсюда в силу равенства (39) следует (37).

Лемма 2 доказана.

При $\lambda \ge \lambda_0$ билинейная форма $\exp(i\theta_r)\mathcal{B}_r[u,v]$ удовлетворяет неравенствам (см. (23), (24)):

$$\varkappa_3 \| u; \mathbb{H}_+ \|^2 \le \mathrm{Re} \left\{ \exp(i\theta_j) \mathcal{B}_r[u,u] \right\} + \lambda \left\| u;\, L_2(\Omega) \right\| \tag{41}$$

для всех $u \in \mathbb{H}'_+$;

$$|\mathcal{B}_r[u,v] + \lambda(u,v)_0| \le (M_3 + |\lambda|) \| u;\, \mathbb{H}_+ \| \cdot \| v;\, \mathbb{H}_+ \| \tag{42}$$

для всех $u,\, v \in \mathbb{H}'_+$. Числа $\varkappa_2$, $M_3 > 0$ в этих неравенствах не зависят от $u(x),\ \ v(x)$.

Согласно неравенствам (41), (42) билинейная форма $\exp(i\theta_r)\mathcal{B}_r[u,v] + \lambda(u,v)_0$ замкнута и секториальна. Поэтому в силу [15, гл. 6, теорема 2.1] существует такой m - секториальный оператор $A_r(\lambda)$, что

$$\exp(i\theta_r)\mathcal{B}_r[u,v] + \lambda(u,v)_0 = (A_r(\lambda)u, v) \quad \left(\forall u \in D(A_r(\lambda)) \subset \mathbb{H}'_+, \ \ \forall v \in \mathbb{H}'_+ \right). \tag{43}$$

Пусть $f \in L_2(\Omega)$. Тогда $\mathcal{R}_r(\lambda)f \in \mathbb{H}'_+$ и согласно равенству (25)

$$\exp(i\theta_r)\mathcal{B}_r[\mathcal{R}_r(\lambda)f, v] + \lambda\,(\mathcal{R}_r(\lambda)f, v)_0 = \langle f, v\rangle$$

для всех $v \in \mathbb{H}'_+$. Отсюда и из (43) в силу [15, гл. 6, теорема 2.1] следует, что $A_r(\lambda)\mathcal{R}_r(\lambda)f = f$, $\forall f \in L_2(\Omega)$, то есть

$$\mathcal{R}_r(\lambda)f = A_r(\lambda)^{-1}f \tag{44}$$

для всех $f \in L_2(\Omega)$.

Используя равенство (38) при $u(x) = v(x)$ с учетом равенства (36) получим

$$\left\|B_{\lambda r}^{1/2}u; L_2(\Omega)\right\|^2 = \mathrm{Re}\{\exp(i\theta_r)\mathcal{B}_r[u,u]\} + \lambda\,\|u;\, L_2(\Omega)\| \quad (\lambda \ge \lambda_0 > 0).$$

Отсюда в силу неравенства (23) следует, что

$$\left\|B_{\lambda r}^{1/2}u; L_2(\Omega)\right\| \ge \varkappa_2\,\|u; \mathbb{H}_+\| \ \ (\lambda \ge \lambda_0 > 0)$$

для всех $u \in \mathbb{H}'_+$. Отсюда следует обратимость оператора $B_{\lambda r}^{1/2}$ при $\lambda \ge \lambda_0 > 0$. Применяя [15, гл. 6, теорема 3.2], получим представление

$$A_r(\lambda)^{-1} = B_{\lambda r}^{-1/2}X_r(\lambda)B_{\lambda r}^{-1/2} \ \ (\lambda \ge \lambda_0 > 0), \tag{45}$$

где $X_r(\lambda) : L_2(\Omega) \to L_2(\Omega)$ — некоторый ограниченный оператор и его норма $\|X_r(\lambda)\|$ не превосходит числа $M_1 > 0$, не зависящего от $\lambda \in [\lambda_0, \infty)$.

Переходим к доказательству оценки (34). С этой целью равенство (32) перепишем в виде

$$\mathbb{S}_\lambda[F,\, v] = \sum_{j\in J}\sum_{r=1}^{N}\exp(i\theta_r)\sum\nolimits_j^{(1)} C_{k'}^{k''}\left(\rho^{\tau_j}b_{klr}\psi_r^{(k')}U_{r,\lambda}^{(k'')},\, \rho^{\tau_j}v^{(l)}\right)_0, \tag{46}$$

где $U_{r,\lambda}(x) = (\mathcal{R}_r(\lambda)\Psi_r F)(x), \quad r \in \{1, 2, \ldots, N\}$. Пусть $F \in L_2(\Omega)$. Используя равенства (43) - (46), имеем

$$\mathbb{S}_\lambda[F, v] = \sum_{j\in J}\sum_{r=1}^{N}\sum\nolimits_j^{(1)}\exp(i\theta_r)C_{k'}^{k''}(\rho^{\tau_j}b_{klr}\psi_r^{(k')}D^{k''}A_r(\lambda)^{-1}\Psi_r F, \rho^{\tau_j}v^{(l)})_0 =$$

$$= \sum_{j\in J}\sum_{r=1}^{N}\sum\nolimits_j^{(1)}\exp(i\theta_r)C_{k'}^{k''}(\rho^{\tau_j}b_{klr}\psi_r^{(k')}D^{k''}B_{\lambda r}^{-1/2}X_r(\lambda)B_{\lambda r}^{-1/2}\Psi_r F, \rho^{\tau_j}v^{(l)})_0.$$

Применяя неравенство Коши - Буняковского, получаем

$$|\mathbb{S}_\lambda[F, v]| \le M_{10}\sum_{j\in J}\sum_{r=1}^{N}\sum\nolimits_j^{(1)}\left\|\mathbb{D}_{k'',r,j}(\lambda)\mathbb{F}_{r,\lambda}; L_2(\Omega)\right\|\cdot\left\|\mathbb{P}_{l,r,j}B_{\lambda_0 r}^{1/2}v; L_2(\Omega)\right\|, \tag{47}$$

где

$$\mathbb{D}_{k'',r,j}(\lambda) = \rho^{\tau_j}D^{k''}B_{\lambda r}^{-1/2}, \quad \mathbb{F}_{r,\lambda}(x) = X_r(\lambda)B_{\lambda r}^{-1/2}(\psi_r F)(x), \quad \mathbb{P}_{l,r,j} = \rho^{\tau_j}D^l B_{\lambda_0 r}^{-1/2}. \tag{48}$$

Докажем, что при $\lambda \ge \lambda_0$ справедливо неравенство

$$\|\mathbb{F}_{r,\lambda}; L_2(\Omega)\| \le M_{11}\left\|F; \mathbb{H}'_-\right\|. \tag{49}$$

Пусть $\lambda \geq \lambda_0$. Тогда

$$\|\mathbb{F}_{r,\lambda}; L_2(\Omega)\| \leq M'_{12} \left\|B_{\lambda r}^{-1/2}(\psi_r F); L_2(\Omega)\right\| \leq M_{12} \left\|B_{\lambda_0 r}^{-1/2}(\psi_r F); L_2(\Omega)\right\|. \tag{50}$$

Норму в пространстве $L_2(\Omega)$ можно задавать с помощью равенства

$$\|f; L_2(\Omega)\| = \sup |(f, v)_0|, \tag{51}$$

где супремум берется по всем $v \in L_2(\Omega)$ таким, что $\|v; L_2(\Omega)\| = 1$. Так как $C_0^\infty(\Omega)$ плотно в $L_2(\Omega)$, то в равенстве (51) можно считать, что супремум берется по всем $v \in C_0^\infty(\Omega)$, таким, что $\|v; L_2(\Omega)\| = 1$.

При $\lambda = \lambda_0$ из равенство (38) имеем $\left(B_{\lambda_0 r}^{1/2} u, B_{\lambda_0 r}^{1/2} v\right)_0 = \widetilde{\mathcal{B}}_{\lambda_0 r}[u, v]$.

С другой стороны

$$\mathrm{Re}\widetilde{\mathcal{B}}_{\lambda_0 r}[u, u] \geq \varkappa_4 \|u; \mathbb{H}_+\|^2,$$

$$\left|\widetilde{\mathcal{B}}_{\lambda_0 j}[u, v]\right| \leq (M_{13} + \lambda_0) \|u; \mathbb{H}_+\| \cdot \|v; \mathbb{H}_+\|$$

для всех $u, v \in C_0^\infty(\Omega)$ и согласно теореме Лакса - Мильграма, уравнение

$$\widetilde{\mathcal{B}}_{\lambda_0 r}[u, \widehat{v}] = (w, \widehat{v}) \quad \forall \widehat{v} \in C_0^\infty(\Omega)$$

имеет решение для любого $w \in L_2(\Omega)$. Поэтому из (51) следует, что

$$\|f; L_2(\Omega)\| = \sup \left|\left(B_{\lambda_0 r}^{1/2} f, B_{\lambda_0 r}^{1/2} w\right)_0\right|,$$

где супремум берется по всем $w \in C_0^\infty(\Omega)$ таким, что $\left\|B_{\lambda_0 r}^{1/2} w; L_2(\Omega)\right\| = 1$. С другой стороны в классе $C_0^\infty(\Omega)$ нормы $\|v; \mathbb{H}_+\|$ и $\left\|B_{\lambda_0 j}^{1/2} v; L_2(\Omega)\right\|$ эквивалентны. Поэтому

$$\left\|B_{\lambda_0 r}^{-1/2}(\psi_r F); L_2(\Omega)\right\| = \sup \left|\left(\psi_r F, B_{\lambda_0 r}^{1/2} v\right)_0\right| \leq$$
$$\leq M_{14} \sup |(\psi_r F, v)| \leq M_{15} \left\|\psi_r F; \mathbb{H}'_-\right\| \leq M_{16} \left\|F; \mathbb{H}'_-\right\|, \tag{52}$$

где первый супремум в этой цепочке берется по всем $v \in C_0^\infty(\Omega)$ таким, что $\left\|B_{\lambda_0 r}^{1/2} w; L_2(\Omega)\right\| = 1$, а второй супремум — по всем $v \in C_0^\infty(\Omega) : \|v; \mathbb{H}_+\| = 1$.

Из (50), (52) следует (49).

Согласно лемме 2 оператор (см. (48)) $\mathbb{P}_{l,r,j} = \rho^{\tau_j} D^l B_{\lambda_0 r}^{-1/2}$ является ограниченным, и из (24), (38) следует, что

$$\left\|B_{\lambda_0 r}^{1/2} v; L_2(\Omega)\right\|^2 = |\widetilde{\mathcal{B}}_{\lambda_0 r}[v, v]| \leq M_{17} \|v; \mathbb{H}_+\|^2$$

для всех $v \in \mathbb{H}_+$. Поэтому

$$\left\|\mathbb{P}_{l,r,j} B_{\lambda_0 r}^{1/2} v; L_2(\Omega)\right\| \leq \|v; \mathbb{H}_+\|. \tag{53}$$

Согласно второй части утверждения леммы 2 существует положительная функция $\varepsilon_1(\lambda)$ такая, что

$$\left\|\rho^{\tau_j} D^{k''} B_{\lambda r}^{-1/2}\right\| \leq \varepsilon_1(\lambda)$$

и $\varepsilon_1(\lambda) \to 0$ при $\lambda \to \infty$. Следовательно, (см. (48)) $\lim_{\lambda \to \infty} \left\|\mathbb{D}_{k'' j}(\lambda)\right\| = 0$. Ввиду этого равенства из (47), (49), (53) получим оценку (34).

Доказательство неравенства (35). Для удобства записи интегралы составляющие форму $\mathbb{T}_\lambda[F,\,v]$ обозначим через $\mathbb{I}_{\lambda;j}[F,\,v]$[1].

Согласно равенствам (44), (45)

$$\mathcal{R}_r(\lambda) = A_r(\lambda)^{-1} = B_{\lambda r}^{-1/2} X_r(\lambda) B_{\lambda r}^{-1/2} \quad (\lambda \geq \lambda_0 > 0).$$

Поэтому

$$\mathbb{I}_{\lambda;j}[F,\,v] = \left(\rho^{\tau_j} b_{klr} D^k B_{\lambda r}^{-1/2} X_r(\lambda) B_{\lambda r}^{-1/2} \Psi_r F,\, \rho^{\tau_j} \psi_r^{(l')} D^{l''} v\right)_0.$$

Далее, используя обозначение (см. (48)) $\mathbb{F}_{r,\lambda}(x) = X_r(\lambda) B_{\lambda r}^{-1/2} \Psi_r F$ и равенство

$$D^{l''} v = D^{l''} B_{\lambda_0 j}^{-1/2} B_{\lambda_0 j}^{1/2} v,$$

получим

$$\mathbb{I}_{\lambda;j}[F,\,v] = \left(B_{\lambda_0 r}^{-1/2} D^{l''} \psi_r^{(l')} \rho^{\tau_j} b_{klr} \rho^{\tau_j} D^k B_{\lambda r}^{-1/2} \mathbb{F}_{r,\lambda},\, B_{\lambda_0 r}^{1/2} v\right)_0. \tag{54}$$

Обозначим

$$\mathbb{L}_{j,r,\lambda_0,l''} = b_{klr} \rho^{\tau_j} \psi_r^{(l')} D^{l''} B_{\lambda_0 r}^{-1/2}.$$

Тогда

$$\mathbb{L}^*{}_{j,r,\lambda_0,l''} = B_{\lambda_0 r}^{-1/2} D^{l''} \psi_r^{(l')} \rho^{\tau_j} b_{klr}$$

и равенство (54) примет следующий вид

$$\mathbb{I}_{\lambda;j}[F,\,v] = \left(\mathbb{L}^*{}_{j,r,\lambda_0,l''} \rho^{\tau_j} D^k B_{\lambda r}^{-1/2} \mathbb{F}_{r,\lambda},\, B_{\lambda_0 r}^{1/2} v\right)_0.$$

Вводя обозначение $\mathbb{G}_{j,r,\lambda_0,k} = \rho^{\tau_j} D^k B_{\lambda_0 r}^{-1/2}$, имеем

$$\mathbb{I}_{\lambda;j}[F,\,v] = \left(\mathbb{L}^*{}_{j,r,\lambda_0,l''} \mathbb{G}_{j,r,\lambda_0,k} B_{\lambda_0 r}^{1/2} B_{\lambda r}^{-1/2} \mathbb{F}_{r,\lambda},\, B_{\lambda_0 r}^{1/2} v\right)_0. \tag{55}$$

Так как $B_{\lambda r}$ — самосопряженный оператор, ассоциированный с формой $\widetilde{\mathcal{B}_{\lambda r}}[u,v]$ (см. лемму 2), то

$$\begin{aligned}
\left\| \left(B_{\lambda_0 r}^{1/2} + (\lambda - \lambda_0)^{1/2} E\right) u;\, L_2(\Omega) \right\|^2 \leq \\
&\leq 2 \left\{ \left\| B_{\lambda_0 r}^{1/2} u;\, L_2(\Omega) \right\|^2 + (\lambda - \lambda_0) \left\| u;\, L_2(\Omega) \right\|^2 \right\} \leq \\
&\leq M_{18} \left\{ \left(B_{\lambda_0 r}^{1/2} u,\, B_{\lambda_0 r}^{1/2} u\right)_0 + \theta_r' (\lambda - \lambda_0) (u,\, u)_0 \right\} = \\
&= M_{18} \left[\widetilde{\mathcal{B}_{\lambda_0 r}}[u,u] + \theta_r' (\lambda - \lambda_0) (u,\, u)_0 \right] = \\
&= M_{18} \widetilde{\mathcal{B}_{\lambda r}}[u,u] = M_{18} \left(B_{\lambda r}^{1/2} u,\, B_{\lambda r}^{1/2} u\right)_0 = M_{18} \left\| B_{\lambda r}^{1/2} u;\, L_2(\Omega) \right\|^2,
\end{aligned}$$

где $\theta_r' = \operatorname{Re} \exp(i\theta_r)$. Следовательно, существует число $M_{18} > 0$ такое, что

$$\left\| \left(B_{\lambda_0 r}^{1/2} + (\lambda - \lambda_0)^{1/2} E\right) B_{\lambda r}^{-1/2} \right\| \leq M_{18} \quad (\lambda \geq \lambda_0).$$

[1] Зависимость $\mathbb{I}_{\lambda;j}[F,\,v]$ от r, k, l, l', l'' в данном контексте не существенны, поэтому в обозначении эти символы не используются.

В силу этого неравенства из (55) следует, что

$$|\mathbb{I}_{\lambda;j}[F,\,v]| \le M_{19}\left\|\mathbb{L}^*{}_{j,r,\lambda_0,l''}\mathbb{G}_{j,r,\lambda_0,k}B_{\lambda_0 r}^{1/2}\left(B_{\lambda_0 r}^{1/2}+(\lambda-\lambda_0)^{1/2}E\right)^{-1}\right\|\times$$
$$\times\,\|\mathbb{F}_{r,\lambda};\,L_2(\Omega)\|\cdot\left\|B_{\lambda_0 r}^{1/2}v;\,L_2(\Omega)\right\|. \quad (56)$$

Ниже докажем, что

$$\lim_{\lambda\to\infty}\left\|\mathbb{L}^*{}_{j,r,\lambda_0,l''}\mathbb{G}_{j,r,\lambda_0,k}B_{\lambda_0 r}^{1/2}\left(B_{\lambda_0 r}^{1/2}+(\lambda-\lambda_0)^{1/2}E\right)^{-1}\right\|=0. \quad (57)$$

Используя равенство

$$B_{\lambda_0 r}^{1/2}\left(B_{\lambda_0 r}^{1/2}+(\lambda-\lambda_0)^{1/2}E\right)^{-1}=\left(E+(\lambda-\lambda_0)^{1/2}B_{\lambda_0 r}^{-1/2}\right)^{-1},$$

имеем

$$\mathbb{L}^*{}_{j,r,\lambda_0,l''}\mathbb{G}_{j,r,\lambda_0,k}B_{\lambda_0 r}^{1/2}\left(B_{\lambda_0 r}^{1/2}+(\lambda-\lambda_0)^{1/2}E\right)^{-1}=\mathbb{A}\left(E+(\lambda-\lambda_0)^{1/2}H\right)^{-1}, \quad (58)$$

где

$$\mathbb{A}=\mathbb{T}^*{}_{j,r,\lambda_0,l''}\mathbb{G}_{j,r,\lambda_0,k},\qquad H=B_{\lambda_0 r}^{-1/2}.$$

Так как $|l''|\le j-1$, то оператор $\mathbb{L}_{j,r,\lambda_0,l''}$ вполне непрерывен. Поэтому из ограниченности оператора $\mathbb{G}_{j,r,\lambda_0,k}$ следует вполне непрерывность оператора $\mathbb{A}$. Далее, применяя [16, гл. 5, лемма 7.1], из (58) получаем (57).

Из (56) в силу соотношения (57) следует, что

$$|\mathbb{I}_{\lambda;j}[F,\,v]|\le\delta_3(\lambda)\,\|\mathbb{F}_{r,\lambda};\,L_2(\Omega)\|\cdot\left\|B_{\lambda_0 r}^{1/2}v;\,L_2(\Omega)\right\|, \quad (59)$$

где $\delta_3(\lambda)\to 0$ при $\lambda\to 0$.

Далее заметим, что (см. (42), (48))

$$\|\mathbb{F}_{r,\lambda};\,L_2(\Omega)\|\le\|X_r(\lambda)\|\left\|B_{\lambda r}^{-1/2}\Psi_r F;\,L_2(\Omega)\right\|\le M_{12}\left\|F;\,\mathbb{H}'_-\right\|,$$

$$\left\|B_{\lambda_0 r}^{1/2}v;\,L_2(\Omega)\right\|\le M_{20}\left\|v;\,\mathbb{H}_+\right\|.$$

В силу этих неравенств из (59) следует (35).

Теперь, используя доказанные выше неравенства (34), (35), продолжим доказательство теоремы 1. В силу этих неравенств из (31) следует, что

$$|\langle\mathbb{R}(\lambda)F,v\rangle-\langle F,\,v\rangle|\le(\delta_1(\lambda)+\delta_2(\lambda))\left\|F;\mathbb{H}'_-\right\|\cdot\|v;\mathbb{H}_+\|$$

для всех $F\in L_2(\Omega)$, $v\in\mathbb{H}_+$. Так как $\delta_1(\lambda)\to 0,\quad \delta_2(\lambda)\to 0$ при $\lambda\to\infty$, то существует число $\lambda_0\ge 1$ такое, что

$$|\langle\mathbb{R}(\lambda)F,v\rangle-\langle F,\,v\rangle|\le\frac{1}{2}\left\|F;\mathbb{H}'_-\right\|\cdot\|v;\mathbb{H}_+\| \quad (60)$$

для любого $\lambda\ge\lambda_0$ и всех $F\in L_2(\Omega)$, $v\in\mathbb{H}_+$. Так как $L_2(\Omega)$ плотно в $\mathbb{H}'_-$, то оценка (60) верна для всех $F\in\mathbb{H}'_-$.

Из оценки (60) следует, что при $\lambda>\lambda_0$ оператор $\mathbb{R}(\lambda)$ представляется в виде $\mathbb{R}(\lambda)=$ $=E+\mathbb{P}(\lambda)$, где норма оператора $\mathbb{P}(\lambda):\mathbb{H}'_-\to\mathbb{H}'_-$ не превосходит $1/2$. Поэтому оператор $\mathbb{R}(\lambda):\mathbb{H}'_-\to\mathbb{H}'_-$ непрерывно обратим и $\mathbb{R}^{-1}(\lambda)=(E+\mathbb{P}(\lambda))^{-1}$.

Оператор $\mathcal{R}_j(\lambda)$, определенный равенством (25), действует из $\mathbb{H}'_-$ в $\mathbb{H}'_+$. Поэтому из (27) следует, что оператор $\mathcal{R}(\lambda)$ также действует из $\mathbb{H}'_-$ в $\mathbb{H}'_+$. Следовательно, для любого функционала $F \in \mathbb{H}'_-$ функция $U(x)$, определенная равенством

$$U = \mathcal{R}(\lambda)\mathbb{R}^{-1}(\lambda)F \quad (\lambda \geq \lambda_0), \tag{61}$$

принадлежит пространству $\mathbb{H}'_+$.

С помощью равенства (28) легко проверяется, что функция $U(x)$, определенная формулой (61), удовлетворяет уравнению $B[U,v] + \lambda(U,v)_0 = \langle F, v\rangle \quad \forall v \in C_0^\infty(\Omega)$, то есть является решением задачи D_λ. Так как при $\lambda \geq \lambda_0$ оператор $\mathbb{R}^{-1}(\lambda)$ ограничен, то из (26) и (27) следует, что функция (61) удовлетворяет оценке (8).

Для доказательства единственности решения задачи D_λ рассмотрим сопряженную задачу: для заданного функционала $F \in \mathbb{H}'_-$ найти решение $U_1 \in \mathbb{H}'_+$ уравнения

$$\overline{B[v,U_1] + \lambda(v,U_1)_0} = \langle F, v\rangle \quad \forall v \in \mathbb{H}'_+. \tag{62}$$

Поступая как выше, можно построить операторы $\mathcal{R}_*(\lambda)$, $\mathbb{R}_*(\lambda)$ такие, что функция $U_1 = \mathcal{R}_*(\lambda)\mathbb{R}_*(\lambda)^{-1}F \quad (\lambda \in [\lambda_0^*, \infty))$ принадлежит пространству $\mathbb{H}'_+$ и удовлетворяет уравнению (62).

Пусть функция $u \in \mathbb{H}'_+$ такая, что

$$B[u,v] + \lambda(u,v)_0 = 0 \quad (\forall v \in \mathbb{H}'_+), \tag{63}$$

где $\lambda \geq \lambda'_0 = \max\{\lambda_0^*, \lambda_0\}$, и пусть F — произвольный элемент пространства $\mathbb{H}'_-$. Так как $U_1 = \mathcal{R}_*(\lambda)\mathbb{R}_*(\lambda)^{-1}F$ принадлежит пространству $\mathbb{H}'_+$, то, полагая $v = U_1$ в (63), получаем $B[u,U_1] + \lambda(u,U_1)_0 = 0$, то есть $\overline{B[u,U_1] + \lambda(u,U_1)_0} = 0$.

С другой стороны, функция $U_1 = \mathcal{R}_*(\lambda)\mathbb{R}_*(\lambda)^{-1}F$ удовлетворяет (62). Поэтому $\langle F, u\rangle = 0$ для всех $F \in \mathbb{H}'_+$. Учитывая вложение $\mathbb{H}'_+ \to \mathbb{H}'_-$ и полагая $F = u$, имеем $\langle u, u\rangle = 0$, то есть $u = 0$. Единственность решения задачи D_λ доказана.

Теорема 1 доказана полностью.

4. Доказательство теоремы 2

Пусть задана функция $U_1(x) \in \mathbb{H}_+$. Определим функционал G_λ, где λ — вещественный параметр,

$$< G_\lambda, v >= -B[U_1,\, v] - \lambda(U_1,\, v)_0 \quad \forall v \in C_0^\infty(\Omega). \tag{64}$$

Учитывая ограниченность коэффициентов $b_{kl}(x)$, $|k| = |l| = j \in J$, $x \in \Omega$, и применяя неравенство Коши-Буняковского, имеем

$$|B[U_1,v]| \leq M_{21} \sum_{m=0}^{s} \|U_1; W^{j_m}_{2;\tau_{j_m}}(\Omega)\| \cdot \|v; W^{j_m}_{2;\tau_{j_m}}(\Omega)\| + \\ + M_{21} \sum_{m=0}^{t} \|U_1; W^{i_m}_{2;\tau_{i_m}}(\Omega)\| \cdot \|v; W^{i_m}_{2;\tau_{i_m}}(\Omega)\|$$

для всех $u, v \in C_0^\infty(\Omega)$. Отсюда в силу неравенства (12) и определения пространства $\mathbb{H}'_+$ (см. (3)) следует, что

$$|B[U_1,v]| \leq M_{22}\, \|U_1;\, \mathbb{H}_+\|\, \|v;\, \mathbb{H}_+\|$$

для всех $v \in \mathbb{H}'_+$. Так как (см. (3)) $\|u;\, L_2(\Omega)\| \leq \|u;\, \mathbb{H}_+\|$ для всех $u \in \mathbb{H}_+$, то

$$|(U_1,\, v)_0| \leq \|U_1;\, \mathbb{H}_+\|\, \|v;\, \mathbb{H}_+\|\,.$$

Из последних неравенств имеем

$$| < G_\lambda, v > | \le (M_{22} + |\lambda|) \, \|U_1; \, \mathbb{H}_+\| \, \|v; \, \mathbb{H}_+\|$$

для всех $v \in C_0^\infty(\Omega)$. Следовательно функционал G_λ по непрерывности продолжается на все пространство $\mathbb{H}'_+$, принадлежит пространству $\mathbb{H}'_-$ и его норма удовлетворяет неравенству

$$\left\|G_\lambda; \, \mathbb{H}'_-\right\| \le (M_{22} + |\lambda|) \, \|U_1; \, \mathbb{H}_+\| \, , \tag{65}$$

где число M_{22} не зависит от выбора функции $U_1(x)$.

Рассмотрим следующую вспомогательную задачу: для заданного функционала $F \in \mathbb{H}'_-$ требуется найти решение U_* уравнения

$$B[U_*, \, v] + \lambda (U_*, \, v)_0 =< F + G_\lambda, v > \quad \forall v \in C_0^\infty(\Omega), \tag{66}$$

принадлежащее пространству $\mathbb{H}'_+$.

Согласно теореме 1 существует число $\lambda_0 \ge 0$ такое, что при $\lambda \ge \lambda_0$ вспомогательная задача имеет единственное решение $U_*(x)$ и при этом выполняется неравенство

$$\|U_*; \, \mathbb{H}_+\| \le M_{23} \left\|F + G_\lambda; \, \mathbb{H}'_-\right\| . \tag{67}$$

Пусть $U_*(x)$ — решение вспомогательной задачи. Рассмотрим функцию

$$U(x) = U_*(x) + U_1(x). \tag{68}$$

Из (64), (66) следует, что функция $U(x)$ удовлетворяет уравнению (4).

Так как $U(x) - U_1(x) = U_*(x) \in \mathbb{H}'_+$, то она удовлетворяет также и условию (9). Следовательно, функция $U(x)$, определенная равенством (67), является решением задачи $\mathbb{D}_\lambda$. Из единственности решения вспомогательной задачи следует единственность решения задачи $\mathbb{D}_\lambda$.

Оценка (10) теоремы 2 следует из (65), (67), (68).

Теорема 2 доказана.

5. Заключение

Работа посвящена исследованию разрешимости вариационной задачи Дирихле для эллиптических операторов в ограниченной области с несогласованными вырождениями коэффициентов на границе. Интегро-дифференциальная полуторалинейная форма, ассоциированная с исследуемым оператором, представляется в виде конечного числа полуторалинейных форм и вводится понятие “старшая форма”. Условия, обеспечивающие существование и единственность решения вариационной задачи Дирихле, ставятся только на коэффициенты старших форм.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Никольский С. М. Вариационная проблема для уравнения эллиптического типа с вырождением на границе // Труды Математического института им. В. А. Стеклова АН СССР. 1979. Т. 150. С. 212–238.

2. Лизоркин П. И., Никольский С. М. Коэрцитивные свойства эллиптического уравнения с вырождением. Вариационный метод // Труды Математического института им. В. А. Стеклова АН СССР. 1981. Т. 157. С. 90–118.

3. Лизоркин П. И., Никольский С. М. Коэрцитивные свойства эллиптического уравнения с вырождением и обобщенной правой частью // Труды Математического института им. В. А. Стеклова АН СССР. 1983. Т. 161. С. 157–183.

4. Байдельдинов Б. Л. Об аналоге первой краевой задачи для эллиптических уравнений с вырождением. Метод билинейных форм // Труды Математического института им. В. А. Стеклова АН СССР. 1984. Т. 170. С. 3–11.

5. Лизоркин П. И. К теории вырождающихся эллиптических уравнений // Труды Математического института им. В. А. Стеклова АН СССР. 1985. Т. 172. С. 235–271.

6. Мирошин Н. В. Вариационная задача Дирихле для вырождающегося на границе эллиптического оператора // Дифференциальные уравнения. 1988. Т. 24. № 6. С. 1099–1111.

7. Никольский С. М., Лизоркин П. И., Мирошин Н. В. Весовые функциональные пространства и их приложения к исследованию краевых задач для вырождающихся эллиптических уравнений // Известия Вузов. Математика. 1988. № 8. С. 4–30.

8. Исхоков С. А., Кужмуратов А. Я. О вариационной задаче Дирихле для вырождающихся эллиптических операторов // Доклады Академии наук (Россия). – 2005. Т. 403. № 2. С. 165–168.

9. Бойматов К. Х. Обобщенная задача Дирихле для систем дифференциальных уравнений второго порядка // Доклады АН СССР. 1992. Т.327. № 1. С. 9–15.

10. Бойматов К. Х. Обобщенная задача Дирихле, порожденная некоэрцитивной формой // Доклады Академии наук (Россия). 1993. Т. 330. № 3. С. 285–290.

11. Исхоков С. А. О гладкости решений обобщенной задачи Дирихле и задачи на собственные значения для дифференциальных операторов, порожденных некоэрцитивными билинейными формами // Доклады Академии наук (Россия). 1995. Т. 342. № 1. С. 20–22.

12. Бойматов К. Х., Исхоков С. А. О разрешимости и спектральных свойствах вариационной задачи Дирихле, связанной с некоэрцитивной билинейной формой //Труды Математического института им. В. А. Стеклова РАН. 1997. Т. 214. С. 107–134.

13. Исхоков С. А., Гадоев М. Г., Константинова Т. П. Вариационная задача Дирихле для вырождающихся эллиптических операторов, порожденных некоэрцитивными формами // Доклады Академии наук (Россия). 2015. Т. 462. № 1. С. 7–10.

14. Мирошин Н. В. Обобщенная задача Дирихле для одного класса эллиптических дифференциальных операторов, вырождающихся на границе области. Некоторые спектральные свойства // Дифференциальные уравнения. 1976. Т. 12. № 6. С. 1099–1111.

15. Като Т. Теория возмущений линейных операторов. М.: Мир. 1972.

16. Гохберг И. Ц., Крейн М. Г. Введение в теорию линейных несамосопряженных операторов. М.: Наука, 1965.

REFERENCES

1. Nikol'skii S. M. 1981, "A variational problem for an equation of elliptic type with degeneration on the boundary", Proceedings of the Steklov Institute of Mathematics, vol. 150, pp. 227–254.

2. Lizorkin P. I., Nikol'skii S. M. 1983, "Coercive properties of elliptic equations with degeneration. Variational method", vol. 157. pp. 95–125.

3. Lizorkin P. I., Nikol'skii S. M. 1984, "Coercive properties of an elliptic equation with degeneration and a generalized right-hand side", Proc. Steklov Inst. Math., vol. 161, pp. 171–198

4. Baidel'dinov B. L. 1987, "An analogue of the first boundary value problem for elliptic equations with degeneration. The method of bilinear forms", Proceedings of the Steklov Institute of Mathematics, vol. 170, pp. 1–10.

5. Lizorkin P. I. 1987, "On the theory of degenerate elliptic equations", Proceedings of the Steklov Institute of Mathematics, vol. 172, pp. 257–274.

6. Miroshin N. V. 1988, "The variational Dirichlet problem for an elliptic operator that is degenerate on the boundary", Differential Equations, vol. 24:3, pp. 323–329.

7. Nikolskii S. M., Lizorkin P. I., Miroshin N. V. 1988, "Weighted functional spaces and their application to investigation of boundary value problems for degenerate elliptic equations", Soviet Math. (Izv. VUZ), vol. 32, No. 8. pp. 1–40.

8. Iskhokov S. A., Kuzhmuratov A. Ya. 2005, "On the variational Dirichlet problem for degenerate elliptic operators" Doklady Mathematics, vol. 72, no. 1, pp. 512–515.

9. Boimatov K. Kh. 1993, "The generalized Dirichlet problem for systems of second-order differential equations" Russian Acad. Sci. Dokl. Math., vol. 46, no. 3, pp. 403–409.

10. Boimatov K. Kh. 1993, "The generalized Dirichlet problem associated with a noncoercive bilinear form", Russian Acad. Sci. Dokl. Math., vol. 47, no. 3, pp. 455–463.

11. Iskhokov S. A. 1995, "On the smoothness of a solutions of the generalized Dirichlet problem and the eigenvalue problem for differential operators generated by noncoercive bilinear forms", Doklady Mathematics, vol. 51, no. 3, pp. 323–325.

12. Boimatov K. Kh., Iskhokov S. A. 1996, "On the solvability and smoothness of a solution of the variational Dirichlet problem associated with a noncoercive bilinear form", Proceedings of the Steklov Institute of Mathematics, no. 3(214), pp. 101–127.

13. Iskhokov S. A., Gadoev M. G., Konstantinova T. P. 2015, "Variational Dirichlet problem for degenerate elliptic operators generated by noncoercive forms", Doklady Mathematics, vol. 91, no. 3, pp. 255–258. DOI: 10.1134/S1064562415030011.

14. Miroshin N. V. 1976, "A generalized Dirichlet problem for a certain class of elliptic differential operators that are degenerate on the boundary of the domain. Some spectral properties", Differ. Uravn., vol. 12:6, pp. 1099–1111.

15. Kato T. 1967, "Perturbation theory of linear operators", Springer-Verlag, 592 p.

16. Gokhberg I. Ts., Krein M.G. 1965, "Introduction to the theory of non-selfadgoint linear operators", Nauka: Moscow, 448 p.

Получено 22.04.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.321 DOI 10.22405/2226-8383-2018-19-3-183-201

Оценка взвешенных сумм Клоостермана с помощью аддитивного сдвига[1]

Королёв Максим Александрович — доктор физико-математических наук, ведущий научный сотрудник Отдела теории чисел, Математический институт им. В. А. Стеклова РАН, 119991, Москва, ул. Губкина, 8.
e-mail: korolevma@mi-ras.ru

Аннотация

Аддитивный сдвиг – один из часто используемых приёмов оценки тригонометрических сумм и сумм значений характеров. Он состоит в замене переменной суммирования n выражением вида $n+x$ с последующим суммированием по искусственно введённой переменной x. Превращение исходной однократной суммы в кратную открывает дополнительные возможности, позволяющие получить её нетривиальную оценку. Этот приём широко использовался в работах Й. Г. ван дер Корпута, И. М. Виноградова, Д. А. Бёрджесса, А. А. Карацубы и многих других исследователей. Он оказался весьма полезным рабочим инструментом и при работе с суммами значений характеров в конечных полях, а также с кратными тригонометрическими суммами. Э. Фуври и П. Мишель (1998), Ж. Бургейн (2005) стали успешно применять этот приём к оценкам сумм Клоостермана по простому модулю.

Э. Фуври и П. Мишель сочетали аддитивный сдвиг с глубокими результатами, которые получаются средствами алгебраической геометрии. Метод Ж. Бургейна полностью элементарен. Так, его использование позволило автору дать полностью элементарный вывод оценки суммы Клоостермана с простыми числами по простому модулю q в случае, когда длина N такой суммы превосходит $q^{1/2+\varepsilon}$.

В настоящей статье даются новые примеры применения аддитивного сдвига к взвешенным суммам Клоостермана вида

$$\sum_{n\leqslant N} f(n)\exp\left(\frac{2\pi i a}{q}\,(n+b)^*\right),\quad (ab,q)=1,\quad mm^*\equiv 1\ (\mathrm{mod}\, q),$$

где q - простое число, а весовая функция $f(n)$ берётся равной числу $\tau(n)$ делителей n или же количеству $r(n)$ представлений n суммою двух квадратов целых чисел. Полученные оценки нетривиальны уже при $N\geqslant q^{2/3+\varepsilon}$.

Следствием таких оценок являются новые результаты о распределении дробных долей вида

$$\left\{\frac{a}{q}\,(uv+b)^*\right\},\quad \left\{\frac{a}{q}\,(u^2+v^2+b)^*\right\},$$

в случае, когда целочисленные переменные u, v меняются в гиперболической ($uv\leqslant N$) и круговой ($u^2+v^2\leqslant N$) областях, соответственно.

Ключевые слова: обратные вычеты, суммы Клоостермана, аддитивный сдвиг, функция делителей.

Библиография: 49 названий.

[1]Работа выполнена при поддержке Российского научного фонда (грант № 14-11-00433).

Для цитирования:
М. А. Королёв. Оценка взвешенных сумм Клоостермана с помощью аддитивного сдвига // Чебышевский сборник, 2018, т. 19, вып. 3, с. 183–201.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.321 DOI 10.22405/2226-8383-2018-19-3-183-201

The estimate of weighted Kloosterman sums by additive shift[2]

Korolev Maxim Aleksandrovich — Doctor Phys.-Math. Sci., Steklov Mathematical Institute of Russian Academy of Sciences, Department of Number Theory, Leading Scientific Researcher, 119991, Moscow, Russia, Gubkina str., 8.
e-mail: korolevma@mi-ras.ru

Abstract

Additive shift is a widely used tool in the estimating of exponential sums and character sums. It bases on the replacement of the summation variable n by the expression of the type $n+x$ and the summation over artificially introduced variable x. The transformation of the simple sum to multiple sum gives an additional opportunities, which allow one on obtain the non-trivial bound for the initial sum. This shift was widely used by I.G. van der Corput, I.M. Vinogradov, D.A. Burgess, A.A. Karatsuba and many other researchers. It became very useful tool also in dealing with character sums in finite fields and with multiple exponential sums.

E. Fouvry and P. Michel (1998) and then J. Bourgain (2005) used successfully this shift to the estimation of Kloosterman sums. E. Fouvry and P. Michel combine additive shift with deep-lying results from algebraic geometry. On the contrary, the method of J. Bourgain is completely elementary. For example, it allows to the author to give elementary proof of the estimate of Kloosterman sum prime modulo q with primes in the case when its length N exceeds $q^{1/2+\varepsilon}$.

In this paper, we give some new elementary applications of additive shift to weighted Kloosterman sums of the type

$$\sum_{n\leqslant N} f(n)\exp\left(\frac{2\pi i a}{q}\,(n+b)^*\right), \quad (ab,q)=1.$$

Here q is prime and weight function $f(n)$ is equal to $\tau(n)$, that is, the number of divisors of n, or equal to $r(n)$, which is the number of representations of n by the sum of two squares of integers. The bounds for these sums are non-trivial for $N \geqslant q^{2/3+\varepsilon}$.

As a corollary of such estimates, we obtain some new results concerning the distribution of the fractional parts of the following type

$$\left\{\frac{a}{q}\,(uv+b)^*\right\}, \quad \left\{\frac{a}{q}\,(u^2+v^2+b)^*\right\},$$

where the integers u, v run through the hyperbolic ($uv \leqslant N$) and circle ($u^2+v^2 \leqslant N$) domains, consequently.

Keywords: inverse residues, Kloosterman sums, additive shift, divisor function.

Bibliography: 49 titles.

For citation:
M. A. Korolev, 2018, "The estimate of weighted Kloosterman sums by additive shift" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 183–201.

[2]The work was supported by the Russian science Foundation (grant № 14-11-00433).

Памяти Юрия Владимировича Линника

1. Введение

Суммой Клоостермана по модулю $q > 2$ называется тригонометрическая сумма вида

$$\sum_{n\in A} e_q(a\overline{n} + bn) = \sum_{n\in A} e_q\left(\frac{a}{n} + bn\right), \tag{1}$$

где $e_q(u) = e^{2\pi iu/q}$, a, b — целые числа, $a \not\equiv 0 \pmod q$, $\overline{n} = 1/n = n^*$ — решение сравнения $n\overline{n} \equiv 1 \pmod q$, A - некоторое подмножество приведённой системы вычетов $\mathbb{Z}_q^*$ по модулю q.

Суммы (1) и им подобные возникают во многих задачах теории чисел (см., например, обзоры Д. Р. Хизбрауна [1] и П. Сарнака [2], гл. 11, 16 и 20 книги Х. Иванца и Э. Ковальского [4], монографию А. В. Устинова [3], а также приведённые в этих работах библиографии; разумеется, этот список не является сколь-нибудь полным).

Наряду с суммами (1) рассматриваются и суммы Клоостермана с весами, т.е. суммы вида

$$\sum_{n\in A} f(n)e_q(a\overline{n} + bn), \tag{2}$$

где $f(n)$ — некоторая арифметическая функция. Оценкам таких сумм посвящены, в частности, работы [5]–[10].

При оценках тригонометрических сумм вида

$$S = \sum_{M<n\leqslant M+N} e(\varphi(n)), \quad N > 1, \quad e(z) = e^{2\pi iz},$$

часто применяется следующий приём, который условно можно назвать "аддитивным сдвигом" переменной суммирования. Заключается он в следующем. Пусть X – целое число, причем $1 \leqslant X \leqslant N^{1-\delta}$, где $\delta > 0$ – достаточно малая постоянная. Задавшись произвольным целым x с условием $1 \leqslant x \leqslant X$, преобразуем сумму S следующим образом:

$$S = \sum_{M<n+x\leqslant M+N} e(\varphi(n+x)) = \sum_{M-x<n\leqslant M+N-x} e(\varphi(n+x)) =$$
$$= \sum_{M<n\leqslant M+N} e(\varphi(n+x)) + 2\theta x, \quad |\theta| \leqslant 1.$$

Суммируя обе части по $1 \leqslant x \leqslant X$, получим:

$$S = X^{-1} \sum_{M<n\leqslant M+N} \sum_{x=1}^{X} e(\varphi(n+x)) + 2\theta_1 X, \quad |\theta_1| \leqslant 1.$$

Наличие двойного суммирования (по n и по x) открывает дополнительные возможности, позволяющие получить нетривиальную оценку исходной суммы.

Этот приём и его модификации широко и успешно применялись Й. Г. ван дер Корпутом, И. М. Виноградовым, А. А. Карацубой, Д. А. Берджессом и многими другими исследователями при решении ряда задач аддитивной теории чисел, теории дзета-функции Римана, характеров Дирихле, характеров в конечных полях, кратных тригонометрических сумм (см., например, [14]–[37]; и этот список, конечно, не является исчерпывающим).

Аддитивный сдвиг оказывается наиболее эффективным в задачах, где функция $\varphi(n)$ либо является многочленом, либо хорошо им приближается: в таких случаях имеется определённая

"гибкость" в работе с выражениями вида $\varphi(n+x)$, где x мало по сравнению с n. Однако функции вида

$$\varphi(n) = \frac{1}{q}(a\overline{n} + bn) \pmod 1$$

такими свойствами, вообще говоря, не обладают.

Тем не менее, в ряде случаев аддитивный сдвиг удаётся применить и к оценкам сумм Клоостермана и их обобщениям. Так, в 1997 г. Э. Фуври и П. Мишель, сочетая этот приём с методами алгебраической геометрии, смогли получить оценки билинейных форм вида

$$\sum_{M<m\leqslant M_1}\sum_{N<n\leqslant N_1}\alpha_m\beta_n e_q(f(mn)),$$

где модуль q — простое число, а $f(x) = P(x)/Q(x) = P(x)\overline{Q(x)}$ — рациональная функция над $\mathbb{Z}_q^*$ достаточно общего вида. Следствием оценок таких форм явилась, в частности, оценка суммы с простыми числами вида

$$\sum_{p\leqslant N} e_q(f(p)) \ll N^{25/36}q^{3/16+\varepsilon},$$

нетривиальная при $N \geqslant q^{6/7+\varepsilon}$.

В 2005 г. Ж. Бургейн [39], также используя аддитивный сдвиг, в случае простого модуля q смог получить оценку билинейной формы

$$\sum_{c<m\leqslant c+M}\sum_{d<n\leqslant d+N}\alpha_m\beta_n e_q(a\overline{mn} + bmn),$$

где $MN \geqslant q^{1/2+\varepsilon}$, $q^\varepsilon < M, N \leqslant \sqrt{q}$, а c, d — произвольные числа. Наряду с оценкой

$$\sum_{M<n\leqslant M+N} e_q(a\overline{n} + bn) \ll \sqrt{q}\ln q, \tag{3}$$

следующей из классического неравенства А. Вейля [40] вида

$$\left|\sum_{n=1}^{q-1} e_q(a\overline{n} + bn)\right| \leqslant 2\sqrt{q}$$

это приводит к следующей оценке суммы Клоостермана с простыми числами:

$$\sum_{p\leqslant N} e_q(a\overline{p} + bp) \ll Nq^{-\delta}, \quad N \geqslant q^{1/2+\varepsilon}, \quad \delta = c\varepsilon^4. \tag{4}$$

Дальнейшее развитие метод Бургейна (применительно к суммам Клоостермана) получил в работах [41]–[45]. В частности, в работах [43], [45] с помощью элементарных рассуждений (т.е. не опирающихся на средства алгебраической геометрии), включающих аддитивный сдвиг, автору удалось получить оценки вида

$$\sum_{M<n\leqslant M+N} e_q(a\overline{n} + bn) \ll Nq^{-c\varepsilon^2},$$

нетривиальные при $N \geqslant q^{1/2+\varepsilon}$. В соединении с методом Бургейна это дало полностью элементарный вывод неравенства (4).

Метод Бургейна практически без изменения переносится на взвешенные суммы типа

$$\sum_{n\leqslant N} f(n)e_q(a\overline{n}) = \sum_{n\leqslant N} f(n)e_q\left(\frac{a}{n}\right),$$

где $f(n)$ — одна из функций $\tau_k(n)$, $\mu(n)$ (см. [45]), а также $f(n) = r(n)$ (как обычно, $\tau_k(n)$ — многомерная функция делителей, $\mu(n)$ — функция Мёбиуса, $r(n)$ — количество представлений n суммою двух квадратов целых чисел). Однако этот метод (во всяком случае, без внесения существенных изменений в рассуждения) не позволяет получить, например, оценки сумм вида

$$S_1 = S_1(q,N;a,b) = \sum_{1\leqslant n\leqslant N} \tau(n)e_q\left(\frac{a}{n+b}\right) = \sum_{\substack{1\leqslant uv\leqslant N\\ u,v\geqslant 1}} e_q\left(\frac{a}{uv+b}\right),$$

$$S_2 = S_2(q,N;a,b) = \sum_{1\leqslant n\leqslant N} r(n)\, e_q\left(\frac{a}{n+b}\right) = \sum_{1\leqslant u^2+v^2\leqslant N} e_q\left(\frac{a}{u^2+v^2+b}\right),$$

где q — простое число, $(ab,q)=1$, $\tau(n)=\tau_2(n)$ — число делителей n.

В 2000 г. А. А. Карацуба [46] применил аддитивный сдвиг вида $n\mapsto n+xy$ (с последующим суммированием по x и y) к задаче оценки суммы значений неглавного характера Дирихле χ_q по простому модулю q с весами типа $\tau_k(n)$, $r(n)$. В частности, ему удалось получить оценки вида

$$\sum_{n\leqslant N} \tau(n)\chi_q(n+a), \quad \sum_{n\leqslant N} r(n)\chi_q(n+a), \quad 0<|a|\leqslant\sqrt{q},$$

нетривиальные при $N\geqslant q^{1/3+\varepsilon}$, и тем самым значительно уточнить свой предыдущий результат [47].

В настоящей статье мы применяем идею работы [46] к оценке взвешенных сумм Клоостермана $S_j = S_j(q,N;a,b)$, $j=1,2$. Основным результатом является следующая

Теорема 1. *Пусть $0<\varepsilon<0.1$ — сколь угодно малое фиксированное число, $q\geqslant q_0(\varepsilon)$ — простое, $(ab,q)=1$, N — целое, причём $q^{2/3+\varepsilon}<N\leqslant q$. Тогда для определённых выше сумм S_1, S_2 справедливы следующие оценки:*

$$S_1,\ S_2 \ll Nq^{-\varepsilon^2/35}.$$

Эта теорема позволяет получить некоторые утверждения, касающиеся распределения дробных долей вида

$$\left\{\frac{a}{uv+b}\right\}, \quad \left\{\frac{a}{u^2+v^2+b}\right\}$$

при изменении целых чисел u,v в гиперболической и круговой областях, соответственно (см. теоремы 2–4).

2. Вспомогательная лемма

В настоящем параграфе мы получаем верхнюю оценку для числа решений системы сравнений специального вида. Метод доказательства этой оценки восходит к работе [48].

Лемма 1. *Пусть $c_1,c_2>1$ – произвольные абсолютные постоянные, $q\geqslant q_0(c_1,c_2)$ – достаточно большое простое число. Пусть, далее, числа X,U,U_1,V,V_1 удовлетворяют условиям*

$$(\ln q)^3 < U < U_1 \leqslant c_1U, \quad (\ln q)^3 < V < V_1 \leqslant c_2V, \quad U\leqslant V,$$
$$X_0(c_1,c_2) < X \leqslant V, \quad U_1V_1 < q, \quad XV\leqslant qU. \quad (5)$$

Тогда для количества $I = I(q; X; U, U_1; V, V_1)$ *решений системы сравнений*

$$\begin{cases} x_1 u_1 \equiv x_2 u_2 \pmod q, \\ x_1 v_1 \equiv x_2 v_2 \pmod q \end{cases} \tag{6}$$

с условиями $1 \leqslant x_1, x_2 \leqslant X$, $U < u_1, u_2 \leqslant U_1$, $V < v_1, v_2 \leqslant V_1$ *справедлива следующая оценка:*

$$I \leqslant 2c_1c_2XUV \ln q.$$

Доказательство. Ввиду неравенств $1 \leqslant x_1u_1, x_2u_2 \leqslant XU_1 < q$ первое сравнение системы оказывается уравнением: $x_1u_1 = x_2u_2$. Разобьём все решения (6) на классы, относя к классу $E(\delta)$ все решения $(x_1, x_2, u_1, u_2, v_1, v_2)$, отвечающие условию $(x_1, x_2) = \delta$. Обозначая через $I(\delta)$ число решений в классе $E(\delta)$, будем, следовательно, иметь:

$$I = \sum_{1 \leqslant \delta \leqslant X} I(\delta). \tag{7}$$

Оценим величину $I(\delta)$. Если x_1, x_2 – компоненты произвольного решения из класса $E(\delta)$, то $x_j = \delta y_j$, $j = 1, 2$, где

$$(y_1, y_2) = 1, \quad 1 \leqslant y_1, y_2 \leqslant X\delta^{-1}. \tag{8}$$

Зафиксируем произвольную пару y_1, y_2 с условиями (8). Тогда из второго сравнения системы (6) получим:

$$\delta y_1 v_1 - \delta y_2 v_2 = qn,$$

где n — некоторое целое число. Поскольку q простое, то необходимо $n = \delta m$, так что

$$y_1 v_1 - y_2 v_2 = qm,$$

причём

$$|m| \leqslant \frac{1}{q} |y_1 v_1 - y_2 v_2| \leqslant \frac{XV_1}{q\delta} \leqslant \frac{c_2 XV}{q\delta}. \tag{9}$$

Фиксируя произвольное целое m с условием (9), оценим сверху число $I(\delta; y_1, y_2, m)$ четвёрок (u_1, u_2, v_1, v_2), удовлетворяющих системе

$$\begin{cases} y_1 u_1 = y_2 v_2, \\ y_1 v_1 - y_2 v_2 = qm, \\ U < u_1, u_2 \leqslant U_1,\ V < v_1, v_2 \leqslant V_1. \end{cases} \tag{10}$$

В силу (8) из первого уравнения (10) получаем $u_1 = sy_2$, $u_2 = sy_1$, где s — некоторое целое число. Тогда $U < sy_1, sy_2 \leqslant U_1$, откуда несложно заключить, что величина s может принимать не более

$$\min\left(\frac{U_1 - U}{y_1}, \frac{U_1 - U}{y_2}\right) + 1 \leqslant (c_1 - 1) \min\left(Uy_1^{-1}, Uy_2^{-1}\right) + 1 = \nu$$

значений.

Зафиксируем произвольное решение $v_1^{(0)}, v_2^{(0)}$ второго уравнения системы (10). Тогда для любого другого решения v_1, v_2 будем иметь:

$$y_1 v_1^{(0)} - y_2 v_2^{(0)} = qm = y_1 v_1 - y_2 v_2,$$

откуда $y_1(v_1 - v_1^{(0)}) = y_2(v_2 - v_2^{(0)})$. В силу (8) отсюда имеем: $v_1 - v_1^{(0)} = ty_2$, $v_2 - v_2^{(0)} = ty_1$, где t — целое число. Область изменения t определяется неравенствами

$$V < ty_1 + v_2^{(0)} \leqslant V_1, \quad V < ty_2 + v_1^{(0)} \leqslant V_1,$$

так что

$$\max\left(\frac{V-v_2^{(0)}}{y_1},\frac{V-v_1^{(0)}}{y_2}\right) < t \leqslant \min\left(\frac{V_1-v_2^{(0)}}{y_1},\frac{V_1-v_1^{(0)}}{y_2}\right).$$

Следовательно, величина t может принимать не более

$$\min\left(\frac{V_1-V}{y_1},\frac{V_1-V}{y_2}\right)+1 \leqslant (c_2-1)\min\left(Vy_1^{-1},Vy_2^{-1}\right)+1 = \lambda$$

значений. Так находим:

$$I(\delta;y_1,y_2,m) \leqslant \lambda\nu \leqslant \left((c_1-1)\min\left(Uy_1^{-1},Uy_2^{-1}\right)+1\right)\left((c_2-1)\min\left(Vy_1^{-1},Vy_2^{-1}\right)+1\right). \quad (11)$$

Суммируя неравенство (11) по всем целым m с условием (9), получим:

$$\sum_{|m|\leqslant c_2XV(q\delta)^{-1}} I(\delta;y_1,y_2,m) \leqslant$$
$$\leqslant \left(\frac{2c_2XV}{q\delta}+1\right)\left((c_1-1)\min\left(Uy_1^{-1},Uy_2^{-1}\right)+1\right)\left((c_2-1)\min\left(Vy_1^{-1},Vy_2^{-1}\right)+1\right).$$

Далее, суммирование по всем парам y_1, y_2, удовлетворяющих (8), даёт:

$$I(\delta) \leqslant 2\left(\frac{2c_2XV}{q\delta}+1\right)\sum_{1\leqslant y_1\leqslant y_2\leqslant X\delta^{-1}}\left((c_1-1)Uy_2^{-1}+1\right)\left((c_2-1)Vy_2^{-1}+1\right) \leqslant$$
$$\leqslant 2\left(\frac{2c_2XV}{q\delta}+1\right)\sum_{1\leqslant y_2\leqslant X\delta^{-1}}\left((c_1-1)(c_2-1)UVy_2^{-1}+(c_1-1)U+(c_2-1)V+y_2\right) \leqslant$$
$$\leqslant 2\left(\frac{2c_2XV}{q\delta}+1\right)\left((c_1-1)(c_2-1)UV(\ln X+1)+(c_1-1)XU\delta^{-1}+(c_2-1)XV\delta^{-1}+X^2\delta^{-2}\right).$$

Переходя, наконец, к оценке величины I, согласно (7) будем иметь:

$$I \leqslant 2\sum_{1\leqslant\delta\leqslant X}\left(\frac{2c_2XV}{q\delta}+1\right)\times$$
$$\times\left((c_1-1)(c_2-1)UV(\ln X+1)+(c_1-1)XU\delta^{-1}+(c_2-1)XV\delta^{-1}+X^2\delta^{-2}\right) \leqslant$$
$$\leqslant 2\Big((c_1-1)(c_2-1)XUV(\ln X+1)+(c_1-1)XU(\ln X+1)+(c_2-1)XV(\ln X+1)+$$
$$+\frac{\pi^2}{6}X^2+2c_2(c_1-1)(c_2-1)\frac{XUV^2}{q}(\ln X+1)^2+\frac{\pi^2}{3}c_2(c_1-1)\frac{X^2UV}{q}+$$
$$+\frac{\pi^2}{3}c_2(c_2-1)\frac{X^2V^2}{q}+2\zeta(3)c_2\frac{X^3V}{q}\Big) = 2XUV\Delta,$$

где

$$\Delta = (\ln X+1)\left\{(c_1-1)(c_2-1)+(c_1-1)V^{-1}+(c_2-1)U^{-1}\right\}+$$
$$+2c_2(c_1-1)(c_2-1)\frac{V}{q}(\ln X+1)^2+$$
$$+\frac{\pi^2}{6}\frac{X}{UV}+\frac{\pi^2}{3}c_2(c_1-1)\frac{X}{q}+\frac{\pi^2}{3}c_2(c_2-1)\frac{XV}{qU}+2\zeta(3)c_2\frac{X^2}{qU}.$$

Принимая во внимание условия (5), находим:

$$\frac{X}{UV} \leqslant \frac{1}{U} \leqslant (\ln q)^{-3}, \quad \frac{X}{q} \leqslant \frac{V}{q} \leqslant \frac{1}{U} \leqslant (\ln q)^{-3}, \quad \frac{X^2}{qU} \leqslant \frac{XV}{qU} \leqslant 1.$$

Следовательно,

$$\Delta \leqslant (c_1-1)(c_2-1)(\ln X+1) + (c_1+c_2-2)(\ln X+1)(\ln q)^{-3} + \frac{\pi^2}{6}(\ln q)^{-3} + \\ + 2c_2(c_1-1)(c_2-1)(\ln X+1)^2(\ln q)^{-3} + \frac{\pi^2}{3}c_2(c_1-1)(\ln q)^{-3} + \\ + \frac{\pi^2}{3}c_2(c_2-1) + 2\zeta(3)c_2 < c_1c_2\ln q.$$

Лемма доказана. □

3. Доказательство теоремы 1

Поскольку сумма S_2 оценивается подобно сумме S_1, далее мы приведём достаточно подробный вывод оценки S_1, а затем укажем на необходимые изменения, которые нужно внести в рассуждения для получения оценки S_2.

Положим $\delta = 0.5\varepsilon$; представляя S_1 в виде

$$S_1 = \sum_{1\leqslant uv\leqslant N} e_q\Big(\frac{a}{uv+b}\Big),$$

разобьём область изменения каждой из переменных u, v на промежутки $U < u \leqslant U_1$, $V < v \leqslant V_1$, где $1 \leqslant U, V \leqslant 0.5N$, $U_1 \leqslant 2U$, $V_1 \leqslant 2V$. Соответственно, S_1 разобьётся на $\ll (\ln q)^2$ сумм

$$S(U,V) = \sum_{U<u\leqslant U_1}\sum_{\substack{V<v\leqslant V_1\\ 1\leqslant uv\leqslant N}} e_q\Big(\frac{a}{uv+b}\Big).$$

Очевидно, вклад в S_1 от сумм $S(U,V)$ с условием $UV \leqslant Nq^{-\delta}$ не превосходит по порядку $N(\ln q)^2q^{-\delta} < Nq^{-\varepsilon^2}$. Поэтому всюду далее будем рассматривать лишь те пары U, V, для которых $Nq^{-\delta} < UV \leqslant N$ (в случае $UV > N$ сумма $S(U,V)$, очевидно, пуста). Далее, поскольку переменные u, v входят в $S(U,V)$ симметрично, не ограничивая общности можно считать, что $U \leqslant V$. Наконец, если $1 \leqslant U \leqslant q^{1/6}$, то $V \geqslant NU^{-1}q^{-\delta} \geqslant q^{1/2+\varepsilon/2}$, так что в этом случае неравенство (3) даёт:

$$\sum_{\substack{V<v\leqslant V_1\\ 1\leqslant v\leqslant Nu^{-1}}} e_q\Big(\frac{a}{uv+b}\Big) = \sum_{V<v\leqslant V_2} e_q\Big(\frac{a\overline{u}}{v+b\overline{u}}\Big) = \sum_{b_1+V<n\leqslant b_1+V_2} e_q(a_1\overline{n}) \ll \sqrt{q}\ln q,$$

откуда

$$S(U,V) \ll U\sqrt{q}\ln q \ll q^{2/3}\ln q \ll Nq^{-\varepsilon}\ln q \ll Nq^{-0.5\varepsilon}$$

(здесь обозначено: $a_1 \equiv a\overline{u} \pmod q$, $b_1 \equiv b\overline{u} \pmod q$, $1 \leqslant b_1 < q$, $V_2 = \min(V_1, Nu^{-1})$). Следовательно, всюду далее можно считать, что $U > q^{1/6}$.

Итак, пусть U, V — произвольная пара с условиями $q^{1/6} < U \leqslant V$, $Nq^{-\delta} \leqslant UV \leqslant N$. Зададимся целыми числами $X, Y \geqslant 1$ такими, что $2XU < q$, $2XY < V$ (точные значения X, Y

будут выбраны ниже). Тогда, вновь полагая $V_2 = \min(V_1, Nu^{-1})$ для заданного u, для любых целых x, y таких, что $1 \leqslant x \leqslant X$, $1 \leqslant y \leqslant Y$, будем иметь:

$$S(U,V) = \sum_{U<u\leqslant U_1}\sum_{V<v\leqslant V_2} e_q\left(\frac{a\overline{u}}{v+b\overline{u}}\right) = \\ = \sum_{U<u\leqslant U_1}\sum_{V<v+xy\leqslant V_2} e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right) = \sum_{U<u\leqslant U_1}\sum_{V-xy<v\leqslant V_2-xy} e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right).$$

Просуммируем обе части последнего равенства по x и y; получим:

$$XYS(U,V) = \sum_{U<u\leqslant U_1}\sum_{x=1}^{X}\sum_{y=1}^{Y}\sum_{V-xy<v\leqslant V_2-xy} e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right) = \\ = \sum_{U<u\leqslant U_1}\sum_{V-XY<v\leqslant V_2-1}\sum_{x=1}^{X}\sum_{\substack{0<y\leqslant Y\\ (V-v)/x<y\leqslant(V_2-v)/x}} e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right).$$

Положив

$$y_1 = \max\left(0, \frac{V-v}{x}\right), \quad y_2 = \min\left(Y, \frac{V_2-v}{x}\right), \quad h = 2[V+1]+1,$$

будем иметь: $0 \leqslant y_1 < y_2 \leqslant Y < h$, $V_2 \leqslant V_1 < h$. Следовательно, сумма по y принимает вид

$$\sum_{y_1<y\leqslant y_2} e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right) = \\ = \sum_{y=1}^{Y}\left(\frac{1}{h}\sum_{|c|\leqslant h/2}\sum_{y_1<\xi\leqslant y_2} e_h(c(y-\xi))\right)e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right) = \\ = \sum_{|c|\leqslant h/2}\frac{1}{h}\left(\sum_{y_1<\xi\leqslant y_2} e_h(-c\xi)\right)\sum_{y=1}^{Y} e_h(cy)e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right) = \\ = \sum_{|c|\leqslant h/2}\frac{f(c;u,v,x)}{|c|+1}\sum_{y=1}^{Y} e_h(cy)e_q\left(\frac{a\overline{u}}{v+xy+b\overline{u}}\right),$$

где

$$f(c;u,v,x) = \frac{|c|+1}{h}\sum_{y_1<\xi\leqslant y_2} e_h(-c\xi).$$

Несложно проверить, что $|f(c;u,v,x)| \leqslant 1$ для всех рассматриваемых c, u, v и x. Действительно, если $c = 0$, то

$$f(c;u,v,x) = \frac{[y_2]-[y_1]}{h} \leqslant \frac{Y}{h} \leqslant \frac{Y}{2V} \leqslant \frac{1}{4X} < 1.$$

Если же $0 < |c| \leqslant 0.5h$, то

$$|f(c;u,v,x)| = \frac{|c|+1}{h}\cdot\left|\frac{e_h(-c[y_2]) - e_h(-c[y_1])}{e_h(-c)-1}\right| \leqslant \frac{|c|+1}{h}\left|\sin\frac{\pi c}{h}\right|^{-1} \leqslant \frac{|c|+1}{h}\cdot\frac{h}{2|c|} \leqslant 1.$$

Следовательно,

$$S(U,V) = (XY)^{-1}\sum_{|c|\leqslant h/2}\frac{S_c(U,V)}{|c|+1},$$

где

$$S_c(U,V) = \sum_{U<u\leqslant U_1}\sum_{V-XY<v\leqslant V_2-1}\sum_{x=1}^{X} f(c;u,v,x)\sum_{y=1}^{Y} e_h(cy)e_q\Big(\frac{a\overline{u}}{v+xy+b\overline{u}}\Big).$$

Замечая, что $V-XY\geqslant 0.5V$, $V_2\leqslant V_1$, переходя к оценкам, будем иметь:

$$|S_c(U,V)|\leqslant \sum_{U<u\leqslant U_1}\sum_{0.5V<v\leqslant V_1}\sum_{x=1}^{X}\Big|\sum_{y=1}^{Y} e_h(cy)e_q\Big(\frac{a\overline{x}\overline{u}}{y+\overline{x}(b\overline{u}+v)}\Big)\Big| = \\ = \sum_{z=1}^{q}\sum_{t\in T}\mu(z;t)\Big|\sum_{y=1}^{Y} e_h(cy)e_q\Big(\frac{z}{y+t}\Big)\Big|,$$

где $\mu(z;t)$ — количество решений системы сравнений

$$\begin{cases} a\overline{x}\overline{u}\equiv z \pmod q,\\ \overline{x}(b\overline{u}+v)\equiv t \pmod q\end{cases}$$

с неизвестными u,v,x, удовлетворяющими условиям $1\leqslant x\leqslant X$, $U<u\leqslant U_1$, $0.5V<v\leqslant V_1$. Здесь через T обозначено множество значений, которые принимает по модулю q величина $\overline{x}(b\overline{u}+v)$ в случае, когда переменные u,v,x независимо друг от друга пробегают указанные промежутки (очевидно, $|T|\leqslant 2XUV$).

Зададимся целым числом $k\geqslant 14$, зависящим лишь от ε (точное значение k будет выбрано ниже). Дважды применяя к сумме $S_c(U,V)$ неравенство Гёльдера, получим:

$$|S_c(U,V)|\leqslant \Sigma_1^{2k-2}\Sigma_2\Sigma_3,$$

где

$$\Sigma_1 = \sum_{z=1}^{q}\sum_{t\in T}\mu(z;t),\quad \Sigma_2 = \sum_{z=1}^{q}\sum_{t\in T}\mu^2(z;t),\quad \Sigma_3 = \sum_{z=1}^{q}\sum_{t\in T}\Big|\sum_{y=1}^{Y} e_h(cy)e_q\Big(\frac{z}{y+t}\Big)\Big|^{2k}.$$

Поскольку Σ_1 совпадает с числом всех возможных троек u,v,x, то $|\Sigma_1|\leqslant|T|\leqslant 2XUV$. Далее, Σ_2 совпадает с числом решений системы сравнений

$$\begin{cases} a\overline{x}_1\overline{u}_1\equiv a\overline{x}_2\overline{u}_2 \pmod q,\\ \overline{x}_1(b\overline{u}_1+v_2)\equiv \overline{x}_2(b\overline{u}_2+v_1) \pmod q,\\ 1\leqslant x_1,x_2\leqslant X,\ U<u_1,u_2\leqslant U_1,\ 0.5V<v_1,v_2\leqslant V_1,\end{cases}$$

или, что то же, системы

$$\begin{cases} x_1u_1\equiv x_2u_2 \pmod q,\\ x_1v_1\equiv x_2v_2 \pmod q\end{cases}$$

с теми же ограничениями на переменные. В силу леммы, $\Sigma_2\leqslant 12XUV\ln q$.

Далее,

$$\Sigma_3 = \sum_{z=1}^{q}\sum_{t\in T}\sum_{\mathbf{y}} e_h(c(y_1+\ldots+y_k-y_{k+1}-\ldots-y_{2k}))\times \\ \times e_q\Big(z\Big(\frac{1}{t+y_1}+\ldots+\frac{1}{t+y_k}-\frac{1}{t+y_{k+1}}-\ldots-\frac{1}{t+y_{2k}}\Big)\Big)\leqslant q\sum_{\mathbf{y}} N_q(\mathbf{y}),$$

где $\mathbf{y} = (y_1, \dots, y_{2k})$ пробегает все целочисленные наборы с условием $1 \leqslant y_1, \dots, y_{2k} \leqslant Y$, а $N_q(\mathbf{y})$ обозначает количество решений сравнения

$$\frac{1}{t+y_1} + \dots + \frac{1}{t+y_k} \equiv \frac{1}{t+y_{k+1}} + \dots + \frac{1}{t+y_{2k}} \pmod q$$

в числах $t \in T$. Согласно лемме 1 из [43],

$$\Sigma_3 \leqslant q(k!Y^k|T| + 2kY^{2k}) < 2qk^k(Y^kXUV + Y^{2k}) = 2(kY^2)^kXUV\left(\frac{q}{Y^k} + \frac{q}{XUV}\right).$$

Возвращаясь к оценке $S_c(U,V)$, будем иметь:

$$|S_c(U,V)|^{2k} \leqslant 6(\ln q)(2XUV)^{2k}(kY^2)^k\left(\frac{q}{Y^k} + \frac{q}{XUV}\right),$$

откуда

$$|S_c(U,V)| \leqslant 2\sqrt{k}(6\ln q)^{1/(2k)}XYUV\left(\frac{q}{Y^k} + \frac{q}{XUV}\right)^{1/(2k)}.$$

Положим теперь $Y = \left[q^{2/k}\right] + 1$, так что $Y \leqslant q^{1/7} + 1 < U < V$. Тогда $qY^{-k} \leqslant q^{-1}$. Далее, пусть $X = \left[0.5VY^{-1}\right]$, тогда

$$2XY \leqslant V, \quad X \geqslant 0.5VY^{-1} - 1 \geqslant 0,5V(q^{2/k}+1)^{-1} \geqslant 0.25Vq^{-2/k} > 0.25q^{1/6-1/7} > 1$$

и, кроме того,

$$\frac{q}{XUV} \leqslant \frac{3qY}{UV^2}.$$

Поскольку $UV \geqslant Nq^{-\delta}$, $V \geqslant \sqrt{UV} \geqslant \sqrt{N}q^{-\delta/2}$, то

$$\frac{q}{XUV} \leqslant \frac{3qY}{UV^2} \leqslant \frac{3q^{1+1.5\delta}Y}{N^{3/2}} \leqslant \frac{4q^{1+1.5\delta+2/k}}{q^{1+1.5\varepsilon}} \leqslant 4q^{-0.75\varepsilon+2/k}.$$

Беря $k = \left[4\varepsilon^{-1}\right] + 1$, получим: $-0.75\varepsilon + 2/k \leqslant -0.25\varepsilon$, так что

$$\begin{aligned}
&\frac{q}{Y^k} + \frac{q}{XUV} \leqslant q^{-1} + 4q^{-0.25\varepsilon} < 5q^{-0.25\varepsilon},\\
&|S_c(U,V)| \leqslant \frac{5}{\sqrt{\varepsilon}}(30\ln q)^{1/(2k)}XYUVq^{-\varepsilon/(8k)} < XYUVq^{-\varepsilon^2/33},\\
&|S(U,V)| < UVq^{-\varepsilon^2/33}(\ln q + 1) < Nq^{-\varepsilon^2/33}(\ln q + 1).
\end{aligned}$$

Суммарный вклад в S_1 от всех таких пар U, V не превосходит по порядку

$$Nq^{-\varepsilon^2/33}(\ln q)^3.$$

Окончательно находим:

$$|S_1| \ll Nq^{-\varepsilon^2/33}(\ln q)^3 + Nq^{-\varepsilon/2}(\ln q)^2 < Nq^{-\varepsilon^2/35}.$$

Рассмотрим теперь сумму S_2. Замечая, что

$$r(n) = 4\sum_{u|n}\chi_4(u), \quad \text{где} \quad \chi_4(u) = \begin{cases} 1, & u \equiv 1 \pmod 4,\\ -1, & u \equiv 3 \pmod 4,\\ 0, & u \equiv 0 \pmod 2 \end{cases}$$

— неглавный характер по модулю 4, находим:

$$S_2 = 4\sum_{1\leqslant uv\leqslant N}\chi(u)e_q\Bigl(\frac{a}{uv+b}\Bigr) = 4\sum_{U,V} S(U,V),$$

где

$$S(U,V) = \sum_{U<u\leqslant U_1}\ \sum_{V<v\leqslant V_1}\chi(u)e_q\Bigl(\frac{a}{uv+b}\Bigr)$$

(все обозначения сохраняют тот же смысл, что и выше). Достаточно оценить сумму $S(U,V)$ при условии $Nq^{-\delta} < UV \leqslant N$, $\min(U,V) > q^{1/6}$. Если $U \leqslant V$, то искомая оценка получается дословным повторением приведённых выше рассуждений. Пусть $q^{1/6} < V < U$; имеем тогда: $S(U,V) = S^{(1)}(U,V) - S^{(3)}(U,V)$, где

$$S^{(j)}(U,V) = \sum_{V<v\leqslant V_1}\ \sum_{\substack{U<u\leqslant U_1\\ u\equiv j\ (\mathrm{mod}\,4)}} e_q\Bigl(\frac{a}{uv+b}\Bigr).$$

Полагая $u = 4w + j$, будем иметь:

$$S^{(j)}(U,V) = \sum_{V<v\leqslant V_1}\ \sum_{W<w\leqslant W_2} e_q\Bigl(\frac{a\overline{v}}{4w+j+b\overline{v}}\Bigr) = \sum_{V<v\leqslant V_1}\ \sum_{W<w\leqslant W_2} e_q\Bigl(\frac{\overline{4}a\overline{v}}{w+\overline{4}(j+b\overline{v})}\Bigr),$$

где $W = (U-j)/4$, $W_1 = (U_1-j)/4$, $W_2 = \min(W_1, Nv^{-1})$. Задавшись целыми X и Y с условиями $2XV < q$, $2XY < W$, $X, Y \geqslant 1$ и преобразуя сумму по w с помощью замены $w \mapsto w + xy$, где $1 \leqslant x \leqslant X$, $1 \leqslant y \leqslant Y$, получим:

$$|S^{(j)}(U,V)| \leqslant \sum_{|c|\leqslant h/2}\frac{|S_c^{(j)}(W,V)|}{|c|+1},$$

$$S^{(j)}(U,V) = \sum_{V<v\leqslant V_1}\ \sum_{W-XY<w\leqslant W_2-1}\ \sum_{x=1}^{X} f(c;v,w,x)\sum_{y=1}^{Y} e_h(cy)e_q\Bigl(\frac{\overline{4}a\overline{v}}{w+xy+\overline{4}(j+b\overline{v})}\Bigr),$$

где $h = 2[W+1]+1$, и $|f(c;v,w,x)| \leqslant 1$ для всех рассматриваемых c, v, w и x. Переходя к оценкам, будем иметь:

$$|S^{(j)}(U,V)| \leqslant \sum_{V<v\leqslant V_1}\ \sum_{0.5W<w\leqslant W_1}\ \sum_{x=1}^{X}\Bigl|\sum_{y=1}^{Y} e_h(cy)e_q\Bigl(\frac{\overline{4}a\overline{v}\overline{x}}{y+\overline{x}(w+\overline{4}(j+b\overline{v}))}\Bigr)\Bigr| =$$

$$= \sum_{z=1}^{q}\sum_{t\in T}\mu(z;t)\Bigl|\sum_{y=1}^{Y} e_h(cy)e_q\Bigl(\frac{z}{y+t}\Bigr)\Bigr|,$$

где $\mu(z;t)$ — число решений системы

$$\begin{cases}\overline{4}a\overline{v}\overline{x} \equiv z \pmod q,\\ \overline{x}(w+\overline{4}(j+b\overline{v})) \equiv t \pmod q,\\ 1\leqslant x\leqslant X,\ 0.5W < w \leqslant W_1,\ V < v \leqslant V_1,\end{cases}$$

а T — множество значений, которые принимает по модулю q величина $\overline{x}(w+\overline{4}(j+b\overline{v}))$ в случае, когда переменные v, w и x независимо друг от друга пробегают указанные промежутки

(очевидно, $|T| \leqslant XUV$). Задавшись целым $k \geqslant 14$ и применяя неравенство Гёльдера, получим: $|S^{(j)}(U,V)|^{2k} \leqslant \Sigma_1^{2k-2}\Sigma_2\Sigma_3$, где Σ_1, Σ_2 и Σ_3 определяются как и выше.

Сумма Σ_2 совпадает с числом решений системы

$$\begin{cases} \overline{4}a\overline{v}_1\overline{x}_1 \equiv \overline{4}a\overline{v_2x_2}x_2 \pmod q, \\ \overline{x}_1(w_2 + \overline{4}(j + b\overline{v}_1)) \equiv \overline{x}_2(w_1 + \overline{4}(j + b\overline{v}_2)) \pmod q \end{cases}$$

с неизвестными $1 \leqslant x_1, x_2 \leqslant X$, $0.5W < w_1, w_2 \leqslant W_1$, $V < v_1, v_2 \leqslant V_1$, или, что то же, системы

$$\begin{cases} x_1v_1 \equiv x_2v_2 \pmod q, \\ x_1(w_1 + \overline{4}j) \equiv x_2(w_2 + \overline{4}j) \pmod q \end{cases}$$

с теми же ограничениями. Положив $u_r = 4w_r + j$, придём к системе рассмотренного выше вида, число решений которой оценивается с помощью леммы. Так получим:

$$\Sigma_2 < 3XUV \ln q.$$

Дальнейшие рассуждения совпадают с приведёнными выше. Теорема доказана. □

4. Следствия основной теоремы

Полученные выше оценки тригонометрических сумм позволяют сделать ряд заключений о поведении дробных долей функций вида

$$\left\{\frac{a}{uv+b}\right\}, \quad \left\{\frac{a}{u^2+v^2+b}\right\}$$

в случаях, когда целочисленные переменные u, v меняются в гиперболической ($uv \leqslant N$, $u, v \geqslant 1$) или круговой ($u^2 + v^2 \leqslant N$) областях. В частности, имеют место следующие утверждения.

Теорема 2. *В условиях теоремы 1 справедливы следующие асимптотические формулы:*

$$\sum_{n\leqslant N}\tau(n)\left\{\frac{a(n+c)^*}{q}\right\} = \sum_{1\leqslant uv\leqslant N}\left\{\frac{a(uv+c)^*}{q}\right\} = \frac{1}{2}N(\ln N + 2\gamma - 1) + O\big(Nq^{-(\varepsilon/6)^2}\big),$$

$$\sum_{n\leqslant N} r(n)\left\{\frac{a(n+c)^*}{q}\right\} = \sum_{1\leqslant u^2+v^2\leqslant N}\left\{\frac{a(u^2+v^2+c)^*}{q}\right\} = \pi N + O\big(Nq^{-(\varepsilon/6)^2}\big),$$

где γ — постоянная Эйлера.

Теорема 3. *Пусть $0 \leqslant \alpha < \beta < 1$. Тогда, в условиях теоремы 1, для величин $K_j = K_j(\alpha, \beta; q, N; a, c)$, $j = 1, 2$, обозначающих, соответственно, количества решений неравенств*

$$\alpha < \left\{\frac{a(uv+c)^*}{q}\right\} \leqslant \beta, \quad \alpha < \left\{\frac{a(u^2+v^2+c)^*}{q}\right\} \leqslant \beta$$

в целых числах u и v с условиями $uv \leqslant N$, $u, v \geqslant 1$ и $u^2 + v^2 \leqslant N$, справедливы следующие формулы:

$$K_1 = (\beta - \alpha)N(\ln N + 2\gamma - 1) + O\big(Nq^{-(\varepsilon/6)^2}\big), \quad K_2 = (\beta - \alpha)\pi N + O\big(Nq^{-(\varepsilon/6)^2}\big).$$

Теорема 4. *Пусть ξ – произвольное вещественное число, $0 \leqslant \xi < 1$. Тогда, в условиях теоремы 1, имеют место следующие неравенства:*

$$\min_{\substack{1\leqslant uv\leqslant N\\ u,v\geqslant 1}}\left\|\xi - \frac{a(uv+c)^*}{q}\right\| \ll q^{-(\varepsilon/6)^2}, \quad \min_{1\leqslant u^2+v^2\leqslant N}\left\|\xi - \frac{a(u^2+v^2+c)^*}{q}\right\| \ll q^{-(\varepsilon/6)^2},$$

где $\|z\| = \min(\{z\}, 1-\{z\})$ – расстояние от z до ближайшего целого числа.

Доказательство.

Доказательства теорем 2 и 3 получаются применением стандартной техники (см., например, [49, гл. I]); теорема 4 есть прямое следствие формул теоремы 3.

5. Заключительные замечания

Приведённые выше рассуждения практически без изменений переносятся на случай сумм

$$\sum_{1\leqslant n\leqslant N}\tau(n)e_q\left(\frac{a}{(n+b)^r}\right), \quad \sum_{1\leqslant n\leqslant N} r(n)\, e_q\left(\frac{a}{(n+b)^r}\right),$$

где $r \geqslant 2$ — произвольное фиксированное число. Кроме того, оценки, подобные оценкам теоремы 1, могут быть получены и для сумм вида

$$\sum_{1\leqslant n\leqslant N}\tau(n)e_q\left(\frac{a}{n+b}+cn\right), \quad \sum_{1\leqslant n\leqslant N} r(n)\, e_q\left(\frac{a}{n+b}+cn\right),$$

где $(c,q)=1$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Heath-Brown D. R. Arithmetic applications of Kloosterman sums // *Nieuw Archief voor Wiskunde. Serie 5*, **4** (2000), 380–384.
2. Sarnak P. Kloosterman, qudratic forms and modular forms // *Nieuw Archief voor Wiskunde. Serie 5*, **4** (2000), 385–389.
3. Устинов А. В. Приложения сумм Клоостермана к арифметике и геометрии. Алгоритм Евклида, цепные дроби, решетки и числа Фробениуса. LAMBERT Academic Publishing, 2011.
4. Иванец Х., Ковальский Э. Аналитическая теория чисел. М., Изд-во МЦНМО, 2014.
5. Hajela D., Pollington A., Smith B. On Kloosterman sums with oscillating coefficients // *Canad. Math. Bull.*, **31**:1 (1988), 32–36.
6. Wang G., Zheng Z. Kloosterman sums with oscillating coefficients // *Chinese Ann. Math.*, **19** (1998), 237–242 (кит.); англ. пер.: *Chinese J. Contemp. Math.* **19** (1998), 185–191.
7. Deng P. On Kloosterman sums with oscillating coefficients // *Canad. Math. Bull.* **42**:3 (1999), 285–290.
8. Gong K., Jia C. Kloosterman sums with multiplicative coefficients //
   `arXiv:1401.4556v4 [math.NT]`.

9. Королёв М. А. Короткие суммы Клоостермана с весами // *Матем. заметки*, **88**:3 (2010), 415–427.

10. Королёв М. А. Суммы Клоостермана с мультипликативными коэффициентами // *Изв. РАН. Сер. матем.*, **82**:4 (2018) (в печати).

11. van der Corput I. G. Verschärfung der Abshchätzungen beim Teilerproblem // *Math. Ann.*, **87** (1922), ss. 39-65.

12. van der Corput I. G. Neue zahlentheoretische Abshchätzungen // *Math. Ann.*, **89** (1923), ss. 215–254.

13. van der Corput I. G. Neue zahlentheoretische Abshchätzungen // *Math. Zeitschr.*, **29** (1928), ss. 397–426.

14. Vinogradow I. On Weyl's sums // *Матем. сб.*, **42**:5 (1935), 521–530.

15. Vinogradow I. On asymptotic formula in Warings problem // *Матем. сб.*, **1(43)**:2 (1936), 169–174.

16. Виноградов И. М. Новый метод в аналитической теории чисел // *Тр. Матем. ин-та им. В.А. Стеклова*, **10**, Изд-во АН СССР, М.–Л., 1937, 5–122.

17. Виноградов И. М. Некоторые общие леммы и их применение к оценке тригонометрических сумм // *Матем. сб.*, **3(45)**:3 (1938), 435–471.

18. Виноградов И. М. Две теоремы из аналитической теории чисел // *Труды Тбилисск. матем. ин-та*, **5** (1938), 153–180.

19. Виноградов И. М. Улучшение оценок тригонометрических сумм // *Изв. АН СССР. Сер. матем.*, **6**:1-2 (1942), 33–40.

20. Виноградов И. М. Метод тригонометрических сумм в теории чисел // *Тр. МИАН СССР*, **23**, Изд-во АН СССР, М.–Л., 1947, 3–109.

21. Виноградов И. М. Общие теоремы о верхней границе модуля тригонометрической суммы // *Изв. АН СССР. Сер. матем.*, **15**:2 (1951), 109–130.

22. Виноградов И. М. Новая оценка функции $\zeta(1+it)$ // *Изв. АН СССР. Сер. матем.*, **22**:2 (1958), 161–164.

23. Виноградов И.М. Оценка одной суммы, распространенной на простые числа арифметической прогрессии // *Изв. АН СССР. Сер. матем.*, **30**:3 (1966), 481–496.

24. Карацуба А. А. Тригонометрические суммы специального вида и их приложения // *Изв. АН СССР. Сер. матем.*, **28**:1 (1964), 237–248.

25. Карацуба А. А. О системах сравнений // *Изв. АН СССР. Сер. матем.*, **29**:4 (1965), 935–944.

26. Карацуба А. А. Суммы характеров и первообразные корни в конечных полях // *Докл. АН СССР*, **180** (1968), 1287–1289.

27. Карацуба А. А. Об оценках сумм характеров // *Изв. АН СССР. Сер. матем.*, **34**:1 (1970), 20–30.

28. Карацуба А. А. Суммы характеров с простыми числами // *Докл. АН СССР*, **190** (1970), 517–518.

29. Карацуба А. А. Оценки тригонометрических сумм методом И.М. Виноградова и их применения // *Тр. МИАН СССР*, **112**, 1971, 241–255.

30. Карацуба А. А. Суммы характеров по последовательности сдвинутых простых чисел и их применения // *Матем. заметки*, **17**:1 (1975), 155–159.

31. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Верхняя граница модуля кратной тригонометрической суммы // *Тр. МИАН СССР*, **143**, 1977, 3–31.

32. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Точная оценка числа решений одной системы диофантовых уравнений // *Изв. АН СССР. Сер. матем.*, **42**:6 (1978), 1187–1226.

33. Карацуба А. А. Суммы символов Лежандра от многочленов второй степени с простыми числами // *Изв. АН СССР. Сер. матем.*, **42**:2 (1978), 315–324.

34. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Кратные тригонометрические суммы и их приложения // *Изв. АН СССР. Сер. матем.*, **44**:4 (1980), 3–125.

35. Архипов Г. И., Карацуба А. А., Чубариков В. Н. Кратные тригонометрические суммы // *Тр. МИАН СССР*, **151**, 1980, 3–128.

36. Burgess D. A. The distribution of quardratic residues and non-residues // *Mathematika*, **4** (1957), 106–112.

37. Burgess D. A. On character sums and L-series. II // Proc. London Math. Soc., **(3)13**:1 (1963), 524–536.

38. Fouvry E., Michel P. Sur certaines sommes d'exponentielles sur les nombres premiers // *Ann. scient. Éc. Norm. Sup.*, 31:1 (1998), 93–130.

39. Bourgain J. More on the sum-product phenomenon in prime fields and its applications // *Int. J. Number Theory*, **1** (2005), 1–32.

40. Weil A. On some exponential sums, *Proc. Nat. Acad. Sci. USA*, **34** (1948), 204–207.

41. Baker R. C. Kloosterman sums with prime variable // *Acta Arith.*, **152**:4 (2012), 351–372.

42. Бургейн Ж., Гараев М. З. Сумма множеств, образованных обратными элементами в полях простого порядка, и полилинейные суммы Клоостермана // *Изв. РАН. Сер. матем.*, **78**:4 (2014), 19–72.

43. Королёв М. А. О нелинейной сумме Клоостермана // *Чебышевский сб.*, **17**:1 (2016), 140–147.

44. Королёв М. А. Обобщенная сумма Клоостермана с простыми числами // *Тр. МИАН*, **296**, МАИК, М., 2017, 163–180.

45. Королёв М. А. Элементарное доказательство оценки суммы Клоостермана с простыми числами // *Матем. заметки*, **103**:5 (2018), 720–729.

46. Карацуба А. А. Суммы характеров с весами // *Изв. РАН. Сер. матем.*, **64**:2 (2000), 29–42.

47. Карацуба А. А. Об одной арифметической сумме // *ДАН СССР*, **199**:4 (1971), 770–772.

48. Ayyad A., Cochrane N., Zheng Z. The congruence $x_1x_2 \equiv x_3x_4 (\mathrm{mod}\, p)$, the equation $x_1x_2 = x_3x_4$, and mean value of character sums // *J. Number Theory.* **59** (1996), pp. 398–413.

49. Карацуба А. А. Основы аналитической теории чисел. 2-е изд. М., Наука, 1983.

REFERENCES

1. Heath-Brown D. R. 2000, "Arithmetic applications of Kloosterman sums", *Nieuw Archief voor Wiskunde. Serie 5*, vol. 4, pp. 380–384.

2. Sarnak P. 2000, "Kloosterman, qudratic forms and modular forms", *Nieuw Archief voor Wiskunde. Serie 5*, vol. 4, pp. 385–389.

3. Ustinov A. V. 2011, Applications of Kloosterman Sums in Arithmetic and Geometry, LAMBERT Academic Publishing.

4. Iwaniec H., Kowalski E. 2004, Analytic Number Theory. Colloquium Publications, vol. 53. Amer. Math. Soc. Providence, Rhode Island.

5. Hajela D., Pollington A., Smith B. 1988, "On Kloosterman sums with oscillating coefficients", *Canad. Math. Bull.*, vol. 31, no. 1, pp. 32–36.

6. Wang G., Zheng Z. 1998, "Kloosterman sums with oscillating coefficients", *Chinese Ann. Math.*, vol. 19, pp. 237–242 (chinese); engl. transl.: *Chinese J. Contemp. Math.*, vol. 19, pp. 185–191.

7. Deng P. 1999, "On Kloosterman sums with oscillating coefficients", *Canad. Math. Bull.*, vol. 42, no. 3, pp. 285–290.

8. Gong K., Jia C. 2014, "Kloosterman sums with multiplicative coefficients",
`arXiv:1401.4556v4 [math.NT]`.

9. Korolev M. A. 2010, "Short Kloosterman Sums with Weights", *Math. Notes*, vol. 88, no. 3, pp. 374–385.

10. Korolev M. A. 2018, "On Kloosterman sums with multiplicative coefficients", *Izv. Math.* (to appear).

11. van der Corput I. G. 1922, "Verschärfung der Abshchätzungen beim Teilerproblem", *Math. Ann.*, vol. 87, pp. 39-65.

12. van der Corput I. G. 1923, "Neue zahlentheoretische Abshchätzungen", *Math. Ann.*, vol. 89, pp. 215–254.

13. van der Corput I. G. 1928, "Neue zahlentheoretische Abshchätzungen", *Math. Zeitschr.*, vol. 29, pp. 397–426.

14. Vinogradow I. 1935, "On Weyl's sums", *Recueil Mathém. Nouv. sér.*, vol. 42, no. 5, pp. 521–530.

15. Vinogradow I. 1936, "On asymptotic formula in Warings problem", *Recueil Mathém. Nouv. sér.*, vol. 1(43), no. 2, pp. 169–174.

16. Vinogradov I. M. 1937, "A new method in analytic number theory", *Travaux Inst. Math. Stekloff*, vol. 10, Acad. Sci. USSR, Moscow–Leningrad.

17. Vinogradow I. 1938, “Some general lemmas and their application to the estimation of trigonometrical sums”, *Recueil Mathém. Nouv. sér.*, vol. 3(45), no. 3, pp. 435–471.

18. Vinogradoff I. 1938, “Zwei Sätze aus der Analytischen Zahlentheorie”, *Acad. Sci. URSS, Fil. Géorgienne, Trav. Inst. math. Tbilissi*, vol. 5, pp. 153–180.

19. Vinogradow I. 1942, “An improvement of the estimation of trigonometrical sums”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 6, no. 1-2, pp. 33–40.

20. Vinogradov I. M. 1947, “The method of trigonometrical sums in the theory of numbers”, *Trudy Mat. Inst. Steklov.*, vol. 23, Acad. Sci. USSR, Moscow–Leningrad.

21. Vinogradov I. M. 1951, “General theorems on the upper bound of the modulus of a trigonometric sum”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 15, no. 2, pp. 109–130.

22. Vinogradov I. M. 1958, “A new estimate of the function $\zeta(1+it)$”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 22, no. 2, pp. 161–164.

23. Vinogradov I. M. 1966, “An estimate for a certain sum extended over the primes of an arithmetic progression”, *Izv. Akad. Nauk SSSR. Ser. Mat.*, vol. 30, pp. 481–496.

24. Karatsuba A. A. 1964, “Trigonometric sums of a special type and their applications”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 28, no. 1, pp. 237–248.

25. Karatsuba A. A. 1965, “On systems of congruences”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 29, no. 4, pp. 935–944.

26. Karatsuba A. A. 1968, “Character sums and primitive roots in finite fields”, *Sov. Math., Dokl.* vol. 9, pp. 755–757.

27. Karatsuba A. A. 1970, “Estimates of character sums”, *Math. USSR-Izv.*, vol. 4, no. 1, pp. 19–29.

28. Karatsuba A. A. 1970, “On sums of characters with primes”, *Sov. Math., Dokl.* vol. 11, pp. 135–137.

29. Karatsuba A. A. 1971, “Estimates for trigonometric sams by Vinogradov’s method and some applications”, *Tr. Mat. Inst. Steklova*, vol. 112, pp. 241–255.

30. Karatsuba A. A. 1975, “Sums of characters in sequences of shifted prime numbers, with applications”, *Math. Notes*, vol. 17, no. 1, pp. 91–93.

31. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N. 1980, “An upper bound of the modulus of a multiple trigonometric sum”, *Proc. Steklov Inst. Math.*, vol. 143, pp. 1–31.

32. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N. 1979, “A sharp estimate for the number of solutions of a system of Diophantine equations”, *Math. USSR-Izv.*, vol. 13, no. 3, pp. 461–497.

33. Karatsuba A. A. 1978, “Sums of Legendre symbols of polynomials of second degree over prime numbers”, *Math. USSR-Izv.*, vol. 12, no.2, pp. 299–308.

34. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N. 1981, “Multiple trigonometric sums and their applications”, *Math. USSR-Izv.*, vol. 17, no. 1, pp. 1–54.

35. Arkhipov G. I., Karatsuba A. A., Chubarikov V. N. 1982, “Multiple trigonometric sums”, *Proc. Steklov Inst. Math.*, vol. 151, no. 2, pp. 1–126.

36. Burgess D. A. 1957, "The distribution of quardratic residues and non-residues", *Mathematika*, vol. 4, pp. 106–112.

37. Burgess D. A. 1963, "On character sums and L-series. II", *Proc. London Math. Soc.*, vol. (3)13, no. 1, pp. 524–536.

38. Fouvry E., Michel P. 1998, "Sur certaines sommes d'exponentielles sur les nombres premiers", *Ann. scient. Éc. Norm. Sup.*, vol. 31, no. 1, pp. 93–130.

39. Bourgain J. 2005, "More on the sum-product phenomenon in prime fields and its applications", *Int. J. Number Theory*, vol. 1, pp. 1–32.

40. Weil A. 1948, "On some exponential sums", *Proc. Nat. Acad. Sci. USA*, vol. 34, pp. 204–207.

41. Baker R. C. 2012, "Kloosterman sums with prime variable", *Acta Arith.*, vol. 152, no. 4, pp. 351–372.

42. Bourgain J., Garaev M. Z. 2014, "Sumsets of reciprocals in prime fields and multilinear Kloosterman sums", *Izv. RAN. Ser. Mat.*, vol. 78, no. 4, pp. 656–707.

43. Korolev M. A. 2016, "On non-linear Kloosterman sum", *Chebyshevskii Sb.*, vol. 17, no. 1, pp. 140–147.

44. Korolev M. A. 2017, "Generalized Kloosterman sum with primes", *Proc. Steklov Inst. Math.*, vol. 296, pp. 154–171.

45. Korolev M. A. 2018, "Elementary Proof of an Estimate for Kloosterman Sums with Primes", *Mat. Zametki*, vol. 103, no. 5, pp. 720–729.

46. Karatsuba A. A. 2000, "Weighted character sums", *Izv. Math.*, vol. 64, no. 2, pp. 249–263.

47. Karatsuba A. A. 1971, "A certain arithmetic sum", *Soviet Math. Dokl.*, vol. 12, pp. 1172–1174.

48. Ayyad A., Cochrane N., Zheng Z. 1996, "The congruence $x_1x_2 \equiv x_3x_4 (\mathrm{mod}\, p)$, the equation $x_1x_2 = x_3x_4$, and mean value of character sums", *J. Number Theory.* vol. 59, pp. 398–413.

49. Karatsuba A. A. 1993, Basic Analytic Number Theory, Springer-Verlag Berlin Heidelberg.

Получено 08.06.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-202-209

К одной задаче Ю. В. Линника

Кузнецов Валентин Николаевич — доктор технических наук, профессор, профессор кафедры Прикладной математики и системного анализа СГТУ им. Гагарина Ю. А., г. Саратов
e-mail: kuznetsovvalnik@gmail.com
Матвеева Ольга Андреевна — кандидат физико-математических наук
e-mail: olga.matveeva.0@gmail.com

Аннотация

В конце 40-х годов прошлого века Ю. В. Линник поставил задачу относительно аналитического продолжения целым образом на комплексную плоскость рядов Дирихле, коэффициенты которых определяются конечнозначными числовыми характеристиками, не равными нулю на почти всех простых числах и имеющих ограниченные сумматорные функции. Такие характеры получили название неглавных обобщенных характеров. Решением задачи Ю. В. Линника занимались многие математики. В частности, этой задачей занимался Н. Г. Чудаков, который который видел ее решение в доказательстве высказанного им предположения о том, что неглавный обобщенный характер является характером Дирихле.

Проблема, заключающаяся в решении задачи Ю. В. Линника и гипотезы Н. Г. Чудакова, широко известна в теории чисел. Она носит название проблемы обобщенных характеров.

В данной работе приводится решение задачи Ю. В. Линника, основанное на результатах, полученных ранее авторами относительно аналитического продолжения рядов Дирихле с мультипликативными коэффициентами.

Таким образом, в данной работе приведено частичное решение проблемы обобщенных характеров, поставленной в 1950-м году Ю. В. Линником и Н. Г. Чудаковым.

Ключевые слова: аппроксимационные полиномы Дирихле, принцип симметрии Римана — Шварца, проблема обобщенных характеров.

Библиография: 15 названий.

Для цитирования:
В. Н. Кузнецов, О. А. Матвеева. К одной задаче Ю. В. Линника // Чебышевский сборник, 2018, т. 19, вып. 3, с. 202–209.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-202-209

On a problem of Yu. V. Linnik

Kuznetsov Valentin Nikolaevich — Doctor of technical sciences, professor, Department of Applied Mathematics and Systems Analysis, Saratov State Technical University, Saratov
e-mail: kuznetsovvalnik@gmail.com
Matveeva Olga Andreevna — Candidate of physico-mathematical sciences
e-mail: olga.matveeva.0@gmail.com

Abstract

In the late 40-s of the last century Yu. V. Linnik posed the problem of analytic continuation in an integral way to the complex plane of Dirichlet series whose coefficients are determined by finite-valued numerical characteristics that are not equal to zero on almost all primes and have bounded summation functions. Such characters are called non-principal generalized characters. Many mathematicians dealt with Linnik's problem. In particular, this task was handled by N. G. Chudakov, who saw the way to solving it in proving his suggestion that the non-principal generalized character is the Dirichlet character.

Linnik's problem and the hypothesis of N. G. Chudakov is widely known in number theory. It is called the problem of generalized characters.

In this paper we solve the problem of Yu. V. Linnik, based on the results obtained earlier by the authors concerning the analytic continuation of Dirichlet series with multiplicative coefficients.

Thus, in this paper a partial solution of the generalized character problem posed in the 1950-s Yu. V. Linnik and N. G. Chudakov.

Keywords: approximation Dirichlet polynomials, the Riemann-Schwarz symmetry principle, the problem of generalized characters

Bibliography: 15 titles.

For citation:
V. N. Kuznetsov, O. A. Matveeva. 2018, "On a problem of Yu. V. Linnik", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 202–209.

1. Введение

Знаменитый подход Римана в задаче аналитического продолжения дзета-функции, основанный на функциональном уравнении для тэта-функции, стал в начале 20-го века основополагающим при решении задач, связанных с аналитическим продолжением рядов Дирихле. Здесь, в первую очередь нужно отметить работы Гекке, Тейта ([1]) и многих других известных авторов, внесших весомый вклад в развитие идеи Римана. Но следует отметить значительное усложнение математического аппарата при решении соответствующих задач. Это побудила в конце 40-х годов прошлого века Ю. В. Ленника к поиску новых подходов в задаче аналитического продолжения рядов Дирихле. Им была поставлена задача аналитического продолжения рядов Дирихле вида

$$f(s)=\sum_{n=1}^{\infty}\frac{h(n)}{n^s},\quad s=\sigma+it, \tag{1}$$

где $h(n)$ — конечнозначный числовой характер, отличный от нуля почти для всех простых, имеющий ограниченную сумматорную функцию

$$S(x)=\sum_{n\le x}h(n)=O(1).$$

В дальнейшем (см. [2],[3]) такие характеры получили название неглавных обобщенных характеров.

Решением задачи Ю. В. Линника занимались многие известные математики. Долгие годы этой задачей занимался Н. Г. Чудаков. Он видел решение этой задачи в доказательстве высказанной им гипотезы о том, что неглавный обобщенный характер является характером Дирихле (см., например, [4],[5]).

В данной работе приведено решение задачи Ю. В. Линника, не связанное с решением гипотезы Н. Г. Чудакова. В основе решения задачи аналитического продолжения рядов Дирихле, коэффициенты которых определяются неглавными обобщенными характерами, лежит так

называемый аппроксимационный подход, разработанный О. А. Матвеевой в работах [6]–[9]. Суть этого подхода заключается в построении последовательности полиномов Дирихле, приближающих функцию, определенную рядом Дирихле, в правой полуплоскости комплексной плоскости и изучении тех свойств полиномов Дирихле, которые удается перенести на ряды Дирихле.

В последние годы авторы изучали применение аппроксимационного подхода к задаче аналитического продолжения рядов Дирихле (см. [10]–[13]).

Приведенное здесь решение задачи Ю. В. Линника является следствием этих исследований.

2. Аналитическое продолжение рядов Дирихле [1] целым образом на комплекную плоскость

В работах [10]–[13] было показано, что для рядов Дирихле (1) существует последовательность полиномов Дирихле $Q_n(s)$, удовлетворяющих условиям:

(i). В любой полосе: $0 < \sigma_0 \le \sigma < \infty, |t| \le T$, последовательность полиномов $Q_n(s)$ равномерно сходится к функции $f(s)$, определенной рядом Дирихле (1);

(ii). Пусть $\varepsilon_n \to 0$. Тогда для любого ε_{n_0} существует n_1, что при $n \ge n_1$ в полосе: $0 < \sigma_0 \le \sigma < \infty, |t| \le T$, выполняется неравенство

$$|f(s) - Q_n(s)| < C \cdot \varepsilon_n,$$

где константа C не зависит от n и ε_{n_0};

(iii). Для любой полосы: $0 < \sigma_0 \le \sigma < \infty$, $|t| \le T$, существует n_0, что при $n \ge n_0$ нормы полиномов $Q_n(s)$ ограничены константой, зависящей только от величины T.

В работе [13] было показано, что свойства таких аппроксимационных полиномов Дирихле позволяют воспользоваться основными идеями принципа симметрии Римана — Шварца (см. [14], [15]) в задаче аналитического продолжения рядов Дирихле (1). В этой работе доказано следующее утверждение

Теорема 1. *Ряд Дирихле (1) тогда и только тогда аналитически продолжен как целая функция на комплексную плоскость, когда функция $f(s)$, определенная рядом (1), является регулярной во всех точках мнимой оси.*

В данной работе мы покажем, что функция $f(s)$ является регулярной на мнимой оси, тем самым имеет место

Теорема 2. *Ряд Дирихле (1) аналитически продолжен целым образом на комплексную плоскость.*

Доказательству теоремы 2 предпошлём доказательство ряда лемм.

Рассмотрим аппроксимационный полином

$$Q_n(s) = \sum_{k=1}^{n} \frac{a_k}{k^s}. \tag{2}$$

Лемма 1. *Для производной m-го порядка аппроксимационного полинома $Q_n(s)$ в полосе $0 < \sigma_0 \le \sigma < \infty$, $|t| \le T$ имеет место оценка*

$$\left|Q_n^{(m)}(s)\right| \le C \ln^m n,$$

где константа C зависит только от величины T.

Доказательство. Применив к производной полинома Дирихле (2) формулу суммирования Абеля получим

$$\left|Q_n'(s)\right| \leq \ln(n)\,|Q_n(s)|$$

Учитывая, что в полосе: $0 < \sigma < \infty, |t| \leq T$

$$|Q_n(s)| < C,$$

где константа зависит только от T, и повторив рассуждение m раз получим утверждение леммы 1. □

Лемма 2. *Пусть $Q_{n_k}(s)$ — последовательность аппроксимационных полиномов, где $n_k = k^n$ и где $k > 2$ — некоторое натуральное. Тогда в полосе: $0 < \sigma < \infty, |t| \leq T$ для любого m имеет место оценка вида*

$$\left|Q^{(m)}_{(n+1)_k}(s) - Q^{(m)}_{n_k}(s)\right| = O\left(\frac{(n+1)^m \ln^m k}{n^l \ln^l k}\right), \tag{3}$$

где l — любое натуральное, а константа в символе «O» зависит от T и l.

Доказательство. В работе [11] показано, что для аппрксимационных полиномов $Q_n(s)$ ряда Дирихле (1) в полосе: $0 < \sigma < \infty, |t| \leq T$, выполняется оценка

$$|f(s) - Q_{n_k}(s)| = O\left(\frac{1}{\ln^l k}\right),$$

где l — любое натуральное, а константа в символе «O» зависит от T и l.

Отсюда получаем

$$\left|Q_{(n+1)_k}(s) - Q_{n_k}(s)\right| = O\left(\frac{1}{n^l \ln^l k}\right), \tag{4}$$

где l — любое натуральное, а константа в символе «O» зависит от T и l.

В силу оценки (4) и леммы 1 получаем утверждение леммы 2. □

Лемма 3. *В полосе: $0 < \sigma < \infty, |t| \leq T$ для любого m имеет место оценка*

$$\left|f^{(m)}(s)\right| = O\left(\frac{1}{(l-m-1)n_0^{l-m} \ln^{l-m} k}\right),$$

где l – натуральное, большее чем m; n_0 – некоторое натуральное, которое может быть достаточно большим; константа в символе «O» зависит от T и l.

Доказательство. Рассмотрим разложение функции $f(s)$ в ряд

$$f(s) = Q_{(n_0)_k}(s) + \sum_{n \geqslant n_0}^{\infty} \left(Q_{(n+1)_k}(s) - Q_{n_k}(s)\right),$$

который в силу (4) абсолютно сходится при любом s из полосы : $0 < \sigma < \infty, |t| \leq T$.

В результате его почленного дифференцирования имеем

$$f^{(m)}(s) = Q^{(m)}_{(n_0)_k}(s) + \sum_{n \geqslant n_0}^{\infty} (Q^{(m)}_{(n+1)_k}(s) - Q^{(m)}_{n_k}(s),$$

где ряд сходится абсолютно при любом s и при любом m, что следует из леммы 2.

Отсюда в силу леммы 2 получаем оценку вида

$$\left|f^{(m)}(s)\right| = O\left(\sum_{n\geq n_0} \frac{n^m \ln^m k}{n^l \ln^l k}\right) \tag{5}$$

где l – любое натуральное, а константа в символе «O» зависит от T и l .

Положим в формуле (5) $l > m$. Тогда получим

$$\left|f^{(m)}(s)\right| = O\left(\sum_{n\geq n_0} \frac{1}{n^{l-m}\ln^{l-m} k}\right) = O\left(\frac{1}{n_0^{l-m}\ln^{l-m} k}\sum_{n\geq n_0}\frac{1}{(\frac{n}{n_0})^{l-m}}\right) =$$

$$= O\left(\frac{1}{n_0^{l-m}\ln^{l-m} k}\int_1^\infty \frac{1}{x^{l-m}}dx\right) = O\left(\frac{1}{n_0^{l-m}}\frac{1}{\ln^{l-m} k}\frac{1}{(l-m-1)}\right)$$

что и завершает доказательство леммы 3. □

Пусть C_l обозначает наименьшее число, входящее в символ «O» оценки леммы 3. Приведем оценку этой константы в зависимости от величины l.

Докажем следующее утверждение

Лемма 4. *Имеет место оценка*

$$C_l \leq \left|\left|g^{(l)}(x)\right|\right|_{C[0;1-\varepsilon]},$$

где $g(x)$ — функция, определенная степенным рядом, соответсвующим ряду Дирихле (1), *ε — некоторое положительное число, меньшее, чем 1.*

Доказательство. При выводе основной оценки леммы 3 мы воспользовались результатом доказательства леммы 5 и теоремы 2 работы [11]

$$\omega_k\left(\frac{1}{n}, g\right) \leq C\ln^{-k} n,$$

где $\omega_k\left(\frac{1}{n}, g\right)$ — модуль непрерывности k-го порядка функции $g(x)$ на отрезке $[0;1-\varepsilon]$, и где константа C не зависит от n и ε. Эта константа и определяет константу C_l в нашем случае. В силу известного неравенства для отрезка $[0;1-\varepsilon]$

$$\omega_k\left(\frac{1}{n}, g\right) \leq \left|\left|g^{(k)}(x)\right|\right|_{C[0;1-\varepsilon]} \cdot \frac{1}{n^k}.$$

Можно считать $C_k \leq \left|\left|g^{(k)}(x)\right|\right|_{C[0;1-\varepsilon]}$. Это завершает доказательство леммы 4. □

Как следствие леммы 4 получаем следующее утверждение.

Лемма 5. *Имеет место неравенство*

$$\overline{\lim}\sqrt[l]{\frac{C_l}{l!}} < \infty.$$

Доказательство. Пусть $0 < \varepsilon < 1$. Для любой точки $x_0 \in [0;1-\varepsilon]$ имеет место неравенство

$$\overline{\lim}\sqrt[l]{\frac{|g^{(l)}(x_0)|}{l!}} < \infty,$$

Что связано с положительностью радиуса сходимости ряда Тейлора функции $g(x)$ в точке x_0. Взяв в качестве x_0 предельную точку для точек x_m, в которых достигается $||g^{(m)}(x)||_{C[0;1-\varepsilon]}$,

то последнее неравенство, в силу леммы 4, доказывает утверждение леммы 5. Действительно, взяв в качестве x_0 предельную точку всех x_m, в которых достигается величина $||g^{(m)}(x)||_{C[0;1]}$, то получим наше неравенство. □

Доказательство. Доказательство теоремы 2

Рассмотрим формальный ряд Тейлора функции $f(s)$ в точке s_0

$$f(s) = f(s_0) + \sum_{m=1}^{\infty} \frac{f^{(m)}(s_0)}{m!}(s - s_0)^m, \tag{6}$$

где s_0 лежит на мнимой оси, и покажем что он имеет ненулевой радиус сходимости R.

Известно, что

$$\overline{\lim_m} \sqrt[m]{\frac{f^{(m)}(s_0)}{m!}} = \frac{1}{R}$$

Положим в лемме 3 $l = m + 2$. Тогда в силу (6) и леммы 5 получаем

$$\frac{1}{R} = \overline{\lim} \sqrt[m]{\frac{C_m}{m!}} < \infty.$$

Таким образом, функция $f(s)$ регулярна во всех точках мнимой оси. Отсюда в силу теоремы 1 получаем утверждение теоремы 2. □

3. Заключение

Таким образом, решение задачи Ю. В. Линника, приведенное в данной работе, основывается на результатах, полученных ранее авторами относительно аналитического продолжения рядов Дирихле с мультипликативными коэффициентами.

В данной работе приведено частичное решение проблемы обобщенных характеров, поставленной в 1950-м году Ю. В. Линником и Н. Г. Чудаковым. В следующей работе будут продолжены исследования на эту тему.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Lang S. D. Algebraic Number Theory – New. Jork, 1970, P. 384.
2. Чудаков Н. Г., Линник Ю. В. Об одном классе вполне мультипликативных функций // ДАН СССР, 1950. Т. 74, №2. С. 133–136.
3. Чудаков Н. Г., Родосский К. А. Об обобщенном характере // ДАН СССР, 1950. Т. 74, №4. С. 1137—1138.
4. Чудаков Н. Г. Об одном классе вполне мультипликативных функций // Успехи мат. наук, 1953. Т. 8, вып. 3, С. 149–150.
5. Чудаков Н. Г. Обобщенные характеры // Междунар. конгресс матиматиков в Ницце – 1970. Доклад советских математиков – М.: Наука, 1972. С. 335.
6. Матвеева О. А. О нулях полиномов Дирихле, аппроксимирующих в критической полосе L–функции Дирихле // Чебышевский сборник, 2013. Т. 14, вып. 2. С. 117–121.
7. Матвеева О. А. Аппроксимационные полиномы и поведение L-функций Дирихле в критической полосе // Известия Сарат. ун-та. Математика, Механика. Информатика — Саратов: Изд-во СГУ, 2013. Вып. 4, ч. 2. С. 80–84.

8. Коротков А. Е., Матвеева О. А. Об одном численном алгоритме определения нулей целых функций, определяемых рядами Дирихле с периодическими коэффициентами // Науч. ведомости Белгородского гос. ун-та — Белгород: Изд-во БелГУ, 2011. Вып. 24. С. 47–84.

9. Матвеева О. А. Аналитические свойства определённых классов рядов Дирихле и некоторые задачи теории L-функций Дирихле: Диссертация на соискание ученой степени канд. физ.-мат. наук по специальности 01.01.06 — Ульяновск, 2014.

10. Кузнецов В. Н., Матвеева О. А. О граничном поведении одного класса рядов Дирихле // Чебышевский сборник, 2016. Т. 17, вып. 2. С. 162–169.

11. Кузнецов В. Н., Матвеева О. А. О граничном поведении одного класса рядов Дирихле с мультипликативными коэффициентами // Чебышевский сборник, 2016. Т. 17, вып. 3. С. 115–124.

12. Кузнецов В. Н., Матвеева О. А. К задаче аналитического продолжения рядов Дирихле с конечнозначными коэффициентами как целых функций на комплексную плоскость // Чебышевский сборник, 2017. Т. 18, вып. 4. С. 285–295.

13. Кузнецов В. Н., Матвеева О. А. Граничное поведение и задача аналитического продолжения одного класса рядов Дирихле с мультипликативными коэффициентами как целых функций на компелксную плоскость // Чебышевский сборник, 2018. Т. 19, вып. 1. С. 124–137.

14. Маркушевич А. Н. Теория аналитических функций — М.: Наука, 1967. Т. 2. 624 с.

15. Гурвиц А., Нурант Р. Теория функций — М.: Наука, 1968. 646 с.

REFERENCES

1. Lang S. D., 1970, “Algebraic Number Theory“ *New. Jork*, P. 384.

2. Chudakov, N. G., Linnik, Yu. V., 1950, “Ob odnom klasse vpolne mul’tiplikativnyh funkcij“, *DAN SSSR*, vol. 74, issue 2, pp. 133–136.

3. Chudakov, N. G., Rodosskij K. A., 1950, “Ob obobshhennom haraktere“, *DAN SSSR*, vol. 74, issue 4, pp. 1137–1138.

4. Chudakov, N. G., 1953, “Ob odnom klasse mul’tiplikativnyh funkcij“, *Uspehi mat. nauk*, vol. 8, issue 3, pp. 149–150.

5. Chudakov, N. G., 1972, “Obobshhennye haraktery“, *Mezhdunar. kongress matimatikov v Nicce. Doklad sovetskih matematikov*, M.: Nauka, pp. 335.

6. Matveeva O. A., 2013, “On the zeros of Dirichlet polynomials that approximate Dirichlet L-functions in the critical band “ *Chebyshevskij sbornik*, Tula, publ TPGU, vol. 14, issue 2, pp. 117–121.

7. Matveeva, O. A., 2013, “Approksimacionnye polinomy i povedenie L-funkcij Dirihle v kriticheskoj polose“, *Saratov: izd-vo SGU, Izvestija Sarat. un-ta. Matematika, Mehanika. Informatika.*, iss. 4, vol. 2, pp. 80–84.

8. Korotkov, A. E. Matveeva, O. A. 2011, “Ob odnom chislennom algoritme opredelenija nulej celyh funkcij, opredeljaemyh rjadami Dirihle s periodicheskimi kojefficientami“, *Belgorod: Nauchnye vedomosti BelGU.*, iss. 24, pp. 47–54.

9. Matveeva, O. A., 2014, “Analiticheskie svojstva opredeljonnyh klassov rjadov Dirihle i nekotorye zadachi teorii L-funkcij Dirihle: Dissertacija na soiskanie uchenoj stepeni kand. fiz.-mat. nauk po special'nosti 01.01.06“, *Ul'janovsk*.

10. Kuznetsov, V. N. Matveeva, O. A. 2016, “O granichnom povedenii odnogo klassa rjadov Dirihle“, *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 2, vol. 17, pp. 162–169.

11. Kuznetsov, V. N. Matveeva, O. A. 2016, “O granichnom povedenii odnogo klassa rjadov Dirihle s mul'tiplikativnymi kojefficientami“, *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 4, vol. 17, pp. 115–124.

12. Kuznetsov, V. N. Matveeva, O. A. 2017, “On the problem of analytical continuation of Dirichlet series with finite coefficients as entire functions onto the complex plane“, *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 4, vol. 18, pp. 285–295.

13. Kuznetsov, V. N. Matveeva, O. A. 2018, “Boundary behavior and the problen of analytic continuation of a certain class of Dirichlet series with multiplicative coefficients as an integral functions on the complex plane“, *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 2, vol. 19.

14. Markushevich, A. I., 1968, “Theory of analitical functions“ *"Nauka", Moscow*, vol. 2, pp. 624.

15. Gurvic A., Nurant R., 1968, “Teoriya funkcij“ *"Nauka", Moscow*, pp. 646.

Получено 18.08.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-210-218

К проблеме обобщённых характеров

Кузнецов Валентин Николаевич — доктор технических наук, профессор, профессор кафедры Прикладной математики и системного анализа СГТУ им. Гагарина Ю. А., г. Саратов
e-mail: kuznetsovvalnik@gmail.com
Матвеева Ольга Андреевна — кандидат физико-математических наук
e-mail: olga.matveeva.0@gmail.com

Аннотация

Проблема обобщённых характеров заключается в решении задачи Ю. В. Линника, поставленной им в 1949 году, относительно аналитического продолжения как целых функций на комплексную плоскость одного класса рядов Дирихле и в решении гипотезы Н. Г. Чудакова, выдвинутой им в 1950 году о том, что любой конечнозначный числовой характер, отличный от нуля почти на всех простых числах и имеющий ограниченную сумматорную функцию, является характером Дирихле. Позднее такие характеры получили название неглавных обобщённых характеров. Коэффициенты рядов Дирихле в задаче Ю. В Линника также определялись неглавными обобщёнными характерами.

Кроме Ю. В. Линника и Н. Г. Чудакова решениями проблемы обобщённых характеров занимались такие известные математики как В. Г. Спринджук, К. А. Родосский, Б. М. Бредихин и многие другие, но проблема оставалась открытой.

Последние годы авторы разработали аппроксимационный подход, основанный на приближении в правой полуплоскости комплексной плоскости функций, заданных рядами Дирихле, полиномами Дирихле, в задаче аналитического продолжения рядов Дирихле с мультипликативными коэффициентами. Ранее этот подход позволил авторам решить задачу Ю. В. Линника, а в данной работе приводится решение гипотезы Н. Г. Чудакова.

Ключевые слова: обобщённый характер, аппроксимационные полиномы Дирихле, проблема обобщённых характеров.

Библиография: 17 названий.

Для цитирования:
В. Н. Кузнецов, О. А. Матвеева. К проблеме обобщённых характеров // Чебышевский сборник, 2018, т. 19, вып. 3, с. 210–218.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-210-218

On the problem of generalized characters

Kuznetsov Valentin Nikolaevich — Doctor of technical sciences, professor, Department of Applied Mathematics and Systems Analysis, Saratov State Technical University, Saratov
e-mail: kuznetsovvalnik@gmail.com
Matveeva Olga Andreevna — Candidate of physico-mathematical sciences
e-mail: olga.matveeva.0@gmail.com

Abstract

The problem of generalized characters lies in the solution of Linnik's problem, posed by him in 1949, with respect to the analytic continuation of entire functions to the complex plane of a class of Dirichlet series and in the solution of the hypothesis of N. G. Chudakov, who put forward in 1950 that any finite-valued numerical character, different from zero on almost all prime numbers and having a bounded summation function, is a Dirichlet character. Later such characters were called non-principal generalized characters. The coefficients of the Dirichlet series in Linnik's problem were also determined by non-principal generalized characters.

Except Yu. V. Linnik and N. G. Chudakov's solutions to the problem of generalized characters were handled by such well-known mathematicians as V. G. Sprindzhuk, K. A. Rodosssky, B. M. Bredikhin and many others, but the problem remained open.

In recent years, the authors have developed an approximation approach based on the approximation in the right half-plane of the complex plane of functions given by Dirichlet series by Dirichlet polynomials in the problem of analytic continuation of Dirichlet series with multiplicative coefficients. Earlier this approach allowed the authors to solve the problem of Yu. V. Linnik, and in this paper the solution of the hypothesis of N. G. Chudakov is given.

Keywords: generalized character, approximate Dirichlet polynomials, the problem of generalized characters.

Bibliography: 17 titles.

For citation:
V. N. Kuznetsov, O. A. Matveeva. 2018, "On the problem of generalized characters" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 210–218.

1. Введение

Рассмотрим ряд Дирихле

$$f(s)=\sum_{n=1}^{\infty}\frac{h(n)}{n^s}, s=\sigma+it, \tag{1}$$

где $h(n)$ – конечнозначный числовой характер, отличный от нуля почти для всех простых и имеющий ограниченную сумматорную функцию

$$S(x)=\sum_{n\le x}h(n)=O(1).$$

Такие характеры в 1950 году получили название неглавных обобщённых характеров (см.[1],[2]).

В случае, когда

$$S(x)=\sum_{n\le x}h(n)=d\cdot x+O(1), d\neq 0.$$

характеры $h(n)$ стали называться главными обобщёнными характерами.

В 1949 году Ю. В. Линник поставил задачу показать аналитическое продолжение ряда (1) как целой функции на комплексную плоскость. Решением задачи Ю. В. Линника занимались многие известные ученые. Но попытки решить эту задачу оказались безуспешными. Профессор Н. Г. Чудаков видел решение задачи Ю. В. Линника в доказательстве высказанного им в 1950 году ([1],[2],[3]) предположения о том, что любой обобщённый характер является характером Дирихле. В течение всей своей жизни Н. Г. Чудаков неоднократно обращался к решению этой гипотезы.

В 1964 году В. В. Глазков, ученик Н. Г. Чудакова, элементарными методами доказал гипотезу для главных обобщённых характеров (см. [4]).

В 1970 году на Международном математическом конгрессе в Ницце Н. Г. Чудаков сформулировал гипотезу для неглавных обобщённых характеров как одну из актуальных задач аналитической теории чисел (см. [5]).

В середине 70-х годов Н. Г. Чудаков пытался доказать свою гипотезу обращаясь к степенным рядам. Он пытался показать, что степенные ряды с неглавными обобщёнными характерами удовлетворяют условиям известных теорем Сёге или Даффина-Шеффера (см. [6]). Но эти попытки были безуспешными.

В 1983 году В. Н. Кузнецов, используя результат теоремы Сёге для степенных рядов, показал, что если ряд Дирихле (1) аналитически продолжим целым образом на комплексную плоскость с определенным порядком роста модуля, то $h(n)$ является характером Дирихле (см. [7]).

В начале 2010-х годов в работах О. А. Матвеевой ([8],[9],[10],[11]) были разработаны основные положения аппроксимационного подхода в задаче изучения аналитических свойств рядов Дирихле, основанного на построении полиномов Дирихле, сходящихся в правой полуплоскости к функции, определенной рядом Дирихле, и переносе отдельных свойств полиномов Дирихле на ряды Дирихле.

В последние годы авторы в результате применения аппроксимационного подхода получили ряд новых результатов в задаче аналитического продолжения рядов как целых функций на комплексную плоскость (см. [12],[13],[14],[15]). Так в работе [14] было получено условие, выраженное в терминах поведения функции, определенной рядом Дирихле, на мнимой оси, при котором ряд Дирихле допускает аналитическое продолжение как целой функции на комплексную плоскость.

В работе [15] авторы показали, что ряды Дирихле (1) удовлетворяют условию аналитического продолжения целым образом на комплексную плоскость, полученному в работе [14], и, тем самым, получили решение задачи Ю. В. Линника.

В данной работе показано, что ряды Дирихле (1), которые в силу результата работы [15] продолжаются целым образом на комплексную плоскость, и при этом выполняется условие на рост модуля, приведенное в работе [7], то есть как отмечалось выше любой неглавный обобщённый характер является характером Дирихле.

Таким образом в работе показано, что гипотеза Н. Г. Чудакова получена как следствие решения задачи Ю. В. Линника и ее решение закрывает проблему обобщённых характеров.

2. Некоторые свойства аппроксимационных полиномов для рядов Дирихле, коэффициенты которых определены неглавными обобщёнными характерами

В работах [12]–[15] приведены определения и отдельные свойства аппроксимационных полиномов $Q_n(s)$, необходимые для решения задачи Ю. В. Линника.

Здесь приведен ряд свойств аппроксимационных полиномов Дирихле $Q_n(s)$, которые будут использованы для доказательства гипотезы Н. Г. Чудакова относительно обобщённых характеров. Как отмечалось в работах [14], [15] аппроксимационные полиномы, то есть последовательность полиномов Дирихле $Q_n(s)$, которые в каждом прямоугольнике $D_T : 0 < \sigma_0 \leq \sigma \leq 1, |t| \leq T$, равномерно сходится к функции $f(s)$, определенной рядом Дирихле (1), и нормы этих полиномов ограничены в D_T константой, зависящей только от величины T, определяется не однозначно. Такие полиномы выбираются определенным образом в зависимости от поставленной задачи. Опишем выбор аппроксимационных полиномов в нашем случае и укажем некоторые свойства таких полиномов.

Рассмотрим степенной ряд, соответствующий ряду Дирихле (1):

$$g(x) = \sum_{n=1}^{\infty} h(n)x^n. \tag{2}$$

В работе [15] показано, что ряд Дирихле (1) определяет целую функцию, следовательно, согласно работе [16] степенной ряд (2) имеет в точке $x = 1$ односторонние производные любого порядка, то есть функция $g(x)$ бесконечное число раз дифференцируема на отрезке [0;1]. Известно (см. [17]), что для величин наилучшего приближения функции $g(x)$ на отрезке [0;1] алгебраическими полиномами степени $n : E_n(g(x))$ имеет место оценка

$$E_n(g(x)) = o\left(\frac{1}{n^m}\right), \tag{3}$$

при любом натуральном m.

Рассмотрим последовательность алгебраических полиномов $\hat{T}_n(x)$, заданных на отрезке [0;1] и полученных из многочленов Чебышева в результате линейного преобразования. Система полиномов $\hat{T}_n(x)$ будет ортоганальной на отрезке [0;1] с соответствующей весовой функцией.

Рассмотрим разложение функции $g(x)$ на отрезке [0;1] на системе полиномов $\hat{T}_n(x)$:

$$g(x) = \sum_{k=0}^{\infty} c_k \hat{T}_k(x) \tag{4}$$

Известно (см. [17]), что последовательность алгебраических полиномов

$$P_m(x) = S_n(x) = \sum_{k=1}^{n} c_k \hat{T}_k(x)$$

приближает функцию $g(x)$ на отрезке [0;1] в $\ln n$ раз хуже, чем наилучшее приближение, т. е.

$$\|g(x) - P_n(x)\|_{c[0;1]} \le (3 + \ln n)E_n(x).$$

Отсюда в силу (3) получаем

$$\|g(x) - P_n(x)\|_{C[0;1]} = O\left(\frac{1}{n^m}\right), \tag{5}$$

где m – любое натуральное, и следовательно

$$|c_n| = O\left(\frac{1}{n^m}\right). \tag{6}$$

Рассмотрим последовательность полиномов $\hat{\hat{T}}_k(x)$, которые отличаются от полиномов $\hat{T}_k(x)$ тем, что в них отсутствуют свободные члены, так как $g(x) = \sum_{k=1}^{\infty} h(k)x^k$, то в силу (5) имеет место оценка

$$\left\|g(x) - \hat{P}_n(x)\right\|_{C[0;1]} = O\left(\frac{1}{n^m}\right), \tag{7}$$

где m – любое натуральное заданное и где

$$\hat{P}_n(x) = \sum_{k=1}^{n} c_k \hat{\hat{T}}_k(x) = \sum_{k=1}^{n} b_{n,k}x^k.$$

Рассмотрим последовательность полиномов Дирихле

$$Q_k(s) = \sum_{k=1}^{n} \frac{b_{n,k}}{k^s} \tag{8}$$

В работе [8] показано, что в силу (7) имеет место оценка

$$\|f(s) - Q_n(s)\|_{C(D_T)} = O\left(\frac{1}{n^m}\right),$$

где m – любое заданное натуральное, и как показано в [12] для функции $f(s)$, определенной рядом Дирихле (1), для каждого заданного m выполняется оценка

$$\|f(s) - Q_k(s)\|_{C(D_T)} \le C \cdot \frac{1}{n^m}, \tag{9}$$

где константа C зависит от величины T.

Следовательно полиномы Дирихле (8) являются аппроксимационными полиномами для ряда Дирихле (1).

Докажем ряд утверждений относительно свойств аппроксимационных полиномов Дирихле вида (6), которые будут использованы при доказательстве основного результата.

Лемма 1. *Для производной k-го порядка полинома $Q_n(s)$ в прямоугольнике D_T имеет место оценка*

$$\left\|Q_n^{(k)}(s)\right\|_{C(D_T)} \le C \ln^k n,$$

где константа C зависит только от величины T.

Доказательство. Применив к производной полинома $Q_n(s)$ формулу суммирования Абеля, получим

$$\left\|Q_n'(s)\right\|_{C(D_T)} \le \ln n \, \|Q_n(s)\|_{C(D_T)}$$

Учитывая, что в полосе : $0 < \sigma < \infty, |t| \le T$

$$|Q_n(s)| < C,$$

где константа C зависит только от T, и повторив рассуждения k раз, получим утверждение леммы 1. □

Лемма 2. *Для любого k в прямоугольнике D_T имеет место оценка*

$$\left\|Q_m^{(k)}(s) - Q_n^{(k)}(s)\right\| \le C \cdot \frac{1}{n^m},$$

где m – любое натуральное, а константа C при каждом m зависит только от T.

Доказательство. В силу условия (3)

$$\|f(s) - Q_n(s)\|_{C(D_T)} = O\left(\frac{1}{n^m}\right),$$

где m – любое заданное натуральное.

Отсюда следует

$$\|Q_{n+1}(s) - Q_n(s)\|_{C(D_T)} = O(\frac{1}{n^m}),$$

где m – любое.

Эта оценка в силу леммы 1 дает утверждение леммы 2. □

Лемма 3. *Для любого заданного натурального k имеет место оценка*

$$\left\| f^{(k)}(s) - Q_n^{(k)}(s) \right\|_{C(D_T)} = O\left(\frac{1}{n^k}\right).$$

Доказательство. Доказательство леммы 3 следует из следующего разложения в ряд в прямоугольнике D_T :

$$f^{(k)}(s) = Q_n^{(k)}(s) + \sum_{c=n}^{\infty}(Q_{c+1}^{(k)}(s) - Q_c^{(k)}(s)),$$

который равномерно сходится в силу леммы 2. □

Лемма 4. *Для любого k и $s_0 = 0$ последовательность $Q_n^{(k)}(s_0)$ сходится к $f^{(k)}(s_0)$.*

Доказательство. Утверждение леммы 4 следует из леммы 3. □

Теорема 1. *Для точек s, лежащих в круге радиуса R с центром в нуле, для любого $\varepsilon > 0$ существует такое n_0, что для всех $n \geq n_0$ имеет место неравенство*

$$|f(s) - Q_n(s)| < \varepsilon.$$

Доказательство. В работе [15] было показано, что ряд Тейлора функции $f(s)$, определенной рядом Дирихле (1), сходится равномерно в любом круге радиуса R с центром в нуле. Следовательно для любого $\varepsilon > 0$ найдется такое N_0, что в круге радиуса R будет иметь место неравенство

$$|f(s) - S_{N_0}(s)| < \frac{\varepsilon}{3}, \tag{10}$$

где $S_{N_0}(s)$ – частичная сумма ряда Тейлора порядка N_0.

В силу леммы 4 и леммы 3 существует n_0, что для всех s, лежащих в круге радиуса R, для $n \geq n_0$ имеет место оценка

$$\left|S_{N_0}(s) - S_{N_{0,n}}(s)\right| < \frac{\varepsilon}{3},$$

где $S_{N_{0,n}}(s)$ – частичная сумма ряда Тейлора многочлена $Q_n(s)$ порядка N_0. Отсюда в силу оценки (k) следует утверждение теоремы 1. □

3. К проблеме обобщённых характеров

Прежде всего докажем гипотезу Н. Г. Чудакова относительно обобщённых характеров.
Имеет место

Теорема 2. *Любой неглавный обобщённый характер является характером Дирихле.*

Доказательство. В работе [7] доказано, что ряд Дирихле с конечнозначными коэффициентами тогда и только тогда определяет целую функцию $f(s)$, удовлетворяющую следующему условию роста модуля

$$|f(x)| < Ce^{|s|\ln|s|+A(s)}, \sigma < 0, \tag{11}$$

где A – некоторая положительная константа, когда коэффициенты этого ряда периодичны, начиная с некоторого номера.

При этом в [7] показано, что в случае периодических, начиная с некоторого номера коэффициентов, константа $A \leq \frac{\pi}{2}$, а константа C определяется величиной $|\hat{g}(e^{-x})|$ на отрезке $[\rho;\infty]$, где $\rho > 0$, $g(x)$ – соответствующий степенной ряд, и $g(e^{-x}) = e^{-x} \cdot \hat{g}(e^{-x})$.

В нашем случае рассмотрим $f_k(s) = Q_n(s)$, где $Q_n(x)$ полиномы Дирихле, определенные по формулам (8), и рассмотрим

$$g_n(e^{-x}) = \sum_{k=1}^{n} b_{n,k} e^{-kx} = \sum_{k=1}^{n} c_k \hat{\hat{T}}_k(e^{-x}).$$

В силу того, что на отрезке [0;1] для всех k выполняется оценка $\left\|\hat{\hat{T}}_k(x)\right\| \leq 2$ и в силу (6) $|c_k| = O(\frac{1}{n^m})$, где m – любое натуральное, для $\hat{g}_n(e^{-x})$ на отрезке $[\rho;\infty]$ имеет место оценка вида

$$\left|\hat{g}_n(e^{-x})\right| < C,$$

где константа C не зависит от n.

Следовательно, для полиномов $Q_n(s)$ выполняется оценка

$$|Q_n(s)| < Ce^{|s|\ln|s|+A|s|},$$

где константа C единая для всех n, и где $A < \frac{\pi}{2}$.

Отсюда в силу Теоремы 1 имеет место оценка вида

$$|f(s)| < Ce^{|s|\ln|s|+A|s|} \tag{12}$$

где $f(s)$ – целая функция, определенная рядом Дирихле (1). Оценка (12) в силу приведенного выше результата работы [7] доказывает периодичность характера $h(n)$, т.е. доказывает утверждение теоремы 2. □

4. Заключение

Отметим, что приведенное здесь доказательство гипотезы Н. Г. Чудакова относительно обобщённых характеров является следствием основного результата работы [15], т.е. является следствием решения задачи Ю. В. Линника относительно аналитического продолжения рядов Дирихле вида (1).

Таким образом, проблема обобщённых характеров, которая заключается в решении задачи Ю. В. Линника и гипотезы Н. Г. Чудакова, получила окончательное решение.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Чудаков Н. Г., Линник Ю. В. Об одном классе вполне мультипликативных функций // ДАН СССР, 1950, Т. 74, №2. С. 133–136.

2. Чудаков Н. Г., Родосский К. А. Об обобщённом характере // ДАН СССР, 1950, Т. 74, №4. С. 1137–1138.

3. Чудаков Н. Г., Павлючук А. К. О сумматорных функциях характеров числовых групп с конечной базой // Труды матем. ин-та им. В. А. Стеклова АН СССР, 1951. Т. 38. С. 366–381.

4. Глазков В. В. Об обобщённых характерах // Некоторые вопросы теории полей. Изд-во СГУ, 1964. С.67–78.

5. Чудаков Н. Г. Обобщённые характеры // Междунар. конгресс матиматиков в Ницце – 1970. Доклад советских математиков – М.: Наука, 1972. С. 335.

6. Бибербах Л. Аналитическое продолжение – М: Наука, 1970.

7. Кузнецов В. Н. Аналог теоремы Сёге для одного класса рядов Дирихле // Мат. заметки, 1984. Т. 36, № 6. С. 805–813.

8. Матвеева О. А. О нулях полиномов Дирихле, приближающих в критической полосе L-функции Дирихле // Чебышевский сборник, 2013. Т. 14, вып. 2. С. 117–121.

9. Матвеева О. А. Аппроксимационные полиномы и поведение L-функций Дирихле в критической полосе // Известия Сарат. ун-та. Математика, Механика. Информатика — Саратов: Изд-во СГУ, 2013. Вып. 4, ч. 2. С. 80–84.

10. Коротков А. Е., Матвеева О. А Об одном численном алгоритме определения нулей целых функций, определяемых рядами Дирихле с периодическими коэффициентами // Науч. ведомости Белгородского гос. ун-та. – Белгород: Изд-во БелГУ, 2013. Вып. 24. С. 47–54.

11. Матвеева О. А. Аналитические свойства определённых классов рядов Дирихле и некоторые задачи теории L-функций Дирихле: Диссертация на соискание учебной степени канд. физ.-мат. наук по специальности 01.01.06. – Ульяновск, 2014.

12. Кузнецов В. Н., Матвеева О. А. О граничном поведении одного класса рядов Дирихле с мультипликативными коэффициентами // Чебышевский сборник, 2016. Т. 17, вып. 3. С. 115–124.

13. Кузнецов В. Н., Матвеева О. А. К задаче аналитического продолжения рядов Дирихле с конечнозначными коэффициентам на комплексную плоскость // Чебышевский сборник, 2017. Т. 18, вып. 4. С. 285–295.

14. Кузнецов В. Н., Матвеева О. А. Граничное поведение и задача аналитического продолжения одного класс рядов Дирихле с мультипликативными коэффициентами как целых функций на компелксную плоскость // Чебышевский сборник, 2018. Т. 19, вып. 1. С. 124–137.

15. Кузнецов В. Н., Матвеева О. А. К одной задаче Ю. В. Линника // Чебышевский сборник, 2018. Т. 19, вып. 3. С. 202–209.

16. Кузнецов В. Н. Об аналитическом продолжении одного класса рядов Дирихле // Вычислит. методы и программирование: межвуз. сб. науч. трудов. – Саратов: Изд-во СГУ, 1987, С. 17–23.

17. Даугавет И. К. Введение в теорию приближения функций. – Ленинград: Изд-во ЛГУ, 1977. 184 с.

REFERENCES

1. Chudakov, N. G., Linnik, Yu. V., 1950, “Ob odnom klasse vpolne mul’tiplikativnyh funkcij“, *DAN SSSR*, vol. 74, issue 2, pp. 133–136.

2. Chudakov, N. G., Rodosskij K. A., 1950, “Ob obobshhennom haraktere“, *DAN SSSR*, vol. 74, issue 4, pp. 1137–1138.

3. Chudakov, N. G., Pavlyuchuk A. K., 1951, “O summatornyh funkciyah harakterov chislovyh grupp s konechnoj bazoj“, *Trudy matem. in-ta im. V.A.Steklova AN SSSRR*, vol. 38, pp. 366–381.

4. Glazkov V. V., 1964, "Ob obobshchennyh harakterah", *Nekotorye voprosy teorii polej. Leningrad.: Izd-vo LGU* pp. 67–78.

5. Chudakov, N. G., 1972, "Obobshhennye haraktery", *Mezhdunar. kongress matimatikov v Nicce. Doklad sovetskih matematikov*, M.: Nauka, pp. 335.

6. Biberbah L., 1970, "Analiticheskoe prodolzhenie", *M.: Nauka.*

7. Kuznetsov, V. N. 1984, "Analog teoremy Sjoge dlja odnogo klassa rjadov Dirihle", *Mat. zametki.*, vol. 38, iss. 6, pp. 805–813.

8. Matveeva O. A., 2013, "On the zeros of Dirichlet polynomials that approximate Dirichlet L-functions in the critical band " *Chebyshevskij sbornik*, Tula, publ TPGU, vol. 14, issue 2, pp. 117–121

9. Matveeva, O. A., 2013, "Approksimacionnye polinomy i povedenie L-funkcij Dirihle v kriticheskoj polose", *Saratov: izd-vo SGU, Izvestija Sarat. un-ta. Matematika, Mehanika. Informatika.*, iss. 4, vol. 2, pp. 80–84.

10. Korotkov, A. E. Matveeva, O. A. 2011, "Ob odnom chislennom algoritme opredelenija nulej celyh funkcij, opredeljaemyh rjadami Dirihle s periodicheskimi kojefficientami", *Belgorod: Nauchnye vedomosti BelGU.*, iss. 24, pp. 47–54.

11. Matveeva, O. A., 2014, "Analiticheskie svojstva opredeljonnyh klassov rjadov Dirihle i nekotorye zadachi teorii L-funkcij Dirihle: Dissertacija na soiskanie uchebnoj stepeni kand. fiz.-mat. nauk po special'nosti 01.01.06", *Ul'janovsk.*

12. Kuznetsov, V. N. Matveeva, O. A. 2016, "O granichnom povedenii odnogo klassa rjadov Dirihle s mul'tiplikativnymi kojefficientami", *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 4, vol. 17, pp. 115–124.

13. Kuznetsov, V. N. Matveeva, O. A. 2017, "On the problem of analytical continuation of Dirichlet series with finite coefficients as entire functions onto the complex plane", *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 4, vol. 18, pp. 285–295.

14. Kuznetsov, V. N. Matveeva, O. A. 2018, "Boundary behavior and the problen of analytic continuation of a certain class of Dirichlet series with multiplicative coefficients as an integral functions on the complex plane", *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 2, vol. 19.

15. Kuznetsov, V. N. Matveeva, O. A. 2018, "On a problem of Yu. V. Linnik", *Tula: izd-vo TPGU, Chebyshevskij sbornik.*, iss. 3, vol. 19.

16. Kuznetsov V. N., 1987, "On the analytic extension of a class of Dirichlet series" *Vychislitel'nye metody i programmirovanie: Mezhvuz. sb. nauch. tr.*, Saratov, publ. SSU, vol. 1, pp. 13–23.

17. Daugavet I. K., 1977, "Vvedenie v teoriyu priblizheniya funkcij" *Leningrad.: Izd-vo LGU*, pp. 184.

Получено 18.08.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-219-230

О совместном распределении значений дзета-функций Гурвица[1]

Францкевич Виолета — докторант, Институт математики, факультет математики и информатики, Вильнюсский университет.
e-mail: violeta.franckevic@stud.mif.vu.lt
Лауринчикас Антанас — доктор физико-математических наук, профессор, Действительный член Академии наук Литвы, ведущий научный сотрудник, Институт математики, факультет математики и информатики, Вильнюсский университет.
e-mail: antanas.laurincikas@mif.vu.lt
Шяучюнас Дариус — доктор математических наук, профессор кафедры математики Шяуляйского университета, старший научный сотрудник, Исследовательский институт, Шяуляйский университет.
e-mail: darius.siauciunas@su.lt

Аннотация

Хорошо известно, что некоторые дзета и L-функции универсальны в смысле Воронина, т.е., ими приближается широкий класс аналитических функций. Некоторые из этих функций также совместно универсальны. В этом случае, набор аналитических функций одновременно приближается набором дзета-функций. В статье рассматривается проблема, связанная со совместной универсальностью дзета-функций Гурвица. Известно, что дзета-функции Гурвица $\zeta(s,\alpha_1),\dots,\zeta(s,\alpha_r)$ совместно универсальны, если параметры $\alpha_1,\dots,\alpha_r$ алгебраически независимы над полем рациональных чисел $\mathbb{Q}$, или в более общем случае, если множество $\{\log(m+\alpha_j) : m\in\mathbb{N}_0,\ j=1,\dots,r\}$ линейно независимо над $\mathbb{Q}$. Мы рассматриваем случай произвольных параметров $\alpha_1,\dots,\alpha_r$ и получаем, что существует непустое замкнутое множество функций $F_{\alpha_1,\dots,\alpha_r}$ пространства $H^r(D)$ аналитических в полосе $D=\left\{s\in\mathbb{C}:\frac{1}{2}<\sigma<1\right\}$ такое, что для любых компактных множеств $K_1,\dots,K_r\subset D$, функций $(f_1,\dots,f_r)\in F_{\alpha_1,\dots,\alpha_r}$ и всякого $\varepsilon>0$ множество $\left\{\tau\in\mathbb{R}:\sup_{1\leqslant j\leqslant r}\sup_{s\in K_j}|\zeta(s+i\tau,\alpha_j)-f_j(s)|<\varepsilon\right\}$ имеет положительную нижнюю плотность. Также рассматривается случай положительной плотности этого множества.

Ключевые слова: вероятностная мера, дзета-функция Гурвица, пространство аналитических функций, слабая сходимость, универсальность.

Библиография: 14 названий.

Для цитирования:
В. Францкевич, А. Лауринчикас, Д. Шяучюнас. О совместном распределении значений дзета-функций Гурвица // Чебышевский сборник, 2018, т. 19, вып. 3, с. 219–230.

[1]Исследование второго автора финансируется Европейским Социальным фондом по направлению “Повышение квалификации исследователей путем внедрения научно-исследовательских проектов мирового уровня” No. 09.3.3-LMT-K-712-01-0037.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-219-230

On joint value distribution of Hurwitz zeta-functions[2]

Franckevič Violeta — doctoral student, Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University.
e-mail: violeta.franckevic@stud.mif.vu.lt
Laurinčikas Antanas — Full member of the AS in Lithuania, doctor of physical and mathematical sciences, professor, chief researcher, Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University.
e-mail: antanas.laurincikas@mif.vu.lt
Šiaučiūnas Darius — doctor of mathematical sciences, professor of the department of mathematics of the Šiualiai University, Research Institute, Šiauliai University.
e-mail: darius.siauciunas@su.lt

Abstract

It is well known that some zeta and L-functions are universal in the Voronin sense, i.e., they approximate a wide class of analytic functions. Also, some of them are jointly universal. In this case, a collection of analytic functions is simultaneously approximated by a collection of zeta-functions. In the paper, a problem related to joint universality of Hurwitz zeta-functions is discussed. It is known that the Hurwitz zeta-functions $\zeta(s,\alpha_1),\ldots,\zeta(s,\alpha_r)$ are jointly universal if the parameters $\alpha_1,\ldots,\alpha_r$ are algebraically independent over the field of rational numbers $\mathbb{Q}$, or, more generally, if the set $\{\log(m+\alpha_j) : m\in\mathbb{N}_0,\ j=1,\ldots,r\}$ is linearly independent over $\mathbb{Q}$. We consider the case of arbitrary parameters $\alpha_1,\ldots,\alpha_r$ and obtain that there exists a non-empty closed set $F_{\alpha_1,\ldots,\alpha_r}$ of the space $H^r(D)$ of analytic functions on the strip $D=\left\{s\in\mathbb{C}:\frac{1}{2}<\sigma<1\right\}$ such that, for every compact sets $K_1,\ldots,K_r\subset D$, $f_1,\ldots,f_r\in F_{\alpha_1,\ldots,\alpha_r}$ and $\varepsilon>0$, the set $\left\{\tau\in\mathbb{R}:\sup_{1\leqslant j\leqslant r}\sup_{s\in K_j}|\zeta(s+i\tau,\alpha_j)-f_j(s)|<\varepsilon\right\}$ has a positive lower density. Also, the case of positive density of the latter set is discussed.

Keywords: Hurwitz zeta-function, probability measure, space of analytic functions, universality, weak convergence.

Bibliography: 14 titles.

For citation:
V. Franckevič, A. Laurinčikas, D. Šiaučiūnas, 2018, "On joint value distribution of Hurwitz zeta-functions" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 219–230.

Памяти Юрия Владимировича Линника посвящается

1. Introduction

The Hurwitz zeta-function $\zeta(s,\alpha)$, $s=\sigma+it$, with parameter α, $0<\alpha\leqslant 1$, is defined, for $\sigma>1$, by the Dirichlet series

$$\zeta(s,\alpha)=\sum_{m=0}^{\infty}\frac{1}{(m+\alpha)^s},$$

[2]The research of the second author is funded by the European Social Fund according to the activity "Improvement of researchers qualification by implementing world-class R&D projects" of Measure No. 09.3.3-LMT-K-712-01-0037.

and has the analytic continuation to the whole complex plane, except for a simple pole at the point $s = 1$ with residue 1. For $\alpha = 1$, the Hurwitz zeta-function reduces to the Riemann zeta-function

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}, \quad \sigma > 1,$$

and

$$\zeta\left(s, \frac{1}{2}\right) = (2^s - 1)\,\zeta(s).$$

Thus, $\zeta(s, \alpha)$ is a generalization of the Riemann zeta-function. The function $\zeta(s)$ has the Euler product over primes

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

while the function $\zeta(s, \alpha)$, except for the values $\alpha = 1$ and $\alpha = \frac{1}{2}$, has no such a product. This fact reflects in value distribution differences of the functions $\zeta(s)$ and $\zeta(s, \alpha)$. For example, it is well known that $\zeta(s) \neq 0$, while the function $\zeta(s, \alpha)$ has infinitely many zeros for all $\alpha \neq 1, \frac{1}{2}$ in the half plane $\sigma > 1$. On the other hand, the functions $\zeta(s)$ and $\zeta(s, \alpha)$ for some classes of the parameter α have a common property of the approximation of a wide class of analytic functions. This interesting property is called universality, and for the function $\zeta(s)$ was obtained by S. M. Voronin [12]. For modern statements of universality theorems it is convenient to use the following notation. Let $D = \left\{s \in \mathbb{C} : \frac{1}{2} < \sigma < 1\right\}$. Denote by $\mathcal{K}$ the class of compact subsets of the strip D with connected complements, and by $H_0(K)$ with $K \in \mathcal{K}$ the class of continuous non-vanishing functions on K that are analytic in the interior of K. Then the modern Voronin universality theorem, see, for example, [7], says that for every $K \in \mathcal{K}$, $f \in H_0(K)$ and $\varepsilon > 0$,

$$\liminf_{T\to\infty} \frac{1}{T}\mathrm{meas}\left\{\tau \in [0, T] : \sup_{s\in K} |\zeta(s + i\tau) - f(s)| < \varepsilon\right\} > 0.$$

The later inequality shows that there are infinitely many shifts $\zeta(s + i\tau, \alpha)$ approximating with accuracy ε a given function $f(s) \in H_0(K)$. Yuri Vladimirovich Linnik knew the Voronin theorem and highly valued it. Moreover, Il'dar Abdulovich Ibragimov imformed the second author that Yu. V. Linnik had a conjecture that all Dirichlet series satisfying some natural growth conditions are universal in the Voronin sense. Now this conjecture is called the Linnik-Ibragimov conjecture (or problem), see, for example, [11].

The universality of the Hurwitz zeta-function differs slightly from that of the function $\zeta(s)$. Denote by $H(K)$ with $K \in \mathcal{K}$ the class of continuous functions on K that are analytic in the interior of K. Thus, $H_0(K) \subset H(K)$ for all $K \in \mathcal{K}$. Then the following universality theorem for the function $\zeta(s, \alpha)$ is known.

THEOREM 1. *Suppose that the parameter α is transcendental or rational $\neq 1, \frac{1}{2}$. Let $K \in \mathcal{K}$ and $f(s) \in H(K)$. Then, for every $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \frac{1}{T}\mathrm{meas}\left\{\tau \in [0, T] : \sup_{s\in K} |\zeta(s + i\tau, \alpha) - f(s)| < \varepsilon\right\} > 0. \tag{1}$$

The theorem in the case of rational α was already known to Voronin [14]. In a slightly different form, the theorem was obtained independently by S. M. Gonek and B. Bagchi in their theses [5], [1].

Unfortunately, the universality of $\zeta(s, \alpha)$ with algebraic irrational parameter α is an open problem. This problem is closely connected to linear independence over the field of rational numbers $\mathbb{Q}$ of the set $L(\alpha) = \{\log(m + \alpha) : m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}\}$. Denote by $H(D)$ the space of analytic functions on D endowed with the topology of uniform convergence on compacta. Then, in [2], the following result towards to universality problem of $\zeta(s, \alpha)$ with algebraic irrational α was obtained.

THEOREM 2. *Suppose that the parameter α is algebraic irrational. Then there exists a closed non-empty set $F_\alpha \subset H(D)$ such that, for every compact set $K \subset D$, $f(s) \in F_\alpha$ and $\varepsilon > 0$, the inequality* (1) *is true.*

Some of zeta-functions are also jointly universal. In this case, a collection of analytic functions are simultaneously approximated by a collection of zeta-functions. The first joint universality results belong to S. M. Voronin. In [13], he considered the joint functional independence of Dirichlet L-functions, and, for this, he applied their joint universality. It is clear, that in the case of joint universality, the approximating zeta-functions must be in some sense independent. For Hurwitz zeta-functions this independence in [10] was described by the algebraic independence over $\mathbb{Q}$ of the parameters $\alpha_1, \dots, \alpha_r$. In [8], the algebraic independence was replaced by the linear independence over $\mathbb{Q}$ for the set

$$L(\alpha_1, \dots, \alpha_r) = \{\log(m + \alpha_j) : m \in \mathbb{N}_0,\ j = 1, \dots, r\}.$$

Thus, the following theorem is known [8].

THEOREM 3. *Suppose that the set $L(\alpha_1, \dots, \alpha_r)$ is linearly independent over $\mathbb{Q}$. For $j = 1, \dots, r$, let $K_j \in \mathcal{K}$ and $f_j(s) \in H(K_j)$. Then, for every $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \frac{1}{T}\operatorname{meas}\left\{\tau \in [0,T] : \sup_{1\leqslant j\leqslant r}\sup_{s\in K_j} |\zeta(s + i\tau, \alpha_j) - f_j(s)| < \varepsilon\right\} > 0.$$

The aim of this paper is to prove a joint generalization of Theorem 2, i.e., to prove a certain theorem on joint approximation by the functions $\zeta(s, \alpha_1), \dots, \zeta(s, \alpha_r)$ without using any independence condition.

THEOREM 4. *Suppose that the numbers α_j, $0 < \alpha_j < 1$, $\alpha_j \neq \frac{1}{2}$, $j = 1, \dots, r$, are arbitrary. Then there exists a closed non-empty set $F_{\alpha_1,\dots,\alpha_r} \subset H^r(D)$ such that, for every compact sets $K_1, \dots, K_r \subset D$, $(f_1, \dots, f_r) \in F_{\alpha_1,\dots,\alpha_r}$ and $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \frac{1}{T}\operatorname{meas}\left\{\tau \in [0,T] : \sup_{1\leqslant j\leqslant r}\sup_{s\in K_j} |\zeta(s + i\tau, \alpha_j) - f_j(s)| < \varepsilon\right\} > 0.$$

Theorem 4 has the following modification.

THEOREM 5. *Suppose that the numbers α_j, $0 < \alpha_j < 1$, $\alpha_j \neq \frac{1}{2}$, $j = 1, \dots, r$, are arbitrary. Then there exists a closed non-empty set $F_{\alpha_1,\dots,\alpha_r} \subset H^r(D)$ such that, for every compact sets $K_1, \dots, K_r \subset D$ and $(f_1, \dots, f_r) \in F_{\alpha_1,\dots,\alpha_r}$, the limit*

$$\lim_{T\to\infty} \frac{1}{T}\operatorname{meas}\left\{\tau \in [0,T] : \sup_{1\leqslant j\leqslant r}\sup_{s\in K_j} |\zeta(s + i\tau, \alpha_j) - f_j(s)| < \varepsilon\right\} > 0$$

exists for all but at most countably many $\varepsilon > 0$.

For the proof of above theorems we will apply the probabilistic approach. This is influenced in a certain sense by Yu. V. Linnik who was an expert not only in number theory but also in probability theory and mathematical statistics.

2. Auxiliary results

In this section, we will prove a joint limit theorem for the functions $\zeta(s,\alpha_1),\dots,\zeta(s,\alpha_r)$ in the space of analytic functions. Denote by $\mathcal{B}(\mathbb{X})$ the Borel σ-field of the space $\mathbb{X}$, and, for $A\subset\mathcal{B}(H^r(D))$, define

$$P_{T,\underline{\alpha}}(A)=\frac{1}{T}\mathrm{meas}\left\{\tau\in[0,T]:\underline{\zeta}(s+i\tau,\underline{\alpha})\in A\right\},$$

where $\underline{\alpha}=(\alpha_1,\dots,\alpha_r)$ and

$$\underline{\zeta}(s,\underline{\alpha})=(\zeta(s,\alpha_1),\dots,\zeta(s,\alpha_r)).$$

THEOREM 6. *Suppose that the numbers α_j, $0<\alpha_j<1$, $\alpha_j\neq\frac{1}{2}$, $j=1,\dots,r$, are arbitrary. Then, on $(H^r(D),\mathcal{B}(H^r(D)))$, there exists a probability measure $P_{\underline{\alpha}}$ such that $P_{T,\underline{\alpha}}$ converges weakly to $P_{\underline{\alpha}}$ as $T\to\infty$.*

We divide the proof of Theorem 6 into lemmas.

Denote by γ the unit circle on the complex plane, and define the set

$$\Omega=\prod_{m\in\mathbb{N}_0}\gamma_m,$$

where $\gamma_m=\gamma$ for all $m\in\mathbb{N}_0$. By the classical Tikhonov theorem, the infinite-dimensional torus Ω with the product topology and pointwise multiplication is a compact topological Abelian group. Define one more set

$$\Omega^r=\prod_{j=1}^{r}\Omega_j,$$

where $\Omega_j=\Omega$ for all $j=1,\dots,r$. Then again by the Tikhonov theorem, Ω^r is a compact topological Abelian group. Denote by $\underline{\omega}=(\omega_1,\dots,\omega_r)$, $\omega_1\in\Omega_1,\dots,\omega_r\in\Omega_r$, the elements of Ω^r Moreover, let $\omega_j(m)$ be the m-th component of the element $\omega_j\in\Omega$, $j=1,\dots,r$, $m\in\mathbb{N}_0$.

For $A\in\mathcal{B}(\Omega^r)$, define

$$Q_{T,\underline{\alpha}}(A)=\frac{1}{T}\mathrm{meas}\left\{\tau\in[0,T]:\left(\left((m+\alpha_1)^{-i\tau}:m\in\mathbb{N}_0\right),\dots,\left((m+\alpha_r)^{-i\tau}:m\in\mathbb{N}_0\right)\right)\in A\right\}.$$

LEMMA 1. *On $(\Omega^r,\mathcal{B}(\Omega^r))$, there exists a probability measure $Q_{\underline{\alpha}}$ such that $Q_{T,\underline{\alpha}}$ converges weakly to $Q_{\underline{\alpha}}$ as $T\to\infty$.*

PROOF. We apply the Fourier transform method. The dual group of Ω^r is isomorphic to

$$\mathcal{G}=\bigoplus_{j=1}^{r}\bigoplus_{m\in\mathbb{N}_0}\mathbb{Z}_{mj},$$

where $\mathbb{Z}_{mj}=\mathbb{Z}$ for all $j=1,\dots,r$, $m\in\mathbb{N}_0$. The element $\underline{k}=(k_{mj}:k_{mj}\in\mathbb{Z},\ j=1,\dots,r,\ \ m\in\mathbb{N}_0)\in\mathcal{G}$, where only a finite number of integers k_{mj} are distinct from zero, acts on Ω^r by

$$\omega\to\omega^{\underline{k}}=\prod_{j=1}^{r}\prod_{m\in\mathbb{N}_0}\omega_j^{k_{mj}}(m).$$

Therefore, the Fourier transform $g_T(\underline{k})$ of $Q_{T,\underline{\alpha}}$ is of the form

$$g_T(\underline{k})=\int_{\Omega^r}\left(\prod_{j=1}^{r}{\prod_{m\in\mathbb{N}_0}}'\omega_j^{k_{jm}}(m)\right)\mathrm{d}Q_{T,\underline{\alpha}},$$

where the sign "$'$" shows that only a finite number of integers k_{mj} are distinct from zero. Thus, by the definition of $Q_{T,\underline{\alpha}}$,

$$g_T(\underline{k}) = \frac{1}{T}\int_0^T \prod_{j=1}^r {\prod_{m\in\mathbb{N}_0}}' (m+\alpha_j)^{-i\tau k_{mj}}\,\mathrm{d}\tau = \frac{1}{T}\int_0^T \exp\left\{-i\tau \sum_{j=1}^r {\sum_{m\in\mathbb{N}_0}}' k_{mj}\log(m+\alpha_j)\right\}\mathrm{d}\tau. \quad (2)$$

Define two collections of integers

$$\{\underline{k}'\} = \left\{k_{mj} : \sum_{j=1}^r {\sum_{m\in\mathbb{N}_0}}' k_{mj}\log(m+\alpha_j) = 0\right\}$$

and

$$\{\underline{k}''\} = \left\{k_{mj} : \sum_{j=1}^r {\sum_{m\in\mathbb{N}_0}}' k_{mj}\log(m+\alpha_j) \neq 0\right\}.$$

Obviously, in view of (2),

$$g_T(\underline{k}) = 1 \quad (3)$$

for $\underline{k} \in \{\underline{k}'\}$. If $\underline{k} \in \{\underline{k}''\}$, then integrating in (2), we find that

$$g_T(\underline{k}) = \frac{1-\exp\left\{-iT\sum_{j=1}^r {\sum_{m\in\mathbb{N}_0}}' k_{mj}\log(m+\alpha_j)\right\}}{iT\sum_{j=1}^r {\sum_{m\in\mathbb{N}_0}}' k_{mj}\log(m+\alpha_j)}.$$

This and (3) show that

$$\lim_{T\to\infty} g_T(\underline{k}) = \begin{cases} 1 & \text{if } \underline{k}\in\{\underline{k}'\},\\ 0 & \text{if } \underline{k}\in\{\underline{k}''\}.\end{cases}$$

The right-hand side of the later equality is continuous in the discrete topology. Therefore, by a continuity theorem for probability measures on compact groups, we obtain that $Q_{T,\underline{\alpha}}$, as $T\to\infty$, converges weakly to a probability measure $Q_{\underline{\alpha}}$ on $(\Omega^r, \mathcal{B}(\Omega^r))$ defined by the Fourier transform

$$g(\underline{k}) = \begin{cases} 1 & \text{if } \underline{k}\in\{\underline{k}'\},\\ 0 & \text{if } \underline{k}\in\{\underline{k}''\}.\end{cases}$$

The lemma is proved. □

Unfortunately, the limit measure $Q_{\underline{\alpha}}$ in Lemma 1 is given by its Fourier transform, we do not know the explicit form of $Q_{\underline{\alpha}}$, and this reflects in Theorems 4 and 5 with non-effective set $F_{\alpha_1,\dots,\alpha_r}$. For example, if the set $L(\alpha_1,\dots,\alpha_r)$ is linearly independent over $\mathbb{Q}$, then

$$g(\underline{k}) = \begin{cases} 1 & \text{if } \underline{k} = \underline{0},\\ 0 & \text{if } \underline{k}\neq\underline{0},\end{cases}$$

and we have that the limit measure $Q_{\underline{\alpha}}$ coincides with the Haar measure on $(\Omega^r, \mathcal{B}(\Omega^r))$.

The next lemma is a joint limit theorem in the space $H^r(D)$ for absolutely convergent Dirichlet series.

Let σ_0 be a fixed number. For $m\in\mathbb{N}_0$ and $n\in\mathbb{N}$, set

$$v_n(m,\alpha_j) = \exp\left\{-\left(\frac{m+\alpha_j}{n+\alpha_j}\right)^{\sigma_0}\right\}, \quad j=1,\dots,r,$$

and define the functions

$$\zeta_n(s,\alpha_j) = \sum_{m=0}^\infty \frac{v_n(m,\alpha_j)}{(m+\alpha_j)^s}, \quad j=1,\dots,r.$$

It is known [9] that the series for $\zeta_n(s,\alpha_j)$ are absolutely convergent for $\sigma > \frac{1}{2}$. For brevity, let

$$\underline{\zeta}_n(s,\underline{\alpha}) = (\zeta_n(s,\alpha_1),\dots,\zeta_n(s,\alpha_r)),$$

and

$$P_{T,n,\underline{\alpha}}(A) = \frac{1}{T}\mathrm{meas}\left\{\tau\in[0,T] : \underline{\zeta}_n(s+i\tau,\underline{\alpha})\in A\right\}, \quad A\in\mathcal{B}(H^r(D)).$$

LEMMA 2. *On $(H^r(D),\mathcal{B}(H^r(D)))$, there exists a probability measure $P_{n,\underline{\alpha}}$ such that $P_{T,n,\underline{\alpha}}$ converges weakly to $P_{n,\underline{\alpha}}$ as $T\to\infty$.*

PROOF. For $\omega_j\in\Omega_j$, define the functions

$$\zeta_n(s,\omega_j,\alpha_j) = \sum_{m=0}^{\infty}\frac{\omega_j(m)v_n(m,\alpha_j)}{(m+\alpha_j)^s}, \quad j=1,\dots,r.$$

Since $|\omega_j(m)|=1$, the series for $\zeta_n(s,\omega_j,\alpha_j)$ is also absolutely convergent for $\sigma>\frac{1}{2}$. Let

$$\underline{\zeta}_n(s,\underline{\omega},\underline{\alpha}) = (\zeta_n(s,\omega_1,\alpha_1),\dots,\zeta_n(s,\omega_r,\alpha_r)).$$

Consider the function $u_{n,\underline{\alpha}}:\Omega^r\to H^r(D)$ given by the formula

$$u_{n,\underline{\alpha}}(\underline{\omega}) = \underline{\zeta}_n(s,\underline{\omega},\underline{\alpha}).$$

In virtue of the absolute convergence of the series for $\zeta_n(s,\omega_j,\alpha_j)$, $j=1,\dots,r$, the function $u_{n,\underline{\alpha}}$ is continuous. Moreover,

$$u_{n,\underline{\alpha}}\left(\left((m+\alpha_1)^{-i\tau} : m\in\mathbb{N}_0\right),\dots,\left((m+\alpha_r)^{-i\tau} : m\in\mathbb{N}_0\right)\right) = \underline{\zeta}_n(s+i\tau,\underline{\alpha}).$$

Therefore, for every $A\in\mathcal{B}(H^r(D))$,

$$\begin{aligned} P_{T,n,\underline{\alpha}}(A) &= \\ &= \frac{1}{T}\mathrm{meas}\left\{\tau\in[0,T] : \left\{\left((m+\alpha_1)^{-i\tau} : m\in\mathbb{N}_0\right),\dots,\left((m+\alpha_r)^{-i\tau} : m\in\mathbb{N}_0\right)\right\}\in u_{n,\underline{\alpha}}^{-1}A\right\} = \\ &= Q_{T,\underline{\alpha}}(u_{n,\underline{\alpha}}^{-1}A). \end{aligned}$$

Hence, $P_{T,n,\underline{\alpha}} = Q_{T,\underline{\alpha}}u_{n,\underline{\alpha}}^{-1}$. Therefore, Theorem 5.1 of [3], Lemma 1 and the continuity of the function $u_{n,\underline{\alpha}}$ imply that $P_{T,n,\underline{\alpha}}$ converges weakly to the measure $P_{n,\underline{\alpha}} = Q_{\underline{\alpha}}u_{n,\underline{\alpha}}^{-1}$ as $T\to\infty$, where $Q_{\underline{\alpha}}$ is the limit measure in Lemma 1. □

The next step of the proof of Theorem 6 consists of the approximation of $\underline{\zeta}(s,\underline{\alpha})$ by $\underline{\zeta}_n(s,\underline{\alpha})$. For this, we recall the metric in the space $H^r(D)$. It is known, see, for example, [4], that there exists a sequence of compact sets $\{K_l : l\in\mathbb{N}\}\subset D$ such that

$$D = \bigcup_{l=1}^{\infty}K_l,$$

$K_l\subset K_{l+1}$ for all $l\in\mathbb{N}$, and, for every compact set $K\subset D$, there exists K_l such that $K\subset K_l$. Let, for $g_1,g_2\in H(D)$,

$$\rho(g_1,g_2) = \sum_{l=1}^{\infty}2^{-l}\frac{\sup_{s\in K_l}|g_1(s)-g_2(s)|}{1+\sup_{s\in K_l}|g_1(s)-g_2(s)|}.$$

Then ρ is a metric in the space $H(D)$ inducing the topology of uniform convergence on compacta. Now, setting, for $\underline{g}_1=(g_{11},\dots,g_{1r}),\underline{g}_2=(g_{21},\dots,g_{2r})\in H^r(D)$,

$$\underline{\rho}(\underline{g}_1,\underline{g}_2) = \max_{1\leqslant j\leqslant r}\rho(g_{1j},g_{2j})$$

gives a metric in the space $H^r(D)$ inducing its product topology.

LEMMA 3. *The equality*

$$\lim_{n\to\infty}\limsup_{T\to\infty}\frac{1}{T}\int_0^T \underline{\rho}\left(\underline{\zeta}(s+i\tau,\underline{\alpha}),\underline{\zeta}_n(s+i\tau,\underline{\alpha})\right)\mathrm{d}\tau = 0$$

holds.

PROOF. The proof of the lemma does not depend on the arithmetic of the numbers $\alpha_1,\dots,\alpha_r$, and can be found in [8], Lemma 7. □

Now, we consider the sequence $\{P_{n,\underline{\alpha}} : n\in\mathbb{N}\}$, where $P_{n,\underline{\alpha}}$ is the limit measure in Lemma 2.

LEMMA 4. *The sequence $P_{n,\underline{\alpha}}$ is tight, i.e., for every $\varepsilon>0$, there exists a compact set $K=K_\varepsilon\subset H^r(D)$ such that*

$$P_{n,\underline{\alpha}}(K) > 1-\varepsilon$$

for all $n\in\mathbb{N}$.

PROOF. For an arbitrary α, $0<\alpha<1$, define

$$P_{T,n,\alpha}(A) = \frac{1}{T}\mathrm{meas}\left\{\tau\in[0,T] : \zeta_n(s+i\tau,\alpha)\in A\right\},\quad A\in\mathcal{B}(H(D)),$$

and denote by $P_{n,\alpha}$ the limit measure of $P_{T,n,\alpha}$ as $T\to\infty$. Then, in [2], it was obtained that the sequences $\{P_{n,\alpha} : n\in\mathbb{N}\}$ is tight. Hence, the sequences

$$\{P_{n,\alpha_j} : n\in\mathbb{N}\},\quad j=1,\dots,r,$$

are tight. Clearly, P_{n,α_j} are the marginal measures of the measure $P_{n,\underline{\alpha}}$, i.e.,

$$P_{n,\alpha_j}(A) = P_{n,\underline{\alpha}}\left(\underbrace{H(D)\times\cdots\times H(D)}_{j-1}\times A\times H(D)\times\cdots\times H(D)\right),\quad A\in\mathcal{B}(H(D)),\tag{4}$$

$j=1,\dots,r$. Since the sequence $\{P_{n,\alpha_j}\}$ is tight, for every $\varepsilon>0$, there exists a compact set $K_j=K_j(\varepsilon)\subset H(D)$ such that

$$P_{n,\alpha_j}(K_j) > 1-\frac{\varepsilon}{r},\quad j=1,\dots,r,\tag{5}$$

for all $n\in\mathbb{N}$. We put $K=K_1\times\cdots\times K_r$. Then the set K is compact in the space $H^r(D)$. Moreover, in view of (4) and (5),

$$\begin{aligned}
P_{n,\underline{\alpha}}(H^r(D)\setminus K) &= P_{n\underline{\alpha}}\left(\bigcup_{j=1}^{r}\left(\underbrace{H(D)\times\cdots\times H(D)}_{j-1}\right)\times(H(D)\setminus K_j)\times H(D)\times\cdots\times H(D)\right)\\
&\leqslant \sum_{j=1}^{r} P_{n,\underline{\alpha}}\left(\underbrace{H(D)\times\cdots\times H(D)}_{j-1}\times(H(D)\setminus K_j)\times H(D)\times\cdots\times H(D)\right)\\
&= \sum_{j=1}^{r} P_{n,\alpha_j}(H(D)\setminus K_j) \leqslant \sum_{j=1}^{r}\frac{\varepsilon}{r} = \varepsilon
\end{aligned}$$

for all $n\in\mathbb{N}$. Therefore,

$$P_{n,\underline{\alpha}}(K) \geqslant 1-\varepsilon$$

for all $n \in \mathbb{N}$. The lemma is proved. □

Proof.[Proof of Theorem 6] We will use the language of convergence in distribution ($\xrightarrow{\mathcal{D}}$). Let the random variable θ be defined on a certain probability space with measure μ, and be uniformly distributed on $[0,1]$. Define the $H^r(D)$-valued random element by the formula

$$X_{T,n,\underline{\alpha}} = X_{T,n,\underline{\alpha}}(s) = \underline{\zeta}_n(s + i\theta T, \underline{\alpha}).$$

Moreover, let $X_{n,\underline{\alpha}} = X_{n,\underline{\alpha}}(s)$ be the $H^r(D)$-valued random element having the distribution $P_{n,\underline{\alpha}}$. Then the assertion of Lemma 2 can be written in the form

$$X_{T,n,\underline{\alpha}} \xrightarrow[T\to\infty]{\mathcal{D}} X_{n,\underline{\alpha}}. \tag{6}$$

Since the sequence $\{P_{n,\underline{\alpha}} : n \in \mathbb{N}\}$ is tight, by the Prokhorov theorem ([3, Theorem 6.1]), it is relatively compact. Therefore, there is a subsequence $\{P_{n_k,\underline{\alpha}}\} \subset \{P_{n,\underline{\alpha}}\}$ such that $P_{n_k,\underline{\alpha}}$ converges weakly to a certain probability measure $P_{\underline{\alpha}}$ on $(H^r(D), \mathcal{B}(H^r(D)))$ as $k \to \infty$. In other words, we have the relation

$$X_{n_k,\underline{\alpha}} \xrightarrow[k\to\infty]{\mathcal{D}} P_{\underline{\alpha}}. \tag{7}$$

Define one more $H^r(D)$-valued random element $X_{T,\underline{\alpha}}$ by the formula

$$X_{T,\underline{\alpha}} = X_{T,\underline{\alpha}}(s) = \underline{\zeta}(s + i\theta T, \underline{\alpha}).$$

Then, the application of Lemma 3 shows that, for every $\varepsilon > 0$,

$$\begin{aligned}
&\lim_{n\to\infty} \limsup_{T\to\infty} \mu\left\{\underline{\rho}\left(X_{T,\underline{\alpha}}, X_{T,n,\underline{\alpha}}\right) \geqslant \varepsilon\right\} \\
&\quad = \lim_{n\to\infty} \limsup_{T\to\infty} \frac{1}{T}\mathrm{meas}\left\{\tau \in [0,T] : \underline{\rho}\left(\underline{\zeta}(s+i\tau,\underline{\alpha}), \underline{\zeta}_n(s+i\tau,\underline{\alpha})\right) \geqslant \varepsilon\right\} \\
&\quad \leqslant \lim_{n\to\infty} \limsup_{T\to\infty} \frac{1}{\varepsilon T}\int_0^T \underline{\rho}\left(\underline{\zeta}(s+i\tau,\underline{\alpha}), \underline{\zeta}_n(s+i\tau,\underline{\alpha})\right) \mathrm{d}\tau = 0.
\end{aligned}$$

The latter equality together with relations (6) and (7) shows that all hypotheses of Theorem 4.2 of [3] are satisfied. Therefore, we obtain the relation

$$X_{T,\underline{\alpha}} \xrightarrow[T\to\infty]{\mathcal{D}} P_{\underline{\alpha}},$$

which is equivalent to the weak convergence of $P_{T,\underline{\alpha}}$ to $P_{\underline{\alpha}}$ as $T \to \infty$. The theorem is proved. □

3. Proof of Theorems 4 and 5

Theorems 4 and 5 follow easily from Theorem 6. For this, the notion of the support of a probability measure is applied. Denote by $F_{\alpha_1,\dots,\alpha_r}$ the support of the limit measure $P_{\underline{\alpha}}$ in Theorem 6. We remind that $F_{\alpha_1,\dots,\alpha_r} \subset H^r(D)$ is a minimal closed set such that $P_{\underline{\alpha}}(F_{\alpha_1,\dots,\alpha_r}) = 1$. The set $F_{\alpha_1,\dots,\alpha_r}$ consists of all elements $\underline{g} \in H^r(D)$ such that, for every open neighborhood G of $\underline{g}$, the inequality $P_{\underline{\alpha}}(G) > 0$ is satisfied.

Also, we will use two equivalents of the weak convergence of probability measures. We recall that a set A is a continuity set of the probability measure P if $P(\partial A) = 0$, where ∂A is the boundary of the set A.

Lemma 5. *Let P_n, $n \in \mathbb{N}$, and P be the probability measures on $(\mathbb{X}, \mathcal{B}(\mathbb{X}))$. Then the following statements are equivalent:*

1° *P_n converges weakly to P as $n \to \infty$;*

2° *For every open set $G \subset \mathbb{X}$,*

$$\liminf_{n\to\infty} P_n(G) \geqslant P(G);$$

3° *For every continuity set A of the measure P,*

$$\lim_{n\to\infty} P_n(A) = P(A).$$

The lemma is Theorem 2.1 of [3].

Proof.[Proof of Theorem 4] Suppose that $F_{\alpha_1,\dots,\alpha_r}$ is the support of the measure $P_{\underline{\alpha}}$. Then $F_{\alpha_1,\dots,\alpha_r}$ is non-empty closed set of the space $H^r(D)$.

Let $(f_1,\dots,f_r) \in F_{\alpha_1,\dots,\alpha_r}$, $K_1,\dots,K_r$ are compact sets of the strip D and $\varepsilon > 0$. Define

$$G_\varepsilon = \left\{(g_1,\dots,g_r) \in H^r(D) : \sup_{1\leqslant j\leqslant r}\sup_{s\in K_j} |g_j(s) - f_j(s)| < \varepsilon\right\}.$$

Then the set G_ε is an open neighborhood of the element $(f_1,\dots,f_r)$ which belongs to the support of the measure $P_{\underline{\alpha}}$. Therefore,

$$P_{\underline{\alpha}}(G_\varepsilon) > 0. \tag{8}$$

Moreover, in view of Theorem 6, and 1° and 2° of Lemma 5, we have that

$$\liminf_{T\to\infty} P_{T,\underline{\alpha}}(G_\varepsilon) \geqslant P_{\underline{\alpha}}(G_\varepsilon).$$

This, the definitions of $P_{T,\underline{\alpha}}$ and G_ε, and (7) show that

$$\liminf_{T\to\infty} \frac{1}{T}\mathrm{meas}\left\{\tau \in [0,T] : \sup_{1\leqslant j\leqslant r}\sup_{s\in K_j} |\zeta(s+i\tau,\alpha_j) - f_j(s)| < \varepsilon\right\} > 0.$$

□

Proof. [Proof of Theorem 5] We use the same notation as in the proof of Theorem 4. We observe that the boundaries $\partial G_{\varepsilon_1}$ and $\partial G_{\varepsilon_2}$ do not intersect for different positive ε_1 and ε_2. Therefore, $P_{\underline{\alpha}}(G_\varepsilon) > 0$ for at most countably many $\varepsilon > 0$. This shows that that the set G_ε is a continuity set of the measure $P_{\underline{\alpha}}$ for all but at most countably many $\varepsilon > 0$. Therefore, using Theorem 6, 1° and 3° of Lemma 5, and inequality (7), we obtain that the limit

$$\lim_{T\to\infty} P_{T,\underline{\alpha}}(G_\varepsilon) = P_{\underline{\alpha}}(G_\varepsilon) > 0$$

exists for all but at most countably many $\varepsilon > 0$. Thus, the definitions of $P_{T,\underline{\alpha}}$ and G_ε prove the theorem. □

4. Conclusions

The Hurwitz zeta-function $\zeta(s,\alpha)$ depends on the parameter α whose arithmetic properties influence the analytic behavior of $\zeta(s,\alpha)$, including the universality. The universality problem is related to the linear independence over $\mathbb{Q}$ of the set

$$L(\alpha) = \{\log(m+\alpha) : m \in \mathbb{N}_0\}.$$

If the parameter α is algebraic irrational, them we have not much information on the set $L(\alpha)$, it is only known by the Cassels theorem that at least 51 percent of elements $L(\alpha)$ in the sense of density

are linearly independent over $\mathbb{Q}$. However, there is not any idea how to use the Cassels theorem for the proof of universality.

A similar situation arises in the investigation of the joint universality for Hurwitz zeta-functions. The linear independence of the set

$$L(\alpha_1,\dots,\alpha_r)=\{\log(m+\alpha_j):m\in\mathbb{N}_0,\ j=1,\dots,r\}$$

leads to joint universality for the functions $\zeta(s,\alpha_1),\dots,\zeta(s,\alpha_r)$. In the paper, we search a way how to avoid involving of the set $L(\alpha_1,\dots,\alpha_r)$. Without using any information about the set $L(\alpha_1,\dots,\alpha_r)$, we prove that there exists a closed non-empty set of analytic functions such that the collections of those functions can be approximated by shifts $(\zeta(s+i\tau,\alpha_1),\dots,\zeta(s+i\tau,\alpha_r))$. It remains a very difficult problem to describe the mentioned set of analytic functions.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bagchi B. The statistical behaviour and universality properties of the Riemann zeta-function and other allied Dirichlet series. Ph. D. Thesis. Calcutta: Indian Statistical Institute, 1981.

2. Бальчюнас А., Дубицкас А., Лауринчикас А. О дзета-функции Гурвица с алгебраическим иррациональным параметром // Матем. заметки. 2019. Т. 105, №2. С. 179–186.

3. Billingsley P. Convergence of Probability Measures. New York: Wiley, 1968.

4. Conway J. B. Functions of one complex variable. Berlin, Heidelberg, New York: Springer, 1978.

5. Gonek S. M. Analytic properties of zeta and L-functions. Thesis. Ann Arbor: University of Michigan, 1979.

6. Воронин С. М., Карацуба А. А. Дзета-функция Римана. Москва: Физматлит, 1994.

7. Laurinčikas A. Limit Theorems for the Riemann Zeta-Function. Dordrecht, Boston, London: Kluwer Academic Publishers, 1996.

8. Laurinčikas A. On the joint universality of Hurwitz zeta-functions // Šiauliai Math. Semin. 2008. V. 3(11). P. 169–187.

9. Laurinčikas A., Garunkštis R. The Lerch Zeta-Function. Dordrecht, Boston, London: Kluwer Academic Publishers, 2002.

10. Nakamura T. The existence and the non-existence of joint t-universality for Lerch zeta-functions // J. Number Theory 2007. V. 125. P. 424–441.

11. Steuding J. Value-Distribution of L-Functions. Lecture Notes Math. vol. 1877. Berlin, Heidelberg, New York: Springer, 2007.

12. Воронин С. М. Теорема об "универсальности" дзета-функции Римана // Изв. АН СССР. Сер. матем. 1975. Т. 39. С. 475–486 ≡ Math. USSR Izv. 1975. V. 9. P. 443–453.

13. Воронин С. М. О функциональной независимости L-функций Дирихле // Acta Arith. 1975. Т. 27. С. 493–503.

14. Воронин С. М. Аналитические свойства производящих функций Дирихле арифметических объектов. Дис. ... докт. физ.-матем. наук. Москва: МИАН, 1977.

REFERENCES

1. Bagchi, B. 1981, *The statistical behavior and universality properties of the Riemann zeta-function and other allied Dirichlet series*, Ph. D. Thesis, Indian Statistical Institute, Calcutta.

2. Balčiūnas, A., Dubickas, A., Laurinčikas, A. 2019, "On the Hurwitz zeta-function with algebraic irrational parameter", *Mat. Zametki*, vol. 105, No 2, pp. 179–186. (in Russian). ≡ Math. Notes, vol. 105, No 2, pp. 173–179.

3. Billingsley, P. 1968, *Convergence of Probability Measures*, Wiley, New York.

4. Conway, J. B. 1978, *Functions of one complex variable.*, Springer, Berlin, Heidelberg, New York.

5. Gonek, S. M. 1979, *Analytic properties of zeta and L-functions*, Thesis, University of Michigan, Ann Arbor.

6. Karatsuba, A. A., Voronin, S. M. 1992, *The Riemann zeta-function*, Walter de Gruyter, Berlin.

7. Laurinčikas, A. 1996, *Limit Theorems for the Riemann Zeta-Function*, Kluwer Academic Publishers, Dordrecht, Boston, London.

8. Laurinčikas, A. 2008, "On the joint universality of Hurwitz zeta-functions", *Šiauliai Math. Semin.*, vol. 3(11), pp. 169–187.

9. Laurinčikas, A., Garunkštis R. 2002, *The Lerch Zeta-Function*, Kluwer Academic Publishers, Dordrecht, Boston, London.

10. Nakamura, T. 2007, "The existence and the non-existence of joint t-universality for Lerch zeta-functions" // *J. Number Theory*, vol. 125, pp. 424–441.

11. Steuding, J. 2007, *Value-Distribution of L-Functions*, Lecture Notes Math. vol. 1877, Springer, Berlin, Heidelberg, New York.

12. Voronin, S. M. 1975, "Theorem on the "universality" of the Riemann zeta-function", *Izv. Akad. Nauk SSSR.*, vol. 39, pp. 475–486 (in Russian) ≡ *Math. USSR Izv.*, vol. 9, pp.443–453.

13. Voronin, S. M. 1975, "On the functional independence of Dirichlet L-functions", *Acta Arith.*, vol. 27, pp. 493–503 (in Russian).

14. Voronin, S. M. 1977, *Analytic properties of Dirichlet generating functions of arithmetic objects*, doct. diss., MIAS, Moscow (in Russian).

Получено 21.08.2018
Принято к печати 10.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 512.554.3 DOI 10.22405/2226-8383-2018-19-3-231-240

Обобщение задачи А. И. Мальцева о коммутативных подалгебрах на алгебры Шевалле[1]

Левчук Владимир Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры и математической логики Института математики и фундаментальной информатики Сибирского федерального университета, 660041, г. Красноярск, пр. Свободный 79, Сибирский федеральный университет
e-mail: vlevchuk@sfu-kras.ru
Сулейманова Галина Сафиулловна — доктор физико-математических наук, доцент, профессор кафедры ПИМиЕД Хакасского технического института — филиала Сибирского федерального университета, 665017, г. Абакан, ул. Щетинкина 27, Хакасский технический институт — филиал Сибирского федерального университета
e-mail: suleymanova@list.ru

Аннотация

В 1945 году А.И. Мальцев исследовал задачу описания абелевых подгрупп наивысшей размерности в комплексных простых группах Ли. Задача инспирирована доказанной ранее И. Шуром теоремой: *Наивысшая размерность абелевых подгрупп группы $SL(n,\mathbb{C})$ равна $[n^2/4]$ и абелевы подгруппы этой размерности при $n > 3$ переводятся автоморфизмами друг в друга.* Свою задачу А.И. Мальцев решил переходом к комплексным алгебрам Ли. В теории Картана – Киллинга полупростые комплексные алгебры Ли классифицированы с использованием классификации систем корней евклидовых пространств V. С любой неразложимой системой корней Φ и полем K ассоциируют алгебру Шевалле $\mathcal{L}_\Phi(K)$; ее базу дают база определенной абелевой самонормализуемой подалгебры H и элементы e_r ($r \in \Phi$) с H-инвариантным подпространством Ke_r. Элементы e_r ($r \in \Phi^+$) образуют базу нильтреугольной подалгебры $N\Phi(K)$. Методы А. И. Мальцева позднее получили развитие в решении проблемы о больших абелевых подгруппах конечных групп Шевалле. В настоящей статье мы используем разработанные методы для перенесения теоремы А.И. Мальцева на алгебры Шевалле. Мы исследуем следующие задачи:

(A) *Описать коммутативные подалгебры наивысшей размерности в алгебре Шевалле $\mathcal{L}_\Phi(K)$ над произвольным полем K.*

(B) *Описать коммутативные подалгебры наивысшей размерности в подалгебре $N\Phi(K)$ алгебры Шевалле $\mathcal{L}_\Phi(K)$ над произвольным полем K.*

В статье приводится описание коммутативных подалгебр наивысшей размерности алгебры $N\Phi(K)$ классического типа над произвольным полем K с точностью до автоморфизмов алгебры $\mathcal{L}_\Phi(K)$ и подалгебры $N\Phi(K)$.

Ключевые слова: алгебра Шевалле, коммутативная подалгебра, нильтреугольная подалгебра.

Библиография: 18 названий.

Для цитирования:
В. М. Левчук, Г. С. Сулейманова. Обобщение задачи А. И. Мальцева о коммутативных подалгебрах на алгебры Шевалле // Чебышевский сборник, 2018, т. 19, вып. 3, с. 231–240.

[1]Исследование выполнено за счет гранта Российского фонда фундаментальных исследований (проект 16-01-00707).

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 512.554.3 DOI 10.22405/2226-8383-2018-19-3-231-240

Generalization of A. I. Mal'tsev problem on commutativa subalgebras for Chevalley algebras[2]

Levchuk Vladimir Mikhailovich — Dr. Phys.-Math. Sci., professor, head of the department of algebra and logic of Siberian Federal University, Krasnoyarsk, 660041 Russia.
e-mail: vlevchuk@sfu-kras.ru
Suleimanova Galina Safiullanovna — Dr. Phys.-Math. Sci., associate professor, professor of Khakas Tecnical Institute — branch of Siberian Federal University, Abakan, 655017 Russia
e-mail: suleymanova@list.ru

Abstract

In 1945 A. I. Mal'tsev investigated the problem on description of abelian subgroups of largest dimension in complex simple Lie groups. This problem's arisen from the theorem of I. Schur: *The largest dimension of abelian subgroups of the group* $SL(n, \mathbb{C})$ *equals to* $[n^2/4]$ *and abelian subgroups of such dimension for* $n > 3$ *are transformed by automorphisms into each other.* A. I. Mal'tsev solved his problem by the reduction to complex Lie algebras. In Cartan – Killing theory semisimple complex Lie algebras are classified making use of the classification of root systems in Euclidean space V. A Chevalley algebra $\mathcal{L}_\Phi(K)$ is associated with the indecomposable root system Φ and with the field K; the base of the Chevalley algebra consists of the base of certain abelian self-normalized subalgebra H and of the elements e_r $(r \in \Phi)$ with H-invariant subspace Ke_r. The elements e_r $(r \in \Phi^+)$ form a base of niltriangular subalgebra $N\Phi(K)$. Methods of A. I. Mal'tsev were developed for the solving of the problem on large abelian subgroups in finite Chevalley groups. In this article we use the worked out methods for the reduction of A. I. Mal'cev theorem for the Chevalley algebras. We investigate the problems:

(A) *to describe commutative subalgebras of largest dimension in a Chevalley algebra* $\mathcal{L}_\Phi(K)$ *over arbitrary field* K.

(B) *to describe commutative subalgebras of largest dimension in subalgebra* $N\Phi(K)$ *of the Chevalley algebra* $\mathcal{L}_\Phi(K)$ *Over arbitrary field* K.

In this article we give the description of all commutative subalgebras of largest dimension in subalgebra $N\Phi(K)$ of classical type over arbitrary field K up to automorphisms of algebra $\mathcal{L}_\Phi(K)$ and of subalgebra $N\Phi(K)$.

Keywords: Chevalley algebra, commutative subalgebra, niltriangular subalgebra.

Bibliography: 18 titles.

For citation:
V. M. Levchuk, G. S. Suleimanova, 2018, "Generalization of A. I. Mal'tsev problem on commutativa subalgebras for Chevalley algebras" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 231–240.

1. Введение

В 1945 году А.И. Мальцев [1] исследовал задачу описания абелевых подгрупп наивысшей размерности в комплексных простых группах Ли. Задача инспирирована доказанной ранее И. Шуром [2] теоремой:

[2]This work was supported by the Russian Foundation for Basic Research (project no. 16-01-00707)

Наивысшая размерность абелевых подгрупп группы $SL(n,\mathbb{C})$ равна $[n^2/4]$ и абелевы подгруппы этой размерности при $n>3$ переводятся автоморфизмами друг в друга.

Свою задачу А.И. Мальцев решил переходом к комплексным алгебрам Ли.

В теории Картана – Киллинга полупростые комплексные алгебры Ли классифицированы с использованием классификации систем корней евклидовых пространств V. С любой неразложимой системой корней Φ и полем K ассоциируют алгебру Шевалле $\mathcal{L}_\Phi(K)$; ее базу дают база определенной абелевой самонормализуемой подалгебры H и элементы e_r $(r\in\Phi)$ с H-инвариантным подпространством Ke_r, [3].

Методы [1] позднее получили развитие в решении проблемы о больших абелевых подгруппах конечных групп Шевалле, [4], [5], [6], [7], [8], [9], [10], [11], [12].

В настоящей статье мы используем разработанные методы для перенесения основной в [1] теоремы на алгебры Шевалле.

С любой неразложимой системой корней Φ и полем K ассоциируют алгебру Шевалле $L_\Phi(K)$; ее базу составляют база определенной абелевой подалгебры H и элементы e_r $(r\in\Phi)$ такие, что $He_r\subseteq Ke_r$, [3]. Элементы e_r $(r\in\Phi^+)$ образуют базу нильтреугольной подалгебры $N\Phi(K)$. Мы исследуем следующие задачи, записанные в [13].

(A) *Описать коммутативные подалгебры наивысшей размерности в алгебре Шевалле $L_\Phi(K)$ над произвольным полем K.*

(B) *Описать коммутативные подалгебры наивысшей размерности в подалгебре $N\Phi(K)$ алгебры Шевалле $L_\Phi(K)$ над произвольным полем K.*

2. Теорема А.И. Мальцева

В теории Картана – Киллинга полупростые комплексные алгебры Ли классифицированы, наряду с системами корней евклидовых пространств V. Простые комплексные (конечномерные) алгебры Ли $\mathcal{L}=\mathcal{L}_\Phi$ взаимнооднозначно соответствуют 9 сериям приведенных неразложимых систем корней Φ, [14, Таблицы I– IX]. Основной в [1] является

Теорема А.И. Мальцева. *Каждая простая алгебра Ли $\mathcal{L}_\Phi$, исключая тип A_2,B_4,D_4,G_2, с точностью до автоморфизмов имеет только одну коммутативную подалгебру наивысшей размерности с нильпотентными элементами. Эта размерность равна $[n^2/4]$ для алгебр A_{n-1} $(n>3)$, $1+n(n-1)/2$ – для B_n $(n>4)$, $n(n+1)/2$ – для C_n $(n\geq 2)$, $n(n-1)/2$ – для D_n $(n>4)$, $16,27,36,9,5$ – соответственно для E_6,E_7,E_8,F_4,B_3. Алгебра B_4 имеет два класса размерности 7, D_4 – два класса размерности 6 и G_2 – три класса размерности 3.*

Для перенесения теоремы А. И. Мальцева на алгебры Шевалле используем схему ее доказательства и соответствующие методы алгебр Шевалле.

Алгебру Шевалле $\mathcal{L}_\Phi(K)$ ассоциируют с любым полем K и системой корней Φ, характеризуя базой Шевалле $\{e_r\ (r\in\Phi),\ \ h_s\ (s\in\Pi)\}$ с целочисленными структурными константами, где Π – система простых корней (или база) в Φ. Более точно, по теореме Шевалле о базисе

$$e_r*e_{-r}=h_r,\quad h_s*h_r=0,\quad h_s*e_r=\frac{2(r,s)}{(r,r)}\,e_r\quad (r,s\in\Phi);$$

$$e_r*e_s=0\ \ (r+s\notin\Phi\cup\{0\}),\quad e_r*e_s=N_{rs}e_{r+s}=-e_s*e_r\ \ (r+s\in\Phi),$$

где $N_{rs}=\pm1$ или $|r|=|s|<|r+s|$ и $N_{rs}=\pm2$ или Φ типа G_2 и $N_{rs}=\pm2$ или ±3. Произвол в выборе знаков констант N_{rs} описан в [3, 4.2.2].

Известно, что $p(\Phi) := \max\{(r,r)/(s,s) \mid r,s \in \Phi\} = 1, 2$ или (тип G_2) 3. *Высотой корня* r называют сумму $\mathrm{ht}(r)$ коэффициентов в разложении r по базису Π. Фиксируем в Φ систему положительных корней $\Phi^+ \supseteq \Pi$.

Элементы e_r $(r \in \Phi^+)$ образуют базу нильтреугольной подалгебры $N\Phi(K)$. Ее стандартный центральный ряд $L_i = \langle Ke_r \mid r \in \Phi^+,\ \mathrm{ht}\,(r) \geqslant i\rangle$ $(i = 1, 2, \dots)$ при $p(\Phi)!K = K$ есть также и нижний и верхний центральный ряд. Для любого корня r отображение $t \to x_r(t) := exp\ (tad.e_r)$ $(t \in K)$ дает изоморфизм аддитивной группы поля K в группу автоморфизмов $Aut\ \mathcal{L}_\Phi(K)$. Корневые подгруппы $X_r = x_r(K)$ порождают *группу Шевалле* $\Phi(K)$ с унипотентной подгруппой $U\Phi(K) = \langle X_r\ (r \in \Phi^+)\rangle$ [3]. В [1] используется

Лемма 1. В алгебре Ли $\mathcal{L}_\Phi = \mathcal{L}_\Phi(C)$ любая максимальная коммутативная подалгебра с нильпотентными элементами переводится автоморфизмом из $\Phi(C)$ в нильпотентную подалгебру $N\Phi(C)$.

А.И. Мальцев [1] назвал подмножество Ψ системы корней Φ *коммутативным*, если $r + s \notin \Phi$ для любых корней $r, s \in \Psi$. В этом случае коммутативны подмножества корней $w(\Psi)$ для любого элемента w группы Вейля

$$W = W(\Phi) = \langle w_r \mid r \in \Phi\rangle = \langle w_r \mid r \in \Pi\rangle, \quad w_r(x) = x - \frac{2(r,x)}{(r,r)}\, r \ \ (x \in V),$$

а также подалгебра $A_\Psi = \sum_{r\in\Psi} Ke_r$. Наибольший порядок коммутативных множеств корней в Φ оказывается равен наивысшей размерности коммутативных подалгебр алгебры $N\Phi(C)$.

Пусть $\{r\}^+$ — множество корней $s \in \Phi^+$ таких, что в разложении $s - r$ по базе Π все коэффициенты неотрицательны, $T(r)$ и $Q(r)$ – подалгебры в $N\Phi(K)$ с базисом, соответственно, $\{e_s \mid s \in \{r\}^+\}$ и $\{e_s \mid s \in \{r\}^+,\ s \neq r\}$.

Приведем описание коммутативных подмножеств корней в Φ наибольшего порядка, которое вытекает из [1]. Для систем корней типа E_m, $m = 6, 7, 8$, и F_4 используем обозначения из [14] простых корней $\alpha_1, \alpha_2, \dots, \alpha_m$.

Лемма 2. Коммутативные множества наибольшего порядка в системе корней Φ типа $\neq G_2$ исчерпывают, с точностью до ее изометрий $^-$и W-сопряженности, следующие.

Тип A_{n-1}**:** $\{r\}^+$, где r - простой корень с $\bar{r} = r$ или $r + \bar{r} \in \Phi,\ r < \bar{r}$.

Тип B_n**:** $\{2a + b\}^+ \cup \{q\}^+$, где a, b – простые корни, $|a| < |b|$, и q - максимальный короткий корень.

Тип C_n**:** $\{q\}^+$, где q - длинный простой корень.

Тип D_n**:** $\{r\}^+$, где r - простой корень и $r < \bar{r}$ для любой симметрии $^-$.

Тип E_8**:** $\{\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6\}^+$.

Тип E_n**, n=6 или 7 :** $\{\alpha_n\}^+$.

Тип F_4**:** $\{\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4\}^+ \cup \{\alpha_2 + 2\alpha_3 + 2\alpha_4\}^+$.

Учитывая w_s-инвариантность подмножества корней $\Phi^+ \setminus \{s\}$ для любого простого корня s, с помощью леммы 2 получаем

Следствие. Пусть Ψ есть коммутативное подмножество корней из леммы для типа A_n, C_n, D_n, E_6 или E_7. Тогда для любого простого корня $s \notin \Psi$ подмножества Ψ и $w_s(\Psi)$ в Φ^+ совпадают или $^-$-симметричны.

3. Большие абелевы подалгебры в алгебрах $N\Phi(K)$ классических типов

Большой $\mathcal{P}$-подгруппой конечной группы ($\mathcal{P}$ – теоретико-групповое свойство) называют всякую $\mathcal{P}$-подгруппу наибольшего порядка. Абелевы подалгебры наивысшей размерности алгебры Ли назовем *большими абелевыми,* аналогично большим абелевым подгруппам конечной группы Шевалле.

С учетом леммы 1, исследуем большие абелевы подалгебры алгебры $N\Phi(K)$. Их описание с точностью до ее автоморфизмов, в отличие от [1], оказывается более единообразным.

Теорема 1. *В алгебре $N\Phi(K)$ классического типа Φ над любым полем K, с точностью до ее автоморфизмов, большая абелева подалгебра M для типов A_n, D_n и C_n совпадает с идеалом $T(r)$ для единственного простого корня r и размерности, соответственно, $[n^2/4]$, $n(n-1)/2$ и $n(n+1)/2$. В остальных случаях M переводится в идеал автоморфизмом из $Aut\ \mathcal{L}_\Phi(K)$, в частности, для типа B_n $(n>4)$ – в централизатор $C(L_n)$.*

Замечание 1. Для типов E_6 и E_7 большая абелева подалгебра M также совпадает с идеалом $T(r)$ для единственного простого корня r .

В [13] записана **гипотеза (А):** *Всякий коммутативный идеал наивысшей размерности алгебры $N\Phi(K)$ является её коммутативной подалгеброй наивысшей размерности.*

Гипотеза была подтверждена в статье [15], вместе с доказательством существования и описанием больших абелевых идеалов алгебры $N\Phi(K)$.

Отметим, что порядки подалгебр из теоремы Мальцева соответствуют порядкам коммутативных подмножеств корней Ψ из леммы 2.

Для простого числа p подмножество $\Psi \subseteq \Phi$ называем *p-коммутативным*, согласно Е. П. Вдовину [10], если в алгебре Ли $N\Phi(K)$ над любым полем K характеристики p имеем $e_r * e_s = 0$ при всех $r, s \in \Psi$. При $p(\Phi)!K = K$ понятия p-коммутативности и коммутативности, очевидно, совпадают.

Ясно, что для коммутативной подалгебры M алгебры $N\Phi(K)$ над полем K характеристики $p > 0$ множество корней $\mathcal{L}_1(M)$ является p-коммутативным. Из [1], [10] и [11] несложно вытекает

Лемма 4. Наивысшая размерность коммутативных подалгебр алгебры Ли $N\Phi(K)$ над полем K характеристики p равна наибольшему порядку p-коммутативных при $2 \le p \le p(\Phi)$ и коммутативных в остальных случаях множеств корней в Φ.

Доказательство. Когда $H \subseteq T(r_1) + T(r_2) + \cdots + T(r_m)$ и любая замена $T(r_i)$ на $Q(r_i)$ нарушает включение, назовём $\{r_1, r_2, \cdots, r_m\} = \mathcal{L}(H)$ *множеством углов для H.*

Как и в [3, Lemma 5.3.1], далее используем *регулярное упорядочение корней* $>$; тогда из неравенства $\mathrm{ht}(r) > \mathrm{ht}(s)$ следует $r > s$.

Первым углом ненулевого элемента $a \in N\Phi(K)$ назовем корень s, если в разложении $a = \sum_{r\in\Phi^+} \lambda_r e_r$ по базе, упорядоченной согласно возрастанию корней, λ_s есть первый ненулевой коэффициент. Множество первых углов всех элементов подмножества $M \subseteq N\Phi(K)$ обозначаем через $\mathcal{L}_1(M)$.

Утверждение леммы сейчас несложно вытекает из леммы 2 и ее следствия.

В [11] подмножество Ψ системы корней Φ названо *нормальным*, если при $r \in \Psi$ всегда имеем $\{r\}^+ \subseteq \Psi$. Очевидно, каждое подмножество $\Psi \subseteq \Phi$ из леммы 2 нормально и поэтому A_Ψ есть коммутативный идеал.

Доказательство теоремы.

Тип A_n. Пусть A – большая коммутативная подалгебра алгебры $N\Phi(K)$. Рассмотрим случай $n = 2m + 1$. Согласно лемме 2, в этом случае имеется единственное максимальное коммутативное подмножество корней $\{r\}^+$, где r - простой корень и $\bar{r} = r$. Если подалгебра A имеет простой угол $q \neq r$, то при подходящей нумерации простых корней q вошёл бы в $\mathcal{L}_1(A)$, и, следовательно, в некоторое максимальное коммутативное подмножество корней, что противоречит лемме 2. Таким образом, $A \subseteq T(r) + L_2$. Предположим, что $A \subseteq T(r) + L_i$ и A имеет угол s высоты i $(2 \leq i \leq m)$, не входящий в $\{r\}^+$. Тогда подалгебра $n_p(1)(A) \subseteq N\Phi(K)$, где p – простой корень с условием $s - p \in \Phi^+$, $n_p(1)$ – мономиальный элемент группы Шевалле [3], будет иметь угол $s - p \notin \{r\}^+$ высоты $i-1$, что противоречит сделанному выше предположению. Таким образом, A содержится в идеале $T(r)$ и совпадает с ним, в силу максимальности.

Рассмотрим случай $n = 2m$. В этом случае, согласно лемме 2, максимальные коммутативные подмножества корней исчерпываются множествами $\{r\}^+$ и $\{\bar{r}\}^+$, где $r, \bar{r}$ – простые корни, $r + \bar{r} \in \Phi^+$. Как и в рассмотренном выше случае $n = 2m + 1$, получаем, что $A \subseteq T(r) + T(\bar{r})$. Предположим, что $\mathcal{L}_1(A) = \{r\}^+$. Пусть $m > 1$ и

$$x = ae_r + be_{\bar{r}} \mod L_2, \quad a \neq 0,$$

$$y = ce_{r+p} + de_{r+\bar{r}} + fe_{\bar{r}+q} \mod L_3, \quad c \neq 0,$$

где $r + p \in \Phi^+$, $p \neq \bar{r}$, $\bar{r} + q \in \Phi^+$, $q \neq r$. Тогда

$$x * y = -afe_{r+\bar{r}+q} + bce_{r+\bar{r}+p} = 0,$$

следовательно, $b = f = 0$, то есть $x, y \in T(r)$, и $A \supseteq Ke_r$. Тогда, в силу коммутативности, s-проекция элементов из A для всех $s \in \{\bar{r}\}^+ \setminus \{r\}^+$ является нулевой, следовательно, $A \subseteq T(r)$. В случае $\mathcal{L}_1(A) = \{\bar{r}\}^+$ аналогично доказывается, что $A = T(\bar{r})$.

Для типа A_2, когда алгебра Ли $N\Phi(K)$ представляется ассоциированной к алгебре $NT(3, K)$ (нижних) нильтреугольных 3×3 матриц над K с матричными единицами e_{ij} $(1 \leq j < i \leq 3)$. В силу [16, Теорема 3], любая матрица $\alpha = ||a_{uv}|| \in GL(2, K)$ дает здесь автоморфизм

$$\bar{\alpha}: \ e_{i+1,i} \to a_{i1}e_{21} + a_{i2}e_{32} \ (i = 1, 2), \quad e_{31} \to (det\ \alpha)e_{31},$$

причем группа $AutN\Phi(K)$ факторизуется подгруппой центральных автоморфизмов и $\bar{GL}(2, K)$. Поэтому все большие абелевы алгебры Ли $N\Phi(K)$ переводятся здесь друг в друга ее автоморфизмами.

Замечание 2. Последнее утверждение не имеет аналога для соответствующей унитреугольной группы $UT(3, K)$, см. там же ее автоморфизмы. (Элементы $e + e_{21}, e + e_{21} + e_{32}$ не автоморфны, в силу различия их жордановой формы, а при $2K = 0$ различны и их групповые порядки.)

Тип B_n. Рассмотрим случай $2K = K$. Обозначим $p_{i,\pm j} = \varepsilon_i \mp \varepsilon_j$, $p_{i0} = \varepsilon_i$ $(1 \leq j < i \leq n)$, где $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ – ортонормированный базис n-мерного евклидова пространства (ср. [14]). Для краткости будем обозначать $e_{p_{ij}} = e_{ij}$. Для типов B_2 и B_3 идеалы $T(p_{21})$ и $T(p_{32})$ будут единственными коммутативными подалгебрами наивысшей размерности 3 и 5, соответственно.

Согласно [1], для типа $G = B_n$, $n > 3$, большие коммутативные подмножества корней исчерпываются множествами $\{p_{2,-1}\}^+ \cup p_{i0}$, $1 \leq i \leq n$, а при $n = 4$ ещё множеством $\{p_{43}\}^+$. Пусть $p_{10} < p_{21} < \cdots < p_{n,n-1}$. В случае $\mathcal{L}_1(A) = \{p_{43}\}^+$ очевидно, что $A = T(p_{43})$.

Пусть $\mathcal{L}_1(A) = \{p_{2,-1}\}^+ \cup p_{10}$. Если подалгебра A имеет простой угол $q \neq p_{10}$, то при подходящей нумерации простых корней q вошёл бы в $\mathcal{L}_1(A)$, и, следовательно, в некоторое максимальное коммутативное подмножество корней, что противоречит [1]. Таким образом, $A \subseteq T(p_{10}) + L_2$. Предположим, что $A \subseteq T(p_{10}) + L_i$ и A имеет угол $p_{k,k-i}$ высоты i $(i + 1 \leq k \leq n, \ 2 \leq i \leq n - 1)$, не входящий в $\{p_{10}\}^+$. Тогда подалгебра

$n_{k-i+1,k-i}(1)(A) \subseteq N\Phi(K)$ будет иметь угол $p_{k,k-i+1}$ высоты $i-1$, что противоречит сделанному предположению. Таким образом, $A \subseteq T(p_{10})$.

Пусть теперь $\mathcal{L}_1(A) = \{p_{2,-1}\}^+ \cup p_{i0}$, $(1 \le i \le n-1)$. Рассмотрим $a \in A$ вида

$$a = a_{i0}e_{i0} + a_{i+1,0}e_{i+1,0} \mod L_{i+3}, \quad a_{i0} \neq 0.$$

С точностью до подходящего автоморфизма $x_{p_{i+1,i}}(t)$ (где $x_{p_{i+1,i}}(t)$ – корневой элемент группы Шевалле [3]), можем считать, что $a_{i+1,0} = 0$. Тогда $B = n_{i+1,i}(1)(A) \subseteq T(p_{10})$ и $\mathcal{L}_1(B)$ содержит $p_{i+1,0}$, откуда $\mathcal{L}_1(B) = \{p_{2,-1}\}^+ \cup p_{i+1,0}$. Таким образом, подалгебра A переводится автоморфизмом алгебры $L\Phi(K)$ в подалгебру $T(p_{2,-1}) + Ke_{n0}$, являющуюся идеалом.

Рассмотрим случай $2K = 0$. Для типа B_2 большие коммутативные подалгебры наивысшей размерности содержат идеал $T(p_{20})$, являющийся центром алгебры $N\Phi(K)$, и исчерпываются подалгебрами $K(ae_{10} + be_{21}) + T_{20}$, $(a,b) \neq (0,0)$, которые являются идеалами. При $n > 2$ единственным 2-коммутативным множеством, в обозначениях леммы 2, является $\{a\}^+$. Это следует из описания больших абелевых подгрупп группы U типа B_n над полем характеристики 2 [5], а также из того, что каждому 2-коммутативному множеству корней соответствует абелева подгруппа, порождённая соответствующими корневыми подгруппами. По аналогии с типом A_n, $n = 2m+1$, убеждаемся, что идеал $T(a)$ будет единственной коммутативной подалгеброй наивысшей размерности.

Тип C_n рассматривается аналогично типу B_n, случай $2K = 0$.

Тип D_n**.** Уточним описание в [13] больших абелевых идеалов в $N\Phi(K)$. Автоморфизмы алгебры Ли $N\Phi(K)$ типа D_4 описаны в [17, Теорема 6]. Графовые автоморфизмы соответствуют симметриям графа Кокстера системы корней Φ, действующим как симметрическая группа подстановок степени 3 на простых корнях $r_1 = r < r_2 = \bar{r} < q = \bar{q} < r_3 = \bar{\bar{r}}$ ($^-$ – симметрия порядка 3). Когда $2K = K$, любой автоморфизм действует по модулю L_2 как произведение диагонального и графового автоморфизмов. При $2K = 0$ расширение дают автоморфизмы $\widehat{\beta}$, сопоставляемые в [17] каждой матрице $\beta = ||b_{uv}|| \in SL(3,K)$. Если $s = q + r_1 + r_2 + r_3$, то

$$\widehat{\beta}: \ e_{r_i} \to \sum_{m=1}^{3} b_{im}e_{r_m}, \quad e_q \to e_q, \quad e_{q+r_i} \to \sum_{m=1}^{3} b_{im}e_{q+r_m}, \quad e_s \to e_s,$$

$$e_{q+r_i+r_j} \to det \begin{bmatrix} b_{i1} & b_{i2} & b_{i3} \\ b_{j1} & b_{j2} & b_{j3} \\ e_{s-r_1} & e_{s-r_2} & e_{s-r_3} \end{bmatrix} \quad (i \neq j), \quad e_{s+q} \to e_{s+q}.$$

Для простых симметричных корней r и $\bar{r} \neq r$ ($\bar{\bar{r}} = r$) системы Φ типа D_n $(n \ge 4)$ определено [17, Теорема 8] изоморфное вложение $\sim$ подгруппы

$$S := \{A = ||a_{uv}|| \in SL(2,K) \ : \ 2a_{11}a_{12} = 2a_{21}a_{22} = 0\}$$

группы $SL(2,K)$ в группу автоморфизмов алгебры Ли $N\Phi(K)$ по правилу

$$\widetilde{A}: \quad e_r \to a_{11}e_r + a_{12}e_{\bar{r}}, \quad e_{\bar{r}} \to a_{21}e_r + a_{22}e_{\bar{r}}, \quad e_s \to e_s \quad (s \in \Pi \setminus \{r, \bar{r}\}).$$

Умножая произвольный автоморфизм алгебры Ли $N\Phi(K)$ типа D_n на выделенные автоморфизмы, добиваемся его тождественности по модулю L_2, то есть сводим его к известным гиперцентральным автоморфизмам [18].

Доказательство того, что произвольная коммутативная подалгебра алгебры $N\Phi(K)$ совпадает с одним из ее идеалов проводится по аналогии с рассмотренными выше типами.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Мальцев А. И. Коммутативные подалгебры полупростых алгебр Ли // Известия АН СССР. Сер. матем. 1945. Т. 9, № 4. С. 291-300.
2. Schur I. Zur theorie der vertauschbaren matrizen // J. reine und angew. Math. 1905. Vol. 130. P. 66-76.
3. Carter R. Simple groups of Lie type // Wiley and Sons, New York, 1972.
4. Barry M. J. J. Large Abelian subgroups of Chevalley groups // J. Austral. Math. Soc. Ser. A. 1979. Vol. 27. № 1. P. 59-87.
5. Barry M. J. J., Wong W. J. Abelian 2-subgroups of finite symplectic groups in characteristic 2 // J. Austral. Math. Soc. Ser. A. 1982. Vol. 33. № 3. P. 345-350.
6. Wong W. J. Abelian unipotent subgroups of finite orthogonal groups // J. Austral. Math. Soc., Ser. A. 1982. Vol. 32, № 2. P. 223-245.
7. Wong W. J. Abelian unipotent subgroups of finite unitary and symplectic groups // J. Austral. Math. Soc., Ser. A. 1982. Vol. 33, № 2. P. 331-344.
8. Кондратьев А. С. Подгруппы конечных групп Шевалле // Успехи математических наук. 1986. Т. 41, № 1 (247). С. 57-96.
9. Вдовин Е. П. Максимальные порядки абелевых подгрупп в конечных группах Шевалле // Матем. заметки. 2000. Т. 68, вып. 1. С. 53-76.
10. Вдовин Е. П. Большие абелевы унипотентные подгруппы конечных групп Шевалле // Алгебра и логика. 2001. Т. 40, № 5. С. 523-544.
11. Levchuk V. M., Suleimanova G. S. Extremal and maximal normal abelian subgroups of a maximal unipotent subgroup in groups of Lie type // J. Algebra. 2012. Vol. 349, iss. 1, № 1. P. 98-116.
12. Levchuk V. M., Suleimanova G. S. Thompson subgroups and large abelian unipotent subgroups of Lie-type groups // J. Siberian Federal University. Math. & Physics. 2013. Vol. 6, № 1. P. 64-74.
13. Levchuk V. M., Suleimanova G. S. The generalized Mal'cev problem on abelian subalgebras of the Chevalley algebras // Lobachevskii Journal of Mathematics. 2015. Vol. 86. № 4. P. 384-388.
14. Бурбаки Н. Группы и алгебры Ли (главы IV – VI). // М.: Мир, 1976.
15. Кириллова Е.А., Сулейманова Г.С. Коммутативные идеалы наибольшей размерности нильтреугольной подалгебры алгебры Шевалле над полем // Труды института математики и механики УрО РАН. 2018. Т.24, №3. С. 98-108.
16. Левчук В.М. Связи унитреугольной группы с некоторыми кольцами. Ч. 2. Группы автоморфизмов // Сибирский математический журнал. 1983. Т. 24. №. 4. С. 64-80.
17. Левчук В. М. Автоморфизмы унипотентных подгрупп групп Шевалле // Алгебра и логика 1990. Т. 29. № 2. С. 315-338.
18. Левчук В. М., Литаврин А. В. Гиперцентральные автоморфизмы нильтреугольных подалгебр алгебр Шевалле // Сиб. электрон. матем. изв. 2016. Т. 13. С. 467-477.

REFERENCES

1. Mal'tsev A.I. 1945, "Commutative subalgebras of semi-simple Lie algebras", *Izvestia Akad. Nauk SSSR*, Ser. Mat., 1945, vol. 9, no. 4, pp. 291–300 (in Russian)

2. Schur I. 1905, "Zur theorie der vertauschbaren matrizen", *J. reine und angew. Math.*, vol. 130, pp. 66-76.

3. Carter R. 1972, "Simple groups of Lie type", *Wiley and Sons, New York.*

4. Barry M. J. J. 1979, "Large Abelian subgroups of Chevalley groups", *J. Austral. Math. Soc. Ser. A.*, vol. 27, no. 1, pp. 59-87.

5. Barry M. J. J., Wong W. J. 1982, "Abelian 2-subgroups of finite symplectic groups in characteristic 2", *J. Austral. Math. Soc., Ser. A*, vol. 33, no. 3, pp. 345-350.

6. Wong W. J. 1982, "Abelian unipotent subgroups of finite orthogonal groups", *J. Austral. Math. Soc., Ser. A*, vol. 32, no. 2, pp. 223-245.

7. Wong W. J. 1982, "Abelian unipotent subgroups of finite unitary and symplectic groups", *J. Austral. Math. Soc., Ser. A*, vol. 33, no. 2, pp. 331-344.

8. Kondrat'ev A.S. 1986, "Subgroups of ?nite Chevalley groups", *Russian Math. Surveys*, vol. 41, no. 1, pp. 65–118.

9. Vdovin E. P. 2001, "Maximal Orders of abelian Subgroups in Finite Chevalley Groups", *Mat. Zametki*, vol. 69, no. 4, pp. 524–549.

10. Vdovin E. P. 2001, "Large abelian unipotent subgroups of finite Chevalley groups", *Algebra and Logic*, vol. 40, no. 5, pp. 292–305.

11. Levchuk V. M., Suleimanova G. S. 2012, "Extremal and maximal normal abelian subgroups of a maximal unipotent subgroup in groups of Lie type", *J. Algebra*, vol. 349, iss. 1, no 1, pp. 98-116.

12. Levchuk V. M., Suleimanova G. S. 2013, "Thompson subgroups and large abelian unipotent subgroups of Lie-type groups", *Journal of Siberian Federal University. Mathematics & Physics*, vol. 6, no.1, pp. 64-74.

13. Levchuk V. M., Suleimanova G. S. 2015, "The generalized Mal'cev problem on abelian subalgebras of the Chevalley algebras", *Lobachevskii Journal of Mathematics*, vol. 86, no 4, pp. 384-388.

14. N. Bourbaki, Groupes et algebres de Lie (Chapt. IV–VI). Paris.: Hermann, 1968.

15. Kirillova E. A., Suleimanova G. S. "Highest dimension commutative ideals of a niltriangular subalgebra of a Chevalley algebra over a field", *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, vol. 24, no 3, pp. 98-108.

16. Levchuk V. M. 1983, "Connections between a unitriangular group and certain rings. 2. Groups of automorphisms", *Siberian mathematical journal*, vol. 24, no. 4, pp. 543-557.

17. V.M. Levchuk. 1990, "Automorphisms of unipotent subgroups of Chevalley groups", *Algebra and Logic*, vol. 29, no. 2, pp. 211–224.

18. Levchuk V. M., Litavrin A. V. 2016, "Hypercentral automorphisms of nil-triangular subalgebras in Chevalley algebras", *Siberian Electronic mathematical Reports*, vol. 13, pp. 467-477.

Получено 25.06.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.9 DOI 10.22405/2226-8383-2018-19-3-241-256

Приближение квадратичных алгебраических решёток и сеток целочисленными решётками и рациональными сетками

Михляева Анна Владимировна — аспирант кафедры алгебры и дискретной математики, Оренбургского государственного университета, г. Оренбург.
e-mail: white.background.invisible@mail.ru

Аннотация

Данная работа посвящена вопросам приближения квадратичных алгебраических решёток и сеток целочисленными решётками и рациональными сетками.

Даётся общая постановка вопроса о приближении алгебраических решёток и соответствующих сеток целочисленными решётками и рациональными сетками.

В случае простого p вида $p = 4k+3$ или $p = 2$ рассматривается целочисленная решётка, заданная m-й подходящей дробью к числу $\sqrt{p}$. В явном виде выписана соответствующая алгебраическая решётка и обобщённая параллелепипедальная сетка.

Для определения качества соответствующей обобщённой параллелепипедальной сетки определена функция качества, которая для своего вычисления требует $O(N)$ арифметических операций, где N — количество точек сетки. Центральным результатом является алгоритм вычисления функции качества за $O\left(\sqrt{N}\right)$ арифметических операций.

Сформулирована гипотеза о существовании алгоритма, требующего $O(\ln N)$ арифметических операций. Намечен подход для вычисления сумм с целыми частями линейных функций.

Ключевые слова: квадратичные поля, приближение алгебраических сеток, функция качества, обобщённая параллелепипедальная сетка.

Библиография: 27 названий.

Для цитирования:
А. В. Михляева. Приближение квадратичных алгебраических решёток и сеток целочисленными решётками и рациональными сетками // Чебышевский сборник, 2018, т. 19, вып. 3, с. 241–256.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.9 DOI 10.22405/2226-8383-2018-19-3-241-256

Approximation of quadratic algebraic lattices and nets by integer lattices and rational nets

Mikhlyaeva Anna Vladimirovna — Postgraduate Student, Department of Algebra and discrete mathematics, Orenburg state University, Orenburg.
e-mail: white.background.invisible@mail.ru

Abstract

This paper is devoted to the approximation of quadratic algebraic lattices and grids by integer lattices and rational grids.

A General formulation of the problem of approximation of algebraic lattices and corresponding meshes by integer lattices and rational meshes is given.

In the case of a simple p of the form $p = 4k + 3$ or $p = 2$, we consider an integer lattice given $m$by a suitable fraction to the number $\sqrt{p}$. The corresponding algebraic lattice and the generalized parallelepipedal grid are written out explicitly.

To determine the quality of the corresponding generalized parallelepipedal grid, a quality function is defined, which requires $O(N)$ arithmetic operations for its calculation, where N — is the number of grid points. The Central result is an algorithm for computing a quality function for $O\left(\sqrt{N}\right)$ arithmetic operations.

We hypothesize the existence of an algorithm that requires $O(\ln N)$ arithmetic operations. An approach for calculating sums with integral parts of linear functions is outlined.

Keywords: quadratic fields, approximation of algebraic grids, quality function, generalized parallelepipedal grid.

Bibliography: 27 titles.

For citation:
A. V. Mikhlyaeva, 2018, "Approximation of quadratic algebraic lattices and nets by integer lattices and rational nets" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 241–256.

1. Введение

Алгебраические решётки и соответствующие алгебраические сетки вошли в науку, как новое самостоятельное направление в теоретико-числовом методе в приближённом анализе, в 1976 году в работах К. К. Фролова [25], [26]. Главное их достоинство заключается в том, что на них достигается правильный порядок погрешности приближенного интегрирования на классах Коробова [20], [27] и правильный порядок гиперболической дзета-функции решёток [12], [13].

К недостаткам квадратурных формул с алгебраическими сетками относится то, что это квадратурные формулы с весами, причём достаточно сложными. При оценке погрешности приближенного интегрирования возникают большие величины констант, которые трудно оценить. В результате применение таких квадратурных формул на практике весьма проблематично.

В связи с этим возникает вопрос о приближении алгебраических сеток рациональными. Так как рациональные параллелепипедальные сетки дают квадратурные формулы с равными весами только в случае, если они образованы точками решётки, взаимной к целочисленной решётке, то возникает проблема приближения алгебраической решётки целочисленной решёткой.

Пусть у нас есть алгебраическая решётка $\Lambda(t, F) = t\Lambda(F)$, где $\Lambda(F)$ — решётка, состоящая из точек $(\Theta^{(1)}, \ldots, \Theta^{(s)})$, образующих полный набор алгебраически сопряжённых чисел, и $\Theta = \Theta^{(1)}$ пробегает кольцо целых алгебраических чисел чисто вещественного алгебраического поля F. Вопрос о приближении алгебраической решётки $\Lambda(t, F)$ целочисленной решёткой $\Lambda(t)$ можно ставить так:

Найти целочисленную решётку $\Lambda(t)$ такую, что расстояние $\rho(\Lambda(t), \Lambda(t, F))$ минимальное для заданного натурального t.

Теория гиперболической дзета-функции решёток показывает, что наиболее важны те решётки Λ, для которых отношение гиперболического параметра решётки $q(\Lambda)$ к $\det\Lambda$ наибольшее. Определение гиперболического параметра смотри ниже на стр. 246.

Для произвольного вектора $\vec{x}$ его дробной частью называется вектор

$$\{\vec{x}\}=(\{x_1\},\ldots,\{x_s\}).$$

Далее везде под произвольной решёткой $\Lambda\subset\mathbb{R}^s$ мы будем понимать только полные решётки, то есть

$$\Lambda=\{m_1\vec{\lambda}_1+\ldots+m_s\vec{\lambda}_s=\vec{m}\cdot A\,|\vec{m}=(m_1,\ldots,m_s)\in\mathbb{Z}^s\},$$

где $\vec{\lambda}_1=(\lambda_{1\,1},\ldots,\lambda_{1\,s}),\ldots,\vec{\lambda}_s=(\lambda_{s\,1},\ldots,\lambda_{s\,s})$ — система линейно-независимых векторов в $\mathbb{R}^s$, а матрица решётки A задана соотношениями

$$A=\begin{pmatrix}\lambda_{1\,1}&\ldots&\lambda_{1\,s}\\ \vdots&\ddots&\vdots\\ \lambda_{s\,1}&\ldots&\lambda_{s\,s}\end{pmatrix}=\begin{pmatrix}\vec{\lambda}_1\\ \vdots\\ \vec{\lambda}_s\end{pmatrix}.$$

Взаимная решётка $\Lambda^*=\{\vec{x}\,|\,\forall\vec{y}\in\Lambda\ (\vec{x},\vec{y})\in\mathbb{Z}\}$. Непосредственно из определения следует равенство $(q\Lambda)^*=\dfrac{1}{q}\Lambda^*$.

Определение 1. *Для произвольной решётки Λ обобщённой параллелепипедальной сеткой $M(\Lambda)$ называется множество $M(\Lambda)=\Lambda^*\cap G_s$, где $G_s=[0;1)^s$.*

Сетка $M_1(\Lambda)=\Lambda^*\cap[-1;1)^s$.

Обобщённой параллелепипедальной сеткой II рода $M'(\Lambda)$ называется множество

$$M'(\Lambda)=\{\vec{x}\,|\,\vec{x}=\{\vec{y}\},\vec{y}\in M_1(\Lambda)\}.$$

Пусть $\vec{a}=(a_0,a_1,\ldots,a_{s-1})$ — целочисленный вектор такой, что многочлен

$$P_{\vec{a}}(x)=\sum_{\nu=0}^{s-1}a_\nu x^\nu+x^s \tag{1}$$

неприводим над полем рациональных чисел $\mathbb{Q}$ и все корни $\Theta_\nu\,(\nu=1,\ldots,s)$ многочлена (1) действительные.

Обозначим через $T(\vec{a})$ матрицу степеней алгебраически сопряжённых целых алгебраических чисел $\Theta_1,\ldots,\Theta_s$ — корней многочлена $P_{\vec{a}}(x)$:

$$T(\vec{a})=\begin{pmatrix}1&\ldots&1\\ \Theta_1&\ldots&\Theta_s\\ \vdots&\vdots&\vdots\\ \Theta_1^{s-1}&\ldots&\Theta_s^{s-1}\end{pmatrix}, \tag{2}$$

а через $\vec{\Theta}=(\Theta_1,\ldots,\Theta_s)$ — вектор полного набора алгебраически сопряжённых чисел — корней многочлена $P_{\vec{a}}(x)$.

Для любого $t>0$ решётка $\Lambda(t\cdot T(\vec{a}))$ называется алгебраической. Она имеет вид

$$\Lambda(t\cdot T(\vec{a}))=\left\{\vec{x}=\left(t\sum_{\nu=1}^{s}\Theta_1^{\nu-1}m_\nu,\ldots,t\sum_{\nu=1}^{s}\Theta_s^{\nu-1}m_\nu\right)=t\cdot\vec{m}\cdot T(\vec{a})\,\middle|\,\vec{m}\in\mathbb{Z}^s\right\}.$$

Таким образом, алгебраическая решётка $\Lambda(t\cdot T(\vec{a}))$ имеет базис $\vec{\lambda}_\nu=t\cdot(\Theta_1^{\nu-1},\ldots,\Theta_s^{\nu-1})$ $(\nu=1,\ldots,s)$.

Естественной научной проблемой является вопрос о приближении алгебраической сетки рациональной сеткой. Из теории обобщённых параллелепипедальных сеток и квадратурных формул с этими сетками возникает следующая постановка.

Дана алгебраическая решётка $\Lambda(t \cdot T(\vec{a}))$ и натуральное t, требуется найти целочисленную решётку $\Lambda_{\mathbb{Z}}(t \cdot T(\vec{a}))$ такую, чтобы величина гиперболического параметра решётки $\Lambda_{\mathbb{Z}}(t \cdot T(\vec{a}))$ была наибольшей, когда

$$\lim_{t\to\infty} \frac{1}{t}\Lambda_{\mathbb{Z}}(t \cdot T(\vec{a})) = \Lambda(T(\vec{a})).$$

В связи с этим можно дать следующее определение наилучшего приближения алгебраической решётки $\Lambda(t, F)$ целочисленной решёткой $\Lambda(t)$.

Целочисленная решётка $\Lambda(t)$ называется наилучшим приближением алгебраической решётки $\Lambda(t, F)$ с показателем β, если для любого натурального $t_1 < t$ выполняется неравенство

$$\frac{q(\Lambda(t)) \cdot \ln^{\beta} \det \Lambda(t)}{\det \Lambda(t)} > \frac{q(\Lambda(t_1)) \cdot \ln^{\beta} \det \Lambda(t_1)}{\det \Lambda(t_1)}.$$

Такая постановка является новой и ранее не встречалась в литературе.

Принципиальный вопрос, который связан с такой постановкой, заключается в следующем.

Какое минимальное значение β допустимо в определении наилучшего приближения алгебраической решётки целочисленной?

Если окажется, что $\beta > 0$, то это означает, что для наилучших приближений алгебраических решёток имеется аналог теоремы Туэ для приближения алгебраических чисел.

В работе [18] рассматривались вопросы приближения алгебраических решёток в случае квадратичных полей, а в работе [21] сделаны попытки рассмотреть общие подходы в этой тематике.

Целью данной работы является рассмотрение вопроса о качестве указанных приближений в случае квадратичных алгебраических решёток.

2. Обозначения и необходимые факты

Рассмотрим квадратичное поле $F = \mathbb{Q}(\sqrt{p})$, где p — простое число и $p = 2$ или $p \equiv 3 \pmod 4$. Тогда кольцо целых алгебраических чисел $\mathbb{Z}_F$ имеет вид: $\mathbb{Z}_F = \{n + k\sqrt{p} | n, k \in \mathbb{Z}\}$.

Через $\Lambda(F)$ обозначим алгебраическую решётку поля F: $\Lambda(F) = \{(\Theta^{(1)}, \Theta^{(2)}) | \Theta = \Theta^{(1)} \in \mathbb{Z}_F\}$ и $\Theta^{(1)}$, $\Theta^{(2)}$ — целые алгебраически сопряжённые числа.

Таким образом, $\Theta^{(1)} = n + k\sqrt{p}$, $\Theta^{(2)} = n - k\sqrt{p}$ $n, k \in \mathbb{Z}$ и $\Theta^{(1)}$, $\Theta^{(2)}$ — корни уравнения $x^2 - 2nx + n^2 - pk^2 = 0$. Базис решётки $\Lambda(F)$ имеет вид: $\vec{\lambda}_1 = (1, 1)$, $\vec{\lambda}_2 = (\sqrt{p}, -\sqrt{p})$, а детерминант решётки $\det \Lambda(F) = 2\sqrt{p}$. Базис взаимной решётки $\Lambda^*(F)$ имеет вид: $\vec{\lambda}_1^* = \left(\frac{1}{2}, \frac{1}{2}\right)$, $\vec{\lambda}_2^* = \left(\frac{\sqrt{p}}{2p}, -\frac{\sqrt{p}}{2p}\right)$ и детерминант взаимной решётки $\det \Lambda^*(F) = \frac{\sqrt{p}}{2p}$.

Рассмотрим разложение $\sqrt{p}$ в цепную периодическую дробь:

$$\sqrt{p} = q_0 + [(q_1, \ldots, q_n, 2q_0)] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots}}}}}$$

с периодом $(q_1, \ldots, q_n, 2q_0)$. Через $\frac{P_m}{Q_m}$ будем обозначать m-ую подходящую дробь к $\sqrt{p}$. Таким образом,

$$\sqrt{p} = \frac{P_m}{Q_m} + \frac{(-1)^m \theta_m}{Q_m^2}, \quad 0 < \theta_m < 1 \quad (m = 0, 1, \ldots). \tag{3}$$

Через $\Lambda_m(F)$ будем обозначать алгебраическую решётку, заданную равенствами:

$$\Lambda_m(F) = \{(Q_m(n + k\sqrt{p}), Q_m(n - k\sqrt{p}))|n, k \in \mathbb{Z}\},$$

а через $\Lambda_m(p)$ — целочисленную решётку, заданную равенствами:

$$\Lambda_m(p) = \{(Q_m n + kP_m, Q_m n - kP_m)|n, k \in \mathbb{Z}\}.$$

Базис решётки $\Lambda_m(F)$ имеет вид $\vec{\lambda}_{m,1} = (Q_m, Q_m)$, $\vec{\lambda}_{m,2} = (Q_m\sqrt{p}, -Q_m\sqrt{p})$, а детерминант решётки $\det\Lambda_m(F) = 2Q_m^2\sqrt{p}$. Базис взаимной решётки $\Lambda_m^*(F)$ имеет вид:

$$\vec{\lambda}_{m,1}^* = \left(\frac{1}{2Q_m}, \frac{1}{2Q_m}\right), \quad \vec{\lambda}_{m,2}^* = \left(\frac{\sqrt{p}}{2pQ_m}, -\frac{\sqrt{p}}{2pQ_m}\right)$$

и детерминант взаимной решётки $\det\Lambda_m^*(F) = \frac{\sqrt{p}}{2pQ_m^2}$.

Для целочисленной решётки $\Lambda_m(p)$ базис имеет вид $\vec{\lambda}_{m,1,Z} = (Q_m, Q_m)$, $\vec{\lambda}_{m,2,Z} = (P_m, -P_m)$, а детерминант решётки $\det\Lambda_m(p) = 2Q_mP_m$. Базис взаимной решётки $\Lambda_m^*(p)$ имеет вид:

$$\vec{\lambda}_{m,1,Z}^* = \left(\frac{1}{2Q_m}, \frac{1}{2Q_m}\right), \quad \vec{\lambda}_{m,2,Z}^* = \left(\frac{1}{2P_m}, -\frac{1}{2P_m}\right)$$

и детерминант взаимной решётки $\det\Lambda_m^*(p) = \frac{1}{2P_mQ_m}$.

Лемма 1. *Для $m \geqslant 0$ справедливы соотношения*

$$\det\Lambda_m(F) = \det\Lambda_m(p) + (-1)^m 2\theta_m,$$
$$\vec{\lambda}_{m,1} = \vec{\lambda}_{m,1,Z}, \quad \vec{\lambda}_{m,2} = \vec{\lambda}_{m,2,Z} + \left(\frac{(-1)^m\theta_m}{Q_m}, \frac{(-1)^{m+1}\theta_m}{Q_m}\right).$$

Доказательство. Доказательство получается прямыми вычислениями. □

Лемма 2. *Для $m \geqslant 0$ справедливы соотношения*

$$\det\Lambda_m^*(F) = \det\Lambda_m^*(p) + 2\left(\det\Lambda_m^*(p)\right)^2 \frac{(-1)^{m+1}\theta_m}{1 + \frac{(-1)^m\theta_m}{P_mQ_m}},$$
$$\vec{\lambda}_{m,1}^* = \vec{\lambda}_{m,1,Z}^*, \quad \left\|\vec{\lambda}_{m,2}^* - \vec{\lambda}_{m,2,Z}^*\right\|_1 = \frac{\theta_m}{\det\Lambda_m(p)\left(P_m + \frac{(-1)^m\theta_m}{Q_m}\right)}.$$

Доказательство. Доказательство получается прямыми вычислениями. □

Рассмотрим следующие две сетки:

$$M_1(\Lambda_m(F)) = \Lambda_m^*(F) \cap [-1; 1)^s, \quad M(\Lambda_m(p)) = \Lambda_m^*(p) \cap [0; 1)^s.$$

Нетрудно видеть, что

$$M_1(\Lambda_m(F)) = \left\{ \left(\frac{n}{2Q_m} + \frac{\sqrt{p}k}{2pQ_m}, \frac{n}{2Q_m} - \frac{\sqrt{p}k}{2pQ_m}\right) \middle| \, k \in A(n), |n| \leqslant 2Q_m - 1 \right\},$$
$$A(n) = \left\{ k \middle| \begin{array}{ll} -2P_m < k < 2P_m, & \text{при } n = 0, \\ -2P_m + \frac{P_mn}{Q_m} < k < 2P_m - \frac{P_mn}{Q_m}, & \text{при } n = 1, \dots 2Q_m - 1, \\ -2P_m - \frac{P_mn}{Q_m} < k < 2P_m - \frac{P_mn}{Q_m}, & \text{при } n = -1, \dots -2Q_m + 1; \end{array} \right\},$$
$$M(\Lambda_m(p)) = \left\{ \left(\frac{n}{2Q_m} + \frac{k}{2P_m}, \frac{n}{2Q_m} - \frac{k}{2P_m}\right) \middle| \, k \in B(n), 0 \leqslant n \leqslant 2Q_m - 1 \right\},$$
$$B(n) = \left\{ k \middle| \begin{array}{ll} k = 0, & \text{при } n = 0, \\ -\frac{P_mn}{Q_m} \leqslant k \leqslant \frac{P_mn}{Q_m}, & \text{при } n = 1, \dots Q_m - 1, \\ -2P_m + \frac{P_mn}{Q_m} < k < 2P_m - \frac{P_mn}{Q_m}, & \text{при } n = Q_m, \dots 2Q_m - 1; \end{array} \right\}.$$

Определение 2. *Квадратурной формулой с обобщённой параллелепипедальной сеткой II типа и весовой функцией $\rho(\vec{x})$ называется формула вида*

$$\int_0^1 \cdots \int_0^1 f(\vec{x})d\vec{x} = (\det\Lambda)^{-1} \sum_{\vec{x}\in M'(\Lambda)} \rho_{\vec{x}} f(\vec{x}) - R_{N'(\Lambda)}[f],$$

$$\text{где} \quad \rho_{\vec{x}} = \sum_{\vec{y}\in M_1(\Lambda),\{\vec{y}\}=\vec{x}} \rho(\vec{y}), \quad N'(\Lambda) = |M'(\Lambda)|,$$

$R_{N'(\Lambda)}[f]$ *— погрешность квадратурной формулы.*

Для погрешности квадратурной формулы с обобщённой параллелепипедальной сеткой II рода на классе E_s^α справедлива оценка[1]

$$R_{N'(\Lambda)}[E_s^\alpha(C)] = \sup_{f\in E_s^\alpha(C)} |R_{N'(\Lambda)}[f]| \leqslant CB\cdot c_1(\alpha)^s \zeta_H(\Lambda|\alpha),$$

где

$$c_1(\alpha) = 2^{\alpha+1}\left(3+\frac{2}{\alpha-1}\right), \quad \zeta_H(\Lambda|\alpha) = \sum_{\vec{x}\in\Lambda}{}'(\overline{x}_1\ldots\overline{x}_s)^{-\alpha}.$$

Для гиперболической дзета-функции $\zeta_H(\Lambda|\alpha$ произвольной решётки Λ справедлива обобщённая теорема Бахвалова [14]

$$\begin{array}{lcll} \zeta_H(\Lambda|\alpha) & \leqslant & C_3(\alpha,s)C_1(\Lambda)^s & \text{при} \quad q(\Lambda)=1, \\ \zeta_H(\Lambda|\alpha) & \leqslant & C_4(\alpha,s)q^{-\alpha}(\Lambda)(\ln q(\Lambda)+1)^{s-1} & \text{при} \quad q(\Lambda)>1, \end{array} \tag{4}$$

где гиперболический параметр решётки

$$q(\Lambda) = \min_{\vec{x}\in\Lambda\setminus\{\vec{0}\}} q(\vec{x})$$

имеет простой геометрический смысл: *гиперболический крест $K_s(T)$ не содержит ненулевых точек решётки Λ при $T<q(\Lambda)$.*

Гиперболическим крестом называется область

$$K_s(T) = \{\vec{x} \mid q(\vec{x}) \leqslant T\},$$

где $q(\vec{x}) = \overline{x}_1\cdot\ldots\cdot\overline{x}_s$ — усечённая норма $\vec{x}$, и для вещественного x обозначаем $\overline{x} = \max(1,|x|)$ ([19], 1963).

В работе [15] доказана следующая асимптотическая формула.

Обозначим через $\zeta_{D_0}(\alpha|F)$ дзета-функцию Дедекинда главных идеалов квадратичного поля F: $\zeta_{D_0}(\alpha|F) = \sum_{(\omega)} |N(\omega)|^{-\alpha}$, тогда $\zeta'_{D_0}(\alpha|F) = -\sum_{(\omega)} \ln(N(\omega))|N(\omega)|^{-\alpha}$.

Теорема 1. *Справедливо асимптотическое равенство*

$$\zeta_H(\Lambda(t)|\alpha) = \frac{2(\det\Lambda)^\alpha \zeta_{D_0}(\alpha|F)}{R}\cdot\frac{\ln\det\Lambda(t)}{(\det\Lambda(t))^\alpha} -$$

$$-\frac{2(\det\Lambda)^\alpha\left(\ln(\det\Lambda)\,\zeta_{D_0}(\alpha|F)+\zeta'_{D_0}(\alpha|F)\right)}{R(\det\Lambda(t))^\alpha} + \frac{2(\det\Lambda)^\alpha\zeta_{D_0}(\alpha|F)}{(\det\Lambda(t))^\alpha}\left(\theta_1(\alpha)+\frac{\theta_2(\alpha)}{\operatorname{sh}\left(\frac{\alpha R}{2}\right)}\right),$$

где $|\theta_1(\alpha)|\leqslant 1$ и $\frac{1}{\varepsilon_0^{(1)\frac{\alpha}{2}}} \leqslant \theta_2(\alpha) \leqslant \varepsilon_0^{(1)\frac{\alpha}{2}}$, ε_0 — фундаментальная единица квадратичного поля F и R — регулятор этого поля.

[1] Здесь и далее символ $\sum'$ обозначает, что из области суммирования исключён нулевой набор.

Доказательство. Доказательство см. [15]. □

Хорошо известно, что граничной функцией класса $E_s^2\left(\cdot, \frac{\pi^2}{6}\right)$ для параллелепипедальных сеток является функция $h(x,y) = 9(1-2\{x\})^2(1-2\{y\})^2$, поэтому для оценки качества сетки $M(\Lambda_m(p))$ можно использовать функцию

$$H(M(\Lambda_m(p))) = \frac{9}{2P_mQ_m}\sum_{n=0}^{2Q_m-1}\sum_{k\in B(n)}\left(1-2\left(\frac{n}{2Q_m}+\frac{k}{2P_m}\right)\right)^2\left(1-2\left(\frac{n}{2Q_m}-\frac{k}{2P_m}\right)\right)^2.$$

Будем для краткости называть это выражение функцией качества. Для вычисления функции качества обобщённой параллелепипедальной сетки $M(\Lambda_m(p))$ требуется $O(N(P_m,Q_m))$ арифметических операций, где $N(P_m,Q_m)$ — количество точек сетки $M(\Lambda_m(p))$.

Цель данной работы — найти алгоритм вычисления функции качества за $O(\sqrt{N(P_m,Q_m)})$ арифметических операций.

3. Преобразование функции качества

Прежде всего, подсчитаем количество слагаемых в выражении для функции качества, которое обозначим через $N = N(P,Q)$, где $P = P_m$, $Q = Q_m$.

Лемма 3. *Для функции качества справедливо равенство* $N = N(P,Q) = 2PQ$.

Доказательство. Действительно,

$$N = \sum_{n=0}^{2Q-1}|B(n)|, \quad |B(n)| = \begin{cases} 1, & \text{при } n = 0, \\ 1+2\left[\frac{P\cdot n}{Q}\right], & \text{при } n = 1,\dots Q-1, \\ 2P-1, & \text{при } n = Q, \\ 1+2\left[2P-\frac{P\cdot n}{Q}\right], & \text{при } n = Q+1,\dots 2Q-1. \end{cases}$$

Отсюда следует, что

$$N = 2Q + 2(P-1) + 2\sum_{n=1}^{Q-1}\left(\left[\frac{P\cdot n}{Q}\right]+\left[P-\frac{P\cdot n}{Q}\right]\right) = 2Q+2(P-1)+2(Q-1)(P-1) = 2PQ,$$

так как

$$\left[\frac{P\cdot n}{Q}\right]+\left[P-\frac{P\cdot n}{Q}\right] = P-\left\{\frac{P\cdot n}{Q}\right\}-\left\{-\frac{P\cdot n}{Q}\right\} = P-1 \quad \text{при } n = 1,2,\dots,Q-1.$$

□

Далее нам потребуются полные суммы дробных долей $S_{\nu,\mu}(P,Q)$, которые задаются равенствами:

$$S_{\nu,\mu}(P,Q) = \frac{1}{Q}\sum_{n=1}^{Q-1}\left(\frac{n}{Q}\right)^{\nu}\left\{\frac{P\cdot n}{Q}\right\}^{\mu}, \quad \nu,\mu \geqslant 0.$$

Мы будем рассматривать только случай $(P,Q) = 1$. Такие суммы рассматривались в работах [1]–[7], [16], [23]–[24]. Аналогичные неполные суммы дробных долей были детально изучены в работах [8]–[11].

Наряду с обозначением $H(M(\Lambda_m(p)))$ будем использовать $H(P,Q)$:

$$H(P,Q) = \frac{9}{N}\sum_{n=0}^{2Q-1}\sum_{k\in B(n)}\left(1-2\left(\frac{n}{2Q}+\frac{k}{2P}\right)\right)^2\left(1-2\left(\frac{n}{2Q}-\frac{k}{2P}\right)\right)^2.$$

Нетрудно видеть, что

$$H(P,Q)=\frac{9}{N}\sum_{n=0}^{2Q-1}\sum_{k\in B(n)}\left(\left(1-\frac{n}{Q}\right)^2-\left(\frac{k}{P}\right)^2\right)^2.$$

Обозначим через $S(n)$ внутреннюю сумму:

$$S(n)=\sum_{k\in B(n)}\left(\left(1-\frac{n}{Q}\right)^2-\left(\frac{k}{P}\right)^2\right)^2,$$

тогда

$$H(P,Q)=\frac{9}{N}\sum_{n=0}^{2Q-1}S(n).$$

Обозначим через $T(n)$ величину $T(n)=\left[\frac{P\cdot n}{Q}\right]$. Ясно, что $T(n+Q)=P+T(n)$.

Лемма 4. *При $n=1,\dots,Q-1$ справедливо равенство*

$$B(Q-n)=B(Q+n)=\left\{k\,\middle|\,\frac{Pn}{Q}-P<k<P-\frac{Pn}{Q}\right\}.$$

Доказательство. Действительно, при $n=1,\dots,Q-1$ из определения множества $B(n)$ имеем

$$B(Q-n)=\left\{k\,\middle|\,\frac{Pn}{Q}-P\leqslant k\leqslant P-\frac{Pn}{Q}\right\}=\left\{k\,\middle|\,\frac{Pn}{Q}-P<k<P-\frac{Pn}{Q}\right\},$$

так как $\frac{Pn}{Q}$ — нецелое число в силу $(P,Q)=1$.

Аналогично, имеем

$$B(Q+n)=\left\{k\,\middle|\,\frac{Pn}{Q}-P<k<P-\frac{Pn}{Q}\right\},$$

что и доказывает утверждение леммы. □

Лемма 5. *Справедливо равенство*

$$H(P,Q)=\frac{9}{N}\left(S(0)+S(Q)+2\sum_{n=1}^{Q-1}S(n)\right).$$

Доказательство. Действительно, из определения величины $S(n)$ и леммы (4) имеем

$$S(Q-n)=\sum_{k\in B(Q-n)}\left(\left(\frac{n}{Q}\right)^2-\left(\frac{k}{P}\right)^2\right)^2=\sum_{k\in B(Q+n)}\left(\left(-\frac{n}{Q}\right)^2-\left(\frac{k}{P}\right)^2\right)^2=S(Q+n).$$

Отсюда следует утверждение леммы. □

Лемма 6. *Справедливы равенства:*
при $n=0$ $S(0)=1$;
при $n=1,\dots,Q-1$

$$S(n)=\left(1-\frac{n}{Q}\right)^4(1+2T(n))-2\left(1-\frac{n}{Q}\right)^2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}+$$
$$+\frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4};$$

при $n=Q$

$$S(Q)=\frac{(P-1)(2P-1)(3P^2-3P-1)}{15P^3}.$$

Доказательство. Действительно, при $n = 0$ имеем:

$$S(0) = \sum_{k\in B(0)} \left(1 - \left(\frac{k}{P}\right)^2\right)^2 = \sum_{k=0} \left(1 - \left(\frac{k}{P}\right)^2\right)^2 = 1.$$

При $n = 1, \ldots, Q-1$ получим:

$$S(n) = \left(1 - \frac{n}{Q}\right)^4 |B(n)| - 2\left(1 - \frac{n}{Q}\right)^2 \sum_{k\in B(n)} \left(\frac{k}{P}\right)^2 + \sum_{k\in B(n)} \left(\frac{k}{P}\right)^4.$$

Имеем $|B(n)| = 1 + 2T(n)$ и

$$\sum_{k\in B(n)} \left(\frac{k}{P}\right)^2 = \frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2},$$

$$\sum_{k\in B(n)} \left(\frac{k}{P}\right)^4 = \frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4}.$$

Отсюда следует, что

$$S(n) = \left(1 - \frac{n}{Q}\right)^4 (1 + 2T(n)) - 2\left(1 - \frac{n}{Q}\right)^2 \frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2} + \\ + \frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4}.$$

При $n = Q$ получим:

$$S(Q) = \sum_{k\in B(Q)} \left(\frac{k}{P}\right)^4 = 2\sum_{k=1}^{P-1} \left(\frac{k}{P}\right)^4 = \frac{P(P-1)(2P-1)(3P^2-3P-1)}{15P^4}.$$

□

Для краткости положим $t(n) = \left\{\frac{P\cdot n}{Q}\right\}$, тогда $T(n) = \frac{P\cdot n}{Q} - t(n)$ и

$$S_{\nu,\mu}(P,Q) = \frac{1}{Q}\sum_{n=1}^{Q-1} \left(\frac{n}{Q}\right)^\nu t^\mu(n), \quad \nu, \mu \geqslant 0.$$

Теорема 2. *Справедливо равенство*

$$H(P,Q) = \frac{9}{N}\left(\frac{2}{5}P + \frac{2}{3P} - \frac{1}{15P^3} + 2\sum_{n=1}^{Q-1}\left(1 + 2T(n) - 2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2} + \right.\right. \\ + \frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4} - \\ -4\frac{n}{Q}\left(1 + 2T(n) - \frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}\right) + \\ + \left(\frac{n}{Q}\right)^2\left(6(1+2T(n)) - 2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}\right) - \\ \left.\left. - \left(\frac{n}{Q}\right)^3 4(1+2T(n)) + \left(\frac{n}{Q}\right)^4 (1+2T(n))\right)\right).$$

Доказательство. Действительно, из лемм 5 и 6 следует, что

$$H(P,Q)=\frac{9}{N}\left(1+2\sum_{n=1}^{Q-1}S(n)+\frac{(P-1)(2P-1)(3P^2-3P-1)}{15P^3}\right)=$$
$$=\frac{9}{N}\left(\frac{2}{5}P+\frac{2}{3P}-\frac{1}{15P^3}+2\sum_{n=1}^{Q-1}S(n)\right).$$

Далее имеем:

$$S(n)=\left(1-\frac{n}{Q}\right)^4(1+2T(n))-2\left(1-\frac{n}{Q}\right)^2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}+$$
$$+\frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4}=$$
$$=S_0(n)+\frac{n}{Q}S_1(n)+\left(\frac{n}{Q}\right)^2S_2(n)+\left(\frac{n}{Q}\right)^3S_3(n)+\left(\frac{n}{Q}\right)^4S_4(n),$$

где

$$S_0(n)=1+2T(n)-2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}+$$
$$+\frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4};$$
$$S_1(n)=-4\left(1+2T(n)-\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}\right);$$
$$S_2(n)=6(1+2T(n))-2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2};$$
$$S_3(n)=-4(1+2T(n));\quad S_4(n)=1+2T(n).$$

Отсюда следует, что

$$H(P,Q)=\frac{9}{N}\left(\frac{2}{5}P+\frac{2}{3P}-\frac{1}{15P^3}+2\sum_{n=1}^{Q-1}\left(1+2T(n)-2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}+\right.\right.$$
$$+\frac{T(n)(T(n)+1)(2T(n)+1)(3T^2(n)+3T(n)-1)}{15P^4}-$$
$$-4\frac{n}{Q}\left(1+2T(n)-\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}\right)+$$
$$+\left(\frac{n}{Q}\right)^2\left(6(1+2T(n))-2\frac{T(n)(T(n)+1)(2T(n)+1)}{3P^2}\right)-$$
$$\left.\left.-\left(\frac{n}{Q}\right)^3 4(1+2T(n))+\left(\frac{n}{Q}\right)^4(1+2T(n))\right)\right).$$

□

4. Об одном подходе для вычисления сумм с целыми частями

Пусть $(P,Q)=1$ и рассмотрим простейшую сумму целых частей

$$S(P,Q)=\sum_{n=0}^{Q-1}\left[\frac{Pn}{Q}\right],$$

которую можно легко вычислить

$$S(P,Q)=\sum_{n=0}^{Q-1}\frac{Pn}{Q}-\sum_{n=0}^{Q-1}\left\{\frac{Pn}{Q}\right\}=\frac{P(Q-1)}{2}-\sum_{n=0}^{Q-1}\left\{\frac{n}{Q}\right\}=\frac{P(Q-1)}{2}-\frac{(Q-1)}{2}=\frac{(P-1)(Q-1)}{2}.$$

Этот метод при переходе к более сложным суммам вызывает при реализации существенные трудности.

Рассмотрим другой метод, который, на наш взгляд, имеет перспективы для обобщения. Мы будем считать, что $P=P_m$, $Q=Q_m$, где P_m и Q_m — числители и знаменатели m-ой подходящей дроби, а $q_0,\ldots,q_m$ — неполные частные. Воспользуемся представлением

$$n=yQ_{m-1}+x,\quad\begin{cases}0\leqslant y\leqslant q_m-1,\quad 0\leqslant x\leqslant Q_{m-1}-1, & \text{при } 0\leqslant n<q_mQ_{m-1},\\ y=q_m,\quad 0\leqslant x\leqslant Q_{m-2}-1 & \text{при } q_mQ_{m-1}\leqslant n\leqslant Q_m-1.\end{cases}$$

Заметим, что

$$\left[\frac{Pn}{Q}\right]=\left[\frac{P_{m-1}n}{Q_{m-1}}+\frac{(-1)^{m-1}n}{Q_mQ_{m-1}}\right]=\left[\frac{P_{m-1}n}{Q_{m-1}}\right]=P_{m-1}y+\left[\frac{P_{m-1}x}{Q_{m-1}}\right].$$

Отсюда следует рекуррентное соотношение при $m\geqslant 2$

$$S(P_m,Q_m)=\sum_{y=0}^{q_m-1}\sum_{x=0}^{Q_{m-1}-1}\left(P_{m-1}y+\left[\frac{P_{m-1}x}{Q_{m-1}}\right]\right)+\sum_{x=0}^{Q_{m-2}-1}\left(P_{m-1}q_m+\left[\frac{P_{m-1}x}{Q_{m-1}}\right]\right)=$$
$$=\frac{q_m(q_m-1)}{2}P_{m-1}Q_{m-1}+q_mS(P_{m-1},Q_{m-1})+q_mP_{m-1}Q_{m-2}+S(P_{m-2},Q_{m-2}).$$

При $m=0$ имеем $Q_0=1$ и

$$S(P_0,Q_0)=\sum_{n=0}^{Q_0-1}\left[\frac{P_0n}{Q_0}\right]=0.$$

Если $Q_1=1$, то $S(P_1,Q_1)=0$. Пусть $Q_1=q_1>1$, тогда

$$S(P_1,Q_1)=\sum_{n=0}^{q_1-1}\left[\frac{(q_0q_1+1)n}{q_1}\right]=q_0\frac{(q_1(q_1-1)}{2}=\frac{(P_1-1)(Q_1-1)}{2}$$

и утверждение леммы верно при $m\leqslant 1$. Далее по индукции имеем:

$$S(P_m,Q_m)=\frac{q_m(q_m-1)}{2}P_{m-1}Q_{m-1}+q_m\frac{(P_{m-1}-1)(Q_{m-1}-1)}{2}+$$
$$+q_mP_{m-1}Q_{m-2}+\frac{(P_{m-2}-1)(Q_{m-2}-1)}{2}=\frac{q_mP_{m-1}q_mQ_{m-1}}{2}-\frac{q_mP_{m-1}}{2}-\frac{q_mQ_{m-1}}{2}+\frac{q_m}{2}+$$
$$+q_mP_{m-1}Q_{m-2}+\frac{P_{m-2}Q_{m-2}}{2}-\frac{P_{m-2}}{2}-\frac{Q_{m-2}}{2}+\frac{1}{2}=\frac{q_mP_{m-1}q_mQ_{m-1}}{2}-\frac{P_m}{2}-\frac{Q_m}{2}+$$
$$+\frac{q_mP_{m-1}Q_{m-2}}{2}+\frac{P_mQ_{m-2}}{2}+\frac{q_m}{2}+\frac{1}{2}=\frac{q_mP_{m-1}Q_m}{2}-\frac{P_m}{2}-\frac{Q_m}{2}+\frac{P_mQ_{m-2}}{2}+\frac{q_m}{2}+\frac{1}{2}=$$
$$=\frac{P_mQ_m}{2}-\frac{P_m}{2}-\frac{Q_m}{2}+\frac{1}{2}+R_m,$$

где

$$R_m=\frac{q_m}{2}+\frac{P_mQ_{m-2}}{2}-\frac{P_{m-2}Q_m}{2}=0,$$

так как по известному тождеству для подходящих дробей имеем

$$P_{m-2}Q_m-P_mQ_{m-2}=q_m.$$

5. Заключение

Теорема 2 позволяет вычислять значение функции качества за $O\left(\sqrt{N(P_m, Q_m)}\right)$ арифметических операций. Мы предполагаем, что найденное выражение для функции качества можно просуммировать по n. В результате должно получиться выражение через числители и знаменатели подходящих дробей к $\sqrt{p}$ и неполные частные. Искомое выражение должно будет позволить вычислять значение функции качества за $O(\ln N(P_m, Q_m))$ арифметических операций.

По-видимому, осуществление этой программы может потребовать значительных ресурсов, так как вычисление в конечном виде более простого выражения

$$H_p(a) = \frac{9}{p}\sum_{n=0}^{p-1}\left(1-2\frac{n}{p}\right)^2\left(1-2\left\{\frac{an}{p}\right\}\right)^2$$

потребовало 50 страниц подробного математического текста (см. [6]).

На возможное использование симметрии в лемме 4 обратил внимание А. В. Родионов, за что выражаю ему свою благодарность.

Также выражаю свою благодарность научному руководителю профессору Н. М. Добровольскому за постановку задачи, полезное обсуждение и постоянное внимание к работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Вронская Г. Т. Квадратичное отклонение плоских сеток [Текст]/ автореферат диссертации на соискание ученой степени канд. физ.-мат. наук: 01.06.06 / Г. Т. Вронская. – М., 2005. – 10 с.

2. Вронская Г. Т. Квадратичное отклонение плоских сеток / Дис. ... канд. физ.-мат. наук. – М.: МПГУ, 2005.

3. Вронская Г. Т., Добровольский Н. М. О двумерных сетках Воронина // Чебышевский сборник 2004 Т. 5. Вып. 1(9). – Тула: Изд-во ТГПУ им. Л. Н. Толстого. С. 74–86.

4. Вронская Г. Т., Добровольский Н. М., Родионова О. В. Сравнения суммы и произведения (тезисы)// Материалы всероссийской конференции "Современные проблемы математики, механики и информатики" ТулГУ. Тула, 2002.

5. Вронская Г. Т., Добровольский Н. М., Родионова О. В. Сравнения, суммы и произведения по приведенной системе вычетов // Известия ТулГУ. Сер. Математика. Механика. Информатика. Т. 8. Вып. 1. Тула, 2002. С. 10–28.

6. Вронская Г. Т., Добровольский Н. Н. Отклонения плоских сеток: Моногр. / Под ред. Н. М. Добровольского. – Тула, 2012.

7. Вронская Г. Т., Родионова О. В. Квадратичное отклонение плоских сеток. – Тула: Изд-во ТГПУ им. Л. Н. Толстого, 2005.

8. Добровольская В. Н. Неполные суммы дробных долей // Чебышевский сборник. Тула, 2004. Т. 5, вып. 2 (10). С. 43–48.

9. Добровольская В. Н. Формула Пика и неполные суммы дробных долей // Изв. Тул. гос. ун-та. Сер. Математика. Механика. Информатика. Т. 10. Вып. 1. Тула: Изд-во ТулГУ, 2004. С. 5–11.

10. Добровольская В. Н. Отклонение плоских параллелепипедальных сеток // Чебышевский сборник. Тула, 2005. Т. 6. Вып. 1 (13). С. 87–97.

11. Добровольская В. Н. Элементарный метод дробных долей Виноградова – Коробова и отклонение плоских сеток Бахвалова // Чебышевский сборник. 2005. Т. 6, вып. 2(14). С. 138–144.

12. Добровольская Л. П., Добровольский М. Н., Добровольский Н. М., Добровольский Н. Н. Многомерные теоретико-числовые сетки и решётки и алгоритмы поиска оптимальных коэффициентов. – Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2012. – 283 с. http://elibrary.ru/item.asp? id=20905960.

13. Добровольская Л. П., Добровольский М. Н., Добровольский Н. М., Добровольский Н. Н. Гиперболические дзета-функции сеток и решёток и вычисление оптимальных коэффициентов // Чебышевский сборник. 2012. Т. 13, вып. 4(44). С. 4–107.

14. Добровольский Н. М. Гиперболическая дзета функция решёток. / Деп. в ВИНИТИ 24.08.84, N 6090–84.

15. Добровольский Н. М., Добровольский Н. Н., Соболева В. Н., Соболев Д. К., Юшина (Климова) Е. И. Гиперболическая дзета-функция решётки квадратичного поля // Чебышевский сб., 2015. Т. 16, вып. 4. С. 100–149. С. 47–52.

16. Добровольский Н. М., Есаян А. Р., Пихтильков С. А., Родионова О. В., Устян А. Е. Об одном алгоритме поиска оптимальных коэффициентов // Известия ТулГУ. Сер. Математика. Механика. Информатика. Т. 5, вып. 1. Тула, 1999. С. 51–71.

17. Добровольский Н. М., Рощеня А. Л. О непрерывности гиперболической дзета-функции решёток // Изв. Тул. гос. ун-та. Сер. Математика. Механика. Информатика. Т. 2. Вып. 1. Тула: Изд-во ТулГУ, 1996. С. 77–87.

18. Климова Е. И., Добровольский Н. Н. Квадратичные поля и квадратурные формулы // Материалы XV Международной конференции Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения, посвященной столетию со дня рождения доктора физико-математических наук, профессора Московского государственного университета имени М. В. Ломоносова Коробова Николая Михайловича. – Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2018. С. 308–310.

19. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. – М.: Физмат-гиз, 1963.

20. Коробов Н. М. Теоретико-числовые методы в приближенном анализе. (второе издание) М.: МЦНМО, 2004. 288 с.

21. Родионов А. В. О рациональных приближениях алгебраических сеток // Материалы XV Международной конференции Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения, посвященной столетию со дня рождения доктора физико-математических наук, профессора Московского государственного университета имени М. В. Ломоносова Коробова Николая Михайловича. – Тула: Изд-во Тул. гос. пед. ун-та им. Л. Н. Толстого, 2018. С. 321–310.

22. Родионов А. В., Чуприн С. Ю. О гиперболических параметрах решётки линейного сравнения // Известия ТулГУ. Естественные науки. Вып. 1. Ч. 1. – Тула: Изд-во ТулГУ, 2014. С. 50–62.

23. Родионова О. В. Рекуррентные формулы первого порядка для степенных сумм дробных долей // Сб.: "Всероссийская научная конференция "Современные проблемы математики, механики, информатики". – Тула, 2000. – С. 50-51.

24. Родионова О. В. Обобщенные параллелепипедальные сетки и их приложения / Дис. ... канд. физ.-мат. наук. – М.: МПГУ, 2000.

25. Фролов К. К. Оценки сверху погрешности квадратурных формул на классах функций // ДАН СССР. 1976. Т. 231. № 4. С. 818–821.

26. Фролов К. К. Квадратурные формулы на классах функций. / Дис. ... канд. физ.-мат. наук. – М.: ВЦ АН СССР, 1979.

27. Шарыгин И. Ф. Оценки снизу погрешности квадратурных формул на классах функций // Журн. вычисл. мат. и мат. физики. 7. 1963. № 4. С. 784–802.

REFERENCES

1. Vronskaya, G. T. 2005, “Quadratic deviation of flat grids” Abstract of Ph.D. dissertation: 01.06.06 / G. T. Vronskaya. – M., – 10 c.

2. Vronskaya, G. T. 2005, “Quadratic deviation of flat grids” / Ph.D. Thesis. Moscow. MSPU.

3. Vronskaya, G. T., Dobrovol’skii, N. M. 2004, “On two-dimensional Voronin grids”, Chebyshevskii sb,Tula, Izd-vo TSPU them. L.N. Tolstoy, vol. 5, no. 1(9). pp. 74–86.

4. Vronskaya, G. T., Dobrovol’skii, N. M., Rodionova, O. V. 2002, “Comparisons sums and works (abstracts)”, Materials of all-Russian conference "Modern problems of mathematics, mechanics and computer science"TulSU. Tula.

5. Vronskaya, G. T.,Dobrovol’skii, N. M., Rodionova, O. V. 2002, "Comparisons, amounts and products on the reduced system of deductions News Of Tulgu. Ser. Mathematics. Mechanics. Informatics.,Tula, vol. 8, no. 1, pp. 10–28.

6. Vronskaya, G. T., Dobrovol’skii, N. N. 2012, "Deviations of flat grids. monograph edited by N. M. Dobrovol’skii. Tula.

7. Vronskaya, G. T., Rodionova, O. V. 2005, "Quadratic deviation of flat grids Tula, izd-vo TSPU them. L. N. Tolstoy.

8. Dobrovol’skaya, V. N. 2004, "Amount incomplete or fractions Chebyshevskii sb., Tula, vol. 5, no. 2 (10), pp. 43–48.

9. Dobrovol’skaya, V. N. 2004, "The formula of the Peak and partial sums of the fractional share Izv. Tul. st. un-ty. Ser. Mathematics. Mechanics.Informatics. Tula: Izd-vo Tulgu, vol. 10, no. 1, pp. 5–11.

10. Dobrovol’skaya, V. N. 2005, "The deviation of the flat parallelepipedal grids Chebyshevskii sb. Tula, vol. 6, no. 1 (13), pp. 87–97.

11. Dobrovol’skaya, V. N. 2005, "The basic method of fractional shares Vinogradova – Korobova and deviation of flat Bakhvalov grids Chebyshevskii sb. vol. 6, no. 2(14), pp. 138–144.

12. Dobrovol'skaya, L. P., Dobrovol'skii, M. N., Dobrovol'skii, N. M., Dobrovol'skii, N. N. 2012, "Multidimensional number-theoretic grids and lattices and algorithms for finding the optimal coefficients Tula: Izd-vo Tul. st. ped. un-ty them. L. N. Tolstoy. – 283 p. http://elibrary.ru/item.asp? id=20905960.

13. Dobrovol'skaya, L. P., Dobrovol'skii, M. N., Dobrovol'skii, N. M., Dobrovol'skii, N. N. 2012, "Hyperbolic Zeta functions of grids and lattices and calculation of optimal coefficients Chebyshevskii sb. vol. 13, no. 4(44), pp. 4–107.

14. Dobrovol'skii, N. M. 1984, "The hyperbolic Zeta function of lattices", Dep. v VINITI, no. 6090–84.

15. Dobrovol'skii, N. M., Dobrovol'skii, N. N., Soboleva,V. N., Sobolev, D. K., Yushina(Klimova), E. I. 2015, "Hyperbolic Zeta function of the lattice of a quadratic field", Chebyshevskii sb. vol. 16, no. 4, pp. 100–149. pp. 47–52.

16. Dobrovol'skii, N. M., Esayan, A. R., Pikhtilkov, S. A., Rodionova, O. V., Ystyan, A. E. 1999, "On one algorithm for finding optimal coefficients Izvestiya Tulgu. Ser. Mathematics. Mechanics. Informatics.Tula. Vol. 5, no. 1, pp. 51–71.

17. Dobrovol'skii, N. M. & Roshhenya, A.L. 1996, "On continuity of the hyperbolic Zeta function of lattices", Izvestiya TulGU. Seriya Matematika. Mekhanika. Informatika, vol. 2, no. 1, pp. 77–87.

18. Klimova,E. I., Dobrovol'skii, N. N. 2018, "Quadratic fields and quadrature formulas", Proceedings of the XV International conference Algebra, number theory and discrete geometry: modern problems and applications, dedicated to the centenary of the doctor of physical and mathematical Sciences, Professor of Moscow state University named after M. V. Lomonosov Korobov Nikolai Mikhailovich. Tula: Publishing house. GOS. PED. UN-TA im. L. N. Tolstoy. pp. 308-310.

19. Korobov, N.M. 1963, Teoretiko-chislovye metody v priblizhennom analize [Number-theoretic methods in approximate analysis], Fizmat-giz, Moscow, Russia.

20. Korobov, N. M. 2004, "Numerical-theoretic methods in approximate analysis Moscow: mtsnmo. 288 p.

21. Rodionov, A. V. 2018, "On rational approximations of algebraic grids Proceedings of the XV International conference Algebra, number theory and discrete geometry: modern problems and applications, dedicated to the centenary of the doctor of physical and mathematical Sciences, Professor of M. V. Lomonosov Moscow state University Nikolai Mikhailovich Korobov. Tula: Publishing house. GOS. PED. UN-TA im. L. N. Tolstoy. pp. 321-310.

22. Rodionov, A. V., Chuprin, S. Yu. 2014, "On hyperbolic parameters of the lattice of linear comparison Izvestiya Tulgu. Natural science. Issue. 1. CH. 1. — Tula: Publishing house of Tulgu. pp. 50–62.

23. Rodionova, O. V. 2000, "Recurrent formulas of the first order for power sums of fractional fractions Sat.:"All-Russian scientific conference "Modern problems of mathematics, mechanics, Informatics Tula, pp. 50-51.

24. Rodionova, O. V. 2000, "Generalized parallelepipedal grids and their applications Dis. ... kand. p. Mat. sciences'. Moscow. Moscow state pedagogical University.

25. Frolov, K. K. 1976, "Upper estimates of the error of quadrature formulas on classes of functions DAN USSR. vol. 231, no. 4, pp. 818–821.

26. Frolov, K. K. 1979, "Quadrature formulas on classes of functions Dis.... kand. p. Mat. sciences'. M.: VTS an SSSR.

27. Sharugin, I. F. 1983, "Lower estimates of the error of quadrature formulas on classes of functions Journal. compute. mate. and mate. physics. vol. 7, no 4, pp. 784–802.

Получено 28.08.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.17+519.114 DOI 10.22405/2226-8383-2018-19-3-257-269

Об алгебре и арифметике биномиальных и гауссовых коэффициентов

Пачев Урусби Мухамедович — доктор физико-математических наук, доцент, профессор кафедры геометрии и высшей алгебры, Кабардино-Балкарский государственный университет имени Х. М. Бербекова.
e-mail: urusbi@rambler.ru

Аннотация

В работе рассматриваются вопросы, касающиеся алгебраических и арифметических свойств таких комбинаторных чисел как биномиальные, полиномиальные и гауссовы коэффициенты.

Для центральных биномиальных коэффициентов $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ установлено новое свойство сравнимости по модулю $p^3 \cdot (2p-1)$, не равному степени простого числа, где p и $(2p-1)$ — простые числа, при этом используется теорема Волстенхолма о том, что при $p \geqslant 5$ эти коэффициенты соответственно сравнимы с числами 2 и 1 по модулю p^3.

В части, относящейся к гауссовым коэффициентам $\binom{n}{k}_q$ исследованы алгебраические и арифметические свойства этих чисел. Пользуясь алгебраической интерпретацией гауссовых коэффициентов, установлено, что число k-мерных подпространств n-мерного векторного пространства над конечным полем из q элементов равно числу $(n-k)$-мерных его подпространств, при этом число q от которого зависит гауссовый коэффициент должно быть степенью простого числа, являющегося характеристикой этого конечного поля.

Получены оценки снизу и сверху для суммы $\sum_{k=0}^{n} \binom{n}{k}_q$ всех гауссовых коэффициентов, достаточно близкие к ее точному значению (формула для точного значения такой суммы пока ещё не установлена), а также асимптотическая формула при $q \to \infty$. В виду отсутствия удобной производящей функции для гауссовых коэффициентов мы пользуемся исходным определением гауссового коэффициента $\binom{n}{k}_q$, при этом считаем, что $q > 1$.

При исследовании арифметических свойств делимости и сравнимости гауссовых коэффициентов используется понятие первообразного корня по данному модулю. Получены условия делимости гауссовых коэффициентов $\binom{p}{k}_q$ и $\binom{p^2}{k}_q$ на простое число p, а также вычислена сумма всех этих коэффициентов по модулю простого числа p.

В заключительной части приводятся некоторые нерешенные задачи теории чисел, связанные с биномиальными и гауссовыми коэффициентами, которые могут представлять интерес для дальнейших исследований.

Ключевые слова: центральные биномиальные коэффициенты, теорема Волстенхолма, гауссовый коэффициент, сумма гауссовых коэффициентов, делимость на простое число, сравнение по данному модулю, первообразный корень по данному модулю.

Библиография: 17 названий.

Для цитирования:
У. М. Пачев. Об алгебре и арифметике биномиальных и гауссовых коэффициентов // Чебышевский сборник, 2018, т. 19, вып. 3, с. 257–269.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.17+519.114 DOI 10.22405/2226-8383-2018-19-3-257-269

On algebra and arithmetic of binomial and gaussian coefficients

Pachev Urusbi Muhamedovich — doctor of physical and mathematical sciences, associate professor, professor of the department of geometry and higher school, Kabardino-Balkarian state university named after H.M. Berbekov.
e-mail: urusbi@rambler.ru

Abstract

In this paper we consider questions relating to algebraic and arithmetic properties of such binomial, polynomial and Gaussian coefficients.

For the central binomial coefficients $\binom{2p}{p}$ and $\binom{2p-1}{p-1}$, a new comparability property modulo $p^3 \cdot (2p-1)$, which is not equal to the degree of a prime number, where p and $(2p-1)$ are prime numbers, Wolstenholm's theorem is used, that for $p \geqslant 5$ these coefficients are respectively comparable with the numbers 2 and 1 modulo p^3.

In the part relating to the Gaussian coefficients $\binom{n}{k}_q$, the algebraic and arithmetic properties of these numbers are investigated. Using the algebraic interpretation of the Gaussian coefficients, it is established that the number of k-dimensional subspaces of an n-dimensional vector space over a finite field of q elements is equal to the number of $(n-k)$ -dimensional subspaces of it, and the number q on which The Gaussian coefficient must be the power of a prime number that is a characteristic of this finite field.

Lower and upper bounds are obtained for the sum $\sum_{k=0}^{n} \binom{n}{k}_q$ of all Gaussian coefficients sufficiently close to its exact value (a formula for the exact value of such a sum has not yet been established), and also the asymptotic formula for $q \to \infty$. In view of the absence of a convenient generating function for Gaussian coefficients, we use the original definition of the Gaussian coefficient $\binom{n}{k}_q$, and assume that $q > 1$.

In the study of the arithmetic properties of divisibility and the comparability of Gaussian coefficients, the notion of an antiderivative root with respect to a given module is used. The conditions for the divisibility of the Gaussian coefficients $\binom{p}{k}_q$ and $\binom{p^2}{k}_q$ by a prime number p are obtained, and the sum of all these coefficients modulo a prime number p.

In the final part, some unsolved problems in number theory are presented, connected with binomial and Gaussian coefficients, which may be of interest for further research.

Keywords: central binomial coefficients, Wolstenholme's theorem, Gaussian coefficient, the sum of Gaussian coefficients, divisibility by prime number, congruences modulo, primitive roots for this module.

Bibliography: 17 titles.

For citation:
U. M. Pachev, 2018, "On algebra and arithmetic of binomial and gaussian coefficients", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 257–269.

1. Введение

В работе рассматриваются некоторые вопросы, относящиеся к таким смежным областям математики как комбинаторика, алгебра и теория чисел. Многие комбинаторные числа представляют собой алгебраические выражения в общем случае дробного вида и нужно установить их целостность, а также делимость на степени простых чисел. Например, для некоторых

вопросов нужно знать наивысший показатель с которым входит данное простое число p в разложение $n!$ на простые множители. Этот показатель, как известно, оказывается равным сумме $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots$, где $[\ ]$ — целая часть числа. Отсюда получается независимое от комбинаторики доказательство целости полиномиального коэффициента $\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$, где $n_1+n_2+\ldots+n_k=n$ и $n_i\geqslant 0$. При этом конечно нужно подсчитать сколько раз входит простое число p в числитель и знаменатель этого выражения и ещё воспользоваться очевидным свойством: $[\alpha+\beta]\geqslant[\alpha]+[\beta]$.

Многочисленные подобные утверждения о целости различных выражений составленных из факториалов можно найти в книге P. Bachmann [1].

В теории чисел большое внимание уделяется вопросу делимости и сравнимости центральных биномиальных коэффициентов $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$, для простого числа p. Первый результат в этом вопросе был получен Волстенхолмом [2] в 1862 г., установившим, что выполняются сравнения $\binom{2p}{p}\equiv 2 \pmod{p^3}$ или что то же самое $\binom{2p-1}{p-1}\equiv 1 \pmod{p^3}$. С помощью этого результата мы в теореме 1 устанавливаем ещё одно свойство сравнимости центральных биномиальных коэффициентов по модулю не равному степени простого числа.

Ближайшим обобщением биномиальных коэффициентов являются полиномиальные коэффициенты, которые появляются в полиномиальной формуле

$$(x_1+\ldots+x_k)^n=\sum_{x_1+\ldots+x_k=n}\binom{n}{n_1,n_2,\ldots,n_k}x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k},$$

где

$$\binom{n}{n_1,n_2,\ldots,n_k}=\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$$

есть полиномиальный коэффициент.

Для них по сравнению с биномиальными коэффициентами мало известных результатов, имеющих приложения особенно в теории чисел. В связи с этим мы в теореме 2 переносим результат предложения 1 о делимости биномиальных коэффициентов на простое число на полиномиальные коэффициенты и как следствие получаем ещё одно доказательство малой теоремы Ферма (относительно трёх имеющихся доказательств этой теоремы см. [3]).

Ещё одним из обобщений биномиальных коэффициентов являются гауссовы коэффициенты, называемые ещё q-биномиальными коэффициентами. Они были введены Гауссом в [4] для решения некоторых важных вопросов теории чисел, в частности для определения знака так называемой гауссовой суммы. Мы будем пользоваться современным обозначением гауссовых коэффициентов, а именно гауссовый коэффициент $\binom{n}{k}_q$ определяется равенством

$$\binom{n}{k}_q=\frac{\left(q^n-1\right)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}$$

При $q=1$ получаем неопределённость вида $\frac{0}{0}$, но если перейти к пределу то

$$\lim_{q\to 1}\binom{n}{k}_q=\binom{n}{k}=\frac{n!}{k!\,(n-k)!}$$

и значит, $\binom{n}{k}_q$ есть обобщение биномиального коэффициента.

Несмотря на то, что гауссовый коэффициент задаётся дробью, тем не менее при каждом значении q, n и k этот коэффициент получается целым числом, иначе говоря, $\binom{n}{k}_q$ есть целочисленный многочлен от q см. [5]. Относительно гауссовых коэффициентов и их применении в алгебре, точнее в теории p-групп, см. [6, 7].

С помощью гауссовых коэффициентов удаётся решить один вопрос о числе k-мерных и $(n-k)$-мерных подпространств n-мерного векторного пространства над конечным полем F_q из

q элементов. Особый интерес представляет вопрос о сумме $\sum_{k=0}^{n} \binom{n}{k}_q$ гауссовых коэффициентов. Для неё не удаётся получить точное значение как в случае биномиальных коэффициентов, ввиду чего мы даём только оценки сверху и снизу и её асимптотику при $q \to \infty$.

Пользуясь понятием первообразного корня по данному модулю p мы доказываем свойство делимости гауссовых коэффициентов $\binom{p}{k}_q$ на простое число p, а также вычисляем сумму всех гауссовых коэффициентов по модулю простого числа p.

2. Арифметические свойства биномиальных и полиномиальных коэффициентов

Биномиальные коэффициенты являются самыми известными среди всех комбинаторных чисел. Сначала они определяются как число k-элементных подмножеств n-элементного множества, называемое числом сочетаний без повторений из n элементов по k элементов. Оно обозначается через C_n^k и равно $\frac{n!}{k!(n-k)!}$, где $0 \leqslant k \leqslant n$.

Эти же числа появляются в биномиальной формуле для $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, где $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ есть биномиальный коэффициент из n по k.

Биномиальные коэффициенты могут быть изучены с различных точек зрения, например, с выявлением интересных алгебраических и арифметических свойства этих чисел.

Мы не будем рассматривать широко известные алгебраические тождества с биномиальными коэффициентами. Гораздо больший интерес представляют исследования арифметических свойств делимости биномиальных коэффициентов.

Самый простейший факт, связанный с делимостью биномиальных коэффициентов на простое число, содержится в следующем утверждении.

Предложение 1. *Если p — простое число и $1 \leqslant k \leqslant p-1$, то биномиальный коэффициент $\binom{p}{k}$ делится на p.*

Доказательство см. [8], где даются два доказательства.

Особый интерес представляют свойства сравнимости для центральных биномиальных коэффициентов вида $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ по модулю степеней числа p. Относительно них известен следующий результат.

Теорема (Волстенхолм). *Пусть простое число $p \geqslant 5$. Тогда $\binom{2p}{p} \equiv 2 \pmod{p^3}$ или, что то же самое, $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$.*

Доказательство было дано Волстенхолмом [2] в 1862 г.

Доказательство также приводится в [3], опираясь на понятие сравнения по любому модулю степеней простого числа p для рациональных чисел, при этом используются также свойства поля классов вычетов $\mathbb{Z}_p$.

Заметим, что без указанных этих дополнительных средств легко доказывается более слабый результат о том, что $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

Действительно, воспользуемся известным соотношением для биномиальных коэффициентов $\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \ldots + \binom{p}{p}^2$.

Учитывая, что $\binom{p}{0} = \binom{p}{p} = 1$ в силу предложения 1 получим $\binom{2p}{p} = 2 + p^2 k$ при некотором целом k, оттуда $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

Согласно теореме Волстенхолма центральные биномиальные коэффициенты $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ при простом p содержатся в классах вычетов $2 \pmod{p^3}$ и $1 \pmod{p^3}$ соответственно, а в силу предложения 1 $\binom{p}{k}$ при $1 \leqslant k \leqslant p-1$ лежит в классе $0 \pmod{p}$. Возникает вопрос в каких классах вычетов будут содержатся $\binom{2p}{p}$ и $\binom{2p-1}{p-1}$ по модулю $p^3\,(2p-1)$, если $2p-1$ также есть простое число. Ответ даёт следующая

Теорема 1. *Если p и $2p-1$ являются простыми числами, то для центральных биномиальных коэффициентов выполняются следующие условия сравнения*

1) $\binom{2p}{p} \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$;

2) $\binom{2p-1}{p-1} \equiv 1-8p^3 \pmod{p^3\cdot(2p-1)}$.

Доказательство.

1) Пусть p и $2p-1$ простые числа. В силу теоремы Волстенхолма имеем сравнение $\binom{2p}{p} \equiv 2 \pmod{p^3}$ и ещё выполняется сравнение $\binom{2p}{p} \equiv 0 \pmod{2p-1}$. Поэтому рассматриваем систему сравнений

$$\begin{cases} x \equiv 2 \pmod{p^3}, \\ x \equiv 0 \pmod{2p-1}, \end{cases}$$

единственным решением которой по модулю $p^3\cdot(2p-1)$ в силу китайской теоремы об остатках является класс вычетов, содержащий число $\binom{2p}{p}$. Следуя доказательству китайской теоремы об остатках в случае двух сравнений по модулям $m_1 = p^3$ и $m_2 = 2p-1$ имеем $x \equiv c_1M_1M_1' + c_2M_2M_2' \pmod{p^3\cdot(2p-1)}$, где в нашем случае $c_1 = 2$, $c_2 = 0$ — правые части этой системы, при этом $M_1 = m_2 = 2p-1$, $M_2 = m_1 = p^3$. Находим обратные для M_1 и M_2 соответственно по модулям p^3 и $2p-1$. Имеем $M_1M_1' \equiv 1 \pmod{m_1}$, т. е. $(2p-1)\,M_1' \equiv 1 \pmod{p^3}$. Решая это сравнение по способу Эйлера получаем $M_1' \equiv (2p-1)^{\varphi\left(p^3\right)-1} \pmod{p^3}$, т. е. $M_1' \equiv (2p-1)^{p^3-p^2-1} \pmod{p^3}$. Применяя биномиальную формулу имеем $M_1' \equiv \sum\limits_{k=0}^{p^3-p^2-1} \binom{p^3-p^2-1}{k}(2p)^k(-1)^{p^3-p^2-1-k} \pmod{p^3}$ и, оставляя в правой части слагаемые при $0 \leqslant k \leqslant 2$, получаем $M_1' \equiv -1+\left(p^3-p^2-1\right)2p-\binom{p^3-p^2-1}{2}4p^2 \pmod{p^3}$, откуда $M_1' \equiv -1-2p-4p^2 \pmod{p^3}$, т. е. можем взять $M_1' = -4p^2-2p-1$.

Аналогично устанавливается, что $M_2' \equiv 8 \pmod{2p-1}$, т. е. $M_2' = 8$.

Тогда по формуле $x \equiv c_1M_1M_1'+c_2M_2M_2' \pmod{p^3\cdot(2p-1)}$, получаем, что $x \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$, и значит, $\binom{2p}{p} \equiv 2\left(1-8p^3\right) \pmod{p^3\cdot(2p-1)}$.

2) Так как $\binom{2p-1}{p-1} = \frac{(p+1)\cdot(p+2)\cdot\ldots\cdot(2p-1)}{(p-1)!}$ и при этом по условию $2p-1$ — простое число, то $\binom{2p-1}{p-1} \equiv 0 \pmod{2p-1}$. Тогда как и в предыдущем случае рассматриваем систему сравнений

$$\begin{cases} x \equiv 1 \pmod{p^3}, \\ x \equiv 0 \pmod{2p-1}, \end{cases}$$

единственным решением которой по модулю $p^3\,(2p-1)$ является класс вычетов, содержащий число $\binom{2p-1}{p-1}$. Следуя предыдущим рассуждениям, получаем, что $\binom{2p-1}{p-1} \equiv 1-8p^2 \pmod{p^3\cdot(2p-1)}$.

Теорема 1 доказана. □

Относительно других результатов, связанных с теоремой Волстенхолма, см. [9], а что касается вопросов разложимости центральных биномиальных коэффициентов в произведение таких же коэффициентов см. [10, 11].

Перейдём теперь к рассмотрению полиномиальных (мультиномиальных) коэффициентов, при этом мы не будем затрагивать их комбинаторные интерпретации.

Полиномиальные коэффициенты появляются в полиномиальной формуле

$$(x_1+x_2+\ldots+x_k)^n = \sum_{\substack{n_1+n_2+\ldots+n_k=n \\ n_1\geqslant 0,\, n_2\geqslant 0,\,\ldots,\, n_k\geqslant 0}} \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k},$$

где

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$$

— есть полиномиальный коэффициент из n по $n_1, n_2, \ldots, n_k$. В частном случае $k = 2$ получаем биномиальные коэффициенты $\binom{n}{n_1,n_2} = \binom{n}{n_1} = \binom{n}{n_2}$.

На полиномиальные коэффициенты мы переносим результат предложения 1 о делимости на простое число p.

Теорема 2. *Если p — простое число и $n_i \neq p$ при всех $i = 1, 2, \ldots, k$, то справедлива делимость $p \mid \binom{n}{n_1,n_2,\ldots,n_k}$.*

Доказательство. По определению полиномиального коэффициента имеем

$$n_1 + n_2 + \ldots + n_k = p, \quad n_1 \geqslant 0, n_2 \geqslant 0, \ldots, n_k \geqslant 0,$$

и значит, в силу условия $n_i \neq 0$ получаем, что $0 \leqslant n_i < p$. Тогда $p \nmid n_i!$ и значит, $p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!$.

Но так как $\frac{p!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!} = p \frac{(p-1)!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$ и учитывая, что $\binom{n}{n_1,n_2,\ldots,n_k}$ есть целое число получаем $\frac{(p-1)!}{p \nmid n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$ также есть целое число и, при этом, p не сокращается с $n_1! \cdot n_2! \cdot \ldots \cdot n_k!$. Следовательно, $p \mid \binom{n}{n_1,n_2,\ldots,n_k}$, ч. т. д. $\square$

Опираясь на теорему 2 в сочетании с тождеством

$$\sum_{\substack{n_1+n_2+\ldots+n_k=n \\ n_1 \geqslant 0,\, n_2 \geqslant 0,\, \ldots,\, n_k \geqslant 0}} \binom{n}{n_1, n_2, \ldots, n_k} = k^n$$

получаем малую теорему Ферма о том, что $p \mid k^p - k$ (относительно трёх других её доказательств см. [3]).

3. Алгебраические свойства гауссовых коэффициентов

Гауссовы коэффициенты впервые появились в работе Гаусса [4] по теории деления круга при вычислении значений периодов длины $\frac{n-1}{2}$, где n — простое число, т. е. когда совокупность корней уравнения деления круга $x^{n-1} + x^{n-2} + \ldots + 1 = 0$ распадается на два периода, являющиеся корнями некоторого квадратного уравнения с некоторыми коэффициентами из кругового поля корней n-ой степени из 1.

Рассматриваемый вопрос был применён Гауссом к определению знака так называемой гауссовой квадратичной суммы

$$G = \sum_r e^{\frac{2\pi i}{n} r},$$

где суммирование проводится по всем квадратичным вычетам r по простому модулю n, лежащим в границах от 1 до $\frac{n-1}{2}$.

Установление знака гауссовой суммы G проводится Гауссом при помощи исследования двух особых рядов:

$$f(x, m) = \sum_{\mu=1}^{\infty} (-1)^{\mu} (m, \mu) \text{ и } F(x, m) = \sum_{\mu=1}^{\infty} x^{\frac{\mu}{2}} (m, \mu),$$

где

$$(m, \mu) = \frac{(1 - x^m)\left(1 - x^{m-1}\right) \cdot \ldots \cdot \left(1 - x^{m-\mu+1}\right)}{(1 - x)\left(1 - x^2\right) \cdot \ldots \cdot \left(1 - x^{\mu}\right)}, \tag{1}$$

при этом (m, μ) в дальнейших исследованиях был назван гауссовым коэффициентом.

Правая часть (1) несмотря на её дробное выражение является многочленом от x с целыми коэффициентами (см. [5]).

Соотношение (1) можно преобразовать следующим образом

$$(m,\mu)=\frac{\left(x^m-1\right)\left(x^{m-1}-1\right)\cdot\ldots\cdot\left(x^{m-\mu+1}-1\right)}{\left(x^\mu-1\right)\left(x^{\mu-1}-1\right)\cdot\ldots\cdot(x-1)}.$$

По аналогии с биномиальными коэффициентами мы будем пользоваться современным обозначением гауссовых коэффициентов

$$\binom{n}{k}_q=\frac{\left(q^n-1\right)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}. \tag{2}$$

Для гауссового коэффициента (2) при $q=1$ получается неопределённость вида $\frac{0}{0}$ и именно в этом неопределённом случае гауссовый коэффициент будет совпадать с биномиальным коэффициентом, т. е. $\binom{n}{k}_1=\binom{n}{k}=\frac{n!}{k!(n-k)!}$.

Действительно, разделив каждый сомножитель числителя и знаменателя левой части (2) на $q-1$, получаем следующее представление гауссового коэффициента

$$\binom{n}{k}_q=\frac{1+q+q^2+\ldots+q^{n-1}}{1}\cdot\frac{1+q+q^2+\ldots+q^{n-2}}{1+q}\cdot\ldots\cdot\frac{1+q+q^2+\ldots+q^{n-k}}{1+q+q^2+\ldots+q^{k-1}}, \tag{3}$$

откуда при $q=1$ имеем

$$\binom{n}{k}_1=\frac{n(n-1)\cdot\ldots\cdot(n-(k-1))}{1\cdot2\cdot\ldots\cdot k}=\frac{n!}{k!(n-k)!}=\binom{n}{k},$$

т. е. получился биномиальный коэффициент $\binom{n}{k}$. Из (2) и (3) получаем $\binom{n}{0}_q=1$ и $\binom{n}{n}=1$.

Рассмотрим смысл гауссовых коэффициентов в теории векторных пространств над конечным полем F_q из q элементов.

Пусть q есть степень простого числа. Через $V_n(q)$ обозначим n-мерное векторное пространство над полем F_q, при этом $V_n(q)=\{(\alpha_1,\alpha_2,\ldots,\alpha_n)\in F_q^n\mid\alpha_i\in F_q\}$.

Предложение 2. *Число k-мерных подпространств n-мерного пространства $V_n(q)$ равно гауссовому коэффициенту $\binom{n}{k}_q$.*

Доказательство см. [12].

Гауссовы коэффициенты $\binom{n}{k}_q$ мы будем рассматривать как q-аналоги биномиальных коэффициентов и в отношении их свойств.

Предложение 3. *Гауссовы коэффициенты обладают свойством симметрии, т. е.* $\binom{n}{k}_q=\binom{n}{n-k}_q$.

Доказательство непосредственно следует из определения.

Из предложений 2 и 3 выводится свойство подпространств конечномерного векторного пространства над конечным полем.

Теорема 3. *Число k-мерных подпространств n-мерного векторного пространства над конечным полем из q элементов рано числу $(n-k)$-мерных его подпространств.*

Доказательство. В силу предложения 2 имеем, что число $G_q(n,k)$ k-мерных подпространств n-мерного векторного пространства $V_n(q)$ над полем F_q из q элементов равно гауссовому коэффициенту $\binom{n}{k}_q$, т. е. $G_q(n,k)=\binom{n}{k}_q$. Но так как по предложению 3 справедливо равенство $\binom{n}{k}_q=\binom{n}{n-k}_q$, то $G_q(n,k)=G_q(n,n-k)$, ч. т. д. □

Как и биномиальные коэффициенты гауссовы коэффициенты обладают свойством унимодальности, т. е. имеет место следующее.

Предложение 4. *Пусть $n\in\mathbb{N}$. Последовательность $\left\{\binom{n}{k}_q\mid k=0,\ldots,n\right\}$ гауссовых коэффициентов удовлетворяет свойствам:*

а) $\binom{n}{0}_q < \binom{n}{1}_q < \ldots < \binom{n}{\frac{n}{2}}_q > \binom{n}{\frac{n}{2}+1}_q > \ldots > \binom{n}{n}_q$ *при чётном* n*;*

б) $\binom{n}{0}_q < \binom{n}{1}_q < \ldots < \binom{n}{\frac{n-1}{2}}_q = \binom{n}{\frac{n-1}{2}}_q > \ldots > \binom{n}{n}_q$ *при нечётном* n*.*

Доказательство проводится аналогично случаю биномиальных коэффициентов изложенному в [14].

Рассмотрим ещё вопрос о сумме $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ всех гауссовых коэффициентов. Для суммы всех биномиальных, так и полиномиальных коэффициентов имеются точные значения.

Насколько нам известно, в математической литературе нигде не встречается решение этого вопроса в случае гауссовых коэффициентов.

Для биномиальных коэффициентов имеется производящая функция равная $(1+x)^n$, т. е. $(1+x)^n = \sum\limits_{k=0}^{n}\binom{n}{k}x^k$. Приведём имеющийся q-аналог для этого равенства.

Предложение 5. (q-бином Ньютона). *При любом натуральном* q *справедливо равенство* $\prod\limits_{k=1}^{n}\left(1+xq^k\right) = \sum\limits_{k=0}^{n}\binom{n}{k}_q q^{\frac{k(k+1)}{2}}x^k$*, где* $\binom{n}{k}_q$ *— гауссовый коэффициент.*

Доказательство см. [13]. Довольно простой вывод этого равенства имеется в [6].

Приведённое равенство представляет собой обобщение биномиальной формулы так как при подстановке $q=1$ оно переходит в обычный бином Ньютона вида $(1+x)^n$.

Из предложения 5 следует, что произведение $(1+xq)\left(1+xq^2\right)\cdot\ldots\cdot(1+xq^n)$ является производящей функцией для $\binom{n}{k}_q q^{\frac{k(k+1)}{2}}$.

Пользуясь предложением 5 можно получить следующее неравенство $\sum\limits_{k=0}^{n}\binom{n}{k}_q \leqslant 2^n q^{\frac{n(n+1)}{2}}$.

Для получения более точной оценки сверху мы воспользуемся исходным определением гауссового коэффициента.

Теорема 4. *Для суммы всех гауссовых коэффициентов при* $q>1$ *справедливы неравенства*

$$\frac{1}{2^{\frac{n}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}} < \sum_{k=0}^{n}\binom{n}{k}_q \leqslant 2^n q^{\frac{n^2}{4}}.$$

Доказательство. Сначала доказываем верхнюю оценку. Имеем $\sum_{k=0}^{n}\binom{n}{k}_q = 2+\sum_{k=1}^{n-1}\binom{n}{k}_q$. Получим оценку сверху для каждого гауссового коэффициента.

Из $\binom{n}{k}_q = \frac{(q^n-1)\left(q^{n-1}-1\right)\cdot\ldots\cdot\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdot\ldots\cdot(q-1)}$ получаем $\binom{n}{k}_q < \frac{q^n\cdot q^{n-1}\cdot\ldots\cdot q^{n-k+1}}{\frac{1}{2}q^k\cdot\frac{1}{2}q^{k-1}\cdot\ldots\cdot\frac{1}{2}q} = 2^k\cdot q^{nk-k^2} < 2^k\cdot q^{\frac{n^2}{4}}$, при этом учитывается, что $nk-k^2 \leqslant \frac{n^2}{4}$ при $0\leqslant k\leqslant n$.

Тогда, включая и случай $q=1$, будем иметь $\sum_{k=0}^{n}\binom{n}{k}_q \leqslant (2^n-2)\,q^{\frac{n^2}{4}} \leqslant 2^n q^{\frac{n^2}{4}}$, тем самым верхняя оценка доказана.

Теперь перейдём к нижней оценке. Имеем $\sum_{k=0}^{n}\binom{n}{k}_q > \max\limits_{0\leqslant k\leqslant n}\binom{n}{k}_q$.

В силу предложения 4 имеем

$$\max_{0\leqslant k\leqslant n}\binom{n}{k}_q = \begin{cases}\binom{n}{\frac{n}{2}}_q & \text{если } n\text{ — чётно,}\\ \binom{n}{\frac{n-1}{2}}_q & \text{если } n\text{ — нечётно,}\end{cases}$$

Соответственно этому рассмотрим два случая:

а) $\binom{a}{\frac{n}{2}}_q > \frac{\frac{1}{2}q^n\cdot\frac{1}{2}q^{n-1}\cdot\ldots\cdot\frac{1}{2}q^{n-\frac{n}{2}+1}}{q^{\frac{n}{2}}\cdot q^{\frac{n}{2}-1}\cdot\ldots\cdot q} = \frac{1}{2^{\frac{n}{2}}}q^{\frac{n}{2}\cdot\frac{n}{2}} = \frac{1}{2^{\frac{n}{2}}}q^{\frac{n^2}{4}}$

б) $\left(\frac{a}{\frac{n-1}{2}}\right)_q > \frac{\frac{1}{2}q^n\cdot\frac{1}{2}q^{n-1}\cdot\ldots\cdot\frac{1}{2}q^{n-\left(\frac{n-1}{2}-1\right)}}{q^{\frac{n-1}{2}}\cdot q^{\frac{n-1}{2}-1}\cdot\ldots\cdot q} = \frac{1}{2^{\frac{n-1}{2}}}q^{n-\frac{n-1}{2}\cdot\frac{n-1}{2}} = \frac{1}{2^{\frac{n-1}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}}$

Объединяя теперь случаи а) и б), получаем $\sum_{k=0}^{n}\binom{n}{k}_q > \frac{1}{2^{\frac{n-1}{2}}}q^{\frac{n^2}{4}-\frac{1}{4}}$. Теорема 4 доказана. □

Несмотря на то, что гауссовы коэффициенты не обладают производящей функцией с удобным алгебраическим описанием, тем не менее, для суммы всех гауссовых коэффициентов удаётся получить асимптотическую формулу при $q\to\infty$ (комбинаторное описание коэффициентов производящей функции для $\binom{n}{k}_q$ даётся в [13]).

Теорема 5. *Для суммы всех гауссовых коэффициентов справедлива асимптотическая формула*

$$\sum_{k=0}^{n}\binom{n}{k}_q \sim \begin{cases} q^{\frac{n^2}{4}} & \text{при чётных } n,\\ 2q^{\frac{n^2}{4}-\frac{1}{4}} & \text{при нечётных } n>1,\end{cases}$$

где $\sim$ — знак асимптотической эквивалентности.

Доказательство.

1) Сначала рассматриваем случай чётного n. Так как $\binom{n}{k}_q$ есть многочлен относительно q, то для степени такого многочлена имеем $\deg\binom{n}{k}_q = nk-k^2$. Но учитывая, что $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ также есть многочлен от q, будем иметь

$$\deg\sum_{k=0}^{n}\binom{n}{k}_q = \max_{0\leqslant k\leqslant n}\left\{\deg\binom{n}{k}_q\right\} = \max_{0\leqslant k\leqslant n}\left\{nk-k^2\right\} = \frac{n^2}{4}.$$

Тогда многочлен $\sum\limits_{k=0}^{n}\binom{n}{k}_q$ можно представить в следующем виде

$$\sum_{k=0}^{n}\binom{n}{k}_q = q^{\frac{n^2}{4}} + a_1q^{\frac{n^2}{4}-1} + \ldots + a_s,$$

где $a_1, a_2, \ldots, a_s$ — целые числа зависящие только от n; $s=\frac{n^2}{4}$. Запишем эту сумму ещё в следующем виде $\sum\limits_{k=0}^{n}\binom{n}{k}_q = q^{\frac{n^2}{4}}\left(1+\frac{a_1}{q}+\ldots+\frac{a_s}{q^{\frac{n^2}{4}}}\right)$, откуда при $q\to\infty$ получаем, что $\sum\limits_{k=0}^{n}\binom{n}{k}_q \sim q^{\frac{n^2}{4}}$.

2) Пусть теперь n — нечётное число. В этом случае $\deg\sum\limits_{k=0}^{n}\binom{n}{k}_q = \frac{n^2}{4}-\frac{1}{4}$. Учитывая, что в случае нечётного n имеются два равных центральных гауссовых коэффициентов, являющихся наибольшими из всех этих коэффициентов (это следует из предложения 4), получаем $\deg\sum\limits_{k=0}^{n}\binom{n}{k}_q = \frac{n^2}{4}-\frac{1}{4}$ и используя теперь предыдущие рассуждения из первого случая, получаем $\sum\limits_{k=0}^{n}\binom{n}{k}_q \sim 2q^{\frac{n^2}{4}-\frac{1}{4}}$.

Теорема 5 доказана. □

Относительно оценок и асимптотик для разных видов сумм, содержащих биномиальные коэффициенты см. [15].

4. Арифметические свойства гауссовых коэффициентов

Распространим на гауссовы коэффициенты арифметические свойства делимости и сравнимости. Рассмотрение таких свойств для гауссовых коэффициентов опирается на понятие первообразного корня по простому модулю p, при этом целое число g называется первообразным корнем по простому модулю p, если $g^{p-1} \equiv 1 \pmod p$, но $g^k \not\equiv 1 \pmod p$ при $1 \leqslant k < p-1$. В теории чисел доказывается, что первообразные корни существуют только по модулю m вида $m = 2; 4; p^\alpha; 2p^\alpha$, где p — простое число, α — натуральное число.

Следующий результат о делимости гауссовых коэффициентов даёт q-аналог предложения 1, относящиеся к биномиальным коэффициентам.

Теорема 6. *Если p — простое число и q — первообразный корень по модулю p, то для гауссового коэффициента $\binom{p}{k}_q$ при $2 \leqslant k \leqslant p-2$ справедлива делимость $p \mid \binom{n}{k}_q$.*

Доказательство. Пусть q — первообразный корень по простому модулю p, т. е. $g^{p-1} \equiv 1 \pmod p$, но $g^m \not\equiv 1 \pmod p$ при $m \leqslant p-2$. Значит, $\left(q^k-1\right) \cdot \ldots \cdot (q-1) \not\equiv 0 \pmod p$ при $2 \leqslant k \leqslant p-2$. При этом в числителе гауссового коэффициента $\binom{p}{k}_q$ все сомножители за исключением второго сомножителя не делятся p, а второй сомножитель в силу малой теоремы Ферма делится на p. Значит, учитывая при этом $\binom{p}{1}_q$ и $\binom{p}{p-1}_q$ не делятся на p, получаем, что $p \mid \binom{p}{k}_q$ при $2 \leqslant k \leqslant p-2$, ч. т. д. $\square$

Представляют интерес вопросы, связанные с делимостью гауссовых коэффициентов вида $\binom{p^\alpha}{k}_q$ и $\binom{2p^\alpha}{k}_q$ на возможные степени простого числа p при условии, что q есть первообразный корень по модулю p^α или $2p^\alpha$. Мы рассматриваем этот вопрос в следующем частном случае.

Теорема 7. *Если p — простое число и q — первообразный корень по модулю p^2, то для гауссового коэффициента $\binom{p^2}{k}_q$ справедлива делимость $p \mid \binom{p^2}{k}_q$ при $p+1 \leqslant k \leqslant p^2-p-1$.*

Доказательство. Так как по условию $p+1 \leqslant k \leqslant p^2-p-1$ и q — первообразный корень по модулю q^2, то $p^2 \mid q^{p^2-p}-1$, но $q^k \not\equiv 1 \pmod{p^2}$. Тогда число сомножителей знаменателя $\left(q^k-1\right) \cdot \left(q^{k-1}-1\right) \cdot \ldots \cdot (q-1)$ коэффициента $\binom{p^2}{k}_q$, делящихся точно на p, будет равно целой части $\left[\frac{k}{p-1}\right]$ (это следует из того, что $p^2 \nmid q^{k-l}-1$ при всех $0 \leqslant l < k$). Поэтому получаем следующую точную делимость $p^{\left[\frac{k}{p-1}\right]} \| \left(q^k-1\right) \cdot \left(q^{k-1}-1\right) \cdot \ldots \cdot (q-1)$ на степень простого числа p.

Аналогично, числитель $\left(q^{p^2}-1\right) \cdot \left(q^{p^2-1}-1\right) \cdot \ldots \cdot \left(q^{p^2-k+1}-1\right)$ гауссового коэффициента $\binom{p^2}{k}_q$ также имеет $\left[\frac{k}{p-1}\right]$ сомножителей, делящихся на p. Но так как среди этих сомножителей есть $q^{p^2-p}-1$, который делится на p^2, то имеем делимость

$$p^{\left[\frac{k}{p-1}\right]+1} \mid \left(q^{p^2}-1\right) \cdot \left(q^{p^2-1}-1\right) \cdot \ldots \cdot \left(q^{p^2-k+1}-1\right).$$

Следовательно, $p \mid \binom{p^2}{k}_q$, ч. т. д. $\square$

Следующий результат даёт значение суммы всех гауссовых коэффициентов $\binom{p}{k}_q$ по простому модулю p.

Теорема 8. *Если q — первообразный корень по нечётному простому модулю p, то справедливо сравнение $\sum\limits_{k=0}^{p} \binom{p}{k}_q \equiv 4 \pmod p$.*

Доказательство. По свойствам гауссовых коэффициентов имеем

$$\sum_{k=0}^{p} \binom{p}{k}_q = \binom{p}{0}_q + \binom{p}{p}_q + \binom{p}{1}_q + \binom{p}{p-1}_q + \sum_{k=2}^{p-2} \binom{p}{k}_q = 2 + 2\frac{q^p-1}{q-1} + \sum_{k=2}^{p-2} \binom{p}{k}_q.$$

Отсюда, переходя к сравнению по модулю p, в силу теоремы 5, будем иметь $\sum\limits_{k=0}^{p}\binom{p}{k}_q \equiv 2+2\frac{q^p-1}{q-1} \pmod p$ или, что то же самое, $\sum\limits_{k=0}^{p} \equiv 4+\frac{q^p-q}{q-1} \pmod p$. Так как по условию q — первообразный корень по модулю p, то $p \nmid q-1$. Но по малой теореме Ферма $p \nmid q^p-q$. Следовательно, $\sum\limits_{k=0}^{p}\binom{p}{k}_q \equiv 4 \pmod p$, ч. т. д. $\square$

Замечание. *Результаты теорем 7 и 8 не являются q-аналогами биномиальных коэффициентов в виду того, что в них q выбиралось первообразным корнем по модулям p и p^2 соответственно.*

5. Заключение

В этой части мы приводим некоторые нерешенные задачи теории чисел, связанные с биномиальными гауссовыми коэффициентами, которые могут представлять интерес для дальнейших исследований.

1. Следующая гипотеза о простых делителях биномиальных коэффициентов, представлена Малышевым А. В. в [16].

Гипотеза. *Пусть n, k — целые числа, $0 \leqslant 2k \leqslant n$. Пусть биномиальный коэффициент $\binom{n}{k} = u \cdot v$, где каждый простой множитель числа u меньше чем k, а каждый простой множитель числа v не меньше, чем k.*

Доказаны [17], что $u < v$ за исключением 12 случаев:

$$\begin{gathered}\binom{8}{3}, \quad \binom{9}{4}, \quad \binom{10}{5}, \quad \binom{12}{5}, \quad \binom{21}{7}, \quad \binom{21}{8}, \\ \binom{30}{7}, \quad \binom{33}{13}, \quad \binom{33}{14}, \quad \binom{36}{13}, \quad \binom{36}{17}, \quad \binom{56}{13}.\end{gathered} \tag{$*$}$$

Немного изменим постановку задачи. Пусть $\binom{n}{k} = U \cdot V$, где каждый постой множитель числа U не больше чем k. Доказано, что и здесь $U < V$ за исключением конечного числа пар n и k. Помимо $(*)$ найдено ещё 7 исключений:

$$\binom{9}{3}, \quad \binom{10}{3}, \quad \binom{18}{3}, \quad \binom{28}{5}, \quad \binom{54}{7}, \quad \binom{82}{3}, \quad \binom{162}{3}.$$

Предположено [17], что других исключений нет. Доказать или опровергнуть эту гипотезу.

2. Представляет интерес исследовать сравнение для центральных биномиальных коэффициентов по модулям, содержащим два и более простых делителей.

3. Перенести изложенные результаты на q-мультиномиальные коэффициенты являющиеся q-аналогом полиномиальных коэффициентов (по поводу этого понятия см. [5]).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Bachmann P. Niedere Zahlen theorie. I und II. Teil, Leipzig, 1902 und 1912, 402 p. und 480 p.

2. Wolstenholme J., On certain properties of prime numbers. Quart. J. Pure Appl. Math. 5 (1862), 35–39.

3. Винберг Э. Б., Удивительные свойства биномиальных коэффициентов// Мат. Просвещение. Третья серия. Вып. 12. Изд.-во МЦНМО. 2008.

4. Gauss C. F., Summatio quarumdam serierum singularium, Comment. Soc. Reg. Sci. Gottingensis, 1 (1811): Werke, Vol. 2, P. 11–45

5. Стенли Р. Перечислительная комбинаторика. Изд.-во «Мир», 1990. 440 с.

6. Шокуев В. Н. Гауссовы коэффициенты. 1988. Нальчик: КБГУ. 98 с.

7. Шокуев В. Н. Основы теории перечисления для конечных нильпотентных групп // Записки научных семинаров ПОМИ. 1994. Т. 211. С. 174–183.

8. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. Изд.-во «Мир», 1987. 415 с.

9. Dzhumadil'daev A. S., Yeliussizov D. A. Wolstenholme's theorem ащк црфе binomial coefficients// Сибирские электронные математические известия. Т. 9, 2012, С. 460–463.

10. Erdös P. On some divisibility properties of $\binom{2n}{n}$. Canad. Math. Bull. 1964, Vol. 7, No 4, P. 513–518.

11. Moser R. Insolvability of $\binom{2n}{n} = \binom{2n}{a} \cdot \binom{2b}{b}$. Canad. Math. Bull. 6 (1963). Pp. 167–169.

12. Айгнер М. Комбинаторная теория. М.: «Мир», 1982. 556 с.

13. Polia G., Aalexanderson G. L. Gaussian binomial coefficients// Elemente der Mathematik, Vol. 26, N 5, 1971. pp. 102–109.

14. Липский В., Комбинаторика для программистов. М.: «Мир», 1988. 213 с.

15. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986, 384 с.

16. Берник В. И., Ковалевская Э. И. Нерешённые задачи теории чисел. Минск. 1990. Препринт №35 (335)/ АН БССР. Ин.-т математики.

17. Ecklund (Jr) E. F., Eggleton R. B., Erdös P., Selfridge J. Z. On the prime factorisation of binomial coefficients// Austral. Math. Soc., Ser. A. 1978. Vol. 26. P. 257–269.

REFERENCES

1. Bachmann P. Niedere Zahlen theorie. I und II. Teil, Leipzig, 1902 und 1912, 402 p. und 480 p.

2. Wolstenholme J., On certain properties of prime numbers. Quart. J. Pure Appl. Math. 5 (1862), 35–39.

3. Vinberg, E. B. 2008, Udivitelnie svoistva binomialnih koeffitsientov [Amazing problems of binomial coefficients]. M. 62 pp. (Russian).

4. Gauss C. F., Summatio quarumdam serierum singularium, Comment. Soc. Reg. Sci. Gottingensis, 1 (1811): Werke, Vol. 2, P. 11–45

5. Stanley, R. Enumerative combinatorics. by Wadsworth, inc. California. Vol. 1, 1986.

6. Shokuev, V. N. 1988, "Gauusovi koeffitsienti" [Gaussian coefficients]. Nalchik. 98 p. (Russian).

7. Shokuev, V. N. 1994, "Osnovi teorii perechisleniya dlya konechnikh nilpotentnikh grupp" [Foundations of enumeration theory for finite nilpotent groups]. Zap. Nauchn. Sem. POMI. Vol. 211, pp. 174–183. (Russian).

8. Ireland, K. and Rosen, M. 1982, “Klassichesloe vvedenie v sovremennuyu teotiyu chisel” [A Classical Introduction to Modern Number Theory]. Springer. 385 p.

9. Dzhumadil'daev A. S., Yeliussizov D. A. Wolstenholme's theorem ащк црфе binomial coefficients// Сибирские электронные математические известия. Т. 9, 2012, С. 460–463.

10. Polia G., Aalexanderson G. L. Gaussian binomial coefficients// Elemente der Mathematik, Vol. 26, N 5, 1971. pp. 102–109.

11. Erdös P. On some divisibility properties of $\binom{2n}{n}$. Canad. Math. Bull. 1964, Vol. 7, No 4, P. 513–518.

12. Moser R. Insolvability of $\binom{2n}{n} = \binom{2n}{a} \cdot \binom{2b}{b}$. Canad. Math. Bull. 6 (1963). Pp. 167–169.

13. Ainger, M. Combinatorial theory. Springer–Verlang. Berlin Heidelberg New York, 1979,

14. Lipski, W. 1988, “Kombinatorika dlya progamistov” [Combinatorics for programmers]. M. Mir, 213 pp. (Russian)

15. Yablonsky S. V. 1986, “Vvedenie v diskretnuyu matematiku” M.: Nauka, 384 p. [Introduction to discrete mathematics]. (Russian)

16. Bernik, V. I., Kovalevsky, E. J. 1990, “Nereshennie zadachi v teorii chisel” [Unsolved problems in number theory]. Preprint N35 (435), Minsk. 1990. 39 p. (Russian)

17. Ecklund (Jr) E. F., Eggleton R. B., Erdös P., Selfridge J. Z. On the prime factorisation of binomial coefficients// Austral. Math. Soc., Ser. A. 1978. Vol. 26. P. 257–269.

Получено 30.07.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 514.174.5 DOI 10.22405/2226-8383-2018-19-3-270-281

О рациональных аналогах проблем Нелсона – Хадвигера и Борсука[1]

Соколов Артемий Алексеевич — студент МГУ им. М. В. Ломоносова, механико-математический факультет, кафедра теории чисел, г. Москва.
e-mail: sokolovartem179@yandex.ru.
Райгородский Андрей Михайлович — доктор физико-математических наук, профессор, Московский физико-технический институт (государственный университет), кафедра дискретной математики и лаборатория продвинутой комбинаторики и сетевых приложений; МГУ им. М. В. Ломоносова, механико-математический факультет, кафедра математической статистики и случайных процессов; Адыгейский государственный университет, Кавказский математический центр; Бурятский государственный университет, институт математики и информатики.
e-mail: mraigor@yandex.ru

Аннотация

В этой статье мы рассматриваем аффинно-рациональные аналоги задачи Нелсона-Хадвигера о нахождении хроматического числа рационального пространства и задачи Борсука о разбиении на части меньшего диаметра. Доказаны новые нижние оценки, в частности улучшены оценки минимального контрпримера для гипотезы Борсука.

Ключевые слова: хроматическое число, графы единичных расстояний, проблема Борсука.

Библиография: 38 названий.

Для цитирования:
А. А. Соколов, А. М. Райгородский. О рациональных аналогах проблем Нелсона — Хадвигера и Борсука // Чебышевский сборник, 2018, т. 19, вып. 3, с. 270–281.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 514.174.5 DOI 10.22405/2226-8383-2018-19-3-270-281

On rational analogs of Nelson–Hadwiger's and Borsuk's problems[2]

Sokolov Artemy Alekseevich — student Moscow State University, Mechanics and Mathematics Faculty, Department of Number Theory, Moscow.
e-mail: sokolovartem179@yandex.ru.

[1]Настоящая работа выполнена за счет гранта РФФИ (проект N 18-01-00355) и гранта президента НШ-6760.2018.1.
[2]This work by a grant of RFBR (project N 18-01-00355) and President grant NSH-6760.2018.1.

Raigorodskiy Andrew Mikhailovich — Doctor Phys-Math Sci., professor, Moscow Institute of Physics and Technology, Department of Discrete Mathematics and Laboratory of Advanced Combinatorics and Network Applications; Moscow State University, Mechanics and Mathematics Faculty, Department of Mathematical Statistics and Random Processes; Adyghe State University, Caucasus Mathematical Centre; Buryat State University, Institute of Mathematics and Informatics.
e-mail: mraigor@yandex.ru

Abstract

In this paper, we consider affine-rational analogs of Nelson–Hadwiger problem on finding the chromatic number of the rational space and Borsuk's problem on partitioning into parts of smaller diameter. New lower bounds are proved. In particular, bounds on the minimum dimension of a counterexample to Borsuk's conjecture are found.

Keywords: Chromatic number, unit-distance graphs, Borsuk's problem.

Bibliography: 38 titles.

For citation:
A. A. Sokolov, A. M. Raigorodskiy, 2018, "On rational analogs of Nelson–Hadwiger's and Borsuk's problems" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 270–281.

1. Введение

В 1950 году Э. Нелсон и Г. Хадвигер рассмотрели задачу о нахождении *хроматического числа* пространства $\mathbb{R}^n$ – минимального количества $\chi(\mathbb{R}^n)$ цветов, необходимого для такой покраски всех точек $\mathbb{R}^n$, чтобы никакие две точки одного цвета не находились на расстоянии 1. Точное значение $\chi(\mathbb{R}^n)$ найдено только при $n = 1$: $\chi(\mathbb{R}) = 2$. В остальных размерностях точных значений не известно, но известны различные оценки (см. [1]–[21]).

В 1976 году М. Бенда и М. Перлес определили аналогичным образом величину $\chi(\mathbb{Q}^n)$ и нашли её в размерностях 2, 3 и 4 (см. [22]). Различные оценки величины $\chi(\mathbb{Q}^n)$ можно найти в статьях [1], [20], [23]–[27].

Для удобства дальнейших рассуждений рассмотрим величину $\chi(A)$ – минимальное количество цветов, необходимое для покраски всех точек множества A, чтобы никакие точки одного цвета не находились на расстоянии 1.

В работе [28] было введено в некотором смысле промежуточное по отношению к $\chi(\mathbb{Q}^n)$ и $\chi(\mathbb{R}^n)$ *аффинное хроматическое число* рационального пространства $\chi_{\text{aff}}(\mathbb{Q}^n)$, определяемое следующим образом:

$$\chi_{\text{aff}}(\mathbb{Q}^n) = \max_m \max_{A\subset\mathbb{Q}^m, \operatorname{affdim} A\le n} \chi(A),$$

где $\operatorname{affdim} A$ – размерность минимального аффинного пространства, содержащего A. Разница заключается в том, что рассматриваемые множества A лежат в некотором рациональном пространстве большей размерности, но "настоящая" размерность подпространства не превосходит n. Однако "внутренние" координаты в этом подпространстве уже не будут рациональными.

В работе [29] было введено следующее определение

Определение 8. *Граф $G = (V, E), V \subseteq \mathbb{R}^n$, называется $\sqrt{Q}$-графом единичных расстояний, если для любых $x, y \in V$ имеет место $|x - y|^2 \in \mathbb{Q}$ и для любого ребра $(x, y) \in E$ выполняется $|x - y| = 1$.*

В статье [29] была доказана важная теорема, гласящая, что $\chi_{\text{aff}}(\mathbb{Q}^n) = \chi_{\sqrt{Q}}(\mathbb{R}^n)$, где

$$\chi_{\sqrt{Q}}(\mathbb{R}^n) = \max\left\{\chi(G) : G - \sqrt{Q}\text{-граф единичных расстояний в } \mathbb{R}^n\right\}.$$

Также работа [29] мотивирует введение величины $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n)$, равной

$$\max\Big\{\chi(G) : G - \sqrt{Q}\text{-граф единичных расстояний в } \mathbb{R}^n \text{ и } K_{n+1} \subseteq G\Big\},$$

где K_{n+1} – полный граф на $n+1$ вершинах, т.е. полноразмерный правильный симплекс в $\mathbb{R}^n$.

В статье [29] было доказано, что $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^2) = 3, \chi_{\sqrt{Q},\Delta}(\mathbb{R}^3) = 4$, и выдвинута гипотеза, что $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) = n+1$. Но, как и следовало ожидать в подобной ситуации, гипотеза не подтвердилась.

Более того, имеет место серия результатов, которые мы сформулируем и докажем в разделе 2.

Еще одна классическая проблема комбинаторной геометрии, тесно связанная с задачами о хроматических числах пространств, – это проблема Борсука о разделении множеств на части меньшего диаметра.

Обозначим $b(n)$ минимальное число частей меньшего диаметра, на которые разбивается любое ограниченное множество в $\mathbb{R}^n$. Классическая гипотеза Борсука заключается в том, что $b(n) = n+1$. На данный момент известно, что гипотеза верна при $n \leq 3$ и неверна при $n \geq 64$ (см. [1], [4], [8], [10], [11], [30]–[33]).

В настоящей работе мы рассмотрим следующий аналог числа Борсука:

$$f(n) = \max_{A\subset\mathbb{R}^n, \operatorname{diam} A=1} \chi(A).$$

Отметим, что величина $f(n)$ может не равняться $b(n)$, т.к. разбить множество на части меньшего диаметра – это, вообще говоря, не то же самое, что раскрасить его точки без нахождения точек одного цвета на расстоянии 1: для конечных множеств A это верно, но, например, даже для сферы $S^n \subset \mathbb{R}^{n+1}$ величина $\chi(S^n)$ равна 2, тогда как частей меньшего диаметра нужно $n+2$.

Правильным аналогом величины $f(n)$ в рациональном случае послужит величина

$$g(n) = \max_{A\subset\mathbb{Q}^n, \operatorname{diam} A=1} \chi(A).$$

Наконец, по аналогии с хроматическим числом, введем *аффинно-рациональное* число Борсука, которое равно

$$h(n) = \max_m \max_{A\subset\mathbb{Q}^m, \operatorname{diam} A=1, \operatorname{affdim} A\leq n} \chi(A).$$

Аффинно-рациональный аналог гипотезы Борсука заключается в том, что $h(n) = n+1$. Но, как и следовало ожидать по аналогии с вещественным случаем, гипотеза неверна. В статье [34] доказано, что она неверна при $n \in [561, 757] \cup [903, \infty)$.

В разделе 3 мы сначала объясним, как убрать "зазор" между 757 и 903, а потом докажем, что эта гипотеза неверна во всех размерностях, начиная с 65.

2. Аффинное хроматическое число $\mathbb{Q}^n$

В этом разделе мы опровергнем гипотезу, что $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) = n+1$.

На самом деле, верна следующая теорема

Теорема 1. *$\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) \geq \chi(\mathbb{Q}^{\omega(n)-1})$, где $\omega(n)$ – наибольшее количество точек в $\mathbb{Q}^n$, образующих симплекс со стороной 1. Если выполнено условие, что $\omega(n) = n+1$, то $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) = \chi(\mathbb{Q}^n)$.*

Выпишем для небольших n значения $\omega(n)$ и $\chi(\mathbb{Q}^n)$ (см. [35], [36]).

n	1	2	3	4	5	6	7	8
$\omega(n)$	2	2	2	4	4	6	8	9
$\chi(\mathbb{Q}^n)$	2	2	2	4	≥ 8	≥ 8	≥ 9	≥ 10

Из этого выводим, что

$$\chi_{\sqrt{Q},\Delta}(\mathbb{R}^6) \geq \chi(\mathbb{Q}^{6-1}) \geq 8,$$

в связи с чем получаем противоречие с гипотезой. Как мы упоминали ранее, в статье [29] доказано, что $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^2) = 3$ и $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^3) = 4$. Вопрос, верна ли гипотеза в размерностях 4 и 5, все еще остается открытым.

Поскольку $\omega(n) \geq n-2$, то при устремлении n к бесконечности получим, что (см. [25], [26])

$$\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) \geq \chi(\mathbb{Q}^{n-3}) \geq (1.199 + o(1))^n.$$

Но поскольку существует бесконечно большая последовательность $\{n_k\}$ такая, что $\omega(n_k) = n_k + 1$, то при бесконечном количестве n верно, что $\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) = \chi(\mathbb{Q}^n)$.

Для доказательства теоремы 1 нам понадобится следующая лемма

Лемма 1 (Соколов, [29]). *Пусть G – $\sqrt{Q}$-граф в $\mathbb{R}^n$ такой, что* $\operatorname{affdim} G = n$. *Выберем в нем множество вершин $v_0, v_1, \ldots, v_n \in G$ общего положения. Тогда для любой вершины $x \in G$ верно, что $\overrightarrow{v_0x} = \lambda_1\overrightarrow{v_0v_1} + \ldots + \lambda_n\overrightarrow{v_0v_n}$, где $\lambda_i \in \mathbb{Q}$.*

Также нам понадобится "обратная" лемма.

Лемма 2. *Пусть $v_0, v_1, \ldots, v_n$ – точки общего положения в $\mathbb{R}^n$, образующие $\sqrt{Q}$-граф. Пусть для каждой вершины x графа $G = (V, E), V \subset \mathbb{R}^n$ верно, что $\overrightarrow{v_0x} = \lambda_1\overrightarrow{v_0v_1} + \ldots + \lambda_n\overrightarrow{v_0v_n}$, где $\lambda_i \in \mathbb{Q}$. Тогда G является $\sqrt{Q}$-графом.*

Доказательство. Для начала заметим, что для любых $1 \leq i, j \leq n$ выполнено

$$(\overrightarrow{v_0v_i}, \overrightarrow{v_0v_j}) = \frac{|v_0 - v_i|^2 + |v_0 - v_j|^2 - |v_i - v_j|^2}{2} \in \mathbb{Q}.$$

Также для любых $x, y \in G$ выполнено

$$(\overrightarrow{v_0x}, \overrightarrow{v_0y}) = \left(\sum_{i=1}^{n} \lambda_i\overrightarrow{v_0v_i}, \sum_{j=1}^{n} \mu_j\overrightarrow{v_0v_j}\right) = \sum_{i,j=1}^{n} \lambda_i\mu_j\,(\overrightarrow{v_0v_i}, \overrightarrow{v_0v_j}) \in \mathbb{Q}.$$

Наконец, для любых $x, y \in G$ верно $|x - y|^2 = |v_0 - x|^2 + |v_0 - y|^2 - 2\,(\overrightarrow{v_0x}, \overrightarrow{v_0y}) \in \mathbb{Q}$, что и означает, что G является $\sqrt{Q}$-графом. □

Теперь докажем теорему.

Доказательство. [Доказательство теоремы 1]

Рассмотрим полноразмерный симплекс S со стороной 1 в $\mathbb{R}^n$ такой, что $\omega(n)$ его вершин рациональны. Обозначим через T симплекс, образованный этими рациональными вершинами. Пусть V– рациональное подпространство размерности $\omega(n) - 1$, содержащее T. Несложно видеть, что V изоморфно $\mathbb{Q}^{\omega(n)-1}$. Рассмотрим рациональный дистанционный граф $G \subset V$ такой, что $\chi(G) = \chi(\mathbb{Q}^{\omega(n)-1})$, его существование нам гарантирует теорема Эрдеша – Де Брёйна (см. [38]). Рассмотрим граф $H = G \cup S$. Каждая его вершина рационально выражается через вершины симплекса S, а значит, по лемме 2, он является $\sqrt{Q}$-графом. Тогда

$$\chi_{\sqrt{Q},\Delta}(\mathbb{R}^n) \geq \chi(H) \geq \chi(G) = \chi(\mathbb{Q}^{\omega(n)-1}).$$

Докажем теперь вторую часть утверждения теоремы. Пусть натуральное число n таково, что $\omega(n) = n+1$. Рассмотрим граф G такой, что $\chi(G) = \chi_{\sqrt{Q},\Delta}(\mathbb{R}^n)$, пусть также S – полноразмерный симплекс, содержащийся в G. Расположим граф G таким образом, чтобы вершины

симплекса S стали рациональными. Заметим, что по лемме 1 все вершины графа G также будут рациональными. Таким образом, G – дистанционный граф в $\mathbb{Q}^n$. Тогда

$$\chi(\mathbb{Q}^n) \geq \chi(G) = \chi_{\sqrt{\mathbb{Q}},\Delta}(\mathbb{R}^n).$$

Обратное неравенство следует из первой части теоремы. □

3. Аффинно-рациональная проблема Борсука

3.1. Формулировки результатов

В этом разделе мы будем строить контрпримеры к аффинно-рациональной гипотезе Борсука.

В параграфе 3.2 мы рассмотрим конструкцию из статьи [34], дающую контрпримеры к гипотезе в размерностях $n \in [561, 757]$. Далее мы научимся "поднимать" контрпримеры в бóльшую размерность, что позволит опровергнуть аффинно-рациональную гипотезу Борсука для всех $n \geq 561$.

В параграфе 3.3 мы рассмотрим конструкцию из статьи [37] и адаптируем ее для аффинно-рационального случая, что в свою очередь позволит доказать следующую теорему.

Теорема 2. *Аффинно-рациональная гипотеза Борсука неверна во всех размерностях, начиная с 65.*

Предварительно введем следующие обозначения: $X_{m,r} = \mathbb{Q}^m \cap S_r^{m-1}$, $X_m = X_{m,1}$, где $S_r^m \subset \mathbb{R}^{m+1}$ — сфера радиуса r с центром в нуле.

3.2. Контрпримеры при $n \geq 561$

В статье [34] было доказано, что аффинно-рациональная гипотеза Борсука неверна в размерностях $n \in [561, 757] \cup [903, \infty)$. В данном параграфе мы научимся в некоторых случаях "поднимать" контрпримеры к гипотезе Борсука в большую размерность, что позволит убрать "зазор" и опровергнуть гипотезу во всех размерностях, начиная с 561.

Для удобства введем следующее определение.

Определение 9. *Пусть A – некоторое множество точек евклидова пространства. Будем говорить, что множество A* аффинно-рационально *лежит на сфере радиуса r при некотором $r \in \sqrt{\mathbb{Q}}$, если существует такое $n \geq 1$, что в множестве $X_{n,r}$ найдется подмножество, конгруэнтное A.*

Справедлива следующая теорема

Теорема 3. *Пусть множество A дает контрпример к аффинно-рациональной гипотезе Борсука в размерности n, причем A аффинно-рационально лежит на сфере радиуса r при $r \leq \frac{1}{\sqrt{2}}$. Тогда можно построить множество, дающее контрпример в любой бóльшей размерности.*

Докажем сперва следующую лемму.

Лемма 1. *Пусть множество A аффинно-рационально лежит на сфере радиуса r_0. Тогда для любого $r \in \sqrt{\mathbb{Q}}, r > r_0$ верно, что A аффинно-рационально лежит на сфере радиуса r.*

Доказательство. Поскольку число $r^2 - r_0^2$ положительно и рационально, то по теореме Лагранжа его можно представить в виде $a_1^2 + a_2^2 + a_3^2 + a_4^2$, где $a_i \in \mathbb{Q}$. Без ограничения общности можно считать, что $A \subset X_{n,r_0}$ при некотором $n \geq 1$. Рассмотрим множество

$$A' = A \times \{(a_1, a_2, a_3, a_3)\} \subset \mathbb{Q}^{n+4}.$$

Заметим, что множества A и A' конгруэнтны, однако множество A' лежит на сфере радиуса

$$\sqrt{r_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2} = \sqrt{r^2} = r.$$

□

Теперь научимся "поднимать" контрпримеры к гипотезе Борсука в аффинно-рациональном случае, для этого докажем теорему 3.

Доказательство. [Доказательство теоремы 3] Поскольку A аффинно-рационально лежит на сфере радиуса не больше $\frac{1}{\sqrt{2}}$, то по лемме 3 оно аффинно-рационально лежит и на сфере радиуса ровно $\frac{1}{\sqrt{2}}$. Итак, без ограничения общности можно считать, что $A \subset X_{N,\frac{1}{\sqrt{2}}}$ при некотором $N \geq 1$. Пусть мы хотим построить контрпример в аффинной размерности $n+k$. Рассмотрим $\mathbb{Q}^{N+2k}$, и, используя только первые N координат, поместим туда множество A. Далее, используя только последние $2k$ координат рассмотрим точки вида

$$y_i = \left(0 \dots 0, \dots, \frac{1}{2}, \frac{1}{2}, 0, \dots, 0\right),$$

где ненулевые координаты стоят на местах $N + 2i - 1$ и $N + 2i$ соответственно. Заметим, что множество $A \cup \{y_i\}_{i=1}^k$ также лежит на сфере радиуса $\frac{1}{\sqrt{2}}$, и его нельзя разбить на $n+k$ частей меньшего диаметра, таким образом, оно дает контрпример к аффинно-рациональной гипотезе Борсука в размерности $n+k$.

□

Замечание 1. *На самом деле, если мы хотим поднять контрпример в размерность именно $n+k$, то достаточно, чтобы радиус изначального контрпримера был не больше, чем*

$$\sqrt{1 - \left(\sqrt{\frac{k-1}{2k}}\right)^2} = \sqrt{\frac{k+1}{2k}},$$

что немного больше, чем $\frac{1}{\sqrt{2}}$.

Заметим, что множество, полученное в статье [34], подходит под условие теоремы, откуда следует, что аффинно-рациональная гипотеза Борсука неверна для всех размерностей, больших 560.

3.3. Контрпримеры при $n \in [65, 560]$

Теперь построим контрпримеры в размерностях от 65 до 560. Для этого воспользуемся конструкцией из статьи [37], которая тесно связана с понятием *сильно регулярного графа*. Далее мы покажем, как именно эта конструкция применима к нашей задаче.

3.3.1. Описание конструкции

Определение 10. *Граф $G = (V, E)$ называется сильно регулярным с параметрами (n, d, λ, μ), если*

(i). $|V| = n$

(ii). *для любого* $v \in V : \deg v = d$

(iii). *если* $(u, v) \in E : |\{w \in V : (u, w) \in E \ u \ (w, v) \in E\}| = \lambda$

(iv). *если* $(u, v) \notin E : |\{w \in V : (u, w) \in E \ u \ (w, v) \in E\}| = \mu$

Как известно, собственные числа матрицы смежности A графа G выглядят следующим образом:

- d с кратностью 1
- $r = \frac{1}{2}\left(\lambda - \mu + \sqrt{(\lambda-\mu)^2 + 4(d-\mu)}\right)$ с кратностью $f = \frac{1}{2}\left(n - 1 - \frac{2d+(n-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(d-\mu)}}\right)$
- $s = \frac{1}{2}\left(\lambda - \mu - \sqrt{(\lambda-\mu)^2 + 4(d-\mu)}\right)$ с кратностью $g = \frac{1}{2}\left(n - 1 + \frac{2d+(n-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(d-\mu)}}\right)$

Обозначим через y_i векторы-столбцы матрицы $A - sE$. Через x_i, в свою очередь, обозначим отнормированные и центрированные векторы y_i, т.е. x_i коллинеарен y_i, $||x_i|| = 1$ и $\sum\limits_{i=1}^{n} x_i = 0$.

Заметим, что все векторы x_i лежат на единичной сфере в подпространстве размерности не более f.

Также можно заметить, что

$$(x_i, x_j) = \begin{cases} 1, & i = j \\ p, & (i,j) \in E \\ q, & (i,j) \notin E \end{cases}$$

где

$$p = \frac{\lambda - 2s - \beta}{s^2 + d - \beta}; \qquad q = \frac{\mu - \beta}{s^2 + d - \beta}; \qquad \beta = \frac{1}{n}(s^2 + d + d(\lambda - 2s) + (n - d - 1)\mu)$$

Таким образом, полученные векторы образуют на сфере множество с двумя расстояниями.

3.3.2. Применение конструкции.

Рассмотрим сильно регулярный граф $G = G_2(4)$ с параметрами ($n = 416$, $d = 100$, $\lambda = 36$, $\mu = 20$).

Для этого графа описанные величины равны

$$r = 20; \qquad s = -4$$

$$f = 65; \qquad g = 350$$

$$p = \frac{1}{5}; \qquad q = -\frac{1}{15}$$

Таким образом, векторы y_i имеют рациональные координаты, а значит квадраты координат векторов x_i тоже рациональны. Используя рассуждения с теоремой Лагранжа из предыдущего раздела заметим, что полученное множество аффинно-рационально лежит на сфере радиуса 1. При этом оно все так же лежит в подпространстве размерности не более f.

Наконец, докажем теорему 2.

Доказательство. [Доказательство теоремы 2] Построенное множество образует граф с двумя расстояниями, причем наибольшее из них равно $\sqrt{2-2q} = \sqrt{\frac{32}{15}}$, и оно достигается, когда соответствующие вершины не связаны ребром. Снова отнормируем векторы так, чтобы диаметр стал равным 1. Тогда радиус сферы станет равным $\sqrt{\frac{15}{32}} < \sqrt{\frac{1}{2}}$. Заметим, что данное множество нельзя разбить менее, чем на $\frac{n}{\omega(G)}$, где $\omega(G)$ – кликовое число графа G. Известно, что $\omega(G_2(4)) \leq 5$, поэтому $h(65) = h(f) \geq \frac{n}{\omega(G_2(4))} \geq \frac{416}{5} > 83 > 66$.

Затем, поднимая контрпримеры так же, как и в лемме 3, получим, что аффинно-рациональный аналог гипотезы Борсука не верен при $n \geq 65$. □

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. A.M. Raigorodskii, *Coloring Distance Graphs and Graphs of Diameters*, Thirty Essays on Geometric Graph Theory, J. Pach ed., Springer, 2013, 429 - 460.
2. P.K. Agarwal, J. Pach, *Combinatorial geometry*, John Wiley and Sons Inc., New York, 1995.
3. V. Klee, S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, Math. Association of America, 1991.
4. P. Brass, W. Moser, J. Pach, *Research problems in discrete geometry*, Springer, 2005.
5. L.A. Székely, *Erdős on unit distances and the Szemerédi – Trotter theorems*, Paul Erdős and his Mathematics, Bolyai Series Budapest, J. Bolyai Math. Soc., Springer, 11 (2002), 649 - 666.
6. A. Soifer, *The Mathematical Coloring Book*, Springer, 2009.
7. A. de Grey, *The chromatic number of the plane is at least 5*, arXiv:1804.02385, April 2018.
8. А.М. Райгородский, *Проблема Борсука и хроматические числа некоторых метрических пространств*, Успехи матем. наук, 56 (2001), N1, 107 - 146.
9. А.М. Райгородский, *Проблема Эрдеша–Хадвигера и хроматические числа конечных геометрических графов*, Матем. сборник, 196 (2005), N1, 123 - 156.
10. A.M. Raigorodskii, *Cliques and cycles in distance graphs and graphs of diameters*, "Discrete Geometry and Algebraic Combinatorics", AMS, Contemporary Mathematics, 625 (2014), 93 - 109.
11. A.M. Raigorodskii, *Combinatorial geometry and coding theory*, Fundamenta Informatica, 145 (2016), 359 - 369.
12. Л.И. Боголюбский, А.М. Райгородский, *Замечание о нижних оценках хроматических чисел пространств малой размерности с метриками l_1 и l_2*, подано в Матем. заметки.
13. Д.А. Захаров, А.М. Райгородский, *Клико-хроматические числа графов пересечений*, Матем. заметки, 105 (2019), N1, 142–144.
14. А.М. Райгородский, Е.Д. Шишунов, *О числах независимости некоторых дистанционных графов с вершинами в $\{-1, 0, 1\}^n$*, Доклады РАН, 485 (2019), N3.
15. О. А. Костина, "О нижних оценках хроматического числа сферы", Матем. заметки, 105:1 (2019), 18–31

16. Ф. А. Пушняков, “О количествах ребер в порожденных подграфах некоторых дистанционных графов”, Матем. заметки, 105:4 (2019), 592–602

17. Ю. А. Демидович, “Дистанционные графы в рациональном пространстве с большим хроматическим числом и без клик заданного размера”, Матем. заметки, 106:1 (2019), 24–39

18. A.M. Raigorodskii, A.B. Kupavskii, *On the chromatic numbers of small-dimensional Euclidean spaces*, Electronic Notes in Discrete Mathematics, 34 (2009), 435 - 439.

19. А.Я. Канель-Белов, В.А. Воронов, Д.Д. Черкашин, *О хроматическом числе плоскости*, Алгебра и анализ, том 29, выпуск 5, страницы 68–89.

20. Д.Д. Черкашин, А.М. Райгородский, *О хроматических числах пространств малой размерности*, Доклады РАН, 472 (2017), N1, 11 - 12.

21. D. Cherkashin, A. Kulikov, A. Raigorodskii, *On the chromatic numbers of small-dimensional Euclidean spaces*, Discrete and Applied Math., 243 (2018), 125 - 131.

22. M. Benda, M. Perles, *Colorings of metric spaces*, Geombinatorics, 9 (2000), 113 - 126.

23. А.М. Райгородский, *О хроматическом числе пространства с l_q-нормой*, Успехи мат. наук, 59 (2004), N5, 161 - 162.

24. А.М. Райгородский, И.М. Шитова, *О хроматических числах вещественных и рациональных пространств с вещественными или рациональными запрещенными расстояниями*, Матем. сборник, 199 (2008), N4, 107 - 142.

25. Е.И. Пономаренко, А.М. Райгородский, *Новая нижняя оценка хроматического числа рационального пространства*, Успехи матем. наук, 68 (2013), N5, 183 - 184.

26. Е.И. Пономаренко, А.М. Райгородский, *Новая нижняя оценка хроматического числа рационального пространства с одним и двумя запрещенными расстояниями*, Матем. заметки, 97 (2015), N2, 84 - 89.

27. Ю.А. Демидович, *Нижняя оценка хроматического числа рационального пространства с метрикой l_q с одним запрещенным расстоянием*, Матем. заметки, 102 (2017), N4, 532 - 548.

28. Е.И. Пономаренко, А.М. Райгородский, *О хроматическом числе пространства $\mathbb{Q}^n$*, Труды МФТИ, 4 (2012), N1, 127 - 130.

29. А. А. Соколов, *О хроматических числах рациональных пространств*, Матем. заметки, 103:1 (2018), 120–128.

30. V.G. Boltyanski, H. Martini, P.S. Soltan, *Excursions into combinatorial geometry*, Universitext, Springer, Berlin, 1997.

31. A.M. Raigorodskii, *Around Borsuk's conjecture*, J. of Math. Sci., 154 (2008), N4, 604 - 623.

32. A.M. Raigorodskii, *Three lectures on the Borsuk partition problem*, London Mathematical Society Lecture Note Series, 347 (2007), 202 - 248.

33. А.М. Райгородский, *Проблемы Борсука и Грюнбаума для решетчатых многогранников*, Известия РАН, 69 (2005), N3, 81 - 108.

34. А.Б. Купавский, Е.И. Пономаренко, А.М. Райгородский, *О некоторых аналогах проблемы Борсука в пространстве* $\mathbb{Q}^n$, Труды МФТИ, 4 (2012), N1, 81 - 90.

35. K.B. Chilakamarri, *Unit-distance graphs in rational n-spaces*, Discrete Math. 69 (1988), 213 - 218.

36. C. Elsholtz, W Klotz, *Maximal Dimension of Unit Simplices*, Discrete Comput Geom, 34 (2005), 167 - 177.

37. A. Bondarenko, *On Borsuk's Conjecture for Two-Distance Sets*, Discrete Comput Geom, 51 (2014), 509 - 515.

38. N.G. de Bruijn, P. Erdős, *A colour problem for infinite graphs and a problem in the theory of relations*, Proc. Koninkl. Nederl. Acad. Wet., Ser. A, 54 (1951), N5, 371 - 373.

REFERENCES

1. A.M. Raigorodskii, *Coloring Distance Graphs and Graphs of Diameters*, Thirty Essays on Geometric Graph Theory, J. Pach ed., Springer, 2013, 429 - 460.

2. P.K. Agarwal, J. Pach, *Combinatorial geometry*, John Wiley and Sons Inc., New York, 1995.

3. V. Klee, S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, Math. Association of America, 1991.

4. P. Brass, W. Moser, J. Pach, *Research problems in discrete geometry*, Springer, 2005.

5. L.A. Székely, *Erdős on unit distances and the Szemerédi – Trotter theorems*, Paul Erdős and his Mathematics, Bolyai Series Budapest, J. Bolyai Math. Soc., Springer, 11 (2002), 649 - 666.

6. A. Soifer, *The Mathematical Coloring Book*, Springer, 2009.

7. A. de Grey, *The chromatic number of the plane is at least 5*, arXiv:1804.02385, April 2018.

8. A.M. Raigorodskii, *The Borsuk problem and the chromatic numbers of some metric spaces*, Russian Math. Surveys, 56 (2001), N1, 103 - 139.

9. A.M. Raigorodskii, *The Erdős–Hadwiger problem and the chromatic numbers of finite geometric graphs*, Sbornik Math., 196 (2005), N1, 115 - 146.

10. A.M. Raigorodskii, *Cliques and cycles in distance graphs and graphs of diameters*, "Discrete Geometry and Algebraic Combinatorics", AMS, Contemporary Mathematics, 625 (2014), 93 - 109.

11. A.M. Raigorodskii, *Combinatorial geometry and coding theory*, Fundamenta Informatica, 145 (2016), 359 - 369.

12. L.I. Bogoliubsky, A.M. Raigorodskii, *A Remark on Lower Bounds for the Chromatic Numbers of Spaces of Small Dimension with Metrics* l_1, l_2, Math. Notes., 105 (2019), N2, 180 - 203.

13. D.A. Zakharov, A.M. Raigorodskii, *Clique-chromatic numbers of graphs of intersections*, Math. Notes., 105 (2019), N1, 137 - 139.

14. E.A. Shishunov, A.M. Raigorodskii, *On the independence numbers of some distance graphs with vertices in* $\{-1, 0, 1\}^n$, Doklady Math., 99 (2019), N2, 165 - 166.

15. O. A. Kostina, “On Lower Bounds for the Chromatic Number of Spheres”, Math. Notes, 105:1 (2019), 16–27

16. F.A. Pushnyakov, "On the number of edges in induced subgraphs of some distance graphs Math. Notes, 105:4 (2019).

17. Yu. A. Demidovich, *Distance graphs in rational spaces with large chromatic number and without cliques of given size*, Math. Notes, 106:1 (2019).

18. A.M. Raigorodskii, A.B. Kupavskii, On the chromatic numbers of small-dimensional Euclidean spaces, Electronic Notes in Discrete Mathematics, 34 (2009), 435 - 439.

19. A. Ya. Kanel-Belov, V. A. Voronov, D. D. Cherkashin, “On the chromatic number of infinitesimal plane layer”, St. Petersburg Math. J., 29:5 (2018), 761–775.

20. D.D. Cherkashin, A.M. Raigorodskii, *On the chromatic numbers of small-dimensional spaces*, Doklady Math., 95 (2017), N1, 5 - 6.

21. D. Cherkashin, A. Kulikov, A. Raigorodskii, On the chromatic numbers of small-dimensional Euclidean spaces, Discrete and Applied Math., 243 (2018), 125 - 131.

22. M. Benda, M. Perles, Colorings of metric spaces, Geombinatorics, 9 (2000), 113 - 126.

23. A.M. Raigorodskii, *On the chromatic number of a space with l_q-norm*, Russian Math. Surveys, 59 (2004), N5, 973 - 975.

24. A.M. Raigorodskii, I.M. Shitova, *On the chromatic numbers of real and rational spaces with several real or rational forbidden distances*, Sbornik Math., 199 (2008), N4, 579 - 612.

25. E.I. Ponomarenko, A.M. Raigorodskii, *New lower bound on the chromatic number of the rational space*, Russian Math. Surveys, 68 (2013), N5, 960 - 962.

26. E.I. Ponomarenko, A.M. Raigorodskii, *New lower bound on the chromatic number of the rational space with one or two forbidden distances*, Math. Notes, 97 (2015), N2, 255 - 261.

27. Yu. A. Demidovich, “Lower Bound for the Chromatic Number of a Rational Space with Metric l_1 and with One Forbidden Distance”, Math. Notes, 102:4 (2017), 492–507.

28. E.I. Ponomarenko, A.M. Raigorodskii, *On the chromatic number of the space $\mathbb{Q}^n$*, Proceedings of Moscow Institute of Physics and Technology, 4 (2012), N1, 127 - 130.

29. A. Sokolov, “On the Chromatic Numbers of Rational Spaces”, Math. Notes, 103:1-2 (2018), 111–117.

30. V.G. Boltyanski, H. Martini, P.S. Soltan, Excursions into combinatorial geometry, Universitext, Springer, Berlin, 1997.

31. A.M. Raigorodskii, *Around Borsuk's conjecture*, J. of Math. Sci., 154 (2008), N4, 604 - 623.

32. A.M. Raigorodskii, *Three lectures on the Borsuk partition problem*, London Mathematical Society Lecture Note Series, 347 (2007), 202 - 248.

33. A.M. Raigorodskii, *The Borsuk and Grünbaum problems for lattice polytopes*, Izvestiya Math., 69 (2005), N3, 513 - 537.

34. A.M. Raigorodskii, A.B. Kupavskii, E.I. Ponomarenko, *On some analogs of Borsuk's problem in the space* $\mathbb{Q}^n$, Proceedings of of Moscow Institute of Physics and Technology, 4 (2012), N1, 81 - 90.

35. K.B. Chilakamarri, *Unit-distance graphs in rational n-spaces*, Discrete Math. 69 (1988), 213 - 218.

36. C. Elsholtz, W Klotz, *Maximal Dimension of Unit Simplices*, Discrete Comput Geom, 34 (2005), 167 - 177.

37. A. Bondarenko, *On Borsuk's Conjecture for Two-Distance Sets*, Discrete Comput Geom, 51 (2014), 509 - 515.

38. N.G. de Bruijn, P. Erdős, *A colour problem for infinite graphs and a problem in the theory of relations*, Proc. Koninkl. Nederl. Acad. Wet., Ser. A, 54 (1951), N5, 371 - 373.

Получено 29.07.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.6 DOI 10.22405/2226-8383-2018-19-3-282-297

Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях [1]

Федоров Глеб Владимирович — кандидат физико-математических наук, старший научный сотрудник, Научно-исследовательского института системных исследований РАН (ФГУ ФНЦ НИИСИ РАН), г. Москва.
e-mail: fedorov@mech.math.msu.su

Аннотация

К настоящему времени метод непрерывных дробей позволил глубоко изучить проблему существования и построения нетривиальных S-единиц в гиперэллиптических полях в случае, когда множество S состоит из двух линейных нормирований. Данная статья посвящена более общей проблеме, а именно проблеме существования и построения фундаментальных S-единиц в гиперэллиптических полях для множеств S, содержащих нормирования второй степени. Ключевым является случай, когда множество $S = S_h$ состоит из двух сопряжённых нормирований, связанных с неприводимым многочленом h второй степени. Основные результаты получены с помощью теории обобщенных функциональных непрерывных дробей в совокупности с геометрическим подходом к проблеме кручения в якобиевых многообразиях гиперэллиптических кривых.

Нами разработана теория обобщенных функциональных непрерывных дробей и связанных с ними дивизоров гиперэллиптического поля, построенных с помощью нормирований второй степени. Эта теория позволила нам найти новые эффективные методы для поиска и построения фундаментальных S_h-единиц в гиперэллиптических полях.

В качетсве демонстрации полученных результатов, мы подробно разбираем алгоритм поиска фундаментальных S_h-единиц для гиперэллиптических полей рода 3 над полем рациональных чисел и приводим явные вычислительные примеры гиперэллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$ для многочленов f степени 7, обладающих фундаментальными S_h-единицами больших степеней.

Ключевые слова: непрерывные дроби, фундаментальные единицы, S-единицы, кручение в якобианах, гиперэллиптические кривые, дивизоры, группа классов дивизоров.

Библиография: 16 – названий.

Для цитирования:
Г. В. Федоров. Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях // Чебышевский сборник, 2018, т. 19, вып. 3, с. 282–297.

[1] Исследование выполнено за счет гранта Российского научного фонда (проект 16–11–10111).

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.6 DOI 10.22405/2226-8383-2018-19-3-282-297

Periodic continued fractions and S-units with second degree valuations in hyperelliptic fields[2]

Fedorov Gleb Vladimirovich — Ph.D., Senior Research Fellow, Scientific Research Institute of System Analysis (SRISA/NIISI RAS), Moscow.
e-mail: fedorov@mech.math.msu.su

Abstract

Based on the method of continued fractions by now the problem of the existence and construction of nontrivial S-units is deeply studied in hyperelliptic fields in the case when the set S consists of two linear valuations. This article is devoted to a more general problem, namely the problem of the existence and construction of fundamental S-units in hyperelliptic fields for sets S containing valuations of the degree 2. The key case when the set $S = S_h$ consists two conjugate valuations, connected with an irreducible polynomial h of the degree 2. The main results were obtained using the theory of generalized functional continued fractions in conjunction with the geometric approach to the problem of torsion in Jacobian varieties of hyperelliptic curves.

We have developed a theory of generalized functional continued fractions and the divisors of the hyperelliptic field associated with them, constructed with the help of valuations of the degree 2. This theory allowed us to find new effective methods for searching and constructing fundamental S_h-units in hyperelliptic fields.

As a demonstration of the results, we consider in detail algorithm to search for fundamental S_h-units for hyperelliptic fields of genus 3 over the field of rational numbers and give explicit computational examples of hyperelliptic fields $L = \mathbb{Q}(x)(\sqrt{f})$ for polynomials f of degree 7, possessing fundamental S_h-units of large powers.

Keywords: continued fractions, fundamental units, S-units, torsion in the Jacobians, hyperelliptic curves, divisors, the group of divisor classes.

Bibliography: 16 – titles.

For citation:
G. V. Fedorov, 2018, "Periodic continued fractions and S-units with second degree valuations in hyperelliptic fields", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 282–297.

1. Введение

Одной из актуальных современных проблем алгебры и теории чисел является проблема существования и построения фундаментальных S-единиц в гиперэллиптических полях. Эта проблема имеет большую историю, восходящую к Абелю [1] и Чебышеву [2]. Важность этой проблемы подчеркивается глубокой связью с проблемой кручения в якобиевых многообразиях гиперэллиптических кривых и свойствами функциональных непрерывных дробей, в которые могут разлагаться элементы гиперэллиптических полей. В статье [8] предложены два метода для поиска S-единиц в гиперэллиптических полях: метод матричной линеаризации и метод функциональных непрерывных дробей. Метод матричной линеаризации имеет общую природу

[2]The study was carried out at the expense of a grant from the Russian science Foundation (project 16–11–10111).

и применим к произвольному набору нормирований S. В [8] показано, что метод непрерывных дробей имеет более эффективное применение для множеств S, состоящих из бесконечного нормирования и нормирования степени один. Опираясь на метод непрерывных дробей в статьях [3]-[15] была глубоко изучена проблема существования и построения нетривиальных S-единиц в гиперэллиптических полях в случае, когда множество S состоит из двух линейных нормирований. Однако, в статье [8] для S, состоящего из бесконечного нормирования и нормирования степени два, был построен контрпример для которого метод непрерывных дробей в текущем виде теряет свою эффективность.

Данная статья посвящена проблеме существования и построения фундаментальных S-единиц в гиперэллиптических полях для множеств S более общего вида. Отдельно мы выделяем важный случай, когда множество $S = S_h$ состоит из двух сопряжённых нормирований, связанных с неприводимым многочленом h второй степени. Нами впервые найдены методы поиска и построения фундаментальных S_h-единиц в гиперэллиптических полях сравнимые по эффективности с методами для двух линейных нормирований. Получить существенные продвижения удалось благодаря тому, что в проблеме существования и построения фундаментальных S-единиц впервые была применена теория обобщенных функциональных непрерывных дробей в совокупности с геометрическим подходом к проблеме кручения в якобиевых многообразиях гиперэллиптических кривых.

Для случая двух линейных нормирований в статьях [7] и [13] был представлен новый геометрический метод, основанный на последовательном построении специальных дивизоров для заданного элемента гиперэллиптического поля. Многочлены Мамфорда этой последовательности дивизоров оказываются тесно связанными с непрерывной дробью рассматриваемого элемента. Основные результаты данной статьи были получены путем обобщения методов статей [7] и [13] для дивизоров, обобщенных непрерывных дробей и S_h-единиц, связанных с нормированиями второй степени.

2. Обозначения и вспомогательные утверждения

Пусть K — поле характеристики отличной от 2, и $f \in K[x]$ — свободный от квадратов многочлен, $\deg f = 2g+1$, $g \geqslant 1$, $L = K(x)(\sqrt{f})$. Пусть $\mathcal{V}$ — множество нормирований поля L, определенных над полем K. Обозначим $\mathrm{Div}(L)$ — группу K-дивизоров поля L,

$$\mathrm{Div}(L) = \left\{ D = \sum_{v \in \mathcal{V}} n_v v,\ n_v \in \mathbb{Z} \right\},$$

где для каждого дивизора D в наборе чисел $\{n_v\}_{v\in\mathcal{V}}$ только конечное количество отлично от нуля. Там, где ясно, что суммирование берется по $v \in \mathcal{V}$, будем его опускать. Все дивизоры, о которых далее пойдет речь, лежат в $\mathrm{Div}(L)$.

Для дивизора $D \in \mathrm{Div}(L)$, $D = \sum n_v v$, определим степень дивизора

$$\deg D = \sum n_v \deg v.$$

Для фиксированного нормирования $v \in \mathcal{V}$ определим число $v(D) = n_v = n_v(D)$. Дивизор $D \in \mathrm{Div}(L)$ называется эффективным, если $v(D) \geqslant 0$ для всех $v \in \mathcal{V}$. Скажем, что для дивизоров $D, E \in \mathrm{Div}(L)$ выполнено сравнение $D \leqslant E$, если $E - D$ эффективный дивизор.

Для главного дивизора (α) функции $\alpha \in L$, $\alpha \neq 0$, обозначим $(\alpha)_z$ и $(\alpha)_p$ соответственно эффективный дивизор нулей и эффективный дивизор полюсов функции α так, что $(\alpha) = (\alpha)_z - (\alpha)_p$, причем $v\big((\alpha)_z\big) \cdot v\big((\alpha)_p\big) = 0$ для всех $v \in \mathcal{V}$.

Группу дивизоров степени ноль поля L обозначим $\mathrm{Div}^\circ(L)$, группу главных дивизоров поля L обозначим $\mathrm{Princ}(L)$, группу классов дивизоров степени ноль поля L обозначим

$\Delta^\circ(L) = \mathrm{Div}^\circ(L)/\,\mathrm{Princ}(L)$. Скажем, что дивизоры $D, E \in \mathrm{Div}^\circ(L)$ эквивалентны $D \sim E$, если они принадлежат одному классу в группе классов дивизоров $\Delta^\circ(L)$.

Инволюция ι поля L, действуйющая $\iota : \sqrt{f} \to -\sqrt{f}$, $\iota^2 = \mathrm{id}$, может быть естественным образом определена на группе дивизоров $\mathrm{Div}(L)$ поля L.

Обозначим множество целых неотрицательных чисел $\mathbb{N}_0$.

Пусть $h \in K[x]$ — неприводимый многочлен, $\deg h \geqslant 1$, $h \nmid f$. Рассмотрим обобщенную непрерывную дробь вида

$$a_0 + \cfrac{h}{a_1 + \cfrac{h}{a_2 + \cdots}}, \tag{1}$$

где элементы a_j для всех $j \in \mathbb{N}_0$ имеют вид $a_j = \tilde{a}_j \cdot h^{-s_j}$, $s_j \in \mathbb{N}_0$, $\tilde{a}_j \in K[x]$, $h \nmid \tilde{a}_j$, $\deg \tilde{a}_j < (s_j + 1)\deg h$, и $\tilde{a}_j \neq 0$ при $j \geqslant 1$. Мы далее будем рассматривать только такие обобщенные непрерывные дроби, поэтому будем называть выражение (1) непрерывной дробью и сохраним для нее традиционное обозначение $[a_0; a_1, a_2, \ldots]$. Элементы $a_0, a_1, \ldots$ называются неполными частными непрерывной дроби (1). Для $n \in \mathbb{N}_0$ выражения $\alpha_n = [a_n; a_{n+1}, a_{n+2}, \ldots]$ называются полными частными непрерывной дроби (1). Для $j \in \mathbb{N}_0$ справедливы равенства

$$\alpha_{j+1}(\alpha_j - a_j) = h. \tag{2}$$

Обозначим $\Sigma = \{b \in K[x],\ \deg b < \deg h\}$, и $\Sigma((h))$ — множество формальных степенных рядов вида

$$\sum_{j=s}^{\infty} b_j h^j, \tag{3}$$

где $s \in \mathbb{Z}$, и при $j \geqslant s$ имеем $b_j \in \Sigma$, $b_s \neq 0$. Для степенного ряда α вида (3) обозначим $v_h(\alpha) = s$. Множество формальных степенных рядов $\Sigma((h))$ является полем. Для непрерывной дроби (1) неполные частные α_n, $n \in \mathbb{N}_0$, принадлежат полю формальных степенных рядов $\Sigma((h))$. Если непрерывная дробь α_0 конечная, то $\alpha_0 \in K(x) \subset \Sigma((h))$.

Подходящей дробью к непрерывной дроби (1) называется

$$p_j/q_j = [a_0; a_1, \ldots, a_j] \in K(x),\ j \in \mathbb{N}_0.$$

Положим $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$. Тогда аналогично числовому случаю справедливы рекуррентные формулы для построения подходящих дробей

$$p_{j+1} = a_{j+1}p_j + hp_{j-1}, \quad q_{j+1} = a_{j+1}q_j + hq_{j-1}, \quad j \in \mathbb{N}. \tag{4}$$

Кроме того, аналогично числовому случаю при $j \in \mathbb{N}$ справедливы тождества

$$\begin{gathered} p_{j-1}q_j - p_jq_{j-1} = (-1)^j h^j, \\ \alpha_0 = \frac{\alpha_{j+1}p_j + hp_{j-1}}{\alpha_{j+1}q_j + hq_{j-1}}, \\ \alpha_0 - \frac{p_j}{q_j} = \frac{(-1)^j h^{j+1}}{q_j(\alpha_{j+1}q_j + hq_{j-1})}. \end{gathered} \tag{5}$$

Если $a_0 \neq 0$ в непрерывной дроби (1), то из (5) имеем

$$v_h(p_{j+1}) = -s_{j+1} + v_h(p_j) = \sum_{k=0}^{j+1} s_k, \quad v_h(q_{j+1}) = -s_{j+1} + v_h(q_j) = \sum_{k=1}^{j+1} s_k.$$

Элемент $\alpha \in \Sigma((h))$, заданный рядом (3), можно представить в виде непрерывной дроби следующим образом. Определим $a_0 = \sum_{j=s}^{0} b_j h^j = [\alpha_0]_h$, если $s < 0$, а иначе $a_0 = 0$. Далее

положим $\alpha_0 = \alpha$, и, если $\alpha_0 - a_0 \neq 0$, то определим $\alpha_1 = h/(\alpha_0 - a_0)$. Если же $\alpha_0 - a_0 = 0$, то непрерывная дробь α имеет вид $[a_0]$. Так как $v_h(\alpha_0 - a_0) > 0$, то $v_h(\alpha_1) \leqslant 0$. Аналогично, определим $a_1 = [\alpha_1]_h$, причем в силу $v_h(\alpha_1) \leqslant 0$ имеем $a_1 \neq 0$. В случае $\alpha_1 - a_1 \neq 0$ положим $\alpha_2 = h/(\alpha_1 - a_1)$. Продолжая так и далее, мы получим конечную или бесконечную непрерывную дробь типа (1) для элемента α. Далее мы будем рассматривать именно такие непрерывные дроби, то есть непрерывные дроби вида (2) и удовлетворяющие свойству $v_h(\alpha_n) \leqslant 0$ при $n \in \mathbb{N}$. С этим соглашением любой элемент поля $\Sigma((h))$ имеет единственное разложение в непрерывную дробь типа (1).

3. Основные результаты

Рассмотрим неприводимый многочлен $h \in K[x]$, $\deg h = 2$, и свободный от квадратов многочлен $f \in K[x]$, $\deg f = 2g+1$, $g \geqslant 2$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на гиперэллиптическое поле $L = K(x)(\sqrt{f})$. Бесконечное нормирование v_∞ имеет единственное продолжение на поле L, эффективный дивизор, соответствующий бесконечному нормированию поля L, обозначим $\infty \in \mathrm{Div}(L)$. Обозначим $D_h \in \mathrm{Div}(L)$ — эффективный дивизор, соответствующий нормированию v_h^-. Тогда главный дивизор многочлена h можно записать в виде $(h) = D_h + \iota D_h - 4\infty$.

Пусть элемент $\alpha \in L$ имеет вид

$$\alpha = \frac{\sqrt{f} + V}{U}, \tag{6}$$

где

$$U, V \in K[x], \quad U \cdot h \mid f - V^2, \quad g - 1 \leqslant \deg U \leqslant g, \quad \deg V \leqslant \deg U + 1. \tag{7}$$

Определим

$$R = \frac{f - V^2}{U \cdot h}, \quad a = [\alpha]_h^-, \quad W = aU - V, \quad T = \frac{f - W^2}{U \cdot h}, \quad \beta = \frac{\sqrt{f} + W}{T}. \tag{8}$$

Предложение 1. *Справедливы следующие утверждения*

- $R, W, T \in K[x]$ — *многочлены, причем* $g - 1 \leqslant \deg R, \deg T \leqslant g$, $\deg W \leqslant \deg T + 1$;
- *существуют и однозначно определены эффективные дивизоры* D_R, D_U, $D_T \in \in \mathrm{Div}(L)$ *такие, что главные дивизоры многочленов* $R, U, T \in K[x]$ *и функций* $\sqrt{f} - V$, $\sqrt{f} - W \in L$ *имеют вид*

$$(R) = D_R + \iota D_R + r\big(D_h + \iota D_h\big) - \deg R \cdot 2\infty, \quad v_h(R) = r, \tag{9}$$
$$(U) = D_U + \iota D_U + s\big(D_h + \iota D_h\big) - \deg U \cdot 2\infty, \quad v_h(U) = s, \tag{10}$$
$$(T) = D_T + \iota D_T + t\big(D_h + \iota D_h\big) - \deg T \cdot 2\infty, \quad v_h(T) = t, \tag{11}$$
$$\Big(\sqrt{f} - V\Big) = D_R + (r + s + 1)D_h + \iota D_U - \max(2g + 1, 2\deg V) \cdot \infty, \tag{12}$$
$$\Big(\sqrt{f} - W\Big) = D_U + (s + t + 1)D_h + \iota D_T - \max(2g + 1, 2\deg W) \cdot \infty; \tag{13}$$

- *справедливо тождество* $\beta(\alpha - a) = h$.

Доказательство. По построению (6) имеем $U \cdot h \mid f - V^2$ и $2g+1 \leqslant \deg(f - V^2) \leqslant 2g+2$, следовательно, R — многочлен, $g - 1 \leqslant \deg R \leqslant g$. Так как элемент $a = [\alpha]_h^-$ имеет вид $a = \tilde{a} \cdot h^{-s}$, где $\tilde{a} \in K[x]$, $v_h(U) = s$, $\deg \tilde{a} \leqslant 2s + 1$, то W — многочлен степени не превосходящей $g + 1$. Положим $v_h(R) = r$. Определим в качетсве D_R и D_U такие максимальные эффективные дивизоры из $\mathrm{Div}(L)$, что $D_R \leqslant (R \cdot h^{-r})_z$, $D_R \leqslant \big(\sqrt{f} - V\big)_z$, и $D_U \leqslant (U \cdot h^{-s})_z$, $\iota D_U \leqslant \big(\sqrt{f} - V\big)_z$.

В силу того, что по построению (6) справедливо равенство $f - V^2 = R \cdot h \cdot U$, то выполнены соотношения (9), (10), (12).

Далее покажем, что $D_U + (s+1)D_h \leqslant \left(\sqrt{f} - W\right)_z$. Рассмотрим тождество

$$\frac{\sqrt{f} - W}{U} = \frac{\sqrt{f} + V}{U} - a. \tag{14}$$

Поскольку дивизор полюсов главного дивизора функции a имеет вид $s(D_h + \iota D_h)$ и $D_U \leqslant \left(\sqrt{f} + V\right)_z$, то

$$\iota D_U \leqslant \left(\frac{\sqrt{f} + V}{U} - a\right)_p,$$

следовательно, $D_U \leqslant \left(\sqrt{f} - W\right)_z$. С другой стороны, по построению $v_h(a) = -s$ и

$$v_h^-\left(\frac{\sqrt{f} + V}{U} - a\right) = v_h^-(\alpha - a) > 0,$$

следовательно, $(s+1)D_h \leqslant \left(\sqrt{f} - W\right)_z$. Таким образом, $D_U + (s+1)D_h \leqslant \left(\sqrt{f} - W\right)_z$, следовательно, $U \cdot h \mid f - W^2$, откуда получаем, что T — многочлен, причем справедливы соотношения

$$\max(2g+1, 2\deg V) = \deg R + 2 + \deg U,$$
$$\max(2g+1, 2\deg W) = \deg U + 2 + \deg T.$$

Определим $t = v_h(T)$ и D_T — такой максимальный эффективный дивизор из $\mathrm{Div}(L)$, что $D_T \leqslant \left(T \cdot h^{-t}\right)_z$, $\iota D_T \leqslant \left(\sqrt{f} - W\right)_z$. Так как $f - W^2 = U \cdot h \cdot T$, то справедливы соотношения (11) и (13).

Единственность главных дивизоров $D_R, D_U, D_T \in \mathrm{Div}(L)$ следует из соотношений (8) и (9)-(13).

Соотношение $\beta(\alpha - a) = h$ следует из (14) и равенства $f - W^2 = U \cdot h \cdot T$. □

Предложение 1 позволяет с помощью формул (8) для элемента α, определенного в (6), эффективно строить нерерывную дробь вида (2) и ее полные частные α_n.

Предложение 2. *Пусть дан элемент $\alpha_0 = \alpha \in L$ вида (6)-(7). Тогда для $j \in \mathbb{Z}$, $j \geqslant -1$, существуют и однозначно определены многочлены $U_j, V_j \in K[x]$, $g - 1 \leqslant \deg U_j \leqslant g$, $\deg V_j \leqslant g+1$, $\max(2g+1, 2\deg V_j) = \deg U_j + 2 + \deg U_{j+1}$, и эффективные дивизоры $D_j \in \mathrm{Div}(L)$, для которых при $j \geqslant -1$ справедливы следующие формулы:*

$$\alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad f - V_j^2 = U_j \cdot h \cdot U_{j+1}, \tag{15}$$

$$a_{j+1} = [\alpha_{j+1}]_h^-, \quad V_{j+1} = a_{j+1}U_{j+1} - V_j, \tag{16}$$

$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h^-(\alpha_{j+1}), \tag{17}$$

$$(U_j) = D_j + \iota D_j + s_j\left(D_h + \iota D_h\right) - 2\deg U_j \cdot \infty, \tag{18}$$

$$\left(V_j - \sqrt{f}\right) = D_j + (s_j + s_{j+1} + 1)D_h + \iota D_{j+1} - \max(2g+1, 2\deg V_j) \cdot \infty. \tag{19}$$

Доказательство. По элементу α с помощью формул (8) построим элемент β. По построению непрерывной дроби имеем $\alpha_1(\alpha_0 - a_0) = h$, а с другой стороны по предложению 1 имеем $\beta(\alpha - a) = h$. Из того, что $a = a_0$ следует, что $\alpha_1 = \beta$, то есть элементы α_0 и α_1 имеют одинаковый вид:

$$\alpha_j = \frac{\sqrt{f} + V_{j-1}}{U_j}, \ j = \overline{0,1}, \tag{20}$$

где

$$V_{-1} = V,\ U_{-1} = R,\ U_0 = U,\ V_0 = W,\ U_1 = T. \tag{21}$$

Положим

$$D_{-1} = D_R,\ D_0 = D_U,\ D_1 = D_T,\ s_{-1} = r,\ s_0 = s,\ s_1 = t. \tag{22}$$

Продолжая рассуждать аналогично и далее, с помощью предложения 1 получаем (15)-(19) для всех $j \geqslant -1$. $\square$

Из предложения (2) следует, что данному элементу $\alpha \in L$ вида (6)-(7) соответствует корректно определенная последовательность эффективных дивизоров D_j, $j \in \mathbb{N}_0$. Следующее важное предложение играет ключевую роль в доказательстве теоремы 1.

Предложение 3. *Для $n \in \mathbb{N}$ справедливы соотношения*

$$D_n + s_n \cdot \iota D_h - D_0 - s_0 \cdot \iota D_h + (\deg U_n - \deg U_0) \cdot \infty \sim \sum_{j=0}^{n-1} (2s_j + 1)\big(D_h - 2\infty\big). \tag{23}$$

Доказательство. Просуммируем (19) по $j = 0, \ldots, n-1$, получим

$$\sum_{j=0}^{n-1}(2s_j+1)D_h + \sum_{j=0}^{n-1}(D_j + \iota D_j) - \iota D_0 + \iota D_n + (s_n - s_0)\cdot D_h \sim \sum_{j=0}^{n-1} \max(2g+1, 2\deg V_j)\cdot\infty. \tag{24}$$

Так как справедливо соотношение (18), то из (24) следует (23). $\square$

Теорема 1. *Пусть $s_0 = [g/2]$, $U = h^{s_0}$, $V = h^{s_0} \cdot \big[\sqrt{f}h^{-s_0}\big]_h^-$ и элемент $\alpha \in L$ имеет вид (6). Пусть справедливы построения (8), (20)-(22) и (15)-(19) для $j \in \mathbb{N}_0$. Тогда следующие условия эквивалентны*

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = D_0$;*
2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = cU_0$ для некоторой постоянной $c \in K^*$;*
3. *класс дивизора $\big(D_h - 2\infty\big)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*
4. *класс дивизора $\big(D_h - \iota D_h\big)$ имеет конечный порядок m_h в группе классов дивизоров $\Delta^\circ(L)$;*
5. *непрерывная дробь элемента α типа (1), определенная соотношениями (2), периодическая с длиной периода n или $2n$.*

Доказательство. Эквивалентность условий 1. и 2. следует из предложения 2.

Докажем, что из условия 3. следует условие 1.

Предположим, что дивизор $\big(D_h - 2\infty\big)$ имеет порядок $m \in \mathbb{N}$. Тогда найдется такой номер $n \in \mathbb{N}$, что

$$\sum_{j=0}^{n-2}(2s_j+1) < m \leqslant \sum_{j=0}^{n-1}(2s_j+1).$$

Обозначим $\delta = \sum_{j=0}^{n-1}(2s_j+1) - m$, тогда $0 \leqslant \delta \leqslant 2s_{n-1}$. Из предложения 3 следует, что

$$D_n + s_n \cdot \iota D_h - D_0 - s_0 \cdot \iota D_h + (\deg U_n - \deg U_0)\cdot\infty \sim \delta\big(D_h - 2\infty\big). \tag{25}$$

Пусть $\delta = 2\delta_0 - \delta_1$, где $\delta_1 \in \{0, 1\}$, $0 \leqslant \delta_0 \leqslant s_{n-1}$, $\delta_1 \leqslant \delta_0$. Так как

$$2\big(D_h - 2\infty\big) \sim \big(D_h - \iota D_h\big), \tag{26}$$

то из (25) получаем

$$D_n + s_n \cdot \iota D_h \sim D_0 + s_0 \cdot \iota D_h - \delta_0 \cdot \iota D_h + (\delta_0 - \delta_1)D_h + (\deg U_0 - \deg U_n + 2\delta_1) \cdot \infty. \qquad (27)$$

Так как по условию теоремы $s_{n-1} \leqslant s_0$, то в левой и правой частях (27) стоят эффективные дивизоры степени g. Обозначим

$$E = D_n + s_n \cdot \iota D_h - \Big(D_0 + s_0 \cdot \iota D_h - \delta_0 \cdot \iota D_h + (\delta_0 - \delta_1)D_h + (\deg U_0 - \deg U_n + 2\delta_1) \cdot \infty\Big). \quad (28)$$

Поскольку $E \sim 0$ и степень эффективного дивизора полюсов E не превосходит g, то E — главный дивизор некоторой рациональной функции $\beta \in K(x)$ (см. [16]). Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v \neq v_h^{\pm}$ и $v \neq \iota v$, имеем $v(E) \cdot \iota v(E) \leqslant 0$, а так, как E — главный дивизор рациональной функции, то получаем $v(E) = \iota v(E) = 0$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v = \iota v$, имеем $|v(E)| \leqslant 1$, а для главного дивизора рациональной функции E это возможно только, если $v(E) = 0$. Получается, что $\beta = bh^q$ для некоторых $q \in \mathbb{Z}$ и $b \in K^*$. Из (28) имеем $-1 \leqslant v_\infty^-(E) + v_\infty^+(E) \leqslant 3$, следовательно, $q = 0$. Так как по построению $v_h^+(D_n) = v_h^-(D_n) = 0$, то $\delta = 0$ и $D_n = 0$. Отсюда следует условие 1.

Докажем, что из условия 1. следует условие 3.

Предположим, что n — минимальное число такое, что $D_n = 0$, тогда по предложению 3 сразу следует, что класс дивизора $\big(D_h - 2\infty\big)$ имеет конечный порядок m в $\Delta^\circ(L)$.

В силу (26) из условия 3. следует конечность порядка класса дивизора $\big(D_h - \iota D_h\big)$ в $\Delta^\circ(L)$, то есть следует условие 4.

Если справедливо условие 4, то снова из (26) имеем условие 3.

Докажем, что условие 2. эквивалентно условию 5.

При заданном нормировании v_h^- второй степени непрерывная дробь полного частного $\alpha_j \in L$, построенная с помощью соотношений (2), зависит только от значения α_j, поэтому квазипериодичность α_0 эквивалентна условиям $V_n = V_0$ и $U_n = cU_0$ для некоторого минимального $n \in \mathbb{N}$, то есть квазипериодичность α_0 эквивалентна условию 2. Далее, в силу симметрии квазипериода непрерывной дроби (1) имеем $c = 1$, если n четно; для нечетного n длина периода совпадает с длиной квазипериода или в два раза больше длины квазипериода. □

Теорема 1 позволяют для неприводимого многочлена h второй степени сформулировать эффективный алгоритм поиска S_h-единиц и классов дивизоров конечного порядка в $\Delta^\circ(L)$.

Алгоритм 1. *Пусть дан многочлен* $f \in K[x]$, $\deg f = 2g + 1$, $g \geqslant 2$. *Положим* $s_0 = [g/2]$.

(i). Вычисляем

$$\xi = \sum_{j=0}^{s_0} f_j h^j \in K[x], \quad \text{где } \sqrt{f} = \sum_{j=0}^{\infty} f_j h^j \in \Sigma((h));$$

(ii). положим $U_0 = h^{s_0}$ *и* $V_0 = \xi$;

(iii). **цикл:** *для* $j \in \mathbb{N}_0$ *вычисляем*

(a) $U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}$;

(b) $a_{j+1} = \left[\frac{V_j + \xi}{U_{j+1}}\right]_h^-$;

(c) $V_{j+1} = a_{j+1} \cdot U_{j+1} - V_j$;

(d) проверяем, если $U_{j+1} = U_0$ *и* $V_{j+1} = V_0$, *то успешно завершаем цикл.*

Если алгоритм 1 завершился успешно, то есть был найден номер $n \in \mathbb{N}$ такой, что $U_n = U_0$ и $V_n = V_0$, то в поле L существует фундаментальная S_h-единица.

Разберем, как вычислить $a = \left[\frac{T}{U \cdot h^s}\right]_h^-$ для заданных многочленов $T, U \in K[x]$, $v_h(T) = v_h(U) = 0$.

Нам необходимо найти многочлен $A \in K[x]$ такой, что

$$AU \equiv T \pmod{h^{s+1}}, \quad \deg A < \deg h^{s+1} = 2(s+1).$$

Пусть $h = h_2x^2 + h_1x + h_0$ и

$$U = (\tau_s x + \kappa_s)h^s + \ldots + (\tau_0 x + \kappa_0), \quad T = (\zeta_s x + \chi_s)h^s + \ldots + (\zeta_0 x + \chi_0).$$

Будем искать многочлен A в следующем виде

$$A = (\rho_s x + \sigma_s)h^s + \ldots + (\rho_0 x + \sigma_0).$$

Так как

$$(\rho_0 x + \sigma_0)(\tau_0 x + \kappa_0) \equiv (\zeta_0 x + \chi_0) \pmod{h},$$

то в случае $\kappa_0 \neq 0$ имеем

$$\rho_0 = \frac{h_2(\zeta_0\kappa_0 - \tau_0\chi_0)}{h_0\tau_0^2 - h_1\tau_0\kappa_0 + h^2\kappa_0^2}, \quad \sigma_0 = \frac{h_2\chi_0 + h_0\rho_0\tau_0}{h_2\kappa_0},$$

а в случае $\kappa_0 \neq 0$ имеем

$$\rho_0 = -\frac{h_2\chi_0}{h_0\tau_0}, \quad \sigma_0 = \frac{h_2\zeta_0 + h_1\rho_0\tau_0}{h_2\tau_0},$$

причем знаменатели не обращаются в ноль в силу неприводимости многочлена h. Рассматривая сравнение $AU \equiv T \pmod{h^2}$, находим ρ_1 и σ_1 из линейного соотношения

$$(\rho_1 x + \sigma_1)(\tau_0 x + \kappa_0) \equiv (\zeta_1 x + \chi_1) - (\rho_0 x + \sigma_0)(\tau_1 x + \kappa_1) - \frac{\rho_0\tau_0}{h_2} \pmod{h}.$$

Далее, шаг за шагом находим все коэффициенты многочлена A.

Далее подробно разберем работу алгоритма 1 для случая $g = 3$ и $K = \mathbb{Q}$.

Зададимся целью найти бирационально неэквивалентных гиперэллиптические кривые рода три над полем рациональных чисел $\mathbb{Q}$, якобиан которых имеет нетривиальную подгруппу кручения. Для этого нам достаточно рассматривать пары многочленов f, h следующего вида:

$$f = c_7x^7 \ldots + c_0, \quad h = x^2 + h_0,$$

где $h_0, c_0, \ldots, c_7 \in \mathbb{Z}$, многочлен h неприводим, число h_0 свободно от квадратов, $c_7 > 0$ и $c_5 > 0$, либо $c_7 > 0$, $c_5 = 0$ и $c_3 > 0$, либо $c_7 > 0$, $c_5 = c_3 = 0$ и $c_1 \geqslant 0$. Также требуем, чтобы многочлен f был свободен от квадратов и $(f,\ h) \in \mathbb{Q}^*$.

Чтобы нормирование v_h автоматически имело два продолжения на поле

$$L = \mathbb{Q}(x)(\sqrt{f}),$$

мы будем рассматривать многочлен f в следующем виде:

$$f = (f_{00} + f_{01}x)^2 + 2(f_{00} + f_{01}x)(f_{10} + f_{11}x)h + (f_{20} + f_{21}x)h^2 + (f_{30} + f_{31}x)h^3,$$

где $f_{00}, f_{01}, f_{10}, f_{11}, f_{20}, f_{21}, f_{30} \in \mathbb{Z}$, $f_{31} \in \mathbb{N}_0$, причем либо $f_{00} > 0$, либо $f_{00} = 0$ и $f_{01} > 0$, а также либо $f_{31} > 0$ и $f_{21} > 0$, либо $f_{31} > 0$, $f_{21} = 0$ и $f_{11} \geqslant 0$. Заметим, что при этих условиях

$$\left[\frac{\sqrt{f}}{h^2}\right]_h^- = (f_{00} + f_{01}x) + (f_{10} + f_{11}x)h,$$

и в силу (15) для всех $j = 0, 1 \ldots$ справедливы соотношения

$$V_j^2 \equiv f \pmod h, \quad V_j \equiv f_{00} + f_{01}x \pmod h.$$

Положим

$$U_0 = h, \quad V_0 = (f_{00} + f_{01}x) + (f_{10} + f_{11}x)h.$$

Будем последовательно по $j = 1, 2 \ldots$ искать многочлены $U_j, h \cdot a_j, V_j \in \mathbb{Q}[x]$ такие, что $\deg U_j \leqslant 3$, $\deg V_j \leqslant 4$, $\deg(h \cdot a_j) \leqslant 3$ в следующем виде

$$U_j = (u_{00}^{(j)} + u_{11}^{(j)}x) + \big(u_{10}^{(j)} + u_{11}^{(j)}x\big)h, \quad u_{00}^{(j)}, u_{11}^{(j)}, u_{10}^{(j)}, u_{11}^{(j)} \in \mathbb{Q},$$

$$a_j = (a_{00}^{(j)} + a_{01}^{(j)}x) + \frac{a_{10}^{(j)} + a_{11}^{(j)}x}{h}, \quad a_{00}^{(j)}, a_{01}^{(j)}, a_{10}^{(j)}, a_{11}^{(j)} \in \mathbb{Q},$$

$$V_j = (v_{00}^{(j)} + v_{11}^{(j)}x) + \big(v_{10}^{(j)} + v_{11}^{(j)}x\big)h + v_{20}^{(j)}h^2, \quad v_{00}^{(j)}, v_{11}^{(j)}, v_{10}^{(j)}, v_{11}^{(j)}, v_{20}^{(j)} \in \mathbb{Q},$$

до тех пор, пока не встретится номер j, для которого $u_{00}^{(j)} = u_{11}^{(j)} = u_{21}^{(j)} = 0$. Отметим, что $a_{10}^{(j)} + a_{11}^{(j)}x = 0$ до тех пор, пока $h \nmid U_j$.

Предположим, что мы уже знаем многочлены

$$U_{j-1} = u_{00}^{(j-1)} + u_{11}^{(j-1)}x + \big(u_{10}^{(j)} + u_{11}^{(j)}x\big)h = w_3^{(j-1)}x^3 + w_2^{(j-1)}x^2 + w_1^{(j-1)}x + w_0^{(j-1)},$$
$$V_{j-1} = f_{00} + f_{01}x + (v_{10}^{(j-1)} + v_{11}^{(j-1)}x)h + v_{20}^{(j-1)}h^2.$$

На шаге с номером j вычислим коэффициенты $b_0^{(j)}, \ldots, b_6^{(j)} \in \mathbb{Q}$ многочлена

$$\frac{f - V_{j-1}^2}{h} = b_6^{(j)}x^6 + \ldots + b_0^{(j)},$$

следующим образом:

$$b_6^{(j)} = f_{40} - (v_4^{(j-1)})^2,$$
$$b_5^{(j)} = f_{31} - 2v_3^{(j-1)}v_4^{(j-1)},$$
$$b_4^{(j)} = f_{30} + 3f_{40}h_0 - 3h_0(v_4^{(j-1)})^2 - 2v_2^{(j-1)}v_4^{(j-1)} - (v_3^{(j-1)})^2,$$
$$b_3^{(j)} = -2f_{01}v_4^{(j-1)} + f_{21} + 2f_{31}h_0 - 4h_0v_3^{(j-1)}v_4^{(j-1)} - 2v_2^{(j-1)}v_3^{(j-1)},$$
$$b_2^{(j)} = -2f_{00}v_4^{(j-1)} + 2f_{01}f_{11} - 2f_{01}v_3^{(j-1)} + f_{20} + 2f_{30}h_0 + 3f_{40}h_0^2 -$$
$$-3h_0^2(v_4^{(j-1)})^2 - 4h_0v_2^{(j-1)}v_4^{(j-1)} - h_0(v_3^{(j-1)})^2 - (v_2^{(j-1)})^2,$$
$$b_1^{(j)} = 2f_{00}f_{11} - 2f_{00}v_3^{(j-1)} + 2f_{01}f_{10} - 2f_{01}h_0v_4^{(j-1)} - 2f_{01}v_2^{(j-1)} +$$
$$+f_{21}h_0 + f_{31}h_0^2 - 2h_0^2v_3^{(j-1)}v_4^{(j-1)} - 2h_0v_2^{(j-1)}v_3^{(j-1)},$$
$$b_0^{(j)} = 2f_{00}f_{10} - 2f_{00}h_0v_4^{(j-1)} - 2f_{00}v_2^{(j-1)} + f_{20}h_0 + f_{30}h_0^2 +$$
$$+f_{40}h_0^3 - h_0^3(v_4^{(j-1)})^2 - 2h_0^2v_2^{(j-1)}v_4^{(j-1)} - h_0(v_2^{(j-1)})^2.$$

Если $w_3^{(j-1)} \neq 0$, то вычислим

$$w_3^{(j)} = b_6^{(j-1)}/w_3^{(j-1)},$$
$$w_2^{(j)} = \left(b_5^{(j-1)}w_3^{(j-1)} - b_6^{(j-1)}w_2^{(j-1)}\right)/(w_3^{(j-1)})^2,$$
$$w_1^{(j)} = \left(b_4^{(j-1)}(w_3^{(j-1)})^2 - b_5^{(j-1)}w_2^{(j-1)}w_3^{(j-1)} - b_6^{(j-1)}w_1^{(j-1)}w_3^{(j-1)} + b_6^{(j-1)}(w_2^{(j-1)})^2\right)/(w_3^{(j-1)})^3,$$
$$w_0^{(j)} = \Big(b_3^{(j-1)}(w_3^{(j-1)})^3 - b_4^{(j-1)}w_2^{(j-1)}(w_3^{(j-1)})^2 - b_5^{(j-1)}w_1^{(j-1)}(w_3^{(j-1)})^2 + b_5^{(j-1)}(w_2^{(j-1)})^2w_3^{(j-1)} -$$
$$-b_6^{(j-1)}w_0^{(j-1)}(w_3^{(j-1)})^2 + 2b_6^{(j-1)}w_1^{(j-1)}w_2^{(j-1)}w_3^{(j-1)} - b_6^{(j-1)}(w_2^{(j-1)})^3\Big)/(w_3^{(j-1)})^4.$$

Если $w_3^{(j-1)}=0$, $w_2^{(j-1)}\neq 0$, то $b_6^{(j)}=0$ и

$$w_3^{(j)}=b_5^{(j-1)}/w_2^{(j-1)},$$
$$w_2^{(j)}=\left(b_4^{(j-1)}w_2^{(j-1)}-b_5^{(j-1)}w_1^{(j-1)}\right)/(w_2^{(j-1)})^2,$$
$$w_1^{(j)}=\left(b_3^{(j-1)}(w_2^{(j-1)})^2-b_4^{(j-1)}w_1^{(j-1)}w_2^{(j-1)}-b_5^{(j-1)}w_0^{(j-1)}w_2^{(j-1)}+b_5^{(j-1)}(w_1^{(j-1)})^2\right)/(w_2^{(j-1)})^3,$$
$$w_0^{(j)}=\Big(b_2^{(j-1)}(w_2^{(j-1)})^3-b_3^{(j-1)}w_1^{(j-1)}(w_2^{(j-1)})^2-b_4^{(j-1)}w_0^{(j-1)}(w_2^{(j-1)})^2+$$
$$+b_4^{(j-1)}(w_1^{(j-1)})^2w_2^{(j-1)}+2b_5^{(j-1)}w_0^{(j-1)}w_1^{(j-1)}w_2^{(j-1)}-b_5^{(j-1)}(w_1^{(j-1)})^3\Big)/(w_2^{(j-1)})^4.$$

Если $w_3^{(j-1)}=w_2^{(j-1)}=0$, то $b_6^{(j)}=b_5^{(j)}=0$ и

$$w_3^{(j)}=b_4^{(j-1)}/w_1^{(j-1)},$$
$$w_2^{(j)}=\left(b_3^{(j-1)}w_1^{(j-1)}-b_4^{(j-1)}w_0^{(j-1)}\right)/(w_1^{(j-1)})^2,$$
$$w_1^{(j)}=\left(b_2^{(j-1)}(w_1^{(j-1)})^2-b_3^{(j-1)}w_0^{(j-1)}w_1^{(j-1)}+b_4^{(j-1)}(w_0^{(j-1)})^2\right)/(w_1^{(j-1)})^3,$$
$$w_0^{(j)}=\Big(b_1^{(j-1)}(w_1^{(j-1)})^3-b_2^{(j-1)}w_0^{(j-1)}(w_1^{(j-1)})^2+$$
$$+b_3^{(j-1)}(w_0^{(j-1)})^2w_1^{(j-1)}-b_4^{(j-1)}(w_0^{(j-1)})^3\Big)/(w_1^{(j-1)})^4.$$

Если $w_3^{(j-1)}=w_2^{(j-1)}=w_1^{(j-1)}=0$, то $b_6^{(j)}=b_5^{(j)}=b_4^{(j)}=0$ и

$$w_3^{(j)}=b_3^{(j-1)}/w_0^{(j-1)},\quad w_2^{(j)}=b_2^{(j-1)}/w_0^{(j-1)},$$
$$w_1^{(j)}=b_1^{(j-1)}/w_0^{(j-1)},\quad w_0^{(j)}=b_0^{(j-1)}/w_0^{(j-1)}.$$

Далее вычисляем

$$u_{00}^{(j)}=-h_0w_2^{(j)}+w_0^{(j)},\quad u_{01}^{(j)}=-h_0w_3^{(j)}+w_1^{(j)},$$
$$u_{10}^{(j)}=w_2^{(j)},\quad u_{11}^{(j)}=w_3^{(j)}.$$

Рассмотрим два случая: $u_{00}^{(j)}=u_{01}^{(j)}=0$ и $u_{00}^{(j)}\cdot u_{01}^{(j)}\neq 0$.

Если $u_{00}^{(j)}=u_{01}^{(j)}=0$, то при $u_{00}^{(j)}\neq 0$ вычислим

$$a_{01}^{(j)}=\frac{f_{01}u_{00}^{(j)}-f_{00}u_{01}^{(j)}}{h_0(u_{01}^{(j)})^2+(u_{00}^{(j)})^2},\quad a_{00}^{(j)}=\frac{f_{00}+a_1^{(j)}u_{01}^{(j)}h_0}{u_{00}^{(j)}},$$

а при $u_{00}^{(j)}=0$ вычислим

$$a_{01}^{(j)}=-\frac{f_{00}}{h_0u_{01}^{(j)}},\quad a_{00}^{(j)}=\frac{f_{01}}{u_{01}^{(j)}}.$$

Наконец вычисляем коэффициенты многочлена V_j:

$$v_{10}^{(j)}=a_{01}^{(j)}u_{01}^{(j)}+a_{00}^{(j)}u_{10}^{(j)}-h_0a_{01}^{(j)}u_{01}^{(j)}-v_{10}^{(j-1)},$$
$$v_{11}^{(j)}=a_{00}^{(j)}u_{11}^{(j)}+a_{01}^{(j)}u_{10}^{(j)}-v_{11}^{(j-1)},$$
$$v_{20}^{(j)}=a_{01}^{(j)}u_{11}^{(j)}-v_{20}^{(j-1)}.$$

Если $u_{00}^{(j)} \cdot u_{01}^{(j)} \neq 0$, то при $u_{00}^{(j)} \neq 0$ вычислим

$$a_{11}^{(j)} = \frac{f_{01}u_{00}^{(j)} - f_{00}u_{01}^{(j)}}{h_0(u_{01}^{(j)})^2 + (u_{00}^{(j)})^2}, \quad a_{10}^{(j)} = \frac{f_{00} + a_1^{(j)}u_{01}^{(j)}h_0}{u_{00}^{(j)}},$$

а при $u_{00}^{(j)} = 0$ вычислим

$$a_{11}^{(j)} = -\frac{f_{00}}{h_0 u_{01}^{(j)}}, \quad a_{10}^{(j)} = \frac{f_{01}}{u_{01}^{(j)}}.$$

Далее положим

$$r_0^{(j)} = f_{10} + v_{10}^{(j)} - a_{10}^{(j)}u_{10}^{(j)} - a_{11}^{(j)}u_{01}^{(j)} + a_{11}^{(j)}u_{11}^{(j)}h_0,$$
$$r_1^{(j)} = f_{11} + v_{11}^{(j)} - a_{11}^{(j)}u_{10}^{(j)} - a_{10}^{(j)}u_{11}^{(j)},$$

тогда

$$a_{00}^{(j)} = \frac{r_0^{(j)}u_{00}^{(j)} - r_1^{(j)}u_{01}^{(j)}h_0}{h_0(u_{01}^{(j)})^2 + (u_{00}^{(j)})^2}, \quad a_{01}^{(j)} = \frac{r_1^{(j)}u_{00}^{(j)} - r_0^{(j)}u_{01}^{(j)}}{h_0(u_{01}^{(j)})^2 + (u_{00}^{(j)})^2}.$$

Наконец вычисляем коэффициенты многочлена V_j:

$$v_{10}^{(j)} = a_{11}^{(j)}u_{11}^{(j)} + a_{00}^{(j)}u_{10}^{(j)} - h_0 a_{01}^{(j)}u_{11}^{(j)} - v_{10}^{(j-1)},$$
$$v_{11}^{(j)} = a_{00}^{(j)}u_{11}^{(j)} + a_{01}^{(j)}u_{10}^{(j)} - v_{11}^{(j-1)},$$
$$v_{20}^{(j)} = a_{01}^{(j)}u_{11}^{(j)} - v_{20}^{(j-1)}.$$

Далее, согласно алгоритму 1 повторяем вышеописанные операции до тех пор, пока на некотором шаге n не будет выполнено $U_n = U_0$ и $V_n = V_0$.

4. Заключение

В качестве заключения продемонстрируем полученные результаты на примерах, найденных с помощью алгоритма 1 для $g = 3$.

Пример 1. *Рассмотрим поле $K = \mathbb{Q}$, многочлены $h = x^2 + 2$ и*

$$f = x^7 + x^6 + 4x^5 + 3x^4 + 6x^3 + 5x^2 + 4x + 4 =$$
$$= \left(x^2 + x + 2\right)\left(x^5 + 2x^3 + x^2 + x + 2\right).$$

Нормирование v_h поля $\mathbb{Q}(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = \mathbb{Q}(x)(\sqrt{f})$. Элемент $\sqrt{f}$ имеет следующее разложение в $\Sigma((h))$

$$\sqrt{f} = x + (1 - x) \cdot h + \ldots$$

Бесконечное нормирование поля $\mathbb{Q}(x)$ имеет единственное продолжение на поле L. Рассмотрим $D_0 = D_h + \infty$. Находим

$$U_0 = h, \quad V_0 = x + (1 - x) \cdot h + 0 \cdot h^2 = -x^3 + x^2 - x + 2.$$

Далее строим непрерывную дробь для элемента $\sqrt{f}/h$ по нормированию v_h^-:

$$\frac{\sqrt{f}}{h} = \left[-\frac{1}{x^2+2}\left(x^3-x^2+x-2\right); \overline{-\frac{1}{x^2+2}\left(x^3+2x^2+2x+2\right), x, x, 1, -2, 1, x, x, -\frac{1}{x^2+2}\left(x^3+2x^2+2x+2\right), -\frac{2}{x^2+2}\left(x^3-x^2+x-2\right)}\right].$$

Непрерывная дробь элемента $\sqrt{f}/h$ периодическая, причем период симметричен, длина периода равна длине квазипериода и равна 10. Замечаем, что $U_{10} = U_0$ и $V_{10} = V_0$, поэтому справедливы условия теоремы 1 и, следовательно, в якобиане гиперэллиптического поля L класс дивизора $\left(D_h - 2\infty\right)$ имеет порядок $m = 16$, а класс дивизора $\left(D_h - \iota D_h\right)$ имеет порядок $m/2 = 8$. В поле L существует фундаментальная S-единица и степени 16, которую можно найти с помощью (4):

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = h^{16}$$
$$\mu_1 = x^{16} + 18x^{15} + 40x^{14} + 140x^{13} + 242x^{12} + 426x^{11} + 724x^{10} + 664x^9 +$$
$$+1408x^8 + 512x^7 + 1904x^6 + 32x^5 + 1760x^4 - 224x^3 + 1056x^2 - 96x + 320,$$
$$\mu_2 = 6x^{12} + 28x^{11} + 38x^{10} + 152x^9 + 56x^8 +$$
$$+352x^7 - 32x^6 + 480x^5 - 160x^4 + 384x^3 - 192x^2 + 128x - 96.$$

Также в поле L существует фундаментальная S_h-единица u_h степени 8, $u_h = u \cdot h^{-8}$.

Пример 2. *Рассмотрим поле $K = \mathbb{Q}$, многочлены $h = x^2 + 1$ и*

$$f = x^7 + 3x^5 - 3x^4 + 5x^3 - 3x^2 + x = x\left(x^6 + 3x^4 - 3x^3 + 5x^2 - 3x + 1\right).$$

Нормирование v_h поля $\mathbb{Q}(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = \mathbb{Q}(x)(\sqrt{f})$. Элемент $\sqrt{f}$ имеет следующее разложение в $\Sigma((h))$

$$\sqrt{f} = (1-x) + x \cdot h + \ldots$$

Бесконечное нормирование поля $\mathbb{Q}(x)$ имеет единственное продолжение на поле L. Рассмотрим $D_0 = D_h + \infty$. Находим

$$U_0 = h, \quad V_0 = (1-x) + x \cdot h + 0 \cdot h^2 = x^3 + 1.$$

Далее строим непрерывную дробь для элемента $\sqrt{f}/h$ по нормированию v_h^-:

$$\frac{\sqrt{f}}{h} = \left[\frac{(x+1)\left(x^2-x+1\right)}{x^2+1}; \overline{-\frac{x^3-x^2+x+1}{x^2+1}, x-1, -x-1, 1, -2x, x, -\frac{2x\left(x^2-x+2\right)}{x^2+1}, x, -2x, 1, -x-1, x-1, -\frac{x^3-x^2+x+1}{x^2+1}, \frac{2(x+1)\left(x^2-x+1\right)}{x^2+1}}\right].$$

Непрерывная дробь элемента $\sqrt{f}/h$ периодическая, причем период симметричен, длина периода равна длине квазипериода и равна 14. Замечаем, что $U_{14} = U_0$ и $V_{14} = V_0$, поэтому справедливы условия теоремы 1 и, следовательно, в якобиане гиперэллиптического поля L класс дивизора $\left(D_h - 2\infty\right)$ имеет порядок $m = 22$, а класс дивизора $\left(D_h - \iota D_h\right)$ имеет порядок

$m/2 = 11$. В поле L существует фундаментальная S-единица и степени 22, которую можно найти с помощью (4):

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = h^{22}$$
$$\mu_1 = (x+1)\left(x^{21} + 7x^{20} + 12x^{19} + 30x^{18} + 29x^{17} + 61x^{16} + \right.$$
$$+152x^{15} - 120x^{14} + 642x^{13} - 946x^{12} + 2048x^{11} - 2588x^{10} + 3026x^9 - 2062x^8 +$$
$$\left. +936x^7 + 264x^6 - 515x^5 + 379x^4 - 76x^3 - 18x^2 + 17x + 1\right),$$
$$\mu_2 = \left(2x^8 + 4x^7 + 8x^6 - 4x^5 + 20x^4 + 4x^3 + 12x + 2\right) \times$$
$$\times \left(2x^{10} + x^9 + 5x^8 - 2x^7 + 6x^6 + 8x^5 - 16x^4 + 18x^3 - 8x^2 - x + 3\right).$$

Также в поле L существует фундаментальная S_h-единица u_h степени 11, $u_h = u \cdot h^{-11}$.

Пример 3. *Рассмотрим поле $K = \mathbb{Q}$, многочлены $h = x^2 + 2$ и*

$$f = 2x^7 + x^6 + 6x^5 + x^4 + 4x^3 + 4x^2 + 4 =$$
$$= \left(x^2 + 1\right)\left(2x^5 + x^4 + 4x^3 + 4\right).$$

Нормирование v_h поля $\mathbb{Q}(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = \mathbb{Q}(x)(\sqrt{f})$. Элемент $\sqrt{f}$ имеет следующее разложение в $\Sigma((h))$

$$\sqrt{f} = 2x + (1-x)\cdot h + \ldots$$

Бесконечное нормирование поля $\mathbb{Q}(x)$ имеет единственное продолжение на поле L. Рассмотрим $D_0 = D_h + \infty$. Находим

$$U_0 = h, \quad V_0 = 2x + (1-x)\cdot h + 0\cdot h^2 = -x^3 + x^2 + 2.$$

Далее строим непрерывную дробь для элемента $\sqrt{f}/h$ по нормированию v_h^-:

$$\frac{\sqrt{f}}{h} = \left[-\frac{x^3 - x^2 - 2}{x^2+2}; \overline{-1, -2x, -\frac{x\left(x^2+2x+2\right)}{2\left(x^2+2\right)}, \frac{2x\left(x^2+2x+2\right)}{x^2+2}, \frac{x}{2}, 4,}\right.$$
$$\left.\overline{\frac{x^3 - x^2 - 2}{2\left(x^2+2\right)}, 4, \frac{x}{2}, \frac{2x\left(x^2+2x+2\right)}{x^2+2}, -\frac{x\left(x^2+2x+2\right)}{2\left(x^2+2\right)}, -2x, -1, -\frac{2\left(x^3 - x^2 - 2\right)}{x^2+2}}\right].$$

Непрерывная дробь элемента $\sqrt{f}/h$ периодическая, причем период симметричен, длина квазипериода равна 7, длина периода равна 14, коэффициент квазипериода $c = -1/4$ Замечаем, что $U_7 = U_0$ и $V_7 = V_0$, поэтому справедливы условия теоремы 1 и, следовательно, в якобиане гиперэллиптического поля L класс дивизора $\left(D_h - 2\infty\right)$ имеет порядок $m = 13$, класс дивизора $\left(D_h - \iota D_h\right)$ также имеет порядок 13. В поле L существует фундаментальная S-единица и степени 13, которую можно найти с помощью (4):

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = h^{13}$$
$$\mu_1 = x^{13} + 16x^{12} + 45x^{11} + 149x^{10} + 220x^9 + 430x^8 +$$
$$+352x^7 + 584x^6 + 224x^5 + 528x^4 + 48x^3 + 336x^2 + 96,$$
$$\mu_2 = 4x^9 + 19x^8 + 48x^7 + 100x^6 + 112x^5 + 144x^4 + 64x^3 + 80x^2 + 16.$$

Также в поле L существует фундаментальная S_h-единица u_h степени 13.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Abel N. H. Uber die Integration der Differential-Formel $\rho\ \mathrm{d}x/\sqrt{R}$, wenn R und ρ ganze Functionen sind // J. Reine Angew. Math. 1826. №1. P. 185-221.

2. Chebychev P. L. Sur l'integration de la differential $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma}}\mathrm{d}x$ // J. Math. Pures Appl. 1864. Vol. 2, №9. P. 225-246.

3. Платонов В. П., Федоров Г. В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209, №4. С. 54-94.

4. 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.

5. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях // ДАН. 2017. Т. 474, №5. С. 540-544.

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., Жгун В. С., Федоров Г. В. Непрерывные дроби в гиперэллиптических полях и многочлены Мамфорда // ДАН. 2016. Т. 471, №6. С. 640-644.

8. Беняш-Кривец В. В., Платонов В. П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Мат. сборник. 2009. Т. 200, №1. С. 15-44.

9. Петрунин М. М. О периодичности квадратных корней в гиперэллиптических полях // ДАН. 2017. Т. 474, №2. С. 155-158.

10. Платонов В. П., Петрунин М. М. S-единицы и периодичность в квадратичных функциональных полях // УМН. 2016. Т. 71, №5. С. 181-182.

11. Платонов В. П., Петрунин М. М. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // ДАН. 2016. Т. 470, №3. С. 260-265.

12. Платонов В. П., Федоров Г. В., S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // ДАН. 2015. Т. 465, №5. С. 537-541.

13. Жгун В. С., Обобщенные якобианы и непрерывные дроби в гиперэллиптических полях // Чебышевский сборник. 2017. Т. 18, №4. С. 208-220.

14. 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.

15. 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.

16. Мамфорд Д. Лекции о тета-функциях // Мир, Москва, 1988.

REFERENCES

1. Abel, N. H. 1826, "Uber die Integration der Differential-Formel $\rho\,\mathrm{d}x/\sqrt{R}$, wenn R und ρ ganze Functionen sind", *J. Reine Angew. Math.* no. 1, pp. 185-221.

2. Chebychev, P. L. 1864, "Sur l'integration de la differential $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma}}\mathrm{d}x$", *J. Math. Pures Appl.*, vol. 2, no. 9, pp. 225-246.

3. 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.

4. 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.

5. 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.

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., 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.

8. 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. 15871615.

9. Petrunin, M. M. 2017, О периодичности квадратных корней в гиперэллиптических полях // ДАН. 2017. Т. 474, №2. С. 155-158.

10. 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.

11. 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.

12. 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.

13. Zhgoon, V. S. 2017, "On generalized jacobians and retional continued fractions in the hyperelliptic fields", *Chebyshevskii Sbornik*, vol. 18, no. 4, pp. 208-220. (In Russ.)

14. 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.)

15. Petrunin, M. M. 2015, "Calculation of the fndamental 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.)

16. Mumford, D. 1983, 1984, Tata Lectures on Theta I, II, *Progress in Mathematics*, vol. 28, 43.

Получено 06.09.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511.3 DOI 10.22405/2226-8383-2018-19-3-298-310

О полных рациональных тригонометрических суммах и интегралах[1]

Чубариков Владимир Николаевич — доктор физико-математических наук, профессор, заведующий кафедрой математических и компьютерных методов анализа, Механико-математический факультет, Московский государственный университет имени М. В. Ломоносова.
e-mail: chubarik1@mech.math.msu.su chubarik2009@live.ru

Аннотация

Найдены асимптотические формулы при $m \to \infty$ для числа решений системы сравнений вида

$$g_s(x_1) + \cdots + g_s(x_k) \equiv g_s(x_1) + \cdots + g_s(x_k) \pmod{p^m}, 1 \le s \le n,$$

где неизвестные $x_1, \ldots, x_k, y_1, \ldots, y_k$ могут принимать значения из полной системы вычетов по модулю p^m, а степени многочленов $g_1(x), \ldots, g_n(x)$ не превосходят n. Указаны такие многочлены $g_1(x), \ldots, g_n(x)$, для которых эти асимптотики справедливы при $2k > 0,5n(n+1)+1$, а при $2k \le 0,5n(n+1)+1$ данные асимптотики не имеют место.

Кроме того, для многочленов $g_1(x), \ldots, g_n(x)$ с вещественными коэффициентами, причем степени многочленов не превосходят n, найдена асимптотика среднего значения тригонометрических интегралов вида

$$\int_0^1 e^{2\pi i f(x)}, f(x) = \alpha_1 g_1(x) + \cdots + \alpha_n g_n(x),$$

где осреднение ведётся по всем вещественным параметрам $\alpha_1, \ldots, \alpha_n$. Эта асимптотика справедлива при степени осреднения $2k > 0,5n(n+1)+1$, а при $2k \le 0,5n(n+1)+1$ она не имеет места.

Ключевые слова: полные рациональные тригонометрические суммы, тригонометрические интегралы.

Библиография: 15 названий.

Для цитирования:
В. Н. Чубариков. О полных рациональных тригонометрических суммах и интегралах // Чебышевский сборник, 2018, т. 19, вып. 3, с. 298–310.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511.3 DOI 10.22405/2226-8383-2018-19-3-298-310

On complete rational trigonometric sums and integrals[2]

[1]Работа выполнена при финансовой поддержке РФФИ, грант № 16-01-00-071
[2]The work was carried out at the financial the support of RFBR, grant № 16-01-00-071

Chubarikov Vladimir Nikolaevich — doctor of physical and mathematical sciences, professor, head of the department of mathematical and computer methods of analysis, dean of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University.
e-mail: chubarik1@mech.math.msu.su chubarik2009@live.ru

Abstract

Asymptotical formulae as $m \to \infty$ for the number of solutions of the congruence system of a form

$$g_s(x_1) + \cdots + g_s(x_k) \equiv g_s(x_1) + \cdots + g_s(x_k) \pmod{p^m}, 1 \le s \le n,$$

are found, where unknowns $x_1, \ldots, x_k, y_1, \ldots, y_k$ can take on values from the complete system of residues modulo p^m, but degrees of polynomials $g_1(x), \ldots, g_n(x)$ do not exceed n. Such polynomials $g_1(x), \ldots, g_n(x)$, for which these asymptotics hold as $2k > 0,5n(n+1)+1$, but as $2k \le 0,5n(n+1)+1$ the given asymptotics have no place, were shew.

Besides, for polynomials $g_1(x), \ldots, g_n(x)$ with real coefficients, moreover degrees of polynomials do not exceed n, the asymptotic of a mean value of trigonometrical integrals of the form

$$\int_0^1 e^{2\pi i f(x)}, f(x) = \alpha_1 g_1(x) + \cdots + \alpha_n g_n(x),$$

where the averaging is lead on all real parameters $\alpha_1, \ldots, \alpha_n$, is found. This asymptotic holds for the power of the averaging $2k > 0,5n(n+1)+1$, but as $2k \le 0,5n(n+1)+1$ it has no place.

Keywords: complete rational trigonometric sums, trigonometric integrals.

Bibliography: 15 titles.

For citation:
V. N. Chubarikov, 2018, "On complete rational trigonometric sums and integrals" , *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 298–310.

Введение

Настоящая работа находится в русле исследований по круговому методу Харди — Литтлвуда — Рамануджана ([1], [2]) в форме тригонометрических сумм И. М. Виноградова ([3], [4]). К этому кругу вопросов относится p-адический метод доказательства теоремы И. М. Виноградова о среднем, открытый в 1942 г. Ю. В. Линником [6], [7]. В 1963 г. А. А. Карацуба и Н. М. Коробов [9], [10] нашли другой p-адический метод и получили новое доказательство теоремы И. М. Виноградова.

Под p-адическим методом в задачах теории чисел понимают использование сравнений по модулю и арифметических функций с периодом, равными степеням простого числа p.

В 1971 г. Г. И. Архипов [11] доказал p-адическим методом первую теорему о среднем для кратных тригонометрических сумм.

Развивая метод И. М. Виноградова, Хуа Ло-кен ([8], стр. 201–276) при $k \ge k_0$, $k_0 \asymp 3k^2 \log k$, $n \ge 11$, вывел асимптотическую формулу вида

$$\lim_{P \to \infty} P^{0,5n(n+1)-2k} J_k(P) = \gamma\theta,$$

где $J_k(P)$ — число решений в целых числах $1 \le x_1, \ldots, x_k, y_1, \ldots, y_k \le P$ системы уравнений вида

$$x_1^s + \cdots + x_k^s = y_1^s + \cdots + y_k^s (1 \le s \le n),$$

причём γ, σ — соответственно особый интеграл и особый ряд рассматриваемой асимптотики

$$\gamma = \int\limits_{-\infty}^{+\infty} \cdots \int\limits_{-\infty}^{+\infty} \left| \int\limits_0^1 e^{2\pi i(\alpha_1 x + \cdots + \alpha_n x^n)}\, dx \right|^{2k} d\alpha_1 \ldots d\alpha_n,$$

$$\sigma = \sum_{q_1}^{\infty} \cdots \sum_{q_n}^{\infty} \sum_{\substack{a_1=1 \\ (a_1,q_1)=1}}^{q_1} \cdots \sum_{\substack{a_n=1 \\ (a_n,q_n)=1}}^{q_n} \left| (q_1 \ldots q_n)^{-1} \sum_{x=1}^{q_1 \ldots q_n} \exp\left(2\pi i \left(\frac{a_1}{q_1} x + \cdots + \frac{a_n}{q_n} x^n\right)\right) \right|^{2k}.$$

Хуа Ло-кен там же нашёл показатель сходимости $2k_1 = 0,5n(n+1)+2$ особого ряда σ, т.е. для среднего значения полных рациональных тригонометрических сумм.

Для особого интеграла γ показатель сходимости $2k_2 = 0,5n(n+1)+1$ был найден в 1978 г. Г. И. Архиповым, А. А. Карацубой и автором [12].

В настоящей работе продолжены исследования полных рациональных тригонометрических сумм и тригонометрических интегралов с многочленом общего вида в экспоненте (см. [1]–[15]).

Отметим, что в ряде этапов исследования мы существенно пользуемся результатами из нашей книги [12] и работ Г. И. Архипова [11].

§1. О среднем значении полных рациональных сумм общего вида

Пусть $n \geq 2, a_1, \ldots, a_n$ — натуральные числа,

$$g_s(x) = x^s + \sum_{t=1}^{s-1} \alpha(s,t) x^t, \quad s = 1, \ldots, n, \tag{1}$$

— многочлены с целыми коэффициентами.

Пусть, далее, $S(p^m; f)$ обозначает полную рациональную тригонометрическую сумму вида

$$S(p^m; f) = \sum_{x=1}^{p^m} e^{2\pi i f(x)}, \quad f(x) = \sum_{s=1}^{n} \frac{a_s g_s(x)}{p^{m_s}}, \quad (a_s, p) = 1, \quad m_s \leq m.$$

Тогда среднее значение $N(p^m; g)$ этих сумм имеет вид

$$N(p^m; g) = p^{-mn} \sum_{\max\{m_n, \ldots, m_1\} \leq m} \sum_{\substack{a_n=0 \\ (a_n,p)=1}}^{p^{m_n}-1} \cdots \sum_{\substack{a_1=0 \\ (a_1,p)=1}}^{p^{m_1}-1} |S(p^m; f(x))|^{2k}.$$

Положим $t = \max\{m_1, \ldots, m_n\}$. Находим

$$N(p^m; g) = p^{-mn} \sum_{t=0}^{m} \sum_{\substack{a_n=0 \\ (a_n,\ldots,a_1,p)=1}}^{p^t-1} \cdots \sum_{a_1=0}^{p^t-1} \left| S\left(p^m; \frac{a_n g_n(x) + \cdots + a_1 g_1(x)}{p^t}\right) \right|^{2k} =$$

$$= p^{2km-mn} \sum_{t=0}^{m} \sum_{\substack{a_n=0 \\ (a_n,\ldots,a_1,p)=1}}^{p^t-1} \cdots \sum_{a_1=0}^{p^t-1} \left| p^{-t} S\left(p^t; \frac{a_n g_n x^n + \cdots + a_1 g_1(x)}{p^t}\right) \right|^{2k} =$$

$$= p^{m(2k-n)} \sigma(p^m; g). \tag{2}$$

Запишем все рациональные коэффициенты многочлена в экспоненте суммы как дроби со знаменателем p^m. Получим

$$N(p^m;g)=p^{-mn}\sum_{a_n=0}^{p^m-1}\cdots\sum_{a_1=0}^{p^m-1}\left|S\left(p^m;\frac{h(x)}{p^m}\right)\right|^{2k},\quad h(x)=\sum_{s=1}^{n}a_sg_s(x),$$

что равно числу решений следующей системы сравнений

$$\begin{cases} g_1(x_1)+\cdots+g_1(x_k)\equiv g_1(y_1)+\cdots+g_1(y_k) \pmod{p^m}\\ \cdots\quad\cdots\quad\cdots\quad\cdots\\ g_n(x_1)+\cdots+g_n(x_k)\equiv g_n(y_1)+\cdots+g_n(y_k) \pmod{p^m}, \end{cases}\tag{3}$$

где неизвестные $x_1,\dots,x_k,y_1,\dots,y_k$ принимают значения из полной системы вычетов по модулю p^m.

Если существует $\lim\limits_{m\to\infty}\sigma(p^m;g)=\sigma_p(g)$, где

$$\sigma_p(g)=1+\sum_{t=1}^{+\infty}A(p^t),\tag{4}$$

$$A(p^t)=\sum_{\substack{a_n=0\\(a_n,\dots,a_1,p)=1}}^{p^t-1}\cdots\sum_{a_1=0}^{p^t-1}|p^{-t}S(p^t;(a_ng_n(x)+\cdots+a_1g_1(x))/p^t)|^{2k},\tag{5}$$

$$S(p^t;(a_ng_n(x)+\cdots+a_1g_1(x))/p^t)=\sum_{x=1}^{p^t}e^{2\pi i\frac{a_ng_n(x)+\cdots+a_1g_1(x)}{p^t}},\tag{6}$$

то этот предел $\sigma_p(g)$ называется особым рядом системы сравнений (3).

Заметим, что каждое решение системы (3) является решением следующей системы сравнений

$$\begin{cases} x_1+\cdots+x_k\equiv y_1+\cdots+y_k \pmod{p^m}\\ \cdots\quad\cdots\quad\cdots\quad\cdots\\ x_1^n+\cdots+x_k^n\equiv y_1^n+\cdots+y_k^n \pmod{p^m}, \end{cases}\tag{3'}$$

где неизвестные $x_1,\dots,x_k,y_1,\dots,y_k$ принимают значения из полной системы вычетов по модулю p^m, и наоборот. Действительно, первые сравнения этих систем совпадают. Второе сравнение системы (3') является линейной комбинацией первого и второго сравнений из (3) и т.д.

Число решений $N(p^m)$ системы (3') равно $p^{m(2k-n)}\sigma(p^m)$. Пусть $\sigma_p=\lim\limits_{m\to\infty}\sigma(p^m)$

Теорема 1. *Особый ряд $\sigma_p(g)=\sigma_p$ сходится при $2k>0,5n(n+1)+1$ и расходится при $2k\le 0,5n(n+1)+1$.*

§2. Оценка полной суммы

Положим

$$f(x)=\sum_{s=1}^{n}a_sg_s(x),g_s(x)=x^s+\sum_{t=1}^{s-1}\alpha(s,t)x^t,h(y)=f(y+\xi)=\sum_{u=0}^{n}b_uy^u.\tag{7}$$

Имеем

$$h(y)=\sum_{s=1}^{n}a_s\left(\sum_{v=0}^{s}\binom{s}{v}y^v\xi^{s-v}+\sum_{t=1}^{s-1}\alpha(s,t)\sum_{w=0}^{t}\binom{t}{w}y^w\xi^{t-w}\right)=$$

$$= \sum_{v=1}^{n} y^v \sum_{s=v}^{n} a_s \binom{s}{v} \xi^{s-v} + \sum_{s=1}^{n} a_s \sum_{w=1}^{s-1} y^w \sum_{t=w}^{s-1} \alpha(s,t) \binom{t}{w} \xi^{t-w} + f(\xi) =$$

$$= \sum_{v=1}^{n} y^v \sum_{s=v}^{n} a_s \binom{s}{v} \xi^{s-v} + \sum_{v=1}^{n-1} y^v \sum_{s=v+1}^{n} a_s \sum_{t=v}^{s-1} \alpha(s,t) \binom{t}{v} \xi^{t-v} + f(\xi).$$

Отсюда находим

$$\begin{cases} b_n = a_n, \\ b_{n-1} = a_{n-1} + a_n \binom{n}{n-1} \xi + a_n \alpha(n-1, n-1), \\ \dots \quad \dots \quad \dots \\ b_v = a_v + \sum\limits_{s=v+1}^{n} a_s \left(\binom{s}{v} \xi^{s-v} + \sum\limits_{t=v}^{s-1} \alpha(s,t) \binom{t}{v} \xi^{t-v} \right), \\ \dots \quad \dots \quad \dots \\ b_1 = a_1 + \sum\limits_{s=2}^{n} a_s \left(\binom{s}{1} \xi^{s-1} + \sum\limits_{t=1}^{s-1} \alpha(s,t) \binom{t}{1} \xi^{t-1} \right). \end{cases} \tag{8}$$

Пусть $(a_1, \dots, a_n, p) = 1$, $w = [\log n / \log p]$, $p^\tau \| (a_1, 2a_2, \dots, na_n)$.
Тогда $\tau \le w$, $p^\tau \| (b_1, 2b_2, \dots, nb_n)$.

Лемма 1. *Пусть* $l \ge 2(\tau + 1)$,

$$S(p^l; f) = \sum_{\nu=1}^{p} S_\nu, \quad S_\nu = \sum_{\substack{x=1 \\ x \equiv \nu \pmod p}}^{p^l} e^{2\pi i \frac{f(x)}{p^l}}.$$

Тогда, если $p^{-\tau} f'(\nu) \equiv 0 \pmod p$, *то*

$$S_\nu = p^{\tau+1} \sum_{\substack{y=1 \\ y \equiv \nu \pmod p}}^{p^{l-\tau-1}} e^{2\pi i \frac{f(y)}{p^l}},$$

в противном случае $S_\nu = 0$.

Доказательство. Произведем замену переменной суммирования. Имеем

$$x = y + p^{l-\tau-1} z, 1 \le y \le p^{l-\tau-1}, 0 \le z < p^{\tau+1}.$$

Отсюда находим

$$S_\nu = \sum_{\substack{y=1 \\ y \equiv \nu \pmod p}}^{p^{l-\tau-1}} \sum_{z=0}^{p^{\tau+1}-1} e^{2\pi i \frac{f(y + p^{l-\tau-1} z)}{p^l}} =$$

$$= \sum_{\substack{y=1 \\ y \equiv \nu \pmod p}}^{p^{l-\tau-1}} e^{2\pi i \frac{f(y)}{p^l}} \sum_{z=0}^{p^{\tau+1}-1} e^{2\pi i \frac{p^{-\tau} f'(y) z}{p}}.$$

Так как

$$\sum_{z=0}^{p^{\tau+1}-1} e^{2\pi i \frac{p^{-\tau} f'(y) z}{p}} = \begin{cases} p^{\tau+1}, & \text{если} \quad p^{-\tau} f'(y) \equiv 0 \pmod p, \\ 0, & \text{если} \quad p^{-\tau} f'(y) \not\equiv 0 \pmod p, \end{cases}$$

то из этого равенства следует утверждение леммы. □

Заметим, что сравнение

$$p^{-\tau} f'(\nu) \equiv 0 \pmod p, \quad 1 \le \nu \le p, \tag{8}$$

имеет не более $n-1$ решений.

Лемма 2. *Пусть a — корень кратности m многочлена $F(x)$ по простому модулю p, и пусть u — наибольшая степень числа p, делящая все коэффициенты многочлена $H(x) = F(a+px)$. Тогда число корней сравнения $p^{-u}H(x) \equiv 0 \pmod p$ с учётом их кратности, не превосходит m.*

Доказательство. см., например, [12], с. 55, лемма 2. □

Рассмотрим далее любое решение ν_0 сравнения (8). Положим в равенстве (7) $\xi = \nu_0$ и определим показатель $2 \le u_1 \le n$ и многочлен $f_1(y)$ из соотношений

$$p^{u_1} \| (pb_1, p^2 b_2, \dots, p^n b_n), f(\nu_0 + py) - f(\nu_0) = p^{u_1} f_1(y) = p^{u_1} \sum_{s=1}^{n} c_s y^s,$$

$$(c_1, c_2, \dots, c_n, p) = 1, p^{u_1} c_s = p^s b_s (1 \le s \le n).$$

Таким образом, при $l - u_1 > 2w + 1$ получим

$$S_{\nu_0} = e^{2\pi i \frac{f(\nu_0)}{p^l}} \sum_{y=1}^{p^{l-1}} e^{2\pi i \frac{f_1(y)}{p^{l-u_1}}} = p^{u_1 - 1} e^{2\pi i \frac{f(\nu_0)}{p^l}} S(p^{l-u_1}; f_1).$$

Пусть s — наибольший номер такой, что $(b_s, p) = 1$. Тогда из равенства $p^s b_s = p^{u_1} c_s$ находим, что $n \ge s \ge u_1$. Следовательно, по модулю p степень многочлена $f_1(x)$ не превосходит u_1.

В предыдущем рассуждении многочлен $f(x)$ заменим на $f_1(x)$, а многочлен $h(y)$ на многочлен $h_1(y) = f_1(y+\eta) = \sum\limits_{s=0}^{n} d_s y^s$. Определим τ_1 из условия $p^{\tau_1} \| (c_1, 2c_2, \dots, nc_n)$. Тогда для любого η имеем $p^{\tau_1} \| (d_1, 2d_2, \dots, nd_n)$ по тем же соображениям, что и для набора коэффициентов a_s и $b_s (1 \le s \le n)$. Таким образом, получим

$$S(p^{l-u_1}; f_1) = \sum_{\eta=1}^{p} S_{\nu_0,\eta}, S_{\nu_0,\eta} = \sum_{\substack{y=1 \\ y \equiv \eta \pmod p}}^{p^{l-u_1-\tau_1-1}} e^{2\pi i \frac{f(y)}{p^{l-u_1}}} \sum_{z=0}^{p^{\tau_1+1}-1} e^{2\pi i \frac{p^{-\tau_1} f_1'(y) z}{p}}$$

По лемме 1 для любого η с условием $p^{-\tau_1} f_1'(\eta) \not\equiv 0 \pmod p$ имеем $S_{\nu_0,\eta} = 0$.

Число решений сравнения $p^{-\tau_1} f_1'(\eta) \equiv 0 \pmod p$ не превосходит $u_1 - 1$. Возьмём любое решение $\eta = \nu_1$ этого сравнения. Определим показатель $u_2 = u_2(\nu_0, \nu_1)$ и многочлен $f_2(y)$ условиями

$$p^{u_2} \| (pd_1, p^2 d_2, \dots, p^n d_n), p^{u_2} f_2(y) = f_1(\nu_1 + py) - f(\nu_1).$$

при $l - u_1 - u_2 > 2w + 1$ получим

$$S_{\nu_0,\nu_1} = e^{2\pi i \frac{f_1(\nu_1)}{p^{l-u_1}}} \sum_{y=1}^{p^{l-u_1-1}} e^{2\pi i \frac{f_2(y)}{p^{l-u_1-u_2}}} = p^{u_2-1} e^{2\pi i \frac{f(\nu_1)}{p^{l-u_1}}} S(p^{l-u_1-u_2}; f_2).$$

Аналогично определяются показатели $u_3, \dots, u_t$, причём число $t = t(\nu_0, \nu_1, \dots)$ находится из условий

$$l - u_1 - \dots - u_{t-1} > 2w + 1, l - u_1 - \dots - u_{t-1} - u_t \le 2w + 1.$$

Собирая вместе полученные выше результаты, имеем следующее утверждение.

Теорема 2. *Справедлива формула*

$$S(p^l;f)=\sum_{(\nu_0,\nu_1,\dots,\nu_t)} p^{u_1+u_2+\dots+u_t-t}e^{2\pi i(\frac{f(\nu_0)}{p^l}+\frac{f_1(\nu_1)}{p^{l-u_1}}+\dots+\frac{f_{t-1}(\nu_{t-1})}{p^{l-u_1-\dots-u_{t-1}}})}\times$$

$$\times S(p^{l-u_1-u_2-\dots-u_t};f_t), \tag{9}$$

где наборы $(\nu_0,\nu_1,\dots,\nu_t)$ *пробегает решения системы сравнений* $p^{-\tau_s}f_s(\nu_s)\equiv 0 \pmod p$ $(0\le s\le t)$.

§3. Показатель сходимости особого ряда

Нам понадобятся два утверждения, которые являются следствиями леммы 2.

Лемма 3. *Пусть* $f(x)$ *— многочлен степени* n *с целыми коэффициентами, взаимно простыми в совокупности с простым числом* p. *Тогда количество наборов показателей* $(u_1,u_2,\dots)$ *многочлена* $f(x)$ *не превосходит* n.

Лемма 4. *Справедливы неравенства*

$$n\ge u_1\ge u_2\ge\dots\ge 2.$$

Доказательство. см.[12], с. 63, леммы 5 и 6. □

Из леммы 3 следует, что количество решений $(\nu_0,\nu_1,\dots,\nu_t)$ системы сравнений

$$p^{-\tau_s}f_s(\nu_s)\equiv 0 \pmod p (0\le s\le t),$$

не превосходит n.

Приведем только схему *доказательства теоремы 1.*

1^0. Пусть $f(x)=a_1g_1(x)+\dots+a_ng_n(x),(a_1,\dots,a_n,p)=1$ — любой многочлен с целыми коэффициентами, причём многочлены $g_1(x),\dots,g_n(x)$ заданы соотношениями (1), $(u_1,\dots,u_t)$ — набор наименьшей длины для многочлена $f(x)$, определённый в теореме 2. Тогда по теореме 2 имеем

$$p^{-l}|S(p^l;f)|\le np^{-t}.$$

2^0. Оценим количество $K(u_1,\dots,u_t)$ многочленов $f(x)$ с заданной в п.1^0 цепочкой показателей $(u_1,\dots,u_t)$ наименьшей длины t. Из формул (7), (8), подставляя $\xi=py$, находим

$$f(x)=h(x-\xi)=\sum_{t=0}^{n}b_tg_t(x-\xi),$$

$$\begin{cases} a_n=b_n,\\ a_{n-1}=b_{n-1}+b_n\binom{n}{n-1}(-py)+b_n\alpha(n-1,n-1),\\ \dots\quad\dots\quad\dots\\ a_v=b_v+\sum\limits_{s=v+1}^{n}b_s\left(\binom{s}{v}(-py)^{s-v}+\sum\limits_{t=v}^{s-1}\alpha(s,t)\binom{t}{v}(-py)^{t-v}\right),\\ \dots\quad\dots\quad\dots\\ a_1=b_1+\sum\limits_{s=2}^{n}b_s\left(\binom{s}{1}(-py)^{s-1}+\sum\limits_{t=1}^{s-1}\alpha(s,t)\binom{t}{1}(-py)^{t-1}\right). \end{cases}$$

Поскольку $p^{u_1}\|(pb_1, p^2b_2, \dots, p^nb_n)$, получим $pb_1 = p^{u_1}c_1$, $p^2b_2 = p^{u_1}c_2, \dots, p^nb_n = p^{u_1}c_n$, $(c_1, c_2, \dots, c_n, p) = 1$.

Следовательно,

$$\begin{cases} a_{u_1-1} = p^{u_1-(u_1-1)}c_{u_1-1} + A_{u_1-1}, \\ \dots \quad \dots \quad \dots \\ a_v = p^{u_1-v}c_v + A_v, \\ \dots \quad \dots \quad \dots \\ a_1 = p^{u_1-1}c_1 + A_1. \end{cases}$$

Повторяя это рассуждение для показателей $u_2, \dots, u_t$, приходим к системе равенств

$$\begin{cases} a_{u_1-1} = p^{u_1-(u_1-1)}B_{u_1-1} + A^{(t)}_{u_1-1}, \\ \dots \quad \dots \quad \dots \\ a_{u_2-1} = p^{u_1-(u_2-1)+u_2-(u_2-1)}B_{u_2-1} + A^{(t)}_{u_2-1}, \\ \dots \quad \dots \quad \dots \\ a_1 = p^{(u_1-1)+(u_2-1)+\dots+(u_t-1)}B_1 + A^{(t)}_1. \end{cases}$$

Отсюда находим $K(u_1, \dots, u_t) \le p^A$, где

$$A = nl - 0,5u_1(u_1-1) - 0,5u_2(u_2-1) - \dots - 0,5u_t(u_t-1).$$

Положим $U = u_1 + \dots + u_t$, $B = A - n(l-U)$.

Имеем $l - 2w - 1 \le U \le l, 2 \le u_t \le \dots \le u_1 \le n$. Преобразуем

$$B = nU - \sum_{s=1}^{t} 0,5u_s(u_s-1) = \sum_{s=1}^{t}(nu_s - 0,5u_s(u_s-1)) = \sum_{s=1}^{t} H_s(x),$$

где $H(x) = nx - 0,5x(x-1)$.

Найдем максимум $H(x)$ на отрезке $[2, n]$. Находим $H'(x) = n - x + 0,5$. Следовательно, максимум $H(x)$ на отрезке $[2, n]$ достигается в точке $x = n$. Отсюда получим, что $B \le 0,5tn(n+1)$.

Таким образом

$$K(u_1, \dots, u_t) \le p^{B-n(l-U)} \le p^{n(2w+1)}p^{0,5tn(n+1)}.$$

3^0. Оценим количество U_t наборов $(u_1, \dots, u_t)$, отвечающих условиям лемм 3 и 4. Имеем

$$n \ge u_1 \ge u_2 \ge \dots \ge u_t \ge 2, \quad l \ge u_1 + u_2 + \dots + u_t > l - 2w - 1.$$

Отсюда находим $U_t \le l^n$.

4^0. Число N_t многочленов с заданным $(u_1, \dots, u_t)$ не превосходит числа корней $(\nu_0, \dots, \nu_t)$ сравнений (8) с условием $0 \le u_1, \dots, \le u_t < p$. Следовательно, $N_t \le p^t$.

5^0. Таким образом, количество многочленов с цепочкой показателей минимальной длины t не превосходит

$$l^n p^t p^{0,5tn(n+1)+n(2w+1)}$$

6^0. Далее из пп.$1^0, 4^0$ и 5^0 при $t_0 = \max\{1, (l-2w-1)/n\}$ имеем

$$A(p^l) \le \sum_{t \ge t_0} n^{2k} l^n p^{n(2w+1)} p^{-t(2k-0,5n(n+1)+1)}.$$

Отсюда следует искомое утверждение. □

§4. Теорема о среднем для числа решений системы сравнений по модулю, равному степени простого

Теорема 3. *Пусть $n \geq 2, m$ — натуральные числа, $p > n$ — простое число. Тогда при $2k > \frac{n(n+1)}{2} + 1$ и $m \to \infty$ имеем*

$$N(p^m; k; \mathbf{g}) = p^{m(2k-n)}(\sigma_p(g) + O(m^n p^{((m-1)/n)(0{,}5n(n+1)+1-2k)}),$$

где $\mathbf{g} = (g_1(x), \dots, g_n(x))$.

Доказательство. Так как ряд σ_p сходится при $2k > \frac{n(n+1)}{2} + 1$ и

$$A(p^t) \leq n^{2k}(tp)^n p^{((t-1)/n)(0{,}5n(n+1+1-2k))}$$

(см.[13], с.69), то из формулы (2) имеем

$$N(p^m; k; \mathbf{g}) = p^{m(2k-n)}\sigma(p^m) = p^{m(2k-n)}(\sigma_p + O(m^n p^{((m-1)/n)(0{,}5n(n+1+1-2k))})).$$

Теорема 3 доказана. □

§5. Теорема о среднем для числа решений системы сравнений по модулю, равному факториалу натурального числа

Теорема 4. *Пусть $n \geq 2, m$ — натуральные числа, $M = m!$. Тогда при $2k > \frac{n(n+1)}{2} + 2$ и $m \to \infty$ имеем*

$$N(M) = N(M; k; \mathbf{g}) = M^{2k-n}\sigma(1 + o(1)).$$

Доказательство. Пусть $M = m! = \prod\limits_{p \leq m} p^{\alpha_p}$ — каноническое разложение числа M на простые сомножители. Тогда из мультипликативности функции $N(M)$, сходимости особого ряда и из теоремы 3 имеем

$$N(M) = \prod_{p \leq m} N(p^{\alpha_p}) = \prod_{p \leq m} p^{\alpha_p(2k-n)}(\sigma_p + O(\alpha_p^n p^{((\alpha_p-1)/n))(0{,}5n(n+1)+1-2k)}) =$$

$$= M^{2k-n} \prod_{p \leq m} \sigma_p(1 + O(\alpha_p^n p^{((\alpha_p-1)/n))(0{,}5n(n+1)+1-2k)})) = M^{2k-n}\sigma(1 + o(1)).$$

Теорема доказана. □

§6. Показатель сходимости особого интеграла

Особый интеграл имеет вид

$$\gamma = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i f(x)}\, dx \right|^{2k} d\alpha_1 \dots d\alpha_n,$$

где $f(x) = \alpha_1 g(x) + \cdots + \alpha_n g_n(x), g_s(x) = x^s + \sum\limits_{t=1}^{s-1} \beta_{s,t} x^t, 1 \leq s \leq n$ и коэффициенты $\alpha_s, \beta_{s,t}$ — вещественные числа.

Пусть Ω — область точек $(x_1, \dots, x_k, y_1, \dots, y_k)$ в вещественном пространстве размерности $2k$, для которых выполнены условия

$$\left| \sum_{t=1}^{k} (x_t^s - y_t^s) \right| \le h, 0 \le x_t, y_t \le 1, s = 1, \dots, n.$$

Объём области Ω обозначим символом $\mu(h)$.

Справедливо следующее утверждение.

Теорема 5. *При $2k > 0,5n(n+1)+1$ справедливо предельное равенство*

$$\gamma = \lim_{h \to 0} (2h)^{-n} \mu(h).$$

Доказательство. При $-1 < c_1, \dots, c_n < 1$ функция

$$F(c_1, \dots, c_n) = \int_{-c_1}^{c_1} \cdots \int_{-c_n}^{c_n} \gamma(z_1, \dots, z_n)\, dz_1 \dots dz_n,$$

где

$$\gamma(z_1, \dots, z_n) = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i f(x)}\, dx \right|^{2k} e^{2\pi i (z_1\alpha_1 + \cdots + z_n\alpha_n)}\, d\alpha_1 \dots d\alpha_n,$$

представляет собой непрерывную функцию ввиду абсолютной сходимости интеграла $\gamma(\mathbf{c}) = \gamma(c_1, \dots, c_n)$.

Таким образом

$$F(\mathbf{c}) = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i f(x)}\, dx \right|^{2k} \left(\prod_{s=1}^{n} \frac{\sin(2\pi c_s \alpha_s)}{\pi \alpha_s} \right) d\alpha_1 \dots d\alpha_n.$$

Для краткости записи положим $\lambda_s = g_s(x_1) + \cdots + g_s(x_k) - g_s(y_1) - \cdots - g_s(y_k), s = 1, \dots, n$. Тогда из предыдущего соотношения имеем

$$F(c_1, \dots, c_s) = \frac{1}{\pi^n} \int_0^1 \cdots \int_0^1 dx_1 \dots dx_k dy_1 \dots dy_k \times$$

$$\times \left(\prod_{s=1}^{n} \int_{-\infty}^{+\infty} \left(\frac{\sin(2\pi\alpha_s(\lambda_s + c_s))}{\alpha_s} - \frac{\sin(2\pi\alpha_s(\lambda_s - c_s))}{\alpha_s} \right) d\alpha_s \right).$$

Используя значение интеграла Дирихле

$$\int_0^{+\infty} \frac{\sin ax}{x}\, dx = \frac{\pi}{2} \operatorname{sgn} a,$$

найдем

$$F(\mathbf{c}) = \int_0^1 \cdots \int_0^1 \left(\prod_{s=1}^{n} (\operatorname{sgn}(\lambda_s + c_s) - \operatorname{sgn}(\lambda_s - c_s)) \right) dx_1 \dots dx_k dy_1 \dots dy_k =$$

$$= \int\limits_{-c_s\le\lambda_s\le c_s(1\le s\le n)}^{1}\cdots\int\limits_{0}^{1} dx_1\dots dx_k dy_1\dots dy_k.$$

Отсюда получим

$$g(\mathbf{0}) = \left.\frac{\partial^n F(c_1,\dots,c_n)}{\partial c_1\dots\partial c_n}\right|_{\mathbf{c}=\mathbf{0}} = \lim_{h\to 0}(2h)^{-n}\mu(h),$$

где

$$\mu(h)) = \int\limits_{-h\le\lambda_s\le h(1\le s\le n)}^{1}\cdots\int\limits_{0}^{1} dx_1\dots dx_k dy_1\dots dy_k$$

есть объём области Ω. Теорема доказана. $\square$

Заключение

Приведем результаты и программу дальнейших исследований.

1. Получение при $P>1,\alpha_1,\dots,\alpha_n$ — вещественных числах, возможно более точных оценок тригонометрических сумм вида

$$S(P) = S(P;\alpha_1,\dots,\alpha_n) = S(P;\alpha_1,\dots,\alpha_n;g_1,\dots,g_n) =$$

$$= \sum_{x\le P} e^{2\pi i(\alpha_1 g_1(x)+\dots+\alpha_n g_n(x))},$$

где для многочленов $g_1(x),\dots,g_n(x)$ с вещественными коэффициентами матрица их коэффициентов имеет максимальный ранг, равный n, причем степени многочленов не превосходят n.

2. Доказательство аналога теоремы И. М. Виноградова о среднем: при $k\ge k_0$, $k_0\asymp n^2\ln n$ имеем

$$J = J(P;n,k) = \int\limits_0^1\cdots\int\limits_0^1 |S(P;\alpha_1,\dots,\alpha_n)|^{2k}\,d\alpha\dots d\alpha_n \ll$$

$$\ll c(n,k)P^{2k-0,5n(n+1)},$$

где $c(n,k)$ — положительная постоянная.

3. Точные оценки полных рациональных тригонометрических сумм и интегралов и нахождение их показателей сходимости при условии, что количество многочленов $g_1(x),\dots,g_n(x)$ меньше максимальной из их степеней, например,

$$g_s(x) = x^{s+n} + g_{0,s}(x), s = 1,\dots,n,$$

где степень $g_{0,s}$ меньше, чем $s+n$.

Утверждения, подобные теоремам 1-5 для многочленов $g_1(x),\dots,g_n(x)$ общего вида, получаются аналогичными рассуждениями. Точные формулировки предполагается опубликовать позже.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Hardy G. H., Ramanujan S. Asymptotic formulae in combinatory analysis // Proc. London math Soc.(2), 17(1918), p. 75–115.
2. Hardy G. H., Littlewood J. E. A new solution of Waring problem// Gött.Nachr., 1920, p. 33–54.
3. Виноградов И. М. Sur un théorème génèral de Waring// Мат.сб., 1924, т.31, с. 490–507.
4. Виноградов И. М. О теореме Варинга // Изв.АН СССР, ОФМН, 1928, № 4, с. 393–400.
5. Виноградов И.М. Метод тригонометрических сумм в теории чисел. — М.: Наука, 1980.
6. Линник Ю. В. Избранные труды. Теория чисел. Эргодический метод и L-функции. — Л.: Наука, 1979. 432 с.
7. Линник Ю. В. Новые оценки сумм Вейля // Докл. АН СССР, 1942, т.37, № 7, 201–203.
8. Hua Loo-Keng. Selected Papers. — N.-Y., Heidelberg, Berlin: Springer-Verlag, 1983, pp. 888.
9. Карацуба А. А., Коробов Н. М. О теореме о среднем // Докл. АН СССР, 1963, т.149, № 2, 245–248.
10. Карацуба А. А. Теоремы о среднем и полные тригонометрические суммы // Изв. АН СССР, сер. матем., 1966, т.30, 183–206.
11. Архипов Г. И. Избранные труды. Орел: Изд-во Орловского гос.ун-та, 2013. 464 с.
12. Архипов Г.И., Карацуба А.А., Чубариков В.Н. Теория кратных тригонометрических сумм. — М.: Наука. 1987.
13. Arkhipov G.I., Chubarikov V.N., Karatsuba A.A. Trigonometric Sums in Number Theory and Analysis. — Berlin–New York: Walter de Gruyter (de Gruyter Expositions in Mathematics 39). 2004.
14. Чубариков В. Н. Кратные полные рациональные арифметические суммы от значений многочлена // Докл.РАН., 2018, т.478, № 1, 22–24.
15. Архипова Л. Г., Чубариков В. Н., Показатель сходимости особого ряда одной многомерной проблемы // Вестн. Моск. ун-та. Сер.I, Математика, механика. 2018. № 5. 58-61.

REFERENCES

1. Hardy G. H., Ramanujan S. Asymptotic formulae in combinatory analysis // Proc. London math Soc.(2), 17(1918), p. 75–115.
2. Hardy G. H., Littlewood J. E. A new solution of Waring problem// Gött.Nachr., 1920, p. 33–54.
3. Vinogradov I. M. Sur un théorème génèral de Waring// Мат.сб., 1924, v.31, p. 490–507.
4. Vinogradov I. M. On Waring's theorem // Izv. AN SSSR, OFMN, 1928, № 4, p. 393–400.
5. Vinogradov I. M. The method of trigonometric sums in the theory of numbers. — Moscow: Nauka, 1980.
6. *Linnik J. V.* Selected papers. The theory of numbers. The ergodic method and L-functions. — Leningrad: Nauka, 1979. pp. 432.

7. *Linnik J. V.* New estimations of Weyl sums// Dokl. AN SSSR, 1942, v.37, № 7, 201–203.

8. Hua Loo-Keng. Selected Papers. — N.-Y., Heidelberg, Berlin: Springer-Verlag, 1983, pp. 888.

9. *Karatsuba A. A., Korobov N. M.* On the mean-value theorem// Dokl. AN SSSR, 1963, v. 149, № 2, 245–248.

10. *Karatsuba A. A.* Mean-value theorems and complete trigonometric sums// Izv. AN SSSR, ser. math., 1966, v.30, 183–206.

11. *Arkhipov G. I.* Selected Papers. Orjol: Publ. House of the Orjol State University, 2013. pp. 464.

12. Arkhipov G.I., Karatsuba A.A., Chubarikov V.N. The theory of multiple trigonometric sums. — Moscow: Nauka. 1987.

13. Arkhipov G.I., Chubarikov V.N., Karatsuba A.A. Trigonometric Sums in Number Theory and Analysis. — Berlin–New York: Walter de Gruyter (de Gruyter Expositions in Mathematics 39). 2004.

14. Chubarikov V. N. The multiple complete rational arithmetical sums of polynomial values// Dokl.RAN., 2018, v.478, № 1, 22–24.

15. Arkhipova L. G., Chubarikov V. N. The exponent of convergence of the singular series of a multivariate problem// Bull. of Moscow State Univ. Ser.I, Math., mech. 2018. № 5, 58-61.

Получено 08.08.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 511 DOI 10.22405/2226-8383-2018-19-3-311-317

Большие пути в дистанционных графах в векторных пространствах над конечным полем

Штейников Юрий Николаевич — кандидат физико-математических наук, научный сотрудник, Математический институт имени В. А. Стеклова, ФГУ ФНЦ Научно-исследовательский институт системных исследований Российской академии наук, г. Москва.
e-mail: yuriisht@yandex.ru

Аннотация

В статье изучается следующая задача. Пусть $E \subset \mathbb{F}_q^d$ является подмножеством $d-$ мерного векторного пространства над конечным полем из q элементов. Мы определяем так называемый дистанционный граф на множестве E с единичным расстоянием между вершинами. Расстояние между вершинами x, y определяется так $\|x–y\| = (x_1-y_1)^2+\ldots+(x_d-y_d)^2$. Вершины дистанционного графа это элементы множества E и пара вершин $x, y \in E$ соединены ребром если расстояние между ними равно единице. В настоящей работе изучаются длинные пути в этом графе. А именно, получена нижняя оценка на длину самого большого непересекающегося пути в нем. При определенных условиях в работе доказано, что длина такого пути состоит из большинства вершин из множества E. Это дополняет результат из работы А. Иосевича и соавторов. При доказательстве мы используем некоторые комбинаторные идеи и результаты, полученные А. Иосевичем и М. Рудневым а также совместный результат М. Беннета, Дж. Чапмана, Д. Коверта, Д. Харта, А. Иосевича и Дж. Пакианатана. Основная идея построения большого пути в таком графе заключается в следующем. Мы строим много путей меньшей длины стандартными методами. Далее, основываясь на совместном результате М.Руднева и А. Иосевича о распределении расстояний между элементами множества E, мы заключаем, что существуют пара вершин у двух различных путей с расстоянием единица. Тем самым есть возможность соединить какие-то два уже построенных пути за их вершины и получить путь большей длины. Эта процедура повторяется итеративно до тех пор, пока не построится путь заданной нами длины. Отметим, что данный метод и основной результат остается верен и для так определенных дистанционных графов с любым ненулевым расстоянием.

Ключевые слова: конечные поля, расстояние, дистанционный граф, пути графа

Библиография: 4 названия.

Для цитирования:
Ю. Н. Штейников. Большие пути в дистанционных графах в векторных пространствах над конечным полем // Чебышевский сборник, 2018, т. 19, вып. 3, с. 311–317.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 511 DOI 10.22405/2226-8383-2018-19-3-311-317

Long paths in the distance graphs in vector spases over finite fields

Shteinikov Yuriy Nikolaevich — candidat of physical and mathematical sciences, professor, Steklov Mathematical Institute of RAS, Scientific Research Institute of System Analysis, Moscow.
e-mail: yuriisht@yandex.ru

Abstract

We study the following task. Let $E \subset \mathbb{F}_q^d$, be the subset of the $d-$ dimensional vector space over the finite field with q elements. We define so- called distance graph of the set E with distance equal to one. The distance between the vertices $x, y \in E$ is defined as follows $\| x-y \| = (x_1-y_1)^2+\ldots+(x_d-y_d)^2$. The vertices of the distance graph are the elements of E and a pair of vertices $x, y \in E$ are connected by an edge if the distance between them is equal to one. In this paper long paths in the graph are studied. Namely the lower estimate for the length of the longest non-overlapping path in this graph is obtained. Under certain conditions, it is proved that the length of such path consists of the most of vertices of the set E. This complements the result from the paper of A. Iosevich and co-authors. In the proof we use some combinatoric arguments and results obtained by M. Rudnev and A. Iosevich and also joint result of M. Bennett, J. Chapman, D. Covert, D. Hart, A. Iosevich and J. Pakianathan. The main idea of constructing a long path in such a graph is as follows. We construct many paths of shorter length by standard methods. Further, based on the joint result of M.Rudnev and A. Iosevich on the distribution of distances between elements of the set E, we conclude that there exist a pair of vertices of two different paths with distance one. Thus, it is possible to connect some two paths already constructed for their vertices and get a longer path. This procedure is repeated iteratively until the path of the given length is constructed. We note that this method and the main result remains true for such distance graphs with any non-zero distance.

Keywords: finite fields, distance, distance graph, graph paths

Bibliography: 4 titles.

For citation:
Iu. N. Shteinikov, 2018, "Long paths in the distance graphs in vector spases over finite fields", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 311–317.

1. Введение

Напомним немного что такое классический евклидов дистанционный граф на двумерной плоскости. Вершинами графа являются точки этой плоскости. Две вершины соединены ребром, если расстояние между ними равно 1. Известная проблема Хадвигера-Нелсона заключается в поиске величины хроматического числа этого графа. Мы только знаем, что ответ либо число 5, 6 или 7.

В этой работе мы рассматриваем дистанционный граф в $\mathbb{F}_q^d$, где $\mathbb{F}_q^d$ обозначает векторное пространство над конечным полем из q элементов. Вершинами этого графа являются элементы $\mathbb{F}_q^d$. Две вершины $x, y \in \mathbb{F}_q^d$ соединены ребром, если $\| x-y \| = 1$, где $\| x \| = x_1^2+\ldots+x_d^2$. Основной результат этой работы будет относиться к этому случаю.

Имеются множество результатов для этого дистанционного графа в $\mathbb{F}_q^d$, мы отсылаем читателя к статьям [2], [3], [4]. Мы берем произвольное большое подмножество E в $\mathbb{F}_q^d$ и рассматриваем дистанционный граф на множестве E.

Сначала напомним некоторые предшествующие результаты. А. Иосевич и М. Руднев доказали, что если $E \subset \mathbb{F}_q^d$, $d \geq 2, t \neq 0$, то

$$|\{(x,y) \in E \times E : \| x-y \| = t\}| = \frac{|E|^2}{q} + R(t), \tag{1}$$

где

$$|R(t)| \leq 2q^{\frac{d-1}{2}}|E|. \tag{2}$$

Отсюда следует, что при определенных условиях количество ребер в этом графе на множестве E приблизительно равно $\frac{|E|^2}{2q}$.

С.Д. Адхикари, Анирбан Мукхопадхуай и М. Рэм Мерти [1] также изучали количество различных расстояний определяемых множеством E. В их статье они установили, что

$$|\{\| x-y \|: x,y \in E\}| = \Omega(q),$$

при некоторых естественных предположениях и без использования оценок сумм Клоостермана. Этот факт также следует из соотношения (1), полученного М. Рудневым и А. Иосевичем.

Определения. Две вершины a и b назовем соседними если a и b соединены ребром. Набор всех соседей вершины a будем обозначать $N(a)$. Размер множества $N(a)$ будем называть степенью a и обозначать как $\deg(a)$.

Мы говорим, что последовательность вершин $v_1, \dots, v_{k+1} \in G$ образует путь длины k если для всех $0 \le i \le k$ вершины v_i, v_{i+1} соединены ребром. Длины пути s будет обозначаться как $|s|$. Путь длины k назовем несамопересекающимся если все v_j в определении разные. Два пути s_1, s_2 назовем непересекающимися, если они не имеют общих вершин.

Имеются ряд интересных результатов в статье [2] о распределении путей фиксированной длины k. Говоря грубо, если k находится в определенном диапазоне, то эти пути равномерно распределены, - количество таких путей приблизительно равно $|E|^{k+1}/q^k$. Сформулируем соответствующий результат из [2].

Теорема 1. *Пусть $E \subseteq \mathbb{F}_q^d$ где $d \ge 2$ и $|E| > \frac{2k}{\log 2} q^{\frac{d+1}{2}}$. Предположим что $t_i \ne 0, 1 \le i \le k$, и пусть $\tau = (t_1, \dots, t_k)$. Определим*

$$C_k(\tau) = |\{(x^1, \dots, x^{k+1}) \in E \times \dots \times E :\| x^i - x^{i+1} \| = t_i, 1 \le i \le k\}|.$$

Тогда

$$C_k(\tau) = \frac{|E|^{k+1}}{q^k} + D_k(\tau),$$

где

$$|D_k(\tau)| \le \frac{2k}{\log 2} q^{\frac{d+1}{2}} \frac{|E|^k}{q^k}.$$

Целью настоящей работы является получение нижней оценки на наибольшую длину несамопересекающегося пути в дистанционном графе на E. Сформулируем основной результат.

Теорема 2. *Пусть $E \subset \mathbb{F}_q^d$ и величина f определена из равенства $|E| = f q^{\frac{d+1}{2}} \log q$. Тогда имеется несамопересекающийся путь длины $|E|(1 - O(\frac{1}{f}))$ в рассматриваемом дистанционном графе на множестве E.*

В следующем пункте мы формулируем предварительные утверждения. В третьем пункте мы доказываем Теорему 2.

2. Предварительные результаты

Используя результат М. Руднева и А. Иосевича - неравенство (1) – можно вывести два следующих утверждения. Мы дадим набросок их доказательств.

Лемма 1. *Пусть подмножества $A, B \subset \mathbb{F}_q^d, d \ge 2$, A, B непересекаются и $|A|, |B| \ge 4q^{\frac{d+1}{2}}$. Тогда существуют $x \in A, y \in B$ такие что $\| x - y \| = 1$.*

Доказательство. Определим $C = A \sqcup B$. Также зададим множества

$$W_1 = \{(x, y) \in C \times C :\| x - y \|= 1\},$$

$$W_2 = \{(x, y) \in A \times A :\| x - y \|= 1\},$$

$$W_3 = \{(x, y) \in B \times B :\| x - y \|= 1\}$$

Из равенства (1) и неравенства (2) мы заключаем, что

$$|W_1| = \frac{(|A| + |B|)^2}{q} + R_1; |W_2| = \frac{|A|^2}{q} + R_2; |W_3| = \frac{|B|^2}{q} + R_3,$$

где

$$|R_1| \le 2q^{\frac{d-1}{2}}(|A| + |B|), |R_2| \le 2q^{\frac{d-1}{2}}|A|, |R_3| \le 2q^{\frac{d-1}{2}}|B|.$$

Можно заметить, что $|W_1| > |W_2| + |W_3|$. Это означает, что существует пара $(a, b) \in A \times B$ такая, что $\| a - b \|= 1$. Это и завершает доказательство этой леммы.

□

Далее мы представляем следующее утверждение, которое было также отмечено в [2].

Лемма 2. *Существует абсолютная константа $c > 0$ такая что если $E \subset \mathbb{F}_q^d$, $d \ge 2$ и $|E| \ge 10q^{\frac{d+1}{2}}$, тогда существует несамопересекающийся путь длины не менее $\frac{c|E|}{q}$ в рассматриваемом дистанционном графе E.*

Для доказательства этой леммы достаточно доказать такое утверждение.

Предложение Пусть $E \subset \mathbb{F}_q^d, d \ge 2$ и $|E| \ge 10q^{\frac{d+1}{2}}$. Существует такое множество $E' \subset E$, $|E'| = \Omega(|E|)$ со следующим свойством. Если мы рассмотрим дистанционный подграф образованный множеством E' то для каждого $x \in E'$ в этом подграфе будем иметь $\deg(x) = \Omega(|E|/q)$.

Доказательство. Будем использовать $\mathbf{E}$ для обозначения среднего для величины $\deg(x)$ по $x \in E$. Используя неравенство (1) мы можем заключить, что $\mathbf{E} = \Theta(|E|/q)$. Пусть K есть некоторая абсолютная константа, которая будет определена позже. Следующие рассуждения мы оформим в виде некоторого алгоритма. Определим $E_0 = E$. Предположим, что $n \ge 0$ и множество E_n уже определено. Если множество E_n образует дистанционный граф который содержит вершину x с $\deg(x) \le \mathbf{E}/K$ мы определяем $E_{n+1} = E_n \setminus \{x\}$, и продолжаем наш алгоритм. Если нет такой вершины x, то мы завершаем наш алгоритм.

Сначала поймем, почему $|E_n| = \Omega(|E|)$ для всех n. Рассмотрим множество $A_n = = E \setminus E_n$. Легко видеть, что

$$|\{(x, y) \in A_n \times A_n :\| x - y \|= 1\}| \le 2|A_n||\mathbf{E}/K|.$$

С другой стороны, если $|A_n| > 4q^{\frac{d+1}{2}}$ тогда по неравенству (1)

$$|\{(x, y) \in A_n \times A_n :\| x - y \|= 1\}| \ge \frac{|A_n|^2}{10q}.$$

Если $|A_n| > 0.9|E|$ и для подходящей большой константы K два последних неравенства противоречивы.

Когда наш алгоритм завершится мы имеем множество E_n с $|E_n| = \Omega(|E|)$. Для любого $x \in E_n$ в подграфе образованном множеством E_n мы имеем $\deg(x) = \Omega(|E|/q)$. С этим мы завершаем доказательство этого предложения. □

Теперь мы готовы доказать Теорему 2. Говоря грубо, мы будем пытаться соединять пути с помощью Леммы 1. Это будет позволять конструировать большие пути из маленьких. Это один из основных аргументов при доказательстве Теоремы 2.

3. Доказательство основного результата

Сначала мы собираемся доказать следующее утверждение.

Лемма 3. *Пусть $E \subset \mathbb{F}_q^d$ и $|E| \geq Cq^{\frac{d+1}{2}} \log q$, где C какая-то большая абсолютная константа. Тогда существует несамопересекающийся путь длины $\Omega(\frac{|E|}{\log q})$ в этом дистанционном графе на множестве E.*

Доказательство.

С помощью Леммы 2 мы находим несамопересекающийся путь длины $\Omega(\frac{|E|}{q})$. Рассмотрим множество E без вершин этого пути и снова используем Лемму 2, и так далее. Действуя таким образом мы можем образовать некоторое число несамопересекающихся путей и не имеющих между собой общих вершин которые вместе содержат не менее $|E|/2$ вершин из множества E. Мы можем считать, что длина каждого такого пути не меньше чем $l = c|E|/q$, где $c > 0$ какая-то абсолютная константа. Обозначим через S множество этих путей. Далее мы будем делать некоторые транформации с этими путями, однако для краткости будем обозначать замещающие множества путей той же буквой S. Следующие рассуждения представляют из себя некоторый алгоритм. Будем выполнять следующие шаги.

Шаг 1.

Если все пути из S вместе содержат не менее $|E|/2$ вершин из E, мы переходим к следующему шагу.

Если же все пути из S содержат менее $|E|/2$ вершин из E, мы используем Лемму 2 и образуем новые пути, которые не имеют общих вершин с путями из S для которых выполнены следующие свойства:

1)все такие пути имеют длину не меньше l,

2)все эти пути вмсете с путями из S содержат не менее $|E|/2$ элементов из E.

Мы добавляем эти новые пути ко множеству S и получаем новое множество S и переходим к следующему шагу.

Шаг 2.

Предположим имеем множество S. Определим множества путей $S_i, S_{i,1}, S_{i,2}$; $1 \leq i \leq \leq I \ll \log q$.

$$S_i = \{s \in S : |s| \in [2^{i-1}l, 2^i l)\}$$

Множества $S_{i,1}, S_{i,2}$ могут быть определены любым образом с выполнением следующих свойств

1) $S_i = S_{i,1} \sqcup S_{i,2}$;

2)разница количества путей в $S_{i,1}$ и в $S_{i,2}$ не отличается больше чем на единицу.

Когда множества $S_i, S_{i,1}, S_{i,2}$; $1 \leq i \leq I = \frac{\log \frac{|E|}{l}}{\log 2} \ll \log q$ определены мы переходим к следующему шагу.

Шаг 3.

Мы определяем множества A_i, B_i (множество вершин) для каждого $1 \leq i \leq I$. Предположим имеем набор $S_{i,1}, S_{i,2}$.

Рассмотрим $S_{i,1}$. Для каждого пути $s \in S_{i,1}$ мы берем первые t вершин этого пути s, где t произвольно с условием $t \in (0.09|s|, 0.1|s|)$. Мы включаем эти вершины ко множеству A_i.

Множество B_i определяется аналогично A_i, с заменой $S_{i,1}$ на множество $S_{i,2}$.

Когда множества A_i, B_i $1 \leq i \leq I \ll \log q$ определены, мы переходим к следующему шагу.

Шаг 4.

Если существует такое $1 \leq i \leq I$ что $|A_i|, |B_i| \geq 4q^{\frac{d+1}{2}}$, тогда по Лемме 1 существует $x \in A_i, y \in B_i$ и $\| x - y \| = 1$. По определению A_i, B_i существуют два пути $s_1 \in S_{i,1}, s_2 \in S_{i,2}$ и мы можем соединить большие части этих путей s_1, s_2 и образовать новый путь. Мы убираем

пути s_1, s_2 из S и образуем новый путь s из больших частей путей s_1 и s_2. Мы добавляем путь s во множество S и далее переходим к Шагу 1.

Если такое i не существует мы завершаем наш алгоритм.

Сначала убедимся, что наш алгоритм завершит свою работу. Для этого введем понятие лексикографического порядка на множестве путей из S: мы располагаем пути из S в порядке невозрастания. Соответственно напишем последовательность этих чисел. Лексикографический порядок определяется по этой последовательности чисел. Каждый раз, когда переходим к Шагу 4 и если для некоторого i мы имеем $|A_i|, |B_i| \geq 4q^{\frac{d+1}{2}}$, то лексикографический порядок на множестве S увеличивается. Так как множество E конечно, алгоритм завершит свою работу.

Для некоторого $1 \leq i_0 \leq I$ количество вершин во множестве S_{i_0} есть $\Omega(|E|/\log q)$. Если C является большой константой, тогда легко видеть, что множество S_{i_0} содержит только один путь s. Действительно, иначе мы можем образовать более длинный путь из двух различных путей. Этот путь s удовлетворяет условиям исходной леммы и мы завершаем доказательство.

□

3.1. Доказательство Теоремы 2

Доказательство.

Сначала, мы можем считать, что $f > C$, где C - есть некоторая абсолютная константа из Леммы 3. Используя опять же предыдущую лемму мы заключаем, что существует путь s_1 длины $\Omega(\frac{|E|}{\log q})$. Далее, определяем $S_1 = s_1$. Предположим, что $n \geq 1$ и путь S_n уже построен. Если

$$|E| - |S_n| \leq Cq^{\frac{d+1}{2}} \log q$$

мы полагаем $S = S_n$ и завершаем наш алгоритм.

Если

$$|E| - |S_n| > Cq^{\frac{d+1}{2}} \log q$$

мы определяем множество E_n как множество всех вершин E, не принадлежащих пути S_n. Далее, мы используем Лемму 3 для множества E_n, и заключаем, что имеется путь s_{n+1} длины $\Omega(\frac{|E_n|}{\log q})$.

Мы определяем A как первые $[4q^{\frac{d+1}{2}} + 1]$ вершин пути S_n и множество B как набор первых $[4q^{\frac{d+1}{2}} + 1]$ вершин пути s_{n+1}. Используя Лемму 1 мы можем образовать новый путь из больших частей путей S_n и s_{n+1}. Определим этот новый путь как S_{n+1} и продолжим алгоритм.

Несложные вычисления показывают, что $|S_{l+1}| > |S_l|$. Путь S удовлетворяет условиям Теоремы 2 и мы завершаем доказательство.

□

4. Заключение

Данная работа посвящается светлой памяти замечательного ученого и академика Юрия Владимировича Линника. Автор хотел бы поблагодарить С. В. Конягина и И. Д. Шкредова за ценные комментарии, советы и внимание к этой работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Adhikari S. D., Mukhopadhyay A., Ram Murty M. The analog of the Erdos distance problem in finite fields // Int. J. Number Theory. 2017. Vol. 13, №9. P. 2319–2334.

2. Bennett M., Chapman J., Covert D., Hart D., Iosevich A., Pakianathan J. Long paths in the distance graph over large subsets of vector spaces over finite fields // J. Korean Math. Soc. 2016. Vol. 53, P. 115–126.

3. Chapman J., Erdogan M.B., Hart D., Iosevich A., Koh D. Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates // Math Z. 2012. Vol. 271, №1-2, P. 63–93.

4. Iosevich A., Rudnev M. Erdos distance problem in vector spaces over finite fields // Transactions of the AMS. 2007. Vol. 359, №12, P. 6127–6142.

REFERENCES

1. Adhikari, S. D., Mukhopadhyay, A., Murty, M. Ram. 2017, "The analog of the Erdos distance problem in finite fields", *Int. J. Number Theory* vol. 13, no. 09, pp. 2319–2334.

2. Bennett, M., Chapman, J., Covert, D., Hart, D., Iosevich, A., Pakianathan. 2016, "Long paths in the distance graph over large subsets of vector spaces over finite fields", *J. Korean Math. Soc.* vol. 53, pp. 115–126.

3. Chapman, J., Erdogan, M. B., Hart, D., Iosevich, A., Koh, D. 2012, "Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates", *Math Z.*, vol. 271, no. 1–2, pp. 63–93.

4. Iosevich, A., Rudnev, M. 2007, "Erdos distance problem in vector spaces over finite fields", *Transactions of the AMS*, vol. 359, no. 12, pp. 6127–6142.

Получено 16.07.2018
Принято к печати 15.10.2018

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 3.

УДК 51(092) DOI 10.22405/2226-8383-2018-19-3-318-327

Георгий Феодосьевич Вороной (1868–1908)

Долбилин Николай Петрович — доктор физико-математических наук, профессор, профессор кафедры теории чисел, Механико-математический факультет, Московский государственный университет имени М. В. Ломоносова, ведущий научный сотрудник, Математический институт им. В. А. Стеклова РАН, г. Москва.
e-mail: dolbilin@mi-ras.ru

Аннотация

Данная статья посвящена 150-летию со дня рождения выдающегося российского математика Георгия Феодосьевича Вороного.

Ключевые слова: Георгий Феодосьевич Вороной.

Библиография: 3 названия.

Для цитирования:
Н. П. Долбилин. Георгий Феодосьевич Вороной (1868–1908) // Чебышевский сборник, 2018, т. 19, вып. 3, с. 318–327.

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 3.

UDC 51(092) DOI 10.22405/2226-8383-2018-19-3-318-327

Georgy Feodosevich Voronoy (1868–1908)

Dolbilin Nikolay Petrovich — doctor of physical and mathematical sciences, professor, Leading researcher of Geometry and Topology Department, Steklov Mathematical Institute of RAS, Professor of Number theory Chair of Department of Mechanics and Mathematics, Lomonosov Moscow state University.
e-mail: dolbilin@mi-ras.ru

Abstract

This article is devoted to the 150th anniversary of the birth of the outstanding Russian mathematician Georgy Voronoi.

Keywords: Georgy Feodosevich Voronoy.

Bibliography: 3 titles.

For citation:
N. P. Dolbilin, 2018, "Georgy Feodosevich Voronoy (1868–1908)", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 318–327.

Рис. 1: Г. Ф. Вороной (28.04.1868–20.11.1908)

Введение

За свою короткую жизнь (1868–1908) Вороной опубликовал не так много, всего 12 работ: 6 больших мемуаров и 6 относительно небольших заметок. Но благодаря им, имя Георгия Феодосьевича Вороного навсегда вписано золотыми буквами в историю науки, как одного из крупнейших математиков в теории чисел, как создателя целого математического направления – геометрии чисел.

Его исследования являются на протяжении целого века определяющими для нескольких поколений математиков, а знаменитые "диаграммы Вороного" стали инструментом исследований не только в математике и вычислительной геометрии, но и в физике, в геологии и кристаллографии, в биологии и компьютерной графике, повсюду, даже в кинематографе.

Имя Вороного входит в названия тысяч и тысяч опубликованных научных работ.

1. Детство

Георгий Феодосьевич Вороной родился 16(28) апреля 1868 г. в украинской семье в имении своего отца — в селе Журавка, расположенном в очень живописном уголке Полтавской губернии Российской империи, теперь Черниговской области Украины. Отец — Феодосий Вороной получил филологическое образование в Киевском университете, преподавал русскую литературу в Нежинском лицее, затем работал директором гимназий в Кишиневе, Бердянске, Прилуках. Он был активным деятелем народного просвещения, инициатором открытия воскресных школ.

Георгий Вороной начал учиться в Бердянской гимназии, а закончил Прилукскую в 1885 г. Благодаря дневнику, который Вороной вел на русском языке, мы знаем, что детство протекало в очень теплой семейной атмосфере. У мальчика было несколько увлечений: музыка (мальчик играл на двух инструментах: фортепьяно и флейте), шахматы, самодеятельный театр (участие в спектаклях) и даже охота.

В гимназии Георгий Вороной выделялся среди сверстников глубоким интересом к наукам и незаурядными способностями к математике. Огромное влияние на общее развитие Вороного, в том числе и на развитие его математического дарования, оказал учитель математики Иван Владимирович Богословский. Влияние этого замечательного педагога на литературные пристрастия Георгия сказывались даже в университете.

Вороной как и все студенты того времени был увлечен Л. Н. Толстым, интересовался описаниями русской жизни в произведениях "В лесах" и "На горах" П. И. Мельникова-Печерского, но поначалу был несколько равнодушен к творчеству Салтыкова-Щедрина. И только впо-

следствии, под влиянием своего любимого учителя математики, который сам любил сатиру Щедрина, Вороной стал почитателем выдающегося сатирика.

В 1884 г. профессор Киевского университета В. П. Ермаков начал издавать "Журнал элементарной математики", в котором были предложены темы для ученических работ по математике. На одну из тем, именно "Разложение многочленов на множители, основанное на свойствах корней квадратных уравнений", единственная работа была представлена Вороным. Работа понравилась Ермакову и он опубликовал ее в своем журнале в 1885 г.. В этом же году Вороной закончил гимназию и поступил в Петербургский университет.

2. Петербургский университет

В университете Георгий приступил к изучению математических курсов, усердно посещал курсы лекций "по чистой математике, которые все более увлекали" его. В его дневнике мы читаем: "Лекции профессора Сохоцкого по специальному курсу высшей алгебры я предпочитаю всем остальным". Наряду с этим Вороной изучает курс алгебры Серре, теорию двойничных форм по книге Фаа-ди-Бруно, работы Чебышева по теории чисел.

В бытовом отношении жизнь студента Вороного складывалась достаточно трудно. Той помощи, которую мог оказывать ему отец, явно не хватало. После выхода отца в отставку в 1887 году и эта помощь сократилась. Георгий вынужден был давать за небольшие деньги уроки, которые его выматывали, а тяжелые условия в общежитии дополнительно осложняли и отдых и занятия математикой. В дневнике Вороной описывает тяжелую атмосферу недоверия и подозрительности, которая воцарилась в стенах университета в связи с "уваровским указом" от 1884 г., подчинившим университетскую жизнь полицейскому надзору. Эта атмосфера стала еще тяжелей в связи с участием нескольких студентов университета в покушении на Александра III в марте 1887 г..

Условия жизни не только мало способствовали занятиям наукой, но, к сожалению, и негативно сказались на здоровье Вороного. Тем не менее, несмотря на это, а в некоторой степени, вследствие этих тяжелых условий, Вороной предельно сконцентрировался на математике. "Главное, что меня занимает, есть ли у меня достаточно способностей", — читаем в его дневнике. К счастью, математических способностей у Вороного было в избытке, а "постоянно усиливающаяся страсть к математике" охватывает его всецело. В "моменты, когда ум охватывает идею, которая раньше как мячик ускользала, я забываю, что я существую", — записывает в дневнике Вороной в 1887 г. Там же он продолжает: "моими последними успехами я обязан привычке мыслить без пера и бумаги. Все предложения, доказанные мною, возникали совершенно независимо.... Я надеюсь, что эта привычка мыслить таким образом сослужит мне службу."

Чтобы развивать способности, Вороной устраивал себе математический, как говорят сейчас, тренинг: последовательно решал трудные учебные задачи на взятие определенных интегралов, на вычисление сложных симметрических функций, на интегрирование дифференциальных уравнений.

Серьезное научное исследование проведено в его кандидатской диссертации (аналог дипломной работы), над которой Вороной работал на старших курсах под руководством академика Андрея Андреевича Маркова (старшего). В ней Вороной, в частности, доказал теорему, обобщающую известную теорему Адамса о бернуллиевых числах. Эта весьма остроумная работа очень понравилась Маркову и он горячо рекомендовал работу к опубликованию. Однако чрезвычайно требовательный к себе и к своей работе Вороной продолжал некоторое время улучшать рукопись. Первая статья Вороного "О числах Бернулли" появилась на свет в 1890 г. в "Сообщениях Харьковского математического общества".

К окончанию в 1889 г. университета Вороной стал профессиональным математиком, сосредоточившим свое внимание на теории чисел. Он был оставлен при университете "для подготовки к профессорскому званию" (что в некоторой степени соответствует нынешней аспирантуре). Тема магистерской диссертации (в дореволюционной России — это аналог нашей кандидатской диссертации), выполненной под руководством А. А. Маркова, "О целых алгебраических числах, зависящих от корня неприводимого уравнения 3-й степени". Диссертация содержала подробное исследование основных алгоритмических вопросов в теории кубических полей. Диссертация была успешно защищена в Петербургском университете в 1894 году.

3. Варшавский университет

После успешной защиты диссертации Вороной был назначен профессором математики Императорского Варшавского университета (Царство Польское после Венского конгресса 1815 г. до 1915 г. входило в состав Российской империи) по кафедре чистой математики. В Варшавском университете Вороной работал с небольшим перерывом до конца жизни. Здесь он познакомился и подружился с профессором математики и механики Николаем Борисовичем Делоне и его семьей, который в то время работал в Варшавском политехническом институте. Таким образом, сын Н. Б. Делоне, Борис Делоне познакомился с Георгием Феодосьевичем будучи подростком. Борис Николаевич любил рассказывать, как Вороной приходил к ним в гости и допоздна засиживался за беседой с его отцом. Хотя Вороной не был и не мог быть научным руководителем Б. Н. Делоне, поскольку Вороной умер в 1908 г., когда Борис Делоне поступил в Киевский университет), его влияние на творчество Делоне оказалось очень значительным.

Исследования по теории алгебраических чисел 3-й степени, начатые в магистерской диссертации, были продолжены Вороным. И это вполне объяснимо, так как интерес к теории алгебраических чисел был в центре внимания чебышевской школы начиная с 1860 гг.. Теории алгебраических чисел был посвящен ряд работ Е. И. Золотарева, А. А. Маркова, Ю. В. Сохоцкого. Вороной заинтересовался вопросом вычисления основных единиц общего кубического поля как случая отрицательного, так и положительного дискриминанта. Полученные Вороным результаты составили содержание его докторской диссертациии „Об одном обобщении алгорифма непрерывных дробей". В этой очень важной работе Вороной предложил метод, решающий для кубических полей вопросы, аналогичные тем, что в свое время были решены для квадратичных полей при помощи непрерывных дробей Эйлером, Лагранжем и другими.

В принципе, не только вопрос существования основных единиц алгебраического поля, но и проблема их вычисления решаются знаменитой теоремой Дирихле. Однако конечный перебор всевозможных вариантов на том пути, который вытекает из теоремы Дирихле, настолько колоссален, что не оставлял никакой надежды на то, чтобы им можно было воспользоваться на практике. В докторской диссертации Вороной предложил эффективный метод для вычисления основных единиц кубического поля, который можно было реализовать в каждом конкретном случае.

Как вспоминал Д. Граве со слов А. А. Маркова, этот результат настолько поразил Маркова, что тот послал Вороному телеграмму в Варшаву с просьбой срочно приехать в Петербург. Как только Вороной появился в кабинете своего научного руководителя, Марков предложил ему найти основную единицу для кубического уравнения $t^3 = 1$, которая была найдена Марковым самим при помощи сложных, весьма искуственных вычислений. Насколько же был удивлен Марков, когда Вороному понадобилось всего три часа, чтобы посредством своего алгоритма найти искомую единицу.

В этой диссертации, по мнению Делоне, Вороной "мыслил геометрически". Но рассуждая геометрически, Вороной вынужден был переводить ход своих рассуждений на арифметический язык, так как руководители Петербургской школы и особенно Марков, основной оппонент по диссертации, не приветствовали геометрический характер изложения, и диссертацию, написанную на геометрическом языке, могли бы не пропустить. Докторская диссертация была блестяще защищена Вороным в 1897 году в Петербургском университете. Петербургская Академия наук за цикл работ по алгебраической теории чисел, вошедших в магистерскую и докторскую диссертации, отметила Вороного престижной премией имени Буняковского.

Впоследствии эта работа оказала большое влияние на исследования Б. Н. Делоне по диофантовым уравнениям третьей степени. Геометризации алгоритма Вороного были посвящены работы Б. Н. Делоне, а также часть известной монографии Б. Н. Делоне и Д. К. Фаддеева "Теория иррациональностей третьей степени". Диссертация Вороного была напечатана только по-русски, отчасти поэтому ее результаты долго оставались мало известными заграницей и некоторые из них переоткрывались на протяжении десятилетий.

Помимо глубоких исследований по алгебраической теории чисел и геометрии квадратичных форм, Вороной в стенах Варшавского университета выполнил принципиальную работу по аналитической теории чисел. В 1903 г. он опубликовал большую работу „Sur un problème du calcul des fonctions asymptotiques", посвященную исследованию задачи о делителях, поставленной Дирихле. Задача о делителях состоит в оценивании для больших n суммы

$$S_n = \tau(1) + \tau(2) + \cdots + \tau(n),$$

где $\tau(k)$ — число делителей числа k. Так как $S(n)$, очевидно, равно количеству точек (x, y) с целыми положительными координатами, для которых $xy \le n$, эту работу Вороного упоминают, как работу о числе целых точек под гиперболой.

В своей работе 1849 г. Дирихле получил для $S(n)$ следующую формулу:

$$S(n) = n(\log n + 2C - 1) + K_n\sqrt{n}, \tag{1}$$

где $C = 0,57721...$ — эйлерова константа и значение $|K_n|$ при $n \to \infty$ ограниченно при $n \to \infty$.

В дальнейшем на протяжении полувека многочисленные усилия известных математиков, направленные на уточнение порядка остаточного члена, оставались безуспешными. И только в 1903 г. Г. Ф. Вороной, основательно развив метод Дирихле, в результате сложных вычислений улучшил порядок остаточного члена в формуле (1) для $S(n)$:

$$S(n) = n(\log n + 2C - 1) + \theta_n \sqrt[3]{n}\log n, \tag{2}$$

где θ_n ограниченно при $n \to \infty$.

Работа Вороного оказала влияние на работы других замечательных математиков в теории чисел. В. Серпинский, будучи студентом Вороного, применил метод Вороного к задаче о числе $A(n)$ целых точек (x, y) в круге $x^2 + y^2 \le n$ и получил следующую формулу:

$$A(n) = \pi \cdot n + \theta'(n) \cdot \sqrt[3]{n}.$$

Эта работа Г. Ф. Вороного по аналитической теории чисел также, как отмечает Б. Н. Делоне, послужила одним из отправных пунктов для творчества Ивана Матвеевича Виноградова и ряда других выдающихся математиков.

4. Геометрия квадратичных форм: последние мемуары Вороного

В 1904 г. Г. Ф. Вороной участвовал в работе Международного конгресса математиков в Гейдельберге, где встречался с Г. Минковским. Б. Н. Делоне, которому в том году шел 15-й год, тоже был вместе с отцом на Конгрессе. Б. Н. Делоне рассказывал, что, по словам отца, Минковский отнесся к Вороному с огромным интересом и величайшим уважением.

Вопросы геометрии чисел интересовали Вороного к тому времени уже на протяжении почти десятка лет. Но в 1904 г. Вороной вплотную приступает к циклу исследований по геометрии чисел под общим названием "Nouvelles applications des paramèters continus à la thèorie des formes quadratiques" ("Новые приложения непрерывных параметров к теории квадратичных форм"), посвященный крупным проблемам в теории квадратичных форм, как положительных так и неопределенных. В действительности, как писал в 1908 году Вороной редактору журнала Crelle, последний мемуар — работа о параллелоэдрах —, была результатом 12-летних исследований.

В рамках этого проекта Вороной проводит исследования по геометрии положительных квадратичных форм, в том числе и по теории параллелоэдров. Результаты этих основополагающих в геометрии чисел исследований были опубликованы в двух больших мемуарах: „Sur quelques propriétés des formes quadratiques positives parfaites" ("О некоторых свойствах квадратичных положительных совершенных форм", Crelle, Bd. 133, (1907)) и „Recherches sur les paralleloedres primitifs" ("Исследования о примитивных параллелоэдрах", Crelle, Bd 134 (1908), 136(1909)). Публикация второй части последнего мемуара завершилась посмертно.

Благодаря этим фундаментальным исследованиям по геометрии квадратичных форм Г. Ф. Вороной признан наряду с Минковским основоположником геометрии чисел.

Метод непрерывных параметров к исследованию положительных квадратичных форм первым ввел в рассмотрение Ш. Эрмит для нахождения формы от n переменных с наибольшим арифметическим минимумом $\mu(n)$. Эта задача эквивалентна геометрической задаче о нахождении плотнейшей решетчатой упаковки n-мерного евклидова пространства равными шарами, другими словами, задачи о плотнейшем расположении равных шаров, при условии, что их центры образуют целочисленную решетку.

А. Н. Коркин и Е. И. Золотарев (также выдающиеся представители Петербургской школы Чебышева) нашли значения $\mu(n)$ для $n \leq 5$. Более того, рассматривая конус положительных квадратичных форм, они ввели понятие предельной формы, то есть формы, на которой арифметический минимум достигает локального максимума. Они показали, что для предельной формы полная таблица арифметических представлений ее минимума состоит из не менее чем $\frac{(n+1)n}{2}$ элементов, причем эта таблица полностью определяет саму форму. Так как форма с наибольшим арифметическим минимумом $\mu(n)$ – одна из предельных форм, а предельных форм для каждого n, как установили Коркин и Золотарев, конечное число (с точностью до целочисленной эквивалентности), то задача нахождения абсолютного ьаксимума $\mu(n)$ сводится к перечислению всех предельных форм.

Вороной развил эту теорию до алгоритмического уровня. Он ввел понятие *совершенной формы*, как положительной формы, которая однозначно определяется таблицей представлений своих арифметических минимумов. Так как это условие является необходимым для любой предельной формы, но не достаточным, то совершенная форма является более *общей* формой, нежели предельная. Если перевести идеи Вороного на язык геометрических образов, на котором он проводил свои рассуждения, затем их "переодевая в аналитические одежды", то в основе описания совершенных форм лежит некомпактный выпуклый полиэдр П в конусе K положительных квадратичных форм с вершинами на его границе.

Пусть K – конус положительных квадратичных форм $f = \Sigma_{i,j=1}^{n} a_{ij}x_ix_j$ от n. Гео размерность равна $N = \frac{n(n+1)}{2}$. Граница ∂K конуса K состоит из тех квадратичных форм, соответствующих симметричным матрицам (a_{ij}), у которых все главные миноры неотрицательны и хотя бы один из них равен 0. Пусть $(q_1, \dots, q_n)$ – ненулевой набор целых чисел, не имеющих общего делителя, и пусть $q(x_1, \cdots, x_n) = (q_1x_1 + \cdots + q_nx_n)^2)$ -вырожденная неотрицательная квадратичная форма ранга 1. Форма $q(x)$ лежит на границе ∂K. Пусть Q – множество таких форм, построенных для всевозможных ненулевых наборов $(q_1 \dots, q_n) \in \mathbb{Z}^n$ без общих множителей. Выпуклая оболочка $\mathrm{conv}(Q)$ есть полиэдр П, введенный в рассмотрение Вороным. Основное содержание мемуара Вороного состоит в изучении свойств полиэдра П. Исходная идея Вороного заключалась в том, что каждой гиперграни полиэдра П соответствует некоторая совершенная форма f и, обратно, всякой совершенной форме соответствует некоторая гипергрань полиэдра П. При этом коэффициенты уравнения гиперплоскости данной грани суть коэффициенты совершенной формы. Так как размерность гиперграни равна $\frac{n(n+1)}{2} - 1$, то количество вершин у гиперграни

$$(q_{1s}^2, q_{2s}^2, \dots, q_{ns}^2, q_{1s} \cdot q_{2s}, \dots, q_{n-1\,n})$$

не меньше $\frac{n(n+1)}{2}$, а соответствующие целочисленные наборы

$$(q_{1s}, q_{2s}, \cdots, q_{ns})$$

составляют таблицу арифметических представлений минимума формы f.

Для каждого n среди совершенных форм от n переменных имеется т.н. главная совершенная форма

$$x_1^2 + x_2^+ \cdots + x_n^2 + x_1x_2 + \cdots x_{n-1}x_n.$$

Далее Вороной описал как, исходя из соответствующей главной гиперграни полиэдра П и последовательно переходя из одной гиперграни через грани коразмерности 2 в соседние, можно обойти за конечное число шагов все (с точностью до целочисленной эквивалентности) гиперграни полиэдра. Возможность таких переходов в соседние гиперграни Вороной аккуратно обосновал посредством метода непрерывных параметров. Среди конечного числа найденных попарно неэквивалентных совершенных форм содержатся все предельные формы для данного n, из которых можно выделить квадратичную форму с максимальным значением $\mu(n)$ (вообще говоря, таких форм может быть несколько).

Последний мемуар, посвященный теории параллелоэдров, состоит из двух частей. Вторая часть мемуара вышла в свет после смерти Вороного. Стоит отметить, что над теорией параллелоэдров Вороной начал работать задолго до упомянутой встречи с Минковским. По мнению и самого Вороного и других специалистов, в частности, по мнению Делоне, мемуар по теории параллелоэдров является наиболее глубоким из всех исследований, что были проведены Вороным. Так как в мемуаре изучается особый класс многогранников, то, несмотря на аналитический характер изложения, в этой работе мы встречаем геометрические термины: симплексы, грани, разбиения пространства на многогранники и т.д. Параллелоэдр размерности n – это выпуклый евклидов многогранник, параллельными копиями которого, приложенными друг к другу по целым общим граням, можно разбить n-мерное евклидово пространство, то есть заполнить пространство без пропусков и попарных перекрытий.

Понятие 3-мерного параллелоэдра было введено Е. С. Федоровым в связи с потребностями кристаллографии. Он нашел все пять комбинаторных типов трехмерных параллелоэдров.

Для произвольного n Минковский доказал, что n–мерный параллелоэдр – центрально симметричный многогранник с центрально симметричными гранями. Нетрудно также показать,

что любое нормальное, то есть грань-в-грань, разбиение пространства на параллелоэдры транзитивно относительно группы трансляций. Отсюда следует, что центры параллелоэдров образуют целочисленную решетку. Из этого факта Минковский вывел, что число гиперграней в параллелоэдре не превышает $2(2^n - 1)$, откуда следует конечность числа комбинаторных параллелоэдров для каждой размерности.

В мемуаре исследуется проблема перечисления комбинаторных типов параллелоэдров данной размерности. Вороной рассматривает область Дирихле относительно точек решетки, другими словами то, что теперь называют областью Вороного. Области Дирихле-Вороного для решеток являются параллелоэдрами, но параллелоэдрами особого вида, носящими теперь имя Вороного.

В первой части мемуара проблема перечисления произвольных параллелоэдров отчасти сводится к проблеме перечисления параллелоэдров Вороного. Вороной вводит понятие примитивного параллелоэдра, как такого параллелоэдра, что в каждой вершине разбиения n-мерного пространства сходится минимально возможное число (то есть $n+1$) параллелоэдров. Центральный результат первой части – доказательство теоремы о том, что всякий примитивный параллелоэдр аффинно эквивалентен некоторому параллелоэдру Вороного. Тем самым нахождение типов примитивных параллелоэдров Вороной свел к нахождению типов примитивных параллелоэдров Вороного. Эта часть мемуара – очень глубокое исследование, в котором некоторые геометрические идеи (например, принцип Ампера), примененные до него в двумерном случае, Вороной развил для случая многих измерений.

Вороному принадлежит также плодотворная идея подъема разбиения Дирихле-Вороного n-мерного пространства на параболоид вращения в $(n+1)$-мерном пространстве. В 1980-е гг. эта идея была переоткрыта и использована в вычислительной геометрии как инструмент сведения задачи вычисления диаграмм Вороного и триангуляций Делоне для дискретных точечных множеств к задаче вычисления выпуклой оболочки поднятого на параболоид множества точек.

Вороной показал, что всякому разбиению n-мерного пространства на примитивные параллелоэдры соответствует $(n+1)$-мерный полиэдр, описанный около эллиптического параболоида. Аффинное преобразование, переводящее эллиптический параболоид в параболоид вращения, переводит примитивный параллелоэдр разбиения в параллелоэдр Вороного. Вороной выдвинул следующую гипотезу: *всякий параллелоэдр аффинно эквивалентен некоторому параллелоэдру Вороного.*

Во второй части мемуара Вороной исследует вопрос о нахождении комбинаторных типов параллелоэдров Вороного, то есть, повторяем, областей Дирихле-Вороного для целочисленных решеток. Целочисленные решетки "живут" в конусе K положительных квадратичных форм. Вороной устанавливает, что примитивным параллелоэдрам того или иного комбинаторного типа соответствуют формы, составляющие так называемую область данного типа – $\frac{n(n+1)}{2}$-мерный конус с вершиной в вершине в конусе K. Вороной показывает, что каждая область типа представляет собой многогранный угла с конечным числом гиперграней. Эти многогранные области типа, прилегая друг к другу по целым гиперграням, разбивают весь конус K.

Для нахождения всех примитивных типов Вороной предлагает процедуру, которая исходит от особого примитивного параллелоэдра, соответствующего так называемой области I типа. Кстати этот особый параллелоэдр является многогранником, хорошо известным в наше время под названием перестановочный многогранник или пермутоэдр. Переходя из области I типа через гипергрань в смежную область типа, мы получаем, вообще говоря, другой тип параллелоэдра. Вороной описывает характер перестройки комбинаторного типа параллелоэдра, происходящей при переходе через ту или иную гипергрань. Переходя из одной области типа в соседнюю, получаем, вообще говоря, новые типы параллелоэдров. Вороной указывает

условия, при которых можно утверждать, что на каком-то этапе список полученных типов исчерпывает все типы примитивных параллелоэдров Вороного, то есть задача нахождения всех примитивных параллелоэдров для данной размерности решена.

В этом же мемуаре Вороной опробовал свой метод для нахождения примитивных параллелоэдров для размерностей 2, 3 (ранее установленных Е. С. Федоровым), а также 4. Оказалось, что для размерности 4 помимо 4-пермутоэдра имеется еще два примитивных параллелоэдра. В 1929 г. Б. Н. Делоне нашел все 49 непримитивных параллелоэдров (на самом деле Делоне нашел 48 непримитивных и 1 пропущенный был найден М. И. Штогриным полвека спустя). В 1972 г., опираясь на метод Вороного, С. С. Рышков и Е. П. Барановский, а несколько позднее, другим методом, П. Энгел и В. П. Гришухин нашли полный список из 222 примитивных 5-мерных параллелоэдров. Недавно с помощью компьютера М. Дютур Сикирич и др. нашли все 110 244 комбинаторных типа 5-мерных параллелоэдров Вороного (против 52 типов 4-мерных параллелоэдров).

Делоне в книге "Петербургская школа теории чисел" высоко оценил этот мемуар: "Мемуар Вороного о параллелоэдрах — одно из самых глубоких исследований в области геометрии чисел во всей мировой литературе, а своеобразие методов чисто геометрической первой части накладывает на этот мемуар печать гениальности."

Подчеркнем, что несмотря на поразительную глубину метода, Вороной смог реализовать свою программу лишь для примитивных параллелоэдров. Более того, несмотря на серьезные усилия многих математиков и прогресс, достигнутый в работах Делоне, О. К. Житомирского, А. Д. Александрова, Б. А. Венкова, С. С. Рышкова и др., гипотеза Вороного об аффинной эквивалентности n-мерного параллелоэдра некоторому параллелоэдру Вороного остается открытой для $n \geq 5$ на протяжении века.

После завершения работы над вторым мемуаром о положительных квадратичных формах Вороной приступил к исследованиям по теории неопределнных квадратичных форм. Об условиях, в которых протекала эта работа, рассказывает следующая запись в дневнике: "Я делаю большие успехи в разбираемом вопросе; но в то же время здоровье мое все ухудшается и ухудшается. Вчера я первый раз получил отчетливую идею об алгорифме, который должен разрешить все вопросы рассматриваемой теории форм, и вчера же я имел сильный припадок желчной колики, который мне помешал заниматься вечером и не дал возможности заснуть всю ночь. Я так боюсь, чтобы результаты моих долгих усилий, с таким трудом добываемые, не погибли вместе со мной".

Увы, большая рукопись о неопределенных формах, которую видели друзья, посещавшие Вороного в 1908 г., не была найдена. В 1952 г. в полном трехтомном собрании трудов Вороного были опубликованы записи об исследованиях по неопределенных формах, взятые из научного дневника Георгия Феодосьевича.

5. О жизни

В Варшавском университете Вороной проработал с 1894 г. с небольшим перерывом в самом конце жизни. В связи с революционными событиями 1905-07 гг. Варшавский университет был закрыт и Вороной был направлен на работу в Новочеркасск, в только что организованный там Донской политехнический институт, где проработал в течение года в качестве декана факультета механики. За выдающиеся научные достижения Вороной был избран в 1907 г. в возрасте 39 лет членом-корреспондентом Петербургской академии наук.

Г. Ф. Вороной был женат на Ольге Митрофановне Крицкой, девушке из дворянской семьи, чье имение Богданы находилось поблизости от его Журавки. Ольга Крицкая была его большая любовь еще с юности. У них было шестеро детей. Кроме своей многочисленной семьи,

Вороной заботился также о семье его рано овдовевшей сестры с семью детьми. Все дети Георгия Феодосьевича, кроме умершей в детстве одной из дочерей, получили хорошее образование и стали специалистами: врачами, учителями, хирургами. К сожалению, две старшие дочери Александра и Мария и старший сын Александр и их семьи пострадали во время сталинских репрессий. Младший сын Юрий Георгиевич Вороной (1896–1961) стал известным хирургом, доктором медицинских наук, прославился тем, что в 1933 г. сделал первую в мире пересадку почки человеку.

Г. Ф. Вороной не отличался крепким здоровьем, в последние годы страдал от прогрессирующей болезни желчного пузыря. Интенсивная научная и преподавательская работа отягощала его состояние. В последний год жизни врачи строго рекомендовали Георгию Феодосьевичу прекратить работу. Вороной и сам замечал, что напряженная работа отрицательно сказывается на здоровье, но оставить исследования он был не в состоянии. "Только моя жена знает, что математика является для меня главной целью жизни, она (математика) для меня – все".

Лето 1908 г. после года, проведенного в Новочеркасске, Георгий Феодосьевич отдыхал в милой Журавке, несмотря на рекомендации врачей поехать на лечение в Карлсбад. К концу лета ему стало легче, и к началу 1908/09 учебного года Вороной прибыл в Варшавский университет. В начале сентября пишет свое последнее письмо В. А. Стеклову, в котором кратко сообщает о своих исследованиях о параллелоэдрам, а также выражает желание перейти на должность "ординарного профессора" в Петербургском университете, где в это время образовалась вакансия в связи с только что скончавшимся профессором А. Н. Коркиным.

Однако в октябре наступило резкое обострение болезни. В оставшийся ему месяц, страдая от болей, прикованный к постели, Вороной сумел записать "Заметки по поводу последней теоремы Ферма". Через две недели, 7(20) ноября 1908 г., в возрасте сорока лет, Георгий Феодосьевич Вороной скончался. Похоронен по завещанию в его любимой Журавке.

Заключение

Глубокие фундаментальные исследования Георгия Феодосьевича Вороного, одного из самых выдающихся математиков, когда-либо работавших в теории чисел, на протяжении уже более века оказывают огромное влияние на современную теорию чисел, а поставленная им задача об аффинной эквивалентности произвольного параллелоэдра параллелоэдру Вороного является одной из центральных нерешенных проблем геометрии чисел.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Г. Ф. Вороной. Собрание сочинений в 3-х томах. — Киев, 1952–1953.

2. Б. Н. Делоне. Петербургская школа теории чисел. — М. 1947.

3. Б. Н. Делоне, Д. К. Фаддеев. Теория иррациональностей третьей степени. — М. 1940.

REFERENCES

1. G. F. Voronoy, 1952–1953, Collected works in 3 volumes, Kiev.

2. B. N. Delone, 1947, "St. Petersburg school of number theory" Moscow.

3. B. N. Delone, D. K. Faddeev, 1940, "The theory of irrationalities of the third degree" Moscow.

Получено 19.09.2018
Принято к печати 15.10.2018

РЕДКОЛЛЕГИЯ

Том 19 Выпуск 3

THE EDITORIAL BOARD

Volume 19, Issue 3

TABLE OF CONTENTS

Volume 19 Issue 3