ЧЕБЫШЕВСКИЙ СБОРНИК
Том 21. Выпуск 1.

УДК 511.6 DOI 10.22405/2226-8383-2020-21-1-273-296

Периодические элементы $\sqrt{f}$ в эллиптических полях с полем констант нулевой характеристики

В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников

Платонов Владимир Петрович — академик РАН, доктор физико-математических наук, профессор, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН»; Математический институт им. В. А. Стеклова РАН (г. Москва).
e-mail: platonov@mi-ras.ru

Петрунин Максим Максимович — кандидат физико-математических наук, научный сотрудник, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН» (г. Москва).
e-mail: petrunin@niisi.ras.ru

Штейников Юрий Николаевич — кандидат физико-математических наук, научный сотрудник, Федеральный научный центр «Научно-исследовательский институт системных исследований РАН» (г. Москва).
e-mail: yuriisht@gmail.com

Аннотация

Исследование проблемы периодичности функциональных непрерывных дробей элементов эллиптических и гиперэллиптических полей было начато около 200 лет назад в классических работах Н. Абеля и П. Л. Чебышева. В 2014 году В. П. Платоновым был предложен общий концептуальный метод, базирующийся на глубокой связи трех классических проблем: проблема существования и построения фундаментальных S-единиц в гиперэллиптических полях, проблема кручения в якобианах гиперэллиптических кривых и проблема периодичности непрерывных дробей элементов в гиперэллиптических полях. В 2015-2019 годах в работах В. П. Платонова с соавторами был достигнут большой прогресс в исследовании проблемы периодичности элементов в гиперэллиптических полях, в особенности в эффективной классификации таких периодических элементов. Так, например, в указанных работах В. П. Платонова с соавторами были найдены все эллиптические поля $\mathbb{Q}(x)(\sqrt{f})$ такие, что $\sqrt{f}$ разлагается в периодическую непрерывную дробь в $\mathbb{Q}((x))$, а также были получены дальнейшие продвижения в обобщении указанного результата, как на другие числовые поля констант, так и на гиперэллиптические кривые рода 2 и выше. В настоящей статье мы приводим полное доказательство анонсированного нами в 2019 году результата о конечности числа эллиптических полей $k(x)(\sqrt{f})$ над произвольным числовым полем k с периодическим разложением $\sqrt{f}$, для которых соответствующая эллиптическая кривая содержит k-точку четного порядка не превосходящего 18 или k-точку нечетного порядка не превосходящего 11. Для произвольного поля k являющегося квадратичным расширением $\mathbb{Q}$ найдены все такие эллиптические поля, а для поля $k = \mathbb{Q}$ было получено новое доказательство конечности числа периодических $\sqrt{f}$, не использующее параметризацию эллиптических кривых и точек конечного порядка на них.

Ключевые слова: эллиптическое поле, гиперэллиптическое поле, периодичность, непрерывные дроби, длина периода, фундаментальные единицы, S-единицы, результант, базис Грёбнера, квадратичная иррациональность

Библиография: 22 названия.

Для цитирования:
В. П. Платонов, М. М. Петрунин, Ю. Н. Штейников. Периодические элементы $\sqrt{f}$ в эллиптических полях с полем констант нулевой характеристики // Чебышевский сборник, 2020, т. 21, вып. 1, с. 273–296.

CHEBYSHEVSKII SBORNIK
Vol. 21. No. 1.

UDC 511.6 DOI 10.22405/2226-8383-2020-21-1-273-296

Periodic elements $\sqrt{f}$ in elliptic fields with a field of constants of zero characteristic

V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov

Platonov Vladimir Petrovich — Akademician, Chief researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences; Steklov Mathematical Institute of Russian Academy of Sciences (Moscow).
e-mail: platonov@mi-ras.ru
Petrunin Maxim Maximovich — phd, scientific researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences (Moscow).
e-mail: petrunin@niisi.ras.ru
Shteinikov Yurii Nikolaevich — phd, scientific researcher, Scientific Research Institute for System Analysis of the Russian Academy of Sciences (Moscow).
e-mail: yuriisht@gmail.com

Abstract

A study of the periodicity problem of functional continued fractions of elements of elliptic and hyperelliptic fields was begun about 200 years ago in the classical papers of N. Abel and P. L. Chebyshev. In 2014 V. P. Platonov proposed a general conceptual method based on the deep connection between three classical problems: the problem of the existence and construction of fundamental S-units in hyperelliptic fields, the torsion problem in Jacobians of hyperelliptic curves, and the periodicity problem of continued fractions of elements of hyperelliptic fields. In 2015-2019, in the papers of V. P. Platonov et al. was made great progress in studying the problem of periodicity of elements in hyperelliptic fields, especially in the effective classification of such periodic elements. In the papers of V. P. Platonov et al, all elliptic fields $\mathbb{Q}(x)(\sqrt{f})$ were found such that $\sqrt{f}$ decomposes into a periodic continued fraction in $\mathbb{Q}((x))$, and also futher progress was obtained in generalizing the indicated result, as to other fields of constants, and to hyperelliptic curves of genus 2 and higher. In this article, we provide a complete proof of the result announced by us in 2019 about the finiteness of the number of elliptic fields $k(x)(\sqrt{f})$ over an arbitrary number field k with periodic decomposition of $\sqrt{f}$, for which the corresponding elliptic curve contains a k-point of even order not exceeding 18 or a k-point of odd order not exceeding 11. For an arbitrary field k being quadratic extension of $\mathbb{Q}$ all such elliptic fields are found, and for the field $k = \mathbb{Q}$ we obtained new proof about of the finiteness of the number of periodic $\sqrt{f}$, not using the parameterization of elliptic curves and points of finite order on them.

Keywords: elliptical field, hyperelliptic field, periodicity, continued fractions, period length, fundamental units, S-units, resultant, Gröbner basis, quadratic irrationality

Bibliography: 22 titles.

For citation:
V. P. Platonov, M. M. Petrunin, Yu. N. Shteinikov, 2020, "Periodic elements $\sqrt{f}$ in elliptic fields with a field of constants of zero characteristic" , *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 273–296.

1. Введение

Пусть k — поле характеристики 0, и $f \in k[x]$ — многочлен свободный от квадратов. В работах [1, 2, 3, 4, 5] были получены основополагающие результаты, связанные с проблемой периодичности разложения элементов поля $k(x)(\sqrt{f})$ в непрерывную дробь в поле формальных степенных рядов $k((1/x))$. В частности, было показано, что с точки зрения изучения вопросов, связанных с периодичностью элементов поля $L = k(x)(\sqrt{f})$ ключевым является элемент $\sqrt{f}$. Этот элемент периодичен в $k((1/x))$ в случае, когда поле L содержит периодические элементы. Однако в случае непрерывных дробей в поле формальных степенных рядов $k((x))$ даже наличие в поле L периодических элементов не гарантирует периодичность разложения элемента $\sqrt{f}$ в функциональную непрерывную дробь. Более того, периодичность $\sqrt{f}$ — сравнительно редкое явление.

В работах [6, 7, 8, 18] было доказано, что квазипериодический $\sqrt{f} \in k((x))$ с необходимостью является периодическим, и были построены первые примеры периодических $\sqrt{f}$. А в работах [9, 10] с точностью до естественного отношения эквивалентности была доказана конечность числа таких нетривиальных (то есть, не попадающих в серию $cx^3+1, c \in \mathbb{Q}$) многочленов f степени $\deg f = 3$ с рациональными коэффициентами, а также был поставлен вопрос в более общем случае: для каких свободных от квадратов многочленов $f \in \mathbb{Q}[x]$ непрерывная дробь $\sqrt{f} \in \mathbb{Q}((x))$ является периодической.

В работе [11] для гиперэллиптических полей, содержащих фундаментальные S-единицы малых степеней, с помощью метода, основанного на решении норменного уравнения, были получены рекуррентные соотношения на коэффициенты решения норменного уравнения для полей, обладающих S-единицами малых степеней. С помощью этих соотношений были найдены новые примеры периодических элементов $\sqrt{f}$ для $f \in \mathbb{Q}[x]$.

Однако уже в случае, когда многочлен имеет степень 3, для полей, содержащих фундаментальные S-единицы нечётной степени начиная с 9, соотношения на коэффициенты кардинально усложняются, и указанный метод становится неприменим. В работе [12] был предложен новый эффективный метод для решения норменного уравнения, основанный на применении базисов Грёбнера. В работе [12] было доказано, что для любого поля k характеристики 0 с точностью до естественной эквивалентности существует лишь конечное число бесквадратных многочленов над k нечетной степени, отличной от 11, таких, что элемент $\sqrt{f}$ периодичен, а соответствующее гиперэллиптическое поле $k(x)(\sqrt{f})$ содержит S-единицу степени 11. Кроме того, было доказано, что в случае $k = \mathbb{Q}$ многочленов с указанными свойствами нечётной степени отличной от 9 и 11, не существует.

Остаётся открытым естественный вопрос о периодичности $\sqrt{f}$ для эллиптических полей, рассматриваемых над числовым полем. Полного решения нет даже для $\deg f = 3$ и квадратичных расширений поля $\mathbb{Q}$. В работе [13] было сделано продвижение в этом направлении, и было дано описание кубических многочленов $f(x)$ с коэффициентами в квадратичных числовых полях $\mathbb{Q}(\sqrt{5})$ и $\mathbb{Q}(\sqrt{-15})$, для которых разложение в непрерывную дробь иррациональности $f(x)$ над этими полями периодично. Вышеупомянутые квадратичные числовые поля обладают новым кручением, а значит и фундаментальными S-единицами степеней, не встречающихся в эллиптических полях с полем констант $\mathbb{Q}$.

В работе [19] нами был предложен новый метод доказательства конечности таких многочленов, основанный на комбинации последовательного вычисления результантов, применения базисов Грёбнера и нетривиальных вычислениях в системах компьютерной алгебры MAGMA [20] и Sage [21]. Применение более слабого условия конечности позволяет доказать, что существует не более конечного числа неизоморфных эллиптических полей $k(x)(\sqrt{f})$, $\deg f = 3$, содержащих точку четного порядка не превосходящего 18 или точку нечетного порядка $5, 7, 11$, таких, что элемент $\sqrt{f}$ периодичен. Более того, для поля k — квадратичного расширения $\mathbb{Q}$ — удаётся получить полную классификацию многочленов с указанными

свойствами. А для случая $k = \mathbb{Q}$ в качестве следствия было получено новое доказательство конечности числа периодических $\sqrt{f}$, не использующее параметризацию эллиптических кривых и точек конечного порядка на них. Теорема для случая квадратичного поля в качестве поля констант в сочетании с известными к настоящему моменту результатами, связанными с описанием кручения в эллиптических кривых над квадратичными полями, даёт основания предполагать, что количество нетривиальных неэквивалентных многочленов f с коэффициентами из квадратичных расширений $\mathbb{Q}$ с периодическим разложением $\sqrt{f}$ — конечно. В настоящей статье приводится полное доказательство анонсированных в [19] результатов.

Напомним некоторые факты, которые потребуется нам в дальнейшем. Для неприводимого над k многочлена h определим дискретное нормирование ν_h элемента поля $k(x)$ равенством $\nu_h\left(h^m \frac{p}{q}\right) = m$, где взаимно простые многочлены p, q не делятся на h. Бесконечное нормирование ν_∞, в свою очередь, определим равенством $\nu_\infty\left(\frac{p}{q}\right) = \deg q - \deg p$.

Далее считаем, что $\deg h = 1$, и без ограничения общности положим $h = x$. Пусть нормирование ν_x поля $k(x)$ имеет два продолжения ν_x^+ и ν_x^- на поле $L = k(x)(\sqrt{f})$. Если $\deg f = 2g+1$ для $g \in \mathbb{N}$, то бесконечное нормирование ν_∞ поля $k(x)$ имеет единственное продолжение на L, обозначим его также ν_∞, и положим $S = \{\nu_x^+, \nu_\infty\}$. Группа обратимых элементов кольца S-целых элементов поля L называется группой S-единиц. Если существует хотя бы одна нетривиальная S-единица (то есть отличная от константы поля k), то в описанном нами случае группа S-единиц является прямым произведением $k \setminus \{0\}$ и бесконечной циклической группы. Образующие этой циклической группы называются фундаментальными S-единицами. Степенью S-единицы $\lambda_1 + \lambda_2\sqrt{f} \in L$, где $\lambda_1, \lambda_2 \in k(x)$, называется показатель m в норменном выражении $\lambda_1^2 - \lambda_2^2 f = bh^m$, $b \in k \setminus \{0\}$, $m \in \mathbb{Z}$. Для эллиптического поля существование фундаментальной S-единицы степени m равносильно существованию k-точки порядка m соответствующей эллиптической кривой. Вложив поле L в поле формальных степенных рядов $k((x))$ можно разложить элемент поля L в функциональную непрерывную дробь. Необходимым условием для того, чтобы в поле L существовали элементы, разлагающиеся в периодическую непрерывную дробь в $k((x))$ (периодические элементы), является наличие нетривиальной S-единицы в поле L. Более подробные сведения о нормированиях, функциональных непрерывных дробях и S-единицах содержатся в работах [14, 18].

2. Формулировка основных результатов

Поскольку периодичность разложения в непрерывную дробь $\sqrt{f(x)}$ равносильна периодичности $\sqrt{a^2 f(bx)}$ для произвольных $a,\ b \in k \setminus \{0\}$, мы будем рассматривать многочлены с точностью до указанной эквивалентности. Сформулируем основные результаты.

Теорема 1. *Пусть k — произвольное поле нулевой характеристики. Тогда существует универсальная константа C, не зависящая от поля k, такая, что существует не более C попарно неэквивалентных над k многочленов f, $\deg f = 3$, для которых выполнены следующие условия:*

1. *$\sqrt{f}$ — периодичен в $k((x))$;*
2. *поле $L = k(x)(\sqrt{f})$ содержит фундаментальную S-единицу четной степени не превосходящей 18 или нечётной степени $5, 7, 9$ или 11 для $S = \{\nu_\infty, \nu_x^+\}$.*

Нетривиальным многочленом f будем называть многочлен неэквивалентный многочлену $cx^3 + 1$, где $c \in k \setminus \{0\}$.

Теорема 2. *Если в условиях теоремы 1 поле k — расширение $\mathbb{Q}$ степени не более 2 и $k \neq \mathbb{Q}(\sqrt{21})$, то многочлен f может быть равен только одному из следующих представителей:*

$$f = \frac{3}{16}x^3 - \frac{1}{2}x^2 + x + 1,$$
$$f = \frac{12}{8}x^3 - \frac{5}{4}x^2 + x + 1,$$
$$f = -\frac{120}{8}x^3 + \frac{25}{4}x^2 + x + 1.$$

В случае когда $k = \mathbb{Q}(\sqrt{21})$, множество таких многочленов f исчерпывается тремя указанными выше и дополнительно многочленом

$$f = \frac{3}{32}\left(9\sqrt{21} - 41\right)x^3 - \frac{1}{4}\left(3\sqrt{21} - 13\right)x^2 + x + 1.$$

Других нетривиальных многочленов с указанными свойствами с точности до вышеуказанного отношения эквивалентности многочленов f и инволюции поля $\mathbb{Q}(\sqrt{21})$ меняющей знак у $\sqrt{21}$, не существует.

Отметим, что нетривиальный пример кубического многочлена $f \in \mathbb{Q}(\sqrt{21})[x] \setminus \mathbb{Q}[x]$ с периодическим разложением $\sqrt{f} \in \mathbb{Q}(\sqrt{21})((x))$ был впервые получен в [13].

В качестве следствия из теоремы 2 мы получаем альтернативное доказательство конечности числа различных нетривиальных эллиптических полей L с периодичным $\sqrt{f}$ для случая поля констант $k = \mathbb{Q}$, доказанного в [9, 10] с использованием параметризации эллиптических кривых и точек конечного порядка на них.

Следствие 1. *Множество нетривиальных неэквивалентных свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 3$, имеющих периодическое разложение $\sqrt{f}$ в непрерывную дробь, исчерпывается тремя нетривиальными многочленами:*

$$f = \frac{3}{16}x^3 - \frac{1}{2}x^2 + x + 1,$$
$$f = \frac{12}{8}x^3 - \frac{5}{4}x^2 + x + 1,$$
$$f = -\frac{120}{8}x^3 + \frac{25}{4}x^2 + x + 1,$$

и серией многочленов $cx^3 + 1$, где $c \in \mathbb{Q} \setminus \{0\}$.

Доказательство. В [18] показано, что если эллиптическое поле над полем констант k содержит периодические элементы, то оно содержит фундаментальную S-единицу, а также было показано, что степень фундаментальной S-единицы равна порядку некоторой k-точки кручения. Таким образом, из результата Б. Мазура [22] следует, что степень фундаментальной S-единицы в произвольном эллиптическом поле с полем рациональных чисел в качестве поля констант не превосходит 12, и не может быть равна 11. Откуда многочлен $f \in \mathbb{Q}[x]$ степени 3 такой, что элемент $\sqrt{f}$ разлагается в периодическую непрерывную дробь, всегда удовлетворяет условиям теоремы 2, за исключением случая, когда поле $L = \mathbb{Q}(x)(\sqrt{f})$ содержит фундаментальную S-единицу степени 3. Поэтому искомое множество нетривиальных многочленов, для которых степень соответствуюей фундаментальной S-единицы не равна 3, есть множество из трех многочленов, указанное в теореме 2. В случае же когда степень S-единицы равна трем, множество искомых многочленов исчерпывается тривиальной серией $cx^3 + 1$ (см. например [18, 10]). Следствие доказано. □

3. Периодический корень

В работах [6], [18] был доказан критерий периодичности элемента вида $\frac{\sqrt{f}}{x^s}$, а также доказаны факты, полезные в настоящей статье. Приведём здесь критерий в необходимой нам общности.

Теорема 3. *Пусть* $\deg f = 2g+1$. *Элемент* $\sqrt{f}$ *периодичен тогда и только тогда, когда существует решение* $Y, Z \in k[x^{-1}]$, $Y \neq 0$, *уравнения* $Y^2 - Z^2\frac{f}{x^{2g+2}} = b$, *для которого* $Z = Z'x^{-g}, Z' \in k[x^{-1}]$. *Более того, если это условие выполнено для некоторого решения, то оно выполнено для всех таких решений.*

Из теоремы следует, что достаточно рассматривать только фундаментальное решение указанного уравнения, т.е. решение с максимальным значением $\nu_x(Y) < 0$. Такое решение соответствует фундаментальной S-единице чётной степени или квадрату фундаментальной S-единицы нечётной степени поля $k(x)(\sqrt{f})$ (см. [18]). Переформулируем утверждение теоремы 3 на языке многочленов из $k[x]$ (см. также [10]).

Теорема 4. *Пусть многочлен* f *свободен от квадратов, а* $\deg f = 2g+1$. *Элемент* $\sqrt{f}$ *квазипериодичен тогда и только тогда, когда некоторого* $m \in \mathbb{N}$, *существует решение* $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $b \in k \setminus \{0\}$, $f = d_1 d_2$, *уравнения*

$$\mu_1^2 d_1 - \mu_2^2 d_2 = bx^m, \tag{1}$$

и решение для наименьшего такого m *удовлетворяет условиям*

1. $\deg \mu_2 = \frac{m - \deg d_2}{2}$,
2. $\deg \mu_1 \leqslant \frac{m + \deg d_2}{2} - (2g+1)$.

Доказательство. По теореме 3 элемент $\sqrt{f}$ периодичен тогда и только тогда, когда пара Y, Z, где $Z = Z'x^{-g}$ и $Y, Z' \in k[x^{-1}]$, является фундаментальным решением уравнения $Y^2 - Z^2\frac{f}{x^{2g+2}} = b'$. Пусть $v_x(Y) = -m$, тогда

$$\lambda_1^2 - \lambda_2^2 f = b'x^{2m}, \tag{2}$$

где $\lambda_1 = x^m Y$, $\lambda_2 = x^{m-(2g+1)}Z'$. В силу нечётности степени f получаем $\deg \lambda_1 = m$, $\deg \lambda_2 \leqslant m - (2g+1)$, а $b' = b^2$ для некоторого $b \in k \setminus \{0\}$. Кроме того ясно, что λ_1, λ_2 взаимно просты как многочлены.

Воспользуемся формулой разности квадратов:

$$(\lambda_1 - bx^m)(\lambda_1 + bx^m) = \lambda_2^2 f.$$

Обе скобки в левой части взаимно просты, иначе $x \mid \lambda_1$, откуда $x \mid \lambda_2$, что противоречит взаимной простоте λ_1, λ_2.

В этом случае, получаем

$$\begin{aligned} \lambda_1 - bx^m &= \mu_1^2 d_1, \\ \lambda_1 + bx^m &= \mu_2^2 d_2, \\ \mu_1\mu_2 &= \lambda_2. \end{aligned} \tag{3}$$

Откуда $2\lambda_1 = \mu_1^2 d_1 + \mu_2^2 d_2$, и

$$2bx^m = \mu_2^2 d_2 - \mu_1^2 d_1.$$

В силу того, что f свободен от квадратов, мы можем утверждать, что с точностью до умножения на константу такое разложение на d_1, d_2 и μ_1, μ_2 единственное.

Так как степени d_1 и d_2 имеют разную чётность, выполнено или $\deg(\mu_1^2 d_1) = m$ или $\deg(\mu_2^2 d_2) = m$. Без ограничения общности будем считать, что $\deg(\mu_2^2 d_2) = m$ (в противном случае, заменим b на $-b$, и поменяем местами индексы в обозначениях 1 и 2). Откуда в силу (3) и неравенства $\deg \lambda_2 \leqslant m - (2g+1)$ получаем $\deg \mu_1 \leqslant \frac{m+\deg d_2}{2} - (2g+1)$.

Обратно, если находится такое решение, то по формулам выше легко получить решение, удовлетворяющее условию критерия периодичности $\sqrt{f}$. $\square$

Замечание 1. *Если в результате процедуры из доказательства теоремы 3 мы получим* $\deg d_1 = 0$, *то* m *обязано быть нечётным числом, в противном случае мы получим решение уравнения* (2) *с показателем* $m < 2m$ *чего не может быть в силу условия минимальности.*

3.1. Результант

Рассмотрим многочлены $f = \sum_i a_i x^{n-i}, g = \sum_i b_i x^{m-i}$, где $a_0, b_0 \neq 0$. Пусть x_i — корни многочлена f, а y_i — корни многочлена g. Напомним, что величина

$$R(f,g) = a_0^m b_0^n \prod (x_i - y_j)$$

называется результантом пары f, g. Следующая лемма хорошо известна, мы приводим ее без дополнительных пояснений.

Лемма 1. 1. *Результант многочленов* f *и* g *равен определителю матрицы Сильвестра.*

2. $R(f,g)$ *является однородным многочленом степени* m *по переменным* a_i *и степени* n *по переменным* b_j *с коэффициентами из* $\mathbb{Z}$.

3. $R(f,g) = 0$ *только в том случае, когда* f *и* g *имеют общий корень в алгебраическом замыкании.*

Результант, как общеизвестно, позволяет также сводить решение системы алгебраических уравнений к нахождению корней многочленов. В более общей форме, он позволяет исключать переменные из системы алгебраических уравнений. В самом деле, пусть полиномиальная система

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0;$$

где $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ имеет решение при каком-то x_n. Тогда представляя каждый f_i как полином от x_n над кольцом $\mathbb{Q}[x_1, \ldots, x_{n-1}]$ вычисляя $n-1$ результант пар f_1, f_i мы получаем новую полиномиальную систему с $n-1$ уравнением и $n-1$ переменной вида

$$g_i(x_1, \ldots, x_{n-1}) = 0, g_i(x_1, \ldots, x_{n-1}) \in \mathbb{Q}[x_1, \ldots, x_{n-1}].$$

В наших вычислениях и алгоритмах мы несколько модифицируем эту схему. А именно, на каждом шаге предварительно вычисляются попарные наибольшие общие делители многочленов f_i: $\gcd(f_i, f_j)$. Если множество корней первоначальной системы не обнуляет многочлен $\gcd(f_i, f_j)$, то процедура сокращения на многочлен $\gcd(f_i, f_j)$ корректна. Последовательное применение вышеприведённой процедуры позволяет получить в рассматриваемых нами случаях либо константный многочлен, либо многочлен, зависящий только от одной переменной. С помощью переупорядочивания многочленов на каждом шаге, мы можем добиться того, чтобы на последнем шаге был многочлен от заданной переменной. Построение системы из n таких многочленов, полученных для каждой из переменных исходной системы, позволяет найти все корни исходной системы. Для краткости будем называть эту итеративную процедуру R-преобразованием системы или просто R-процедурой.

4. Нетривиальные решения

Пусть $t \in k[x]$, $s = \deg t$, $t = t_0 + t_1 x + t_2 x^2 + \cdots + t_s x^s \in k[x]$. Обозначим через $lc(t) = t_s$, через $plc(t) = t_{s-1}$, а через $fc(t) = t_0$ коэффициент при нулевой степени x.

Определение 1. *Пусть заданы $g, m \in \mathbb{N}$. Будем называть набор $(\mu_1, \mu_2, d_1, d_2, b)$, где $b \in k\backslash\{0\}$, $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $d_1 \neq 0$, $d_2 \neq 0$, $fc(\mu_1) \neq 0$, $\deg d_1 + \deg d_2 = 2g+1$, а произведение $f = d_1 d_2$ свободно от квадратов,* ***решением обобщённого норменного уравнения*** *над k, если выполнено соотношение (1).*

Мы будем писать ***нетривиальное решение норменного уравнения****, если $d_1 = 1$, в этом случае мы будем писать (μ_1, μ_2, f, b) вместо $(\mu_1, \mu_2, 1, d_2, b)$. Мы будем писать просто* ***нетривиальное решение****, если из контекста ясно, что речь идёт о нетривиальном решении норменного или обобщённого норменного уравнения.*

Пусть задано нетривиальное решение обобщённого норменного уравнения. Определим коэффициенты a_i, b_j, h_k, f_k из следующих равенств:

$$\mu_1 = \sum_i a_i x^i; \quad \mu_2 = \sum_i b_i x^i; \quad d_1 = \sum_i h_i x^i; \quad d_2 = \sum_i f_i x^i.$$

Определение 2. *Назовем системой обобщенного норменного уравнения систему уравнений относительно неизвестных a_i, b_j, h_k, f_k к которой сводится обобщенное норменное уравнение (1).*

Замечание 2. *Если $(\mu_1, \mu_2, d_1, d_2, b)$ — нетривиальное решение норменного уравнения. Тогда $f_0 h_0 = a^2$ и $\frac{f_0}{h_0} = a'^2$, для некоторых $a, a' \in k \setminus \{0\}$, в частности, $f_0 = a^2$, если $d_1 = 1$.*

Определение 3. *Будем называть* ***допустимыми преобразованиями*** *нетривиального решения обобщённого норменного уравнения над полем k, если оно переводит набор $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ в один из следующих наборов:*

- $\Gamma_{1,\gamma}(\Omega) = (\mu_1(\gamma x), \mu_2(\gamma x), d_1(\gamma x), d_2(\gamma x), \gamma^m b)$.
- $\Gamma_{2,\gamma}(\Omega) = (\gamma\mu_1, \gamma\mu_2, d_1, d_2, \gamma^2 b)$,
- $\Gamma_{3,\gamma}(\Omega) = (\gamma\mu_1, \mu_2, d_1, \gamma^2 d_2, \gamma^2 b)$,
- $\Gamma_{4,\gamma}(\Omega) = (\mu_1, \mu_2, \gamma d_1, \gamma d_2, \gamma b)$,

для некоторого $\gamma \in k \setminus \{0\}$, или преобразования, полученные путём последовательного применения вышеперечисленных преобразований.

В дальнейшем нам потребуются ещё несколько допустимых преобразований:

- $\Gamma_{5,\gamma}(\Omega) = \Gamma_{2,\frac{1}{\gamma}} \circ \Gamma_{3,\gamma}(\Omega) = (\mu_1, \gamma\mu_2, d_1, \frac{1}{\gamma^2} d_2, b)$,
- $\Gamma_{6,\gamma}(\Omega) = \Gamma_{4,\frac{1}{\gamma^2}} \circ \Gamma_{3,\gamma}(\Omega) = (\gamma\mu_1, \mu_2, \frac{1}{\gamma^2} d_1, d_2, b)$,
- $\Gamma_{7,\gamma}(\Omega) = \Gamma_{4,\gamma^2} \circ \Gamma_{5,\gamma}(\Omega) = (\mu_1, \gamma\mu_2, \gamma^2 d_1, d_2, \gamma^2 b)$,
- $\Gamma_{8,\gamma}(\Omega) = \Gamma_{4,\gamma} \circ \Gamma_{5,\gamma}(\Omega) = (\mu_1, \gamma\mu_2, \gamma d_1, \frac{1}{\gamma} d_2, \gamma b)$,

Нетрудно видеть, что допустимые преобразования, применённые к нетривиальному решению для g, m, снова дают нетривиальное решение для g, m и тем самым, в силу обратимости они задают отношение эквивалентности на нетривиальных решениях, что с учётом соотношения $f = d_1 d_2$ некоторым образом обобщает отношение эквивалентности из §2 и работы [12]. Заметим, что допустимые преобразования меняют коэффициенты многочленов μ_1, μ_2, d_1, d_2 и константу b.

Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение обобщённого норменного уравнения над k, тогда для этого нетривиального решения выполнено $\deg d_2 > 0$. Действительно, из доказательства теоремы 4 следует, что выполнено одно из двух: или m — нечётное число, или $\deg d_1 > 0$ и $\deg d_2 > 0$. Если m — нечётное число, то $\deg d_2$ обязано быть нечётным числом, и, следовательно, $\deg d_2 > 0$.

Лемма 2. *Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение обобщённого норменного уравнения над k, тогда для данного m*

- *существует нетривиальное решение над k с $h_0 = f_0 = 1 = lc(\mu_1)$ и $f_1 = 0$ или $f_1 = 1$.*
- *существует нетривиальное решение над k с $h_0 = f_0 = 1 = lc(\mu_2)$ и $f_1 = 0$ или $f_1 = 1$.*

Доказательство. Пусть $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ — нетривиальное решение. У решения $\Omega_1 = \Gamma_{8,f_0}(\Omega)$ коэффициент $f_0(\Omega_1) = 1$.

Поскольку младший коэффициент нового $d_1(\Omega_1)$ — полный квадрат в k, для

$$\Omega_2 = \Gamma_{7,\frac{1}{\gamma_2}}(\Omega_1) = \left(\mu_1, \frac{\gamma_1}{\gamma_2}\mu_2, \frac{\gamma_1}{\gamma_2^2}d_1, \frac{1}{\gamma_1}d_2, \frac{\gamma_1}{\gamma_2^2}b\right)$$

выполнено $h_0(\Omega_2) = f_0(\Omega_2) = 1$, где $\gamma_2 = \sqrt{fc(d_1)\gamma_1} = \sqrt{fc(d_1)fc(d_2)}$.

Положим $\gamma_3 = 1$ если $f_1 = 0$ и $\frac{\gamma_2^2}{\gamma_1 f_1}$ иначе.

Тогда для

$$\Omega_3 = \Gamma_{1,\gamma_3}(\Omega_2) = \left(\mu_1(\gamma_3 x), \frac{\gamma_1}{\gamma_2}\mu_2(\gamma_3 x), \frac{\gamma_1}{\gamma_2^2}d_1(\gamma_3 x), \frac{1}{\gamma_1}d_2(\gamma_3 x), \frac{\gamma_1\gamma_3^m}{\gamma_2^2}b\right),$$

$f_1(\Omega_3) = 0$ или $f_1(\Omega_3) = 1$.

Наконец, положив $\gamma_4 = lc(\mu_1(\gamma_3 x)) = lc(\mu_1)\gamma_3^{\deg\mu_1}$, получаем, что

$$\begin{aligned}\Omega_4 = \Gamma_{2,\frac{1}{\gamma_4}}(\Omega_3) = \Gamma_{2,\frac{1}{\gamma_4}} \circ \Gamma_{1,\gamma_3} \circ \Gamma_{7,\frac{1}{\gamma_2}} \circ \Gamma_{8,\gamma_1}(\Omega) = \\ = \left(\frac{1}{\gamma_4}\mu_1(\gamma_3 x), \frac{\gamma_1}{\gamma_2\gamma_4}\mu_2(\gamma_3 x), \frac{\gamma_1}{\gamma_2^2}d_1(\gamma_3 x), \frac{1}{\gamma_1}d_2(\gamma_3 x), \frac{\gamma_1\gamma_3^m}{\gamma_2^2\gamma_4^2}b\right),\end{aligned}$$

удовлетворяет условию леммы. Второй случай рассматривается аналогично. Лемма доказана. □

Аналогично предыдущей лемме выводится следующее утверждение.

Лемма 3. *Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение Ω обобщённого норменного уравнения над k, тогда для данного m существует решение с набором из 4 коэффициентов, указанных ниже, равных 1 при условии, что в Ω указанные коэффициенты не обращаются в 0, причём указанное решение может быть получено из Ω помощью допустимых преобразований над $\bar{k}$. Возможны следующие наборы из 4 коэффициентов.*

1. a_i, a_t, b_j, h_k;

2. a_i, a_t, b_j, f_k;

3. b_i, b_t, a_j, h_k;

4. b_i, b_t, a_j, f_k;

5. f_i, f_t, b_j, a_k;

6. h_i, h_t, b_j, a_k;

Доказательство. Доказательство этой леммы проводится по аналогии с доказательством леммы 2 и рассуждениям из работы [12]. □

5. Доказательство основных результатов

Доказательство. По Теореме 4 для того, чтобы $\sqrt{f}$ был периодичен необходимо и достаточно найти решение уравнения (1) для наименьшего m, удовлетворяющего условиям теоремы 1 и теоремы 2. Из доказательства теоремы 4 нетрудно видеть, что если степень фундаментальной S-единицы — чётная, то она равна $2m$, а $\deg d_i > 0$ для $i = 1, 2$. При этом, если степень S-единицы нечётная, то без ограничения общности $\deg d_1 = 0$.

Таким образом, по теореме 4 необходимо и достаточно исследовать конечность числа решений уравнения (1). Что эквивалентно исследованию системы алгебраических уравнений на коэффициенты μ_1, μ_2, d_1, d_2, построенных по (1), для следующих значений $\deg d_1$ и m:

$$\deg d_1 = 0, m = 5, 7, 9, 11; \deg d_1 = 1, m = 4, 6, 8; \deg d_1 = 2, m = 5, 7, 9. \tag{4}$$

Отметим, что конечность числа решений для $m = 11, \deg d_1 = 0$ была получена в [12] с использованием базисов Грёбнера, а случаи $m \leqslant 3$, т.е. случай нечетной степени фундаментальной S-единицы $\leqslant 3$ или четной $\leqslant 6$, не могут давать нужных нам решений за исключением тривиального случая $m = 3, \deg d_1 = 0$, описанного, например, в [18].

Пусть $d_2 = f_0^2 + f_1 x + f_2 x^2 + f_3 x^3$, где f_2, f_3 быть может, принимают нулевые значения. Ясно, что $f_0 \neq 0$, поскольку многочлен f должен иметь ненулевое свободное слагаемое. Далее отмечаем, что $h_0 \neq 0$, так как в противном случае согласно соотношению (1) мы легко приходим к тому, что степень соответствующей S-единицы строго меньше $2m$.

Аналогичным образом мы показываем, что в уравнении (2) для каждого из случаев $\deg \lambda_2 = m - (2g + 1)$ или что тоже самое $lc(\lambda_2) \neq 0$. Предположим обратное, $lc(\lambda_2) = 0$. Тогда согласно Лемме 2 пункту 1, существует решение системы норменного уравнения с $h_0 = f_0 = lc(\mu_1) = f_1 = 1$ или же $h_0 = f_0 = lc(\mu_1) = 1$ и $f_1 = 0$ над полем $\bar{k}$. Однако, базис Гребнера этих систем сводится к ненулевой константе, что эквивалентно отсутствию решений. Итак, это означает, что $lc(\mu_2) \neq 0$.

Можно показать, что не существует решений системы в случае, когда $f_1 = 0$, что позволяет нам положить $f_1 \neq 0$. Действительно, в противном случае, согласно Лемме 3 существует решение над полем $\bar{k}$ с $f_1 = 0$ системы норменого уравнения с инициализированной четверкой из пункта 3) леммы при

$$b_0 = lc(\mu_2) = a_0 = h_0 = 1. \tag{5}$$

Однако же базис Грёбнера этой системы почти для каждой пары $(\deg d_1, m)$ из перечня (4) при условии (5) состоит из единицы, что равносильно отсутствию решений. Поэтому, в каждом из этих случаев $f_1 \neq 0$. Случаи, где указанное рассуждение избыточно, или базис Грёбнера отличен от единицы, отмечены и разобраны отдельно.

Для каждой из исследуемых систем обобщённого норменного уравнения соответствующих парам из перечня (4) применим R-процедуру, описанную в параграфе §3.1 так, чтобы процедура последовательного исключения переменных для каждой из систем приводила к многочлену не более чем одной переменной в качестве результанта последней пары многочленов. С помощью вычислений в системах компьютерной алгебры SageMath и Magma можно показать, что для каждой из систем всякой переменной этой системы можно сопоставить многочлен от этой переменный, полученный применением вышеуказанной R-процедуры. Это позволяет сделать вывод о конечности числа решений изначальной системы, а, как следствие, о конечности различных неэквивалентных многочленов f с периодическим разложением $\sqrt{f}$ для полей, содержащих фундаментальную S-единицу соответствующей степени.

Поле L содержит фундаментальную S-единицу степени 5

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 1, 1, 5)$. Согласно схеме предложенной выше мы делаем вывод, что $h_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Отсюда и из вида обобщенного норменного уравнения следует что и $a_0 \neq 0$. Далее, из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_1 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует, откуда без ограничения общности полагаем $f_1 \neq 0$.

Поэтому подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_1 = 1$ получаем систему из 4 уравнений с 4 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -2a_0a_1 + b_0^2 + 2b_0 = 0 \\ b_0^2 f_2 - a_1^2 + 2b_0 + 1 = 0 \\ b_0^2 f_3 + 2b_0 f_2 + 1 = 0 \\ 2b_0 f_3 + f_2 = 0 \end{cases} \tag{6}$$

После исключения a_0 из первого уравнения, заменяя a_1 на $-1/2b_0 - 1$, а также избавляясь от b_0 из второго уравнения получим систему из трех уравнений с 3 неизвестными.

$$\begin{cases} b_0 f_2 - 1/4b_0 + 1 = 0 \\ b_0^2 f_3 + 2b_0 f_2 + 1 = 0 \\ 2b_0 f_3 + f_2 = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (11) существует единственное интересующее нас решение, а именно: $f_3 = 3/16$, $f_2 = -1/2$, $f_0 = 1$, $a_0 = -4/3$, $f_1 = 1$, $d_0 = 4/3$, $d_1 = 1$, $a_1 = -5/3$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S-единицу степени 7

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 2, 2, 7)$.

Пусть как и раньше

$$d_1 = 1, d_2 = f_3x^3 + f_2x^2 + f_1x + f_0^2,$$
$$\mu_1 = a_2x^2 + a_1x + a_0, \mu_2 = b_2x^2 + b_1x + b_0.$$

Откуда исходная система обобщенного норменного уравнения выглядит следующим образом

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2b_0b_1f_0^2 + b_0^2f_1 - 2a_0a_1 = 0 \\ b_1^2f_0^2 + 2b_0b_2f_0^2 + 2b_0b_1f_1 + b_0^2f_2 - a_1^2 - 2a_0a_2 = 0 \\ 2b_1b_2f_0^2 + b_1^2f_1 + 2b_0b_2f_1 + 2b_0b_1f_2 + b_0^2f_3 - 2a_1a_2 = 0 \\ b_2^2f_0^2 + 2b_1b_2f_1 + b_1^2f_2 + 2b_0b_2f_2 + 2b_0b_1f_3 - a_2^2 = 0 \\ b_2^2f_1 + 2b_1b_2f_2 + b_1^2f_3 + 2b_0b_2f_3 = 0 \\ b_2^2f_2 + 2b_1b_2f_3 = 0. \end{cases}$$

Отдельно обосновываем, что не существует решений с $f_1 = 0$.

Действительно, в противном случае, согласно Лемме 3 существует решение над полем $\bar{k}$ с $f_1 = 0$ системы норменого уравнения с инициализированной четверкой из пункта 3) леммы при

$$b_0 = lc(\mu_2) = a_0 = h_0 = 1. \tag{7}$$

Однако же базис Грёбнера этой системы состоит из единицы, что равносильно отсутствию решений. Поэтому $f_1 \neq 0$. Далее применим Лемму 2 пункт , и положим $f_0 = f_1 = b_2 = 1$. Далее, мы можем выразить переменные a_0, a_1 через остальные. Подставив в систему их выражения $a_0 = -b_0$, $a_1 = -1/2d_0 - d_1$, $a_2 = -1/2b_0f_2 + 1/8b_0 - 1/2b_1 - 1$, получаем систему из 4 уравнений и 4 неизвестных:

$$\begin{cases} -1/2b_0f_2 + b_1f_2 + b_0f_3 + 1/8b_0 - 1/4b_1 + 1 = 0 \\ -1/4b_0^2f_2^2 + 1/8b_0^2f2 - 1/2b_0b_1f2 + b_1^2f_2 + \\ +2b_0b_1f_3 - 1/64b_0^2 + 1/8b_0b_1 - 1/4b_1^2 + b_0f_2 + 1/4b_0 + b_1 = 0 \\ b_1^2f_3 + 2b_1f_2 + 2b_0f_3 + 1 = 0 \\ 2b_1f_3 + f_2 = 0. \end{cases}$$

Из последнего уравнения видно, что переменную f_2 можно исключить из системы. Ее значение определяется однозначно из набора остальных переменных. Вычисляя последовательные результанты по R-процедуре из §3.1 для каждой из переменных b_0, b_1, f_3 мы получаем такое следствие:

$$\begin{cases} (3b_0 - 64)b_0^9(225b_0^2 - 816b_0 + 256)^2 = 0 \\ (3b_1 + 4)^2(3b_1 - 4)^3b_1^5(45b_1^2 - 204b_1 + 80) = 0 \\ (8f_3 - 3)^2(16f_3 - 3)^3f_3^6(256f_3^2 + 1968f_3 - 45) = 0 \end{cases} \tag{8}$$

При вычислениях результанта по процедуре из параграфа 3.1, приводящих к многочленам от переменной f_2 и f_3, мы получаем в процессе R-процедуры один нетривиальный общий множитель равный f_3^2. Сокращение на него в обоих случаях корректно, так как в силу $\deg d_2 = 3$ мы заключаем, что $f_3 \neq 0$.

При вычислении результанта, приводящему к многочлену от переменной b_0, мы получаем в процессе два нетривиальных общих множителя равные f_3^2, $4b_0f_2^3 - b_0f_2^2$. Сокращение второй множитель корректно, так как базис Гребнера исходной системы дополненной этим уравнением дает помимо прочего многочлен b_0. Он не может быть равен нулю в нашем случае для нашей задачи.

При вычислении результанта, приводящему к многочленам от переменной b_1 мы не получаем в процессе нетривиальных общих множителей отличных от константы, в этом случае сокращений не возникает.

Нетрудно видеть, что система (8) имеет не более одного с точностью до инволюции поля констант интересующего нас решения над каким-либо полем k, являющимся квадратичным расширением $\mathbb{Q}$. Причём единственное решение с $b_0 \neq 0$ точностью до инволюции поля $\mathbb{Q}(\sqrt{21})$, меняющей знак у $\sqrt{21}$, она имеет тогда и только тогда, когда $\mathbb{Q}(\sqrt{21}) \subset k$, а именно

$$f_3 = \frac{27\sqrt{21}-123}{32},\ f_2 = \frac{-3\sqrt{21}+13}{4},\ b_1 = \frac{6\sqrt{21}+34}{15},\ b_0 = \frac{24\sqrt{21}+136}{75}.$$

Указанное решение позволяет построить многочлен $f \in \mathbb{Q}(\sqrt{21})[x]$ с периодическим разложением $\sqrt{f} \in \mathbb{Q}(\sqrt{21})((x))$:

$$f = \frac{27\sqrt{21}-123}{32}x^3 - \frac{3\sqrt{21}-13}{4}x^2 + x + 1.$$

В заключение отметим, что в силу (8) каждая из исследуемых переменных b_0, b_1, f_2, f_3 может принимать не более чем конечное число значений для любого поля k. Для каждой переменной это число не превосходит степени соответствующего многочлена в системе (8).

Поле L содержит фундаментальную S-единицу степени 9

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0,3,3,3,9)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 10 уравнений и 13 неизвестных.

$$\begin{cases}
b_0^2 f_0^2 - a_0^2 = 0 \\
2\,b_0 b_1 f_0^2 + b_0^2 f_1 - 2\,a_0 a_1 = 0 \\
b_1^2 f_0^2 + 2\,b_0 b_2 f_0^2 + 2\,b_0 b_1 f_1 + b_0^2 f_2 - a_1^2 - 2\,a_0 a_2 = 0 \\
2\,b_1 b_2 f_0^2 + 2\,b_0 b_3 f_0^2 + b_1^2 f_1 + 2\,b_0 b_2 f_1 + 2\,b_0 b_1 f_2 + b_0^2 f_3 - 2\,a_1 a_2 - 2\,a_0 a_3 = 0 \\
b_2^2 f_0^2 + 2\,b_1 b_3 f_0^2 + 2\,b_1 b_2 f_1 + 2\,b_0 b_3 f_1 + b_1^2 f_2 + 2\,b_0 b_2 f_2 + 2\,b_0 b_1 f_3 - a_2^2 - 2\,a_1 a_3 = 0 \\
2\,b_2 b_3 f_0^2 + b_2^2 f_1 + 2\,b_1 b_3 f_1 + 2\,b_1 b_2 f_2 + 2\,b_0 b_3 f_2 + b_1^2 f_3 + 2\,b_0 b_2 f_3 - 2\,a_2 a_3 = 0 \\
b_3^2 f_0^2 + 2\,b_2 b_3 f_1 + b_2^2 f_2 + 2\,b_1 b_3 f_2 + 2\,b_1 b_2 f_3 + 2\,b_0 b_3 f_3 - a_3^2 = 0 \\
b_3^2 f_1 + 2\,b_2 b_3 f_2 + b_2^2 f_3 + 2\,b_1 b_3 f_3 = 0 \\
b_3^2 f_2 + 2\,b_2 b_3 f_3 = 0 \\
b_3^2 f_3 + c = 0
\end{cases}$$

Воспользуемся Леммой 3, подставим в систему норменного уравнения $b_3 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 9 уравнений и 9 неизвестных:

$$\begin{cases}
-a_0^2 + b_0^2 = 0 \\
-2\,a_0 a_1 + b_0^2 + 2\,b_0 b_1 = 0 \\
b_0^2 f_2 - a_1^2 - 2\,a_0 a_2 + 2\,b_0 b_1 + b_1^2 + 2\,b_0 b_2 = 0 \\
2\,b_0 b_1 f_2 + b_0^2 f_3 - 2\,a_1 a_2 - 2\,a_0 a_3 + b_1^2 + 2\,b_0 b_2 + 2\,b_1 b_2 + 2\,b_0 = 0 \\
b_1^2 f_2 + 2\,b_0 b_2 f_2 + 2\,b_0 b_1 f_3 - a_2^2 - 2\,a_1 a_3 + 2\,b_1 b_2 + b_2^2 + 2\,b_0 + 2\,b_1 = 0 \\
2\,b_1 b_2 f_2 + b_1^2 f_3 + 2\,b_0 b_2 f_3 - 2\,a_2 a_3 + b_2^2 + 2\,b_0 f_2 + 2\,b_1 + 2\,b_2 = 0 \\
b_2^2 f_2 + 2\,b_1 b_2 f_3 - a_3^2 + 2\,b_1 f_2 + 2\,b_0 f_3 + 2\,b_2 + 1 = 0 \\
b_2^2 f_3 + 2\,b_2 f_2 + 2\,b_1 f_3 + 1 = 0 \\
2\,b_2 f_3 + f_2 = 0
\end{cases}$$

Отметим, что в случае $f_1 = 0$ базис Грёбнера дает нулевую размерность данной системы. Решение построенное по этому базису дает многочлен $2x^3+1$, принадлежащий тривиальной серии, в нашем случае он интереса не представляет, поскольку соответствует степени S-единицы равной трем.

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражения: $a_0 = -b_0$, $a_1 = -\frac{1}{2}\,b_0 - b_1$, $a_2 = -\frac{1}{2}\,b_0 f_2 + \frac{1}{8}\,b_0 - \frac{1}{2}\,b_1 - b_2$, $a_3 = \frac{1}{4}\,(b_0 - 2\,b_1) f_2 - \frac{1}{2}\,b_0 f_3 - \frac{1}{16}\,b_0 + \frac{1}{8}\,b_1 - \frac{1}{2}\,b_2 - 1$, В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении

$$-\frac{1}{64}\left(16\,b_0 f_2^2 - 24\,b_0 f_2 + 32\,b_1 f_2 - 64\,b_2 f_2 + 32\,b_0 f_3 - 64\,b_1 f_3 + 5\,b_0 - 8\,b_1 + 16\,b_2 - 64\right) b_0 = 0.$$

После преобразования получается система из 5 уравнений от переменных b_2, f_3, b_1, f_2, b_0:

$$\begin{cases} -\frac{1}{4}\,b_0 f_2^2 + \frac{3}{8}\,b_0 f_2 - \frac{1}{2}\,b_1 f_2 + b_2 f_2 - \frac{1}{2}\,b_0 f_3 + b_1 f_3 - \frac{5}{64}\,b_0 + \frac{1}{8}\,b_1 - \frac{1}{4}\,b_2 + 1 = 0 \\ \frac{1}{4}\,b_0^2 f_2^2 - \frac{1}{2}\,b_0 b_1 f_2^2 - \frac{1}{2}\,b_0^2 f_2 f_3 - \frac{1}{8}\,b_0^2 f_2 + \frac{1}{2}\,b_0 b_1 f_2 - \frac{1}{2}\,b_1^2 f_2 + b_1 b_2 f_2 + \frac{1}{8}\,b_0^2 f_3 - \frac{1}{2}\,b_0 b_1 f_3 + \\ + b_1^2 f_3 + b_0 b_2 f_3 + \frac{1}{64}\,b_0^2 - \frac{3}{32}\,b_0 b_1 + \frac{1}{8}\,b_1^2 - \frac{1}{4}\,b_1 b_2 + b_0 f_2 + \frac{1}{4}\,b_0 + b_1 = 0 \\ -\frac{1}{16}\,b_0^2 f_2^2 + \frac{1}{4}\,b_0 b_1 f_2^2 - \frac{1}{4}\,b_1^2 f_2^2 + \frac{1}{4}\,b_0^2 f_2 f_3 - \frac{1}{2}\,b_0 b_1 f_2 f_3 - \frac{1}{4}\,b_0^2 f_3^2 + \frac{1}{32}\,b_0^2 f_2 - \\ -\frac{1}{8}\,b_0 b_1 f_2 + \frac{1}{8}\,b_1^2 f_2 + \frac{1}{4}\,b_0 b_2 f_2 - \frac{1}{2}\,b_1 b_2 f_2 + b_2^2 f_2 - \frac{1}{16}\,b_0^2 f_3 + \frac{1}{8}\,b_0 b_1 f_3 - \frac{1}{2}\,b_0 b_2 f_3 + 2\,b_1 b_2 f_3 - \\ -\frac{1}{256}\,b_0^2 + \frac{1}{64}\,b_0 b_1 - \frac{1}{64}\,b_1^2 - \frac{1}{16}\,b_0 b_2 + \frac{1}{8}\,b_1 b_2 - \frac{1}{4}\,b_2^2 + \frac{1}{2}\,b_0 f_2 + b_1 f_2 + b_0 f_3 - \frac{1}{8}\,b_0 + \frac{1}{4}\,b_1 + b_2 = 0 \\ b_2^2 f_3 + 2\,b_2 f_2 + 2\,b_1 f_3 + 1 = 0 \\ 2\,b_2 f_3 + f_2 = 0 \end{cases}$$

При вычисленнии R-процедуры для переменной b_2 было проведено сокращение на общий множитель $b_0^2 \cdot b_2^7 \cdot (-48 b_2^2 - 112 b_2 + b_0 - 64)^2$.

При вычисленнии R-процедуры для переменной f_3 было проведено сокращение на следующие общие множители: f_3^2, $f_3^6 \cdot (4 f_3^2 b_0 + 8 f_3 - 3)^2$.

При вычисленнии R-процедуры для переменной b_1 было проведено сокращение на следующие общие множители: $f_2 \cdot (4 f_2 - 1)$, f_2, b_0^6.

При вычисленнии R-процедуры для переменной f_2 было проведено сокращение на следующие общие множители: $f_2 \cdot (4 f_2 - 1)$, f_2, $b_0^3 \cdot (4 f_2 - 1)^4$.

При вычисленнии R-процедуры для переменной b_0 было проведено сокращение на следующие общие множители: $f_2 \cdot (4 f_2 - 1)$, f_2, $b_0^3 \cdot (4 f_2 - 1)^4$. В каждом из этих случаев, базис Гребнера системы дополненный каждым из этих общих множителей, сводится к ненулевой константе. Тем самым мы обосновываем корректность сокращения на общий множитель и поэтому вышеуказанные сокращения корректны. Вычисляя последовательные результанты по R-процедуре из §3.1 для каждой из переменных b_2, f_3, b_1, f_2, b_0, мы получаем в качестве следствия систему из 5 уравнений и 5 неизвестных. В силу большой рациональной высоты коэффициентов, мы приводим данные многочлены в сокращенном виде, указывая лишь переменную и степень неприводимых сомножителей. Как и ранее мы обозначаем через $P_{x,k}$ некоторый неприводимый над $\mathbb{Q}$ многочлен от переменной x степени k.

$$\begin{cases} (3b_2 - 4) b_2 (45 b_2^2 - 204 b_2 + 80) P_{b_2,3} P_{b_2,55} = 0 \\ (16 f_3 - 3) f_3 (256 f_3^2 + 1968 f_3 - 45) P_{f_3,3} P_{f_3,46} = 0 \\ (b_1 - 32)(3b_1 - 64) b_1 (225 b_1^2 - 816 b_1 + 256) P_{b_1,3} P_{b_1,8} P_{b_1,10} P_{b_1,11} P_{b_1,14} P_{b_1,15} * \\ * P_{b_1,66} P_{b_1,90} P_{b_1,92} P_{b_1,112} = 0 \\ (4 f_2 - 3) f_2 (2 f_2 + 1)(4 f_2 - 1)(4 f_2^2 - 26 f_2 - 5) * \\ * P_{f_2,3} P_{f_2,11} P_{f_2,14} P_{f_2,15} P_{f_2,37} P_{f_2,48} P_{f_2,54} P_{f_2,69} = 0 \\ (b_0 - 64) b_0 P_{b_0,3} P_{b_0,11} P_{b_0,14} P_{b_0,15} P_{b_0,37} P_{b_0,48} P_{b_0,54} P_{b_0,69} = 0 \end{cases} \tag{9}$$

Из полученной системы мы извлекаем отсутствие нетривиальных решений над произвольным полем k у которого степень расширения над $\mathbb{Q}$ не более 2. Этот случай мы тоже разобрали.

В заключение отметим, что в силу (9) каждая из исследуемых переменных f_2, d_0, f_3, d_2, d_1 может принимать не более чем конечное число значений для любого поля k,

Поле L содержит фундаментальную S-единицу степени 11

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (0, 3, 4, 4, 11)$. Как отмечалось выше этот случай был разобран в [12] с использованием базисов Грёбнера. При вычислении базиса Грёбнера соответствующей системы, нетрудно видеть, что для поля k, являющегося конечным расширением поля $\mathbb{Q}$ степени не более 2, интересующих нас решений не существует.

Поле L содержит фундаментальную S-единицу степени 8

В данном случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 0, 1, 4)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_1 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует.

Поэтому подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_1 = 1$ получаем систему из 4 уравнений с 4 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 + b_0^2 + 2b_0 == 0 \\ b_0^2 f_2 + 2b_0 + 1 = 0 \\ 2b_0 f_2 + 1 = 0 \end{cases} \tag{10}$$

После исключения a_0 из первого уравнения получим систему из трех уравнений с 3 неизвестными.

$$\begin{cases} -b_0 h_1 + b_0 + 2 = 0 \\ b_0^2 f_2 + 2b_0 + 1 = 0 \\ 2b_0 f_2 + 1 = 0 \end{cases}$$

После упрощения мы получаем такую систему.

$$\begin{cases} f_2(4f_2 - 3) = 0 \\ h_1 + 2 = 0 \\ b_0(3b_0 + 2) = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (10) существует единственное интересующее нас решение, а именно: $f_2 = 3/4$, $a_0 = 2/3$, $b_0 = -2/3$, $h_1 = -2$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S-единицу степени 10

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 0, 2, 5)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 6 уравнений и

9 неизвестных.

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2\,b_0 b_1 f_0^2 + b_0^2 f_1 - a_0^2 h_1 = 0 \\ b_1^2 f_0^2 + 2\,b_0 b_2 f_0^2 + 2\,b_0 b_1 f_1 - a_0^2 h_2 = 0 \\ 2\,b_1 b_2 f_0^2 + b_1^2 f_1 + 2\,b_0 b_2 f_1 = 0 \\ b_2^2 f_0^2 + 2\,b_1 b_2 f_1 = 0 \\ b_2^2 f_1 + c = 0 \end{cases} \tag{11}$$

Воспользуемся Леммой 2, подставим в систему норменного уравнения $b_2 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 5 уравнений и 5 неизвестных:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 + b_0^2 + 2\,b_0 b_1 = 0 \\ -a_0^2 h_2 + 2\,b_0 b_1 + b_1^2 + 2\,b_0 = 0 \\ b_1^2 + 2\,b_0 + 2\,b_1 = 0 \\ 2\,b_1 + 1 = 0 \end{cases}$$

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражение $a_0 = -b_0$. В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении $-(b_0 h_1 - b_0 - 2\,b_1)b_0 = 0$

После преобразования получается система из 4 уравнений от переменных h_2, h_1, b_1, b_0:

$$\begin{cases} -b_0 h_1 + b_0 + 2\,b_1 = 0 \\ -b_0^2 h_2 + 2\,b_0 b_1 + b_1^2 + 2\,b_0 = 0 \\ b_1^2 + 2\,b_0 + 2\,b_1 = 0 \\ 2\,b_1 + 1 = 0 \end{cases}$$

Нетрудно видеть, что в данном случае система легко решается, а именно для любого поля k у системы (11) существует единственное решение: $h_2 = 40/9$, $f_0 = 1$, $a_0 = -3/8$, $f_1 = 1$, $b_1 = -1/2$, $b_0 = 3/8$, $h_1 = -5/3$, $b_2 = 1$. Отметим, что указанное решение было впервые найдено в работе [11].

Поле L содержит фундаментальную S-единицу степени 12

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 1, 2, 6)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_2 \neq 0$. Как отмечалось выше, решений с $f_1 = 0$ не существует, откуда без ограничения общности полагаем $f_1 \neq 0$.

Подставляя согласно Лемме 3 значения $f_1 = 1, f_0 = 1, b_2 = 1$ получаем систему из 6 уравнений с 6 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 - 2a_0 a_1 + b_0^2 + 2b_0 b_1 = 0 \\ b_0^2 f_2 - 2a_0 a_1 h_1 - a_1^2 + 2b_0 b_1 + b_1^2 + 2b_0 = 0 \\ 2b_0 b_1 f_2 - a_1^2 h_1 + b_1^2 + 2b_0 + 2b_1 = 0 \\ b_1^2 f_2 + 2b_0 f_2 + 2b_1 + 1 = 0 \\ 2b_1 f_2 + 1 = 0. \end{cases} \tag{12}$$

Заметим, что можно избавиться от переменных a_0 и b_1 из первого и пятого уравнения. Исключая их после упрощения мы получаем систему из 4 неизвестных.

$$\begin{cases} 3/4b_0h_1^2 + b_0f_2 - 1/2b_0h_1 - b_1h_1 - 1/4b_0 + b_1 + 2 = 0 \\ -1/4b_0^2h_1^3 + 1/2b_0^2h_1^2 + b_0b_1h_1^2 + 2b_0b_1f_2 - 1/4b_0^2h_1 - b_0b_1h_1 - b_1^2h_1 + b_1^2 + 2b_0 + 2b_1 = 0 \\ b_1^2f_2 + 2b_0f_2 + 2b_1 + 1 = 0 \\ 2b_1f_2 + 1 = 0. \end{cases} \tag{13}$$

Вычисляя последовательные результанты по R-процедуре для каждой из текущих переменных b_0, b_1, f_2, h_1 мы получаем такое следствие:

$$\begin{cases} (3b_1 + 2)b_1(5b_1^3 + 6b_1^2 + 12b_1 + 8) = 0 \\ h_1^2(h_1 + 2)(h_1 - 1)(h_1^3 + 6h_1^2 + 6h_1 + 2) = 0 \\ (25b_0^3 + 156b_0^2 + 240b_0 - 32) = 0 \\ (4f_2 - 3)f_2(64f_2^3 - 48f_2^2 + 12f_2 - 5) = 0. \end{cases} \tag{14}$$

При вычислениях результанта в ходе R-преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на нетривиальные общий множитель f_2 или его степени. Сокращение в каждом из случаев корректно, так как $f_2 \neq 0$. Это обосновывает корректность сокращения в ходе R-процедуры. Отметим, что в силу (14) каждая из исследуемых переменных b_0, b_1, h_1, f_2 может принимать не более чем конечное число значений для любого поля k, а для случая поля квадратичного поля k или поля $k = \mathbb{Q}$ нетрудно видеть, что система (14) не имеет решений.

Поле L содержит фундаментальную S-единицу степени 14

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 1, 3, 7)$. Согласно схеме, предложенной в начале доказательства, убеждаемся, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$. Из сравнения степеней левой и правой частей (1) и теоремы 4 также видим, что $lc(\mu_2) = b_2 \neq 0$. В силу того, что $\deg d_2 = 1$, заключаем, что $f_1 \neq 0$.

Поэтому подставляя согласно Лемме 2 значения $h_0 = f_1 = 1, f_0 = 1, b_2 = 1$ получаем систему из 7 уравнений с 7 неизвестными.

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2h_1 - 2a_0a_1 + b_0^2 + 2b_0b_1 = 0 \\ -2a_0a_1h_1 - a_0^2h_2 - a_1^2 + 2b_0b_1 + b_1^2 + 2b_0b_2 = 0 \\ -a_1^2h_1 - 2a_0a_1h_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ -a_1^2h_2 + 2b_1b_2 + b_2^2 + 2b_0 + 2b_1 = 0 \\ b_2^2 + 2b_1 + 2b_2 = 0 \\ 2b_2 + 1 = 0 \end{cases} \tag{15}$$

Заменяя a_0 на b_0 и заменяя a_1 на $1/2b_0h_1 - 1/2b_0 - b_1$ и после упрощения мы получаем систему от 5 неизвестных.

$$\begin{cases} 3/4b_0h_1^2 - 1/2b_0h_1 - b_1h_1 - b_0h_2 - 1/4b_0 + b_1 + 2b_2 = 0 \\ -1/4b_0^2h_1^3 + 1/2b_0^2h_1^2 + b_0b_1h_1^2 + b_0^2h_1h_2 - \\ -1/4b_0^2h_1 - b_0b_1h_1 - b_1^2h_1 - b_0^2h_2 - 2b_0b_1h_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ -1/4b_0^2h_1^2h_2 + 1/2b_0^2h_1h_2 + b_0b_1h_1h_2 - 1/4b_0^2h_2 - b_0b_1h_2 - b_1^2h_2 + 2b_1b_2 + d_2^2 + 2b_0 + 2d_1 = 0 \\ b_2^2 + 2b_1 + 2b_2 = 0 \\ 2b_2 + 1 = 0. \end{cases} \tag{16}$$

Переменные b_2, b_1 явно вычисляются. Вычисляя последовательные результанты по R-процедуре для каждой из текущих переменных мы получаем такое следствие:

$$\begin{cases} (h_2 - 40)h_2(9h_2 - 40)(2025h_2^3 - 39816h_2^2 + 210112h_2 - 75264)\cdot \\ \cdot(1866240000h_2^9 - 55205712000h_2^8 + 606471399225h_2^7 - 3130271733456h_2^6 + \\ +8727283377792h_2^5 - 18049927509504h_2^4 + 34435309195264h_2^3 - \\ -34230846619648h_2^2 - 178494898176h_2 + 1040449536000) = 0 \\ (h_1 - 1)(3h_1 + 5)(45h_1^3 + 273h_1^2 + 791h_1 + 427) = 0 \\ (13824b_0^3 - 92096b_0^2 - 7416b_0 - 405) = 0 \end{cases} \tag{17}$$

При вычислениях результанта в ходе R-преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на многочлены, которые не обнуляются на множестве решений системы, что обосновывает корректность сокращения в ходе R-процедуры. Для случая квадратичного поля k или случая $k = \mathbb{Q}$ нетрудно видеть, что последняя система не имеет нетривиальных решений.

Поле L содержит фундаментальную S-единицу степени 16

В этом случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (1, 2, 2, 3, 8)$

Ясно, что $h_0 \neq 0, a_0 \neq 0, b_0 \neq 0, f_0 \neq 0$, иначе сокращая на x в (1) заключаем, что степень единицы должна быть строго меньше 16. Из сравнения степеней левой и правой частей (1) и теоремы 4 нетрудно видеть, что $lc(\mu_2) = b_3 \neq 0$. Как отмечалось выше, в условиях теоремы 1 и тем более теоремы 2 не существует решений системы с $f_1 = 0$, откуда без ограничения общности полагаем $f_1 \neq 0$.

Воспользуемся Леммой 2, подставим в систему норменного уравнения $f_1 = 1, f_0 = 1, b_3 = 1$, $h_0 = 1$ и получим следующие уравнения:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2h_1 - 2a_0a_1 + b_0^2 + 2b_0b_1 = 0 \\ b_0^2f_2 - 2a_0a_1h_1 - a_1^2 - 2a_0a_2 + 2b_0b_1 + b_1^2 + 2b_0b_2 = 0 \\ 2b_0b_1f_2 - a_1^2h_1 - 2a_0a_2h_1 - 2a_1a_2 + b_1^2 + 2b_0b_2 + 2b_1b_2 + 2b_0 = 0 \\ b_1^2f_2 + 2b_0b_2f_2 - 2a_1a_2h_1 - a_2^2 + 2b_1b_2 + b_2^2 + 2b_0 + 2b_1 = 0 \\ 2b_1b_2f_2 - a_2^2h_1 + b_2^2 + 2b_0f_2 + 2b_1 + 2b_2 = 0 \\ b_2^2f_2 + 2b_1f_2 + 2b_2 + 1 = 0 \\ 2b_2f_2 + 1 = 0. \end{cases} \tag{18}$$

Из этой системы мы можем исключить переменные a_0, a_1, a_2. Замены у нас получаются следующими: $a_0 = -b_0, a_1 = 1/2b_0h_1 - 1/2b_0 - b_1, a_2 = -3/8b_0h_1^2 - 1/2b_0f_2 + 1/4(b_0 + 2b_1)h_1 + 1/8b_0 -$

$-1/2b_1 - b_2$. После простого упрощения системы мы получаем эквивалентную систему от переменных b_0, b_1, b_2, h_1, f_2.

$$\begin{cases} -\frac{5}{8}\,b_0h_1^3 - \frac{1}{2}\,b_0f_2h_1 + \frac{3}{8}\,b_0h_1^2 + \frac{3}{4}\,b_1h_1^2 - \\ -\frac{1}{2}\,b_0f_2 + b_1f_2 + \frac{1}{8}\,b_0h_1 - \frac{1}{2}\,b_1h_1 - b_2h_1 + \frac{1}{8}\,b_0 - \frac{1}{4}\,b_1 + b_2 + 2 = 0 \\ \frac{15}{64}\,b_0^2h_1^4 + \frac{1}{8}\,b_0^2f_2h_1^2 - \frac{7}{16}\,b_0^2h_1^3 - \frac{7}{8}\,b_0b_1h_1^3 - \frac{1}{4}\,b_0^2f_2^2 - \frac{1}{4}\,b_0^2f_2h_1 - \frac{1}{2}\,b_0b_1f_2h_1 + \\ +\frac{5}{32}\,b_0^2h_1^2 + \frac{7}{8}\,b_0b_1h_1^2 + \frac{3}{4}\,b_1^2h_1^2 + \frac{1}{4}\,b_0b_2h_1^2 + \frac{1}{8}\,b_0^2f_2 - \frac{1}{2}\,b_0b_1f_2 + b_1^2f_2 + b_0b_2f_2 + \\ +\frac{1}{16}\,b_0^2h_1 - \frac{1}{8}\,b_0b_1h_1 - \frac{1}{2}\,b_1^2h_1 - \frac{1}{2}\,b_0b_2h_1 - b_1b_2h_1 - \frac{1}{64}\,b_0^2 + \frac{1}{8}\,b_0b_1 - \frac{1}{4}\,b_1^2 + \\ +\frac{1}{4}\,b_0b_2 + b_1b_2 + 2\,b_0 + 2\,b_1 = 0 \\ -\frac{9}{64}\,b_0^2h_1^5 - \frac{3}{8}\,b_0^2f_2h_1^3 + \frac{3}{16}\,b_0^2h_1^4 + \frac{3}{8}\,b_0b_1h_1^4 - \frac{1}{4}\,b_0^2f_2^2h_1 + \frac{1}{4}\,b_0^2f_2h_1^2 + \frac{1}{2}\,b_0b_1f_2h_1^2 + \frac{1}{32}\,b_0^2h_1^3 - \\ -\frac{5}{8}\,b_0b_1h_1^3 - \frac{1}{4}\,b_1^2h_1^3 - \frac{3}{4}\,b_0b_2h_1^3 + \frac{1}{8}\,b_0^2f_2h_1 - \\ -\frac{1}{2}\,b_0b_1f_2h_1 - b_0b_2f_2h_1 - \frac{1}{16}\,b_0^2h_1^2 + \frac{1}{8}\,b_0b_1h_1^2 + \frac{1}{2}\,b_1^2h_1^2 + \frac{1}{2}\,b_0b_2h_1^2 + b_1b_2h_1^2 + 2\,b_1b_2f_2 - \\ -\frac{1}{64}\,b_0^2h_1 + \frac{1}{8}\,b_0b_1h_1 - \frac{1}{4}\,b_1^2h_1 + \frac{1}{4}\,b_0b_2h_1 - b_1b_2h_1 - b_2^2h_1 + b_2^2 + 2\,b_0f_2 + 2\,b_1 + 2\,b_2 = 0 \\ b_2^2f_2 + 2\,b_1f_2 + 2\,b_2 + 1 = 0 \\ 2\,b_2f_2 + 1 = 0 \end{cases} \tag{19}$$

Применим R-преобразование системы. В каждом из случаев получается ненулевой многочлен от каждой из переменных, что завершает доказательств нашей теоремы. Выпишем уравнения, которые получились у нас в результате R-преобразования системы, причём вместо каждого многочлена мы выпишем лишь его радикал. Полученная система является следствием над $\overline{\mathbb{Q}}$ исходной системы. Обозначим через $P_{x,k}$ — некоторый многочлен от переменной x степени k.

$$\begin{cases} b_0P_{b_0,6}P_{b_0,55}P_{b_0,107} = 0 \\ (h_1+2)h_1(h_1-1)P_{h_1,2}P_{h_1,3}P_{h_1,6}P_{h_1,20}P_{h_1,48} = 0 \\ (4f_2-3)(4f_2-1)f_2P_{f_2,2}P_{f_2,3}P_{f_2,6} = 0 \\ (b_2+2)(3b_2+2)b_2P_{b_2,2}P_{b_2,3}P_{b_2,6} = 0 \\ b_1(b_1-4)P_{b_1,2}P_{b_1,3}P_{b_1,6}P_{b_1,20}P_{b_1,48} = 0 \end{cases} \tag{20}$$

В силу ограничений объёма, мы не имеем возможности привести полный вид всех многочленов, входящих в систему (20). Приведём для примера несколько многочленов:

$P_{b_0,6} = 35162859375\,b_0^6 + 964070910000\,b_0^5 + 6924423153600\,b_0^4 - 5147602126848\,b_0^3 -$
$- 48716872445952\,b_0^2 + 63203662036992\,b_0 + 674064760832;$

$P_{f_2,6} = 76877824\,f_2^6 - 162641920\,f_2^5 + 102620928\,f_2^4 - 33014016\,f_2^3 + 8659440\,f_2^2 - 502200\,f_2 + 212625;$

$P_{b_2,6} = 212625\,b_2^6 + 251100\,b_2^5 + 2164860\,b_2^4 + 4126752\,b_2^3 + 6413808\,b_2^2 + 5082560\,b_2 + 1201216;$

$P_{b_1,20} = 8255648563200\,b_1^{20} - 182292029964288\,b_1^{19} +$
$+ 3700176823118016\,b_1^{18} - 41672730322305792\,b_1^{17} + 220048281041334912\,b_1^{16} -$
$- 274861679147380224\,b_1^{15} - 262224058850487424\,b_1^{14} + 132316295279366463 84\,b_1^{13} -$
$- 17982425793551807808\,b_1^{12} - 35374972142113715184\,b_1^{11} +$
$+ 167662143348451723824\,b_1^{10} - 267859272743637980872\,b_1^9 + 220469209547236109547\,b_1^8 -$
$- 85941395765711763492\,b_1^7 - 150095028152499744\,b_1^6 +$
$+ 11146097842624151552\,b_1^5 + 1592601206869000192\,b_1^4 + 44728120934137856\,b_1^3 -$
$- 1174039007592448\,b_1^2 + 32358283608064\,b_1 - 549755813888.$

При вычислениях результанта в ходе R-преобразования системы на шагах, приводящих к этим многочленам, происходит сокращение на нетривиальные общие множители: f_2, b_2, b_0 или произведения их степеней. Сокращение в каждом из случаев корректно, так как $b_0 \neq 0$ или базис Гребнера исходной системы, дополненный каждым из уравнений: $b_2 = 0$ и $f_2 = 0$, сводится к ненулевой константе. Это обосновывает корректность сокращения в ходе R-процедуры.

Также возникает сокращение на множитель b_1^2. Вычисляя Базис Гребнера исходной системы дополненный каждым из этих уравнений, мы находим явно все решения. Эти решения не удовлетворяют условию $b_0 \neq 0$ и, следовательно, нам не подходят.

В заключение отметим, что в силу (20) каждая из исследуемых переменных b_0,b_1,b_2, h_1, f_2 может принимать не более чем конечное число значений для любого поля k, а для случая квадратичного поля k нетрудно видеть, что система (20) не имеет решений.

Поле L содержит фундаментальную S-единицу степени 18

В данном случае $(\deg d_1, \deg d_2, \deg \mu_1, \deg \mu_2, m) = (2, 1, 2, 4, 9)$. Без ограничения общности положим $h_0 = 1$. Тогда система обобщенного норменного уравнения состоит из 10 уравнений и 13 неизвестных. Выпишем ее в явном виде.

$$\begin{cases} b_0^2 f_0^2 - a_0^2 = 0 \\ 2\,b_0 b_1 f_0^2 + b_0^2 f_1 - a_0^2 h_1 - 2\,a_0 a_1 = 0 \\ b_1^2 f_0^2 + 2\,b_0 b_2 f_0^2 + 2\,b_0 b_1 f_1 - 2\,a_0 a_1 h_1 - a_0^2 h_2 - a_1^2 - 2\,a_0 a_2 = 0 \\ 2\,b_1 b_2 f_0^2 + 2\,b_0 b_3 f_0^2 + b_1^2 f_1 + 2\,b_0 b_2 f_1 - a_1^2 h_1 - 2\,a_0 a_2 h_1 - 2\,a_0 a_1 h_2 - 2\,a_1 a_2 = 0 \\ b_2^2 f_0^2 + 2\,b_1 b_3 f_0^2 + 2\,b_0 b_4 f_0^2 + 2\,b_1 b_2 f_1 + 2\,b_0 b_3 f_1 - 2\,a_1 a_2 h_1 - a_1^2 h_2 - 2\,a_0 a_2 h_2 - a_2^2 = 0 \\ 2\,b_2 b_3 f_0^2 + 2\,b_1 b_4 f_0^2 + b_2^2 f_1 + 2\,b_1 b_3 f_1 + 2\,b_0 b_4 f_1 - a_2^2 h_1 - 2\,a_1 a_2 h_2 = 0 \\ b_3^2 f_0^2 + 2\,b_2 b_4 f_0^2 + 2\,b_2 b_3 f_1 + 2\,b_1 b_4 f_1 - a_2^2 h_2 = 0 \\ 2\,b_3 b_4 f_0^2 + b_3^2 f_1 + 2\,b_2 b_4 f_1 = 0 \\ b_4^2 f_0^2 + 2\,b_3 b_4 f_1 = 0 \\ b_4^2 f_1 + c = 0 \end{cases}$$

Поскольку $\deg d_2 = 1$, то отсюда следует, что $f_1 \neq 0$. Поэтому можем воспользоваться Леммой 3, подставим в систему норменного уравнения $b_4 = 1, f_0 = 1, f_1 = 1$, и получим следующую систему из 9 уравнений и 9 неизвестных:

$$\begin{cases} -a_0^2 + b_0^2 = 0 \\ -a_0^2 h_1 - 2\,a_0 a_1 + b_0^2 + 2\,b_0 b_1 = 0 \\ -2\,a_0 a_1 h_1 - a_0^2 h_2 - a_1^2 - 2\,a_0 a_2 + 2\,b_0 b_1 + b_1^2 + 2\,b_0 b_2 = 0 \\ -a_1^2 h_1 - 2\,a_0 a_2 h_1 - 2\,a_0 a_1 h_2 - 2\,a_1 a_2 + b_1^2 + 2\,b_0 b_2 + 2\,b_1 b_2 + 2\,b_0 b_3 = 0 \\ -2\,a_1 a_2 h_1 - a_1^2 h_2 - 2\,a_0 a_2 h_2 - a_2^2 + 2\,b_1 b_2 + b_2^2 + 2\,b_0 b_3 + 2\,b_1 b_3 + 2\,b_0 = 0 \\ -a_2^2 h_1 - 2\,a_1 a_2 h_2 + b_2^2 + 2\,b_1 b_3 + 2\,b_2 b_3 + 2\,b_0 + 2\,b_1 = 0 \\ -a_2^2 h_2 + 2\,b_2 b_3 + b_3^2 + 2\,b_1 + 2\,b_2 = 0 \\ b_3^2 + 2\,b_2 + 2\,b_3 = 0 \\ 2\,b_3 + 1 = 0 \end{cases}$$

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражения: $a_0 = -b_0$, $a_1 = \frac{1}{2}\,b_0 h_1 - \frac{1}{2}\,b_0 - b_1$, $a_2 = -\frac{3}{8}\,b_0 h_1^2 + \frac{1}{4}\,(b_0 + 2\,b_1) h_1 + \frac{1}{2}\,b_0 h_2 + \frac{1}{8}\,b_0 - \frac{1}{2}\,b_1 - b_2$, В силу того, что $b_0 \neq 0$ сократим множитель b_0 в уравнении $-\frac{1}{8}\,\left(5\,b_0 h_1^3 - 3\,b_0 h_1^2 - 6\,b_1 h_1^2 - 12\,b_0 h_1 h_2 - \right.$ $\left. - b_0 h_1 + 4\,b_1 h_1 + 8\,b_2 h_1 + 4\,b_0 h_2 + 8\,b_1 h_2 - b_0 + 2\,b_1 - 8\,b_2 - 16\,b_3\right) b_0 = 0$.

После преобразования получается система из 6 уравнений от переменных $h_2, b_0, h_1, b_3, b_2, b_1$:

$$\begin{cases}
-\frac{5}{8}\,b_0h_1^3+\frac{3}{8}\,b_0h_1^2+\frac{3}{4}\,b_1h_1^2+\frac{3}{2}\,b_0h_1h_2+\frac{1}{8}\,b_0h_1-\frac{1}{2}\,b_1h_1-b_2h_1-\\
-\frac{1}{2}\,b_0h_2-b_1h_2+\frac{1}{8}\,b_0-\frac{1}{4}\,b_1+b_2+2\,b_3=0\\
\frac{15}{64}\,b_0^2h_1^4-\frac{7}{16}\,b_0^2h_1^3-\frac{7}{8}\,b_0b_1h_1^3-\frac{9}{8}\,b_0^2h_1^2h_2+\frac{5}{32}\,b_0^2h_1^2+\frac{7}{8}\,b_0b_1h_1^2+\frac{3}{4}\,b_1^2h_1^2+\frac{1}{4}\,b_0b_2h_1^2+\\
+\frac{5}{4}\,b_0^2h_1h_2+\frac{5}{2}\,b_0b_1h_1h_2+\frac{3}{4}\,b_0^2h_2^2+\frac{1}{16}\,b_0^2h_1-\frac{1}{8}\,b_0b_1h_1-\frac{1}{2}\,b_1^2h_1-\frac{1}{2}\,b_0b_2h_1-b_1b_2h_1-\frac{1}{8}\,b_0^2h_2-\\
-\frac{3}{2}\,b_0b_1h_2-b_1^2h_2-b_0b_2h_2-\frac{1}{64}\,b_0^2+\frac{1}{8}\,b_0b_1-\frac{1}{4}\,b_1^2+\frac{1}{4}\,b_0b_2+b_1b_2+2\,b_0b_3+2\,b_1b_3+2\,b_0=0\\
-\frac{9}{64}\,b_0^2h_1^5+\frac{3}{16}\,b_0^2h_1^4+\frac{3}{8}\,b_0b_1h_1^4+\frac{3}{4}\,b_0^2h_1^3h_2+\frac{1}{32}\,b_0^2h_1^3-\frac{5}{8}\,b_0b_1h_1^3-\\
-\frac{1}{4}\,b_1^2h_1^3-\frac{3}{4}\,b_0b_2h_1^3-\frac{7}{8}\,b_0^2h_1^2h_2-\frac{7}{4}\,b_0b_1h_1^2h_2-\frac{3}{4}\,b_0^2h_1h_2^2-\frac{1}{16}\,b_0^2h_1^2+\frac{1}{8}\,b_0b_1h_1^2+\frac{1}{2}\,b_1^2h_1^2+\\
+\frac{1}{2}\,b_0b_2h_1^2+b_1b_2h_1^2+2\,b_0b_1h_1h_2+b_1^2h_1h_2+2\,b_0b_2h_1h_2+\frac{1}{2}\,b_0^2h_2^2+b_0b_1h_2^2-\\
-\frac{1}{64}\,b_0^2h_1+\frac{1}{8}\,b_0b_1h_1-\\
-\frac{1}{4}\,b_1^2h_1+\frac{1}{4}\,b_0b_2h_1-b_1b_2h_1-b_2^2h_1+\frac{1}{8}\,b_0^2h_2-\frac{1}{4}\,b_0b_1h_2-b_1^2h_2-b_0b_2h_2-2\,b_1b_2h_2+b_2^2+\\
+2\,b_1b_3+2\,b_2b_3+2\,b_0+2\,b_1=0\\
-\frac{9}{64}\,b_0^2h_1^4h_2+\frac{3}{16}\,b_0^2h_1^3h_2+\frac{3}{8}\,b_0b_1h_1^3h_2+\frac{3}{8}\,b_0^2h_1^2h_2^2+\\
+\frac{1}{32}\,b_0^2h_1^2h_2-\frac{5}{8}\,b_0b_1h_1^2h_2-\frac{1}{4}\,b_1^2h_1^2h_2-\frac{3}{4}\,b_0b_2h_1^2h_2-\frac{1}{4}\,b_0^2h_1h_2^2-\frac{1}{2}\,b_0b_1h_1h_2^2-\frac{1}{4}\,b_0^2h_2^3-\\
-\frac{1}{16}\,b_0^2h_1h_2+\frac{1}{8}\,b_0b_1h_1h_2+\frac{1}{2}\,b_1^2h_1h_2+\frac{1}{2}\,b_0b_2h_1h_2+b_1b_2h_1h_2-\frac{1}{8}\,b_0^2h_2^2+\frac{1}{2}\,b_0b_1h_2^2+b_0b_2h_2^2-\\
-\frac{1}{64}\,b_0^2h_2+\frac{1}{8}\,b_0b_1h_2-\frac{1}{4}\,b_1^2h_2+\frac{1}{4}\,b_0b_2h_2-b_1b_2h_2-b_2^2h_2+2\,b_2b_3+b_3^2+2\,b_1+2\,b_2=0\\
b_3^2+2\,b_2+2\,b_3=0\\
2\,b_3+1=0
\end{cases}\tag{21}$$

Вычисление базиса Гребнера данной системы показывает нулевую размерность данной системы, что равносильно конечности числа решений в переменных $h_1, b_1, b_2, h_2, b_0, b_3$. Более того, у всех решений $b_0 = 0$, а следовательно, они нам не подходят. Кроме того, вычисление базиса Грёбнера показывает отсутствие нетривиальных решений над полем $\mathbb{Q}$ и над произвольным квадратичным расширением поля $\mathbb{Q}$. Доказательство теорем завершено.

6. Заключение

В работах [15, 16, 17] доказана ограниченность кручения в эллиптических кривых над квадратичными полями и дано описание возможных групп кручения. Из результатов работ, в частности следует, что в эллиптических полях над квадратичными полями реализуются все степени фундаментальных S-единиц до 18 включительно за исключением 17 и только они. С учётом теоремы 2, чтобы завершить доказательство конечности числа нетривиальных неэквивалентных периодических $\sqrt{f}$ над квадратичными полями в качестве поля констант, остаётся доказать конечность с точностью до отношения эквивалентности таких полей, обладающих фундаментальной S-единицей степени 13 и 15. Последнее, наряду с результатами компьютерных вычислений позволяет выдвинуть следующую гипотезу.

Гипотеза. *Пусть k — квадратичное расширение поля $\mathbb{Q}$. Тогда существует универсальная константа C, не зависящая от поля k, такая, что существует не более C попарно неэквивалентных над k нетривиальных многочленов f, $\deg f = 3$, для которых $\sqrt{f}$ периодичен в $k((x))$.*

□

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Abel N. H. Ueber die integration der differential-formel $\rho dx/\sqrt{R}$ wenn r und ρ ganze functionen sind. *Journal für die reine und angewandte Mathematik*, Vol. 1, P. 185–221, 1826.

2. Tchebicheff P. Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré' // Journal des math. pures et appl. 1857. Vol. 2. P. 168–192.

3. Платонов В. П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // Успехи математических наук. 2014. Т. 69:1, № 415. С. 3–38.

4. Schmidt W. M. On continued fractions and Diophantine approximation in power series fields // Acta arithmetica. 2000. Vol. 95, № 2. P. 139–166.

5. Adams W. W., Razar M. J. Multiples of points on elliptic curves and continued fractions //Proceedings of the London Mathematical Society. – 1980. – Vol. 41 – P. 481-498.

6. Платонов В. П., Петрунин М. М. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // ДАН. 2016. Т. 470, № 3. С. 260–265.

7. Платонов В. П., Петрунин М. М. S-единицы и периодичность в квадратичных функциональных полях // УМН. 2016. Т. 71, № 5. С. 181–182.

8. Петрунин М. М. S-единицы и периодичность квадратного корня в гиперэллиптических полях. 2017. // Доклады Академии наук. 2018.

   Т. 474, № 2. С. 155–158.

9. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в эллиптических полях // Доклады Академии наук. 2017. Т. 475, № 2. С. 133–136.

10. Платонов В. П., Федоров Г. В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Математический сборник. 2018. Т. 4, № 209. С. 54–94.

11. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях // Доклады Академии наук. 2017. Т. 474, № 5. С. 540–544.

12. Платонов В. П., Жгун В. С., Петрунин М. М., Штейников Ю.Н. О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // Доклады Академии наук. 2018. Т. 483, № 6. С. 603–608.

13. Платонов В. П., Жгун В. С., Федоров Г.В. О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант. // Доклады Академии наук. 2018. Т. 482, № 2. С. 137–141.

14. Беняш-Кривец В. В., Платонов В. П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. 2009. Т. 200, № 11. С. 15–44.

15. Kenku M. A., Momose F. Torsion points on elliptic curves defined over quadratic fields // Nagoya Mathematical Journal. 1988. Vol. 109. P. 125–149.

16. Kamienny Sheldon. Torsion points on elliptic curves and q-coefficients of modular forms // Inventiones mathematicae. 1992. Vol. 109, № 1. P. 221–229.

17. Kamienny S., Najman F. Torsion groups of elliptic curves over quadratic fields // Acta Arithmetica. 2012. Vol. 3, № 152. P. 291–305.

18. Платонов В. П., Петрунин М.М. Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Труды МИАН. 2018, Т. 302, С. 354–376.

19. Платонов В. П., Петрунин М. М., Штейников Ю. Н. О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // Докл. РАН. 2019, Т. 488, №3, С. 237–242.

20. Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.

21. SageMath, the Sage Mathematics Software System (Version 9.0), The Sage Developers, 2020, `https://www.sagemath.org`.

22. Mazur B. Rational isogenies of prime degree // Inventiones Mathematicae. 1978. № 2 (44). P. 129–162.

REFERENCES

1. Abel N. H. 1826, "Ueber die integration der differential-formel $\rho dx/\sqrt{R}$ wenn r und ρ ganze functionen sind", *Journal für die reine und angewandte Mathematik*, vol. 1, pp. 185–221.

2. Tchebicheff P. 1857, "Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré", *Journal des math. pures et appl.,* vol. 2. pp. 168–192.

3. Platonov V. P. 2014, "Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field", *Russian Math. Surveys,* vol. 69, no. 1. pp. 1–34.

4. Schmidt W. M. 2000, "On continued fractions and Diophantine approximation in power series fields", *Acta arithmetica,* vol. 95, no. 2. pp. 139–166.

5. Adams, W.W., Razar, M.J., 1980. "Multiples of Points on Elliptic Curves and Continued Fractions", *Proceedings of the London Mathematical Society*, vol. 41, pp. 481–498.

6. Platonov V. P., Petrunin M. M. 2016 "S-units in hyperelliptic fields and periodicity of continued fractions", *Dokl. Math.,* vol. 94, no. 2. pp. 532–537.

7. Platonov V. P., Petrunin M. M. 2016. S-Units and periodicity in quadratic function fields *Russian Math. Surveys,* vol. 71, no. 5. стр. 973–975.

8. Petrunin M. M. 2017 "S-units and periodicity of square root in hyperelliptic fields", *Dokl.Math.,* vol. 95, no. 3. pp. 222–225.

9. Platonov V. P., Fedorov G. V. 2017. "On the periodicity of continued fractions in elliptic fields", *Dokl. Math.*, vol 96, no. 1. pp. 332–335.

10. Platonov V.P., Fedorov G.V. 2018, "On the problem of periodicity of continued fractions in hyperelliptic fields", *Sb.Math.*, vol. 209, no. 4, pp. 519–559.

11. Platonov V. P., Fedorov G. V. 2017, "On the periodicity of continued fractions in hyperelliptic fields", *Dokl. Math.,* vol. 95, no. 3. pp. 254–258.

12. Platonov V. P., Zhgoon V. S., Petrunin M. M., Shteinikov Yu. N. 2018, "On the finiteness of hyperelliptic fields with special properties and periodic expansion of $\sqrt{f}$", *Dokl. Math.,* vol 98, pp. 603–608.

13. Platonov V.P., Zhgoon V.S., Fedorov G.V. 2018, "Continued rational fractions in hyperelliptic fields and the Mumford representation", *Dokl. Math.,* vol. 482, no. 2. pp. 137–141.

14. Benyash-Krivets V.V., Platonov V.P. 2009, "Groups of S-units in hyperelliptic fields and continued fractions", *Sb.Math.,* vol. 200, no.11, pp.1587–1615.

15. Kenku M. A., Momose F. 1988, "Torsion points on elliptic curves defined over quadratic fields", *Nagoya Mathematical Journal,* vol. 109. pp. 125–149.

16. Kamienny S. 1992, "Torsion points on elliptic curves and q-coefficients of modular forms", *Inventiones mathematicae,* vol. 109, no. 1. pp. 221–229.

17. Kamienny S., Najman F. 2012, "Torsion groups of elliptic curves over quadratic fields", *Acta Arithmetica,* vol. 3, no. 152. pp. 291–305.

18. Platonov V. P., Petrunin M.M. 2018, "Groups of S-units and the problem of periodicity of continued fractions in hyperelliptic fields" *Proc. Steklov Inst. math.*, vol. 302, pp. 336–357.

19. Platonov V. P., Petrunin M. M., Shteinikov Yu. N. 2019, "On the finiteness of the number of elliptic fields with given degrees of S-units and periodic expansion of $\sqrt{f}$", *Dokl. Math.*, vol. 100, no. 2, pp. 1–5.

20. Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.

21. SageMath, the Sage Mathematics Software System (Version 9.0), The Sage Developers, 2020, `https://www.sagemath.org`.

22. Mazur B. 1978, "Rational isogenies of prime degree (with appendix by Goldfeld D.)", *Inventiones mathematicae*, vol. 44, no. 2, pp. 129–162.

Получено 27.01.2018 г.
Принято в печать 20.03.2020 г.