ДОКЛАДЫ АКАДЕМИИ НАУК, 2019, том 488, № 3, с. 237–242

МАТЕМАТИКА

УДК 511.6

О КОНЕЧНОСТИ ЧИСЛА ЭЛЛИПТИЧЕСКИХ ПОЛЕЙ С ЗАДАННЫМИ СТЕПЕНЯМИ *S*-ЕДИНИЦ И ПЕРИОДИЧЕСКИМ РАЗЛОЖЕНИЕМ $\sqrt{f}$

Академик РАН В. П. Платонов[1,2,*], М. М. Петрунин[1,], Ю. Н. Штейников[1,***]**

Поступило 01.07.2019 г.

Для поля k характеристики 0 с точностью до естественного отношения эквивалентности доказана конечность числа нетривиальных эллиптических полей $k(x)(\sqrt{f})$ с периодическим разложением в непрерывную дробь $\sqrt{f} \in k((x))$, для которых соответствующая эллиптическая кривая содержит k-точку чётного порядка, не превосходящего 18 или k-точку нечётного порядка не превосходящего 11. Для k – квадратичного расширения $\mathbb{Q}$ найдены все такие поля.

Ключевые слова: эллиптическое поле, *S*-единицы, непрерывные дроби, периодичность, базис Грёбнера, результант.

DOI: https://doi.org/10.31857/S0869-56524883237-242

Пусть k – поле характеристики 0, и $f \in k[x]$ – многочлен, свободный от квадратов, положим $L = k(x)(\sqrt{f})$. В работах [1–4] получены результаты, связанные с проблемой периодичности разложения элементов поля L в непрерывную дробь в $k((1/x))$. В частности, было показано, что с точки зрения изучения вопросов, связанных с периодичностью элементов поля L, 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 $k((x))$ наличие в поле L периодических элементов не гарантирует периодичность $\sqrt{f}$. Более того, периодичность $\sqrt{f}$ – сравнительно редкое явление.

В работах [5, 12] было доказано, что квазипериодический $\sqrt{f} \in k((x))$ с необходимостью является периодическим, и были построены первые примеры периодических $\sqrt{f}$. А в работе [6] с точностью до естественного отношения эквивалентности была доказана конечность числа таких нетривиальных многочленов степени $\deg f = 3$ с рациональными коэффициентами, и все они были приведены явно. Кроме того, был поставлен вопрос: для каких многочленов $f \in \mathbb{Q}[x]$ непрерывная дробь $\sqrt{f} \in \mathbb{Q}((x))$ является периодической.

В работе [6] с помощью метода, основанного на решении норменного уравнения, были получены рекуррентные соотношения на коэффициенты решения норменного уравнения для гиперэллиптических полей, обладающих фундаментальными *S*-единицами малых степеней, и были найдены новые примеры периодического $\sqrt{f}$ для $f \in \mathbb{Q}[x]$.

В работе [7] был предложен новый эффективный метод для решения норменного уравнения, основанный на применении базисов Грёбнера. В работе [7] было доказано, что для любого поля k характеристики 0 с точностью до естественной эквивалентности существует лишь конечное число бесквадратных многочленов над k нечётной степени, отличной от 11, таких, что элемент $\sqrt{f}$ периодичен, а соответствующее гиперэллиптическое поле L содержит *S*-единицу степени 11.

Остаётся открытым естественный вопрос об описании периодических $\sqrt{f}$ для эллиптического случая с числовым полем в качестве поля констант. Полного решения нет даже для $\deg f = 3$ и квадратичных расширений поля $\mathbb{Q}$. В работе [8] было сделано продвижение в этом направлении и дано описание кубических многочленов $f \in k[x]$, где $k = \mathbb{Q}(\sqrt{5})$ или $k = \mathbb{Q}(\sqrt{-15})$, для которых разложение $\sqrt{f}$ над этими полями периодично.

В настоящей работе нами предложен новый метод доказательства конечности многочленов f с периодическим разложением $\sqrt{f} \in k((x))$ для произвольного k при фиксированной степени фундаментальной *S*-единицы в поле L, основанный на комбинации последовательного вычисления результантов, применения базисов Грёбнера и нетривиальных вычислениях в системах компьютерной алгебры Magma и Sage. Нами показано, что с точностью до

[1] *Федеральный научный центр Научно-исследовательский институт системных исследований Российской Академии наук, Москва*

[2] *Математический институт им. В.А. Стеклова Российской Академии наук, Москва*

** E-mail: platonov@niisi.ras.ru*

*** E-mail: petrushkin@yandex.ru*

**** E-mail: yuriisht@yandex.ru*

естественного отношения эквивалентности существует лишь конечное число эллиптических полей L с периодическим разложением $\sqrt{f} \in k((x))$, для которых соответствующая эллиптическая кривая содержит k-точку чётного порядка, не превосходящего 18 или k-точку нечётного порядка 5, 7, 9, 11. А для случая, когда k – квадратичное расширение $\mathbb{Q}$, удаётся найти все такие поля и, соответственно, многочлены с указанными свойствами.

Напомним некоторые факты, которые потребуются нам в дальнейшем. Для неприводимого над k многочлена h определим дискретное нормирование ν_h (элемента поля $k(x)$) равенством $\nu_h(h^m(p/q)) = m$, где многочлены p, q не делятся на h. Бесконечное нормирование ν_∞ 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. Если $\deg f = 2g+1$ для $g \in \mathbb{N}$, то 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 (т.е. отличная от константы поля k), то в описанном нами случае группа S-единиц является прямым произведением $k\setminus\{0\}$ и бесконечной циклической группы, её образующие называются фундаментальными S-единицами. Степенью S-единицы $\lambda_1 + \lambda_2\sqrt{f}$ называется показатель m в норменном выражении $\lambda_1^2 - \lambda_2^2 f = = bh^m$, $b \in k\setminus\{0\}$. Для эллиптического поля существование фундаментальной S-единицы степени m равносильно существованию k-точки порядка m соответствующей эллиптической кривой (более подробно см. [12]).

Будем говорить, что $\alpha \in L$ разлагается в ряд в поле формальных степенных рядов $k((x))$, если имеет место разложение $\alpha = \sum\limits_{j\geq s} u_j x^j$, где $u_j \in k$, $s \in \mathbb{Z}$. Чтобы каждый элемент поля L имел однозначное разложение в $k((x))$, мы без ограничения общности фиксируем одно из вложений поля L в $k((x))$, соответствующее нормированию ν_x^+ (более подробно см. [9]).

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 настоящей работы.

Теорема 1. *Пусть k – поле,* $\operatorname{char} k = 0$. *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 содержит фундаментальную S-единицу чётной степени, не превосходящей* 18 *или нечётной степени* 5, 7, 9 *или* 11 *для* $S = \{\nu_\infty, \nu_x^+\}$.

Нетривиальным многочленом f будем называть многочлен, не эквивалентный многочлену $cx^3 + 1$, где $c \in k\setminus\{0\}$, а соответствующее эллиптическое поле будем называть нетривиальным.

Теорема 2. *Если в условиях теоремы* 1 *поле k – квадратичное расширение $\mathbb{Q}$, то множество таких нетривиальных многочленов содержит многочлены*

$$\begin{aligned} f_1 &= \frac{3}{16}x^3 - \frac{1}{2}x^2 + x + 1,\\ f_2 &= \frac{12}{8}x^3 - \frac{5}{4}x^2 + x + 1,\\ f_3 &= -\frac{120}{8}x^3 + \frac{25}{4}x^2 + x + 1, \end{aligned}$$

а также в случае, когда $\mathbb{Q}(\sqrt{21}) \subset k$, дополнительно содержит многочлен

$$f_4 = \frac{3}{32}\left(9\sqrt{21} - 41\right)x^3 - \frac{1}{4}\left(3\sqrt{21} - 13\right)x^2 + x + 1\,.$$

Других нетривиальных многочленов с указанными свойствами с точностью до вышеуказанного отношения эквивалентности многочленов 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 [8].

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 [6] с использованием параметризации Куберта.

Следствие. *Имеется лишь три нетривиальных неэквивалентных свободных от квадратов многочлена $f \in \mathbb{Q}[x]$,* $\deg f = 3$, *имеющих периодическое разложение $\sqrt{f}$ в непрерывную дробь в $k((x))$. А именно, многочлены f_1, f_2, f_3 из теоремы* 2.

В работах [10, 11] 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. Последнее, наряду с теоремой 2 и 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 $k((x))$.*

В работах [5, 12] был доказан критерий периодичности элемента вида $\sqrt{f}/x^s$, а также доказаны факты, полезные в настоящей работе. Приведём здесь критерий в необходимой нам общности (см. также [6]).

Теорема 3. *Пусть многочлен f свободен от квадратов, а* $\deg f = 2g+1$. *Элемент $\sqrt{f}$ квазипериодичен тогда и только тогда, когда для 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*

$$\mu_1^2 d_1 - \mu_2^2 d_2 = bx^m, \qquad (1)$$

и решение для наименьшего такого m удовлетворяет условиям

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

Легко видеть, что для наименьшего такого m выполнено одно из двух: или $\deg d_1 = 0$ и m – нечётное число, или $\deg d_1 > 0$ и $\deg d_2 > 0$.

Рассмотрим теперь многочлены

$$f = \sum_{i \le r} a_i x^i,\ g = \sum_{j \le s} b_j x^j, \text{ где } a_r, b_s \ne 0.$$

Пусть x_i – корни многочлена f, а y_i – корни многочлена g. Напомним, что величина $R(f, g) = a_r^s b_s^r \prod (x_i - y_j)$ называется результантом пары f, g.

Напомним, что $R(f,g)$ является многочленом с целыми коэффициентами от a_i, b_j, и $R(f,g) = 0$ только в том случае, когда f и g имеют общий корень в алгебраическом замыкании.

Результант позволяет 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

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

где $f_i \in k[x_1, \ldots, x_n]$, имеет решение $(a_1, \ldots, a_n)$. Тогда полиномиальная система $\{R(f_1, f_i) = 0\}$ для $i = 2, ..., n$, где f_i рассматривается как полином от x_n над кольцом $k[x_1, \ldots, x_{n-1}]$, состоит из $n-1$ уравнений от переменных $x_1, \ldots x_{n-1}$ и имеет решение $(a_1, \ldots, a_{n-1})$. Чтобы избежать обнуления результанта, на каждом шаге предварительно вычислим наибольшие общие делители пар многочленов f_i: НОД(f_i, f_j). Если ни один из корней первоначальной системы не обнуляет многочлен НОД(f_i, f_j), то процедура деления многочленов f_i, f_j на многочлен НОД(f_i, f_j) корректна, и мы производим всевозможные такие сокращения.

Последовательное применение шагов по исключению переменной позволяет получить в рассматриваемых нами случаях многочлен от одной переменной. С помощью переупорядочивания многочленов на каждом шаге мы можем добиться того, чтобы на последнем шаге был получен многочлен от заданной переменной. Исследование системы из таких многочленов позволяет найти все корни исходной системы. Для краткости будем называть эту итеративную процедуру R-преобразованием системы. Вообще говоря, её результат не определён однозначно.

Обобщая подход работы [7], введём следующие понятия.

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

Мы будем писать просто нетривиальное решение, если из контекста ясно, что речь идёт о нетривиальном решении обобщённого норменного уравнения.

Пусть задано нетривиальное решение обобщённого норменного уравнения. Определим коэффициенты a_i, b_t, h_j, f_l из следующих равенств:

$$\mu_1 = \sum_i a_i x^i;\ \ \mu_2 = \sum_t b_t x^t;\ \ d_1 = \sum_j h_j x^j;\ \ d_2 = \sum_l f_l x^l.$$

Определение 2. Нетривиальное решение норменного уравнения (1) является также решением полиномиальной системы с переменными a_i, b_t, h_j, f_l. Назовём такую систему системой обобщённого норменного уравнения.

Определение 3. Будем называть преобразование нетривиального решения обобщённого нор-

менного уравнения над полем k допустимым преобразованием, если для некоторого $\gamma \in k\setminus\{0\}$ оно переводит набор $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ в один из следующих наборов:

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

$$\Gamma_{2,\gamma}(\Omega) = (\gamma\mu_1, \gamma\mu_2, d_1, d_2, \gamma^2 b),$$

$$\Gamma_{3,\gamma}(\Omega) = (\gamma\mu_1, \mu_2, d_1, \gamma^2 d_2, \gamma^2 b),$$

$$\Gamma_{4,\gamma}(\Omega) = (\mu_1, \mu_2, \gamma d_1, \gamma d_2, \gamma b),$$

или преобразование, полученное путём последовательного применения вышеперечисленных преобразований.

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 задают отношение эквивалентности на нетривиальных решениях, что с учётом соотношения $f = d_1 d_2$ некоторым образом обобщает введённое выше отношение эквивалентности и отношение эквивалентности из работы [7]. Заметим, что допустимые преобразования меняют коэффициенты многочленов μ_1, μ_2, d_1, d_2 и константу b.

Обозначим через $lc(f)$ старший коэффициент многочлена f. Доказательство следующей леммы нетрудно провести с использованием допустимых преобразований по аналогии с доказательством похожих лемм в работе [7].

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

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

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

3) *при условии $b_i, b_t, a_j, h_l \in k\setminus\{0\}$ существует нетривиальное решение над $\overline{k}$ с $b_i = b_t = a_j = h_l = 1$.*

Доказательство теоремы 1 и теоремы 2. По теореме 3 для того, чтобы $\sqrt{f}$ был периодичен, необходимо и достаточно при фиксированной степени фундаментальной S-единицы найти решение уравнения (1) для наименьшего m. Из результатов работ [9, 12] и теоремы 3 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, в условиях теорем 1 и 2 по теореме 3 нам необходимо исследовать решения системы обобщённого норменного уравнения, построенной по (1), для следующих значений $\deg d_1$ и m:

$$\deg d_1 = 0,\ m = 5, 7, 9, 11;\ \deg d_1 = 1,\ m = 4, 6, 8;$$
$$\deg d_1 = 2,\ m = 5, 7, 9. \qquad (2)$$

Отметим, что конечность числа решений для $m = 11,\ \deg d_1 = 0$ была доказана в [7] с использованием базисов Грёбнера, а случаи $m \le 3$ не могут давать нужных нам решений за исключением тривиального случая $m = 3,\ \deg d_1 = 0$, описанного, например, в [12].

Ясно, что $h_0 \ne 0,\ a_0 \ne 0,\ b_0 \ne 0,\ f_0 \ne 0$, иначе, сокращая на x в (1), заключаем, что m не минимально вопреки предположению. Из сравнения степеней левой и правой частей (1) и теоремы 3 нетрудно видеть, что $lc(\mu_2) = b_{(m-\deg d_2)/2} \ne 0$. В условиях теорем 1 и 2 не существует решений системы с $f_1 = 0$. Действительно, в противном случае, согласно пункту 3 леммы, существует решение над полем $\overline{k}$ с $f_1 = 0$ системы норменного уравнения с $b_0 = lc(\mu_2) = a_0 = h_0 = 1$. Однако же базис Грёбнера этой системы обобщённого норменного уравнения для каждой пары $(\deg d_1, m)$ из перечня (2) состоит из единицы, что равносильно отсутствию решений.

Для каждой из исследуемых систем, соответствующих парам из перечня (2), применим R-преобразование системы. В каждом из случаев получается ненулевой многочлен от каждой из переменных, что завершает доказательство теоремы 1.

Приведём цепочку рассуждений лишь для случая $\deg d_1 = 0,\ m = 7$. Исходная система в этом случае выглядит следующим образом:

$$\begin{gathered}
b_0^2 f_0 - a_0^2 = 0,\\
2b_0b_1f_0 + b_0^2 f_1 - 2a_0a_1 = 0,\\
b_1^2 f_0 + 2b_0b_2f_0 + 2b_0b_1f_1 + b_0^2 f_2 - a_1^2 - 2a_0a_2 = 0,\\
2b_1b_2f_0 + b_1^2 f_1 + 2b_0b_2f_1 + 2b_0b_1f_2 + b_0^2 f_3 - 2a_1a_2 = 0,\\
b_2^2 f_0 + 2b_1b_2f_1 + b_1^2 f_2 + 2b_0b_2f_2 + 2b_0b_1f_3 - a_2^2 = 0,\\
b_2^2 f_1 + 2b_1b_2f_2 + b_1^2 f_3 + 2b_0b_2f_3 = 0,\\
b_2^2 f_2 + 2b_1b_2f_3 = 0.
\end{gathered} \qquad (3)$$

Применим лемму и положим $f_0 = f_1 = b_2 = 1$. По аналогии с подходом из работы [7] мы можем выразить переменные a_0, a_1. Подставив в (3) их выражения $a_0 = -b_0,\ a_1 = -\frac{1}{2}d_0 - d_1$, получаем систему из 4 уравнений и 4 неизвестных:

$$-\frac{1}{2}b_0f_2 + b_1f_2 + b_0f_3 + \frac{1}{8}b_0 - \frac{1}{4}b_1 + 1 = 0;$$

$$\begin{gathered}-\frac{1}{4}b_0^2f_2^2+\frac{1}{8}b_0^2f_2-\frac{1}{2}b_0b_1f_2+b_1^2f_2+2b_0b_1f_3\\ -\frac{1}{64}b_0^2+\frac{1}{8}b_0b_1-\frac{1}{4}b_1^2+b_0f_2+\frac{1}{4}b_0+b_1=0\\ b_1^2f_3+2b_1f_2+2b_0f_3+1=0;\\ 2b_1f_3+f_2=0.\end{gathered}\qquad(4)$$

Вычисляя последовательные результанты в ходе R-преобразования системы, получаем ненулевой многочлен от одной переменной для каждой из переменных b_0, b_1, f_2, f_3. Полученная система с необходимостью имеет решения над $\overline{\mathbb{Q}}$, если решения над $\overline{\mathbb{Q}}$ имела система (3):

$$\begin{gathered}(3b_0-64)b_0^9(225b_0^2-816b_0+256)^2=0,\\ (3b_1+4)^2(3b_1-4)^3b_1^5(45b_1^2-204b_1+80)=0,\\ f_2^2(f_2-1)^2(2f_2+1)^3(4f_2-1)^4(4f_2^2-26f_2-5)=0,\\ (8f_3-3)^2(16f_3-3)^3f_3^6(256f_3^2+1968f_3-45)=0.\end{gathered}\qquad(5)$$

При вычислениях результанта в ходе R-преобразования системы на шагах, приводящих к многочленам от переменных f_2 и f_3, происходит сокращение на один нетривиальный общий множитель f_3^2. Сокращение в обоих случаях корректно, так как $\deg d_2=3$.

При построении многочлена 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 на второй множитель корректно, так как базис Грёбнера системы (4), дополненной этим уравнением, содержит многочлен b_0, а $b_0\neq 0$.

При построении многочлена от переменной b_1 мы не получаем в процессе нетривиальных общих множителей, отличных от константы, в этом случае сокращений не возникает.

Нетрудно видеть, что с точностью до инволюции поля констант система (5) имеет не более одного интересующего нас решения над каким-либо полем k. Причём единственное решение с $b_0\neq 0$ с точностью до инволюции поля, 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 (5) каждая из исследуемых переменных b_0, b_1, f_2, f_3 может принимать не более чем конечное число значений для любого поля k.

СПИСОК ЛИТЕРАТУРЫ

1. *Abel N.H.* Ueber die integration der differential-formel $\rho dx/\sqrt{R}$ wenn r und ρ ganze functionen sind // J. für die reine und angewandte Mathematik. 1826. V. 1. S. 185–221.
2. *Tchebicheff P.* Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré' // J. des math. pures et appl. 1857. V. 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 мат. 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. V. 95. № 2. P. 139–166.
5. *Петрунин М.М.* S-единицы и периодичность квадратного корня в гиперэллиптических полях // ДАН. 2018. Т. 474. № 2. С. 155–158.
6. *Платонов В.П., Федоров Г.В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Мат. сб. 2018. Т. 4. № 209. С. 54–94.
7. *Платонов В.П., Жгун В.С., Петрунин М.М., Штейников Ю.Н.* О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // ДАН. 2018. Т. 483. № 6. С. 603–608.
8. *Платонов В.П., Жгун В.С., Федоров Г.В.* О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант // ДАН. 2018. Т. 482. № 2. С. 137–141.
9. *Беняш-Кривец В.В., Платонов В.П.* Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Мат. сб. 2009. Т. 200. № 11. С. 15–44.
10. *Kenku M.A., Momose F.* Torsion points on elliptic curves defined over quadratic fields // Nagoya Math. J. 1988. V. 109. P. 125–149.
11. *Kamienny Sh., Najman F.* Torsion groups of elliptic curves over quadratic fields // Acta Arithmetica. 2012. V. 3. № 152. P. 291–305.
12. *Платонов В.П., Петрунин М.М.* Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Тр. МИАН. 2018. Т. 302. С. 354–376.

ON THE FINITENESS OF THE NUMBER OF ELLIPTIC FIELDS WITH GIVEN DEGREES OF *S*-UNITS AND PERIODIC EXPANSION OF $\sqrt{f}$

Academician of the RAS V. P. Platonov[1,2], M. M. Petrunin[1], Yu. N. Shteinikov[1]

[1] *Scientific Research Institute for System Analysis, Russian Academy of Sciences, Moscow, Russian Federation*

[2] *Steklov Mathematical Institute, Russian Academy of Sciences, Moscow, Russian Federation*

Received July 1, 2019

For a field k of characteristic 0, up to a natural equivalence relation, it is proved that the number of nontrivial elliptic fields $k(x)(\sqrt{f})$ with a periodic expansion of $\sqrt{f} \in k((x))$, for which the corresponding elliptic curve contains a k-point of even order less or equal than 18 or k-point of odd order less or equal than 11, is finite. In case k is a quadratic extension of $\mathbb{Q}$, all such fields are found.

Keywords: elliptic field, *S*-unit, continued fraction, periodicity, Gröbner basis, resultant.