ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2022, том 505, с. 56–62

МАТЕМАТИКА

УДК 511.6

О ПРОБЛЕМЕ ОПИСАНИЯ ЭЛЕМЕНТОВ ЭЛЛИПТИЧЕСКИХ ПОЛЕЙ С ПЕРИОДИЧЕСКИМ РАЗЛОЖЕНИЕМ В НЕПРЕРЫВНУЮ ДРОБЬ НАД КВАДРАТИЧНЫМИ ПОЛЯМИ КОНСТАНТ

Г. В. Федоров[1,*]

Представлено академиком РАН В.П. Платоновым
Поступило 03.03.2022 г.
После доработки 11.03.2022 г.
Принято к публикации 01.06.2022 г.

Для всех квадратичных числовых полей K получено описание свободных от квадратов многочленов $f(x) \in K[x]$ степени 4 таких, что $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$, а эллиптическое поле $\mathcal{L} = K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени m, $4 \le m \le 12$, $m \ne 11$, где множество S состоит из двух сопряженных нормирований, определенных на поле $\mathcal{L}$ и связанных с униформизующей x поля $K(x)$.

Ключевые слова: непрерывная дробь, фундаментальная S-единица, эллиптическое поле, группа классов дивизоров, круговые многочлены

DOI: 10.31857/S2686954322040087

1. ВВЕДЕНИЕ

Пусть $f(x) \in K[x]$ – свободный от квадратов многочлен степени $2g + 2$, $g \ge 0$, над полем K характеристики, отличной от 2. Дополнительно предположим, что старший коэффициент многочлена f является полным квадратом в мультипликативной группе K^* поля K. Проблема периодичности непрерывных дробей элементов гиперэллиптических полей $\mathcal{L} = K(x)(\sqrt{f})$, построенных в поле $K((x^{-1}))$, приобрела широкую известность еще с работ Абеля и Чебышева, и с тех пор проявлялась в различных разделах теории чисел, анализа и алгебраической геометрии. Современные результаты о периодичности непрерывной дроби $\sqrt{f}$ и эквивалентных условиях изложены в [1–3]. В частности, из этих результатов следует, что в поле $\mathcal{L}$ элемент $\sqrt{f}$ и его разложение в непрерывную дробь играют ключевую роль в вопросах, связанных с поиском фундаментальных единиц и рациональных точек кручения в якобиане гиперэллиптической кривой, заданной уравнением $y^2 = f(x)$.

Пусть теперь $f(x)$ – свободный от квадратов многочлен произвольной степени, и свободный член многочлена $f(x)$ является полным квадратом в группе K^*. В статье [4] доказано следующее утверждение: если для некоторого $s \in \mathbb{Z}$ непрерывная дробь элемента $\sqrt{f}/x^s$, построенная в $K(x)$, квазипериодическая, то она периодическая. В статье [1] сформулирована естественная задача об исследовании периодичности непрерывной дроби элемента $\sqrt{f}$, построенной в поле формальных степенных рядов $K((x))$. А именно, в этой статье сформулирована проблема описания числовых полей K и многочленов $f(x) \in K[x]$, для которых элемент $\sqrt{f}$ имеет периодическую непрерывную дробь, построенную в поле $K((x))$. В статьях [1] и [5] эта проблема полностью решена для эллиптических полей над полем $K = \mathbb{Q}$ рациональных чисел. В [5] сформулирована гипотеза о конечности с точностью до естественного отношения эквивалентности многочленов $f(x)$ над числовыми полями K, являющимися расширениями поля $\mathbb{Q}$ ограниченной степени, с периодическим разложением элемента $\sqrt{f}$ в непрерывную дробь в поле $K((x))$. В статьях [7, 8] эта проблема решена для кубических многочленов $f(x)$, определенных над полями K, $[K : \mathbb{Q}] \le 4$, а в случае $[K : \mathbb{Q}] = 2$ в [6, 7] дано явное описание таких пар $[K, f(x)]$, что $\deg f = 3$ и $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле $K((x))$.

[1] *Университет "Сириус", Сочи, Россия*
**E-mail: fedorov@mech.math.msu.su*

Определим множество S, состоящее из двух сопряженных нормирований, которые определены на поле $\mathcal{L}$ и связаны с униформизующей x поля $K(x)$. Мы продолжаем исследование периодических элементов вида $\sqrt{f}$, $f \in K[x]$ в случае квадратичных полей K и $\deg f = 4$. Найдено полное описание таких свободных от квадратов многочленов f, что $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$, а эллиптическое поле $K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени m, $4 \le m \le 12$, $m \ne 11$.

2. ВСПОМОГАТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

Для натуральных n определим две последовательности многочленов $T_n, Q_n \in \mathbb{Z}[x]$:

$$T_n(x) = \sum_{0 \le j \le n/2} \binom{n}{2j} x^j, \quad Q_n(x) = \sum_{0 \le j < n/2} \binom{n}{2j+1} x^j. \tag{1}$$

Из определения следует, что $\deg T_n = \left[\frac{n}{2}\right]$, $\deg Q_n = \left[\frac{n-1}{2}\right]$. Положим $x = y^2$, тогда справедливо тождество

$$T_n(y^2) + yQ_n(y^2) = \sum_{0 \le k \le n} \binom{n}{k} y^k = (1+y)^n. \tag{2}$$

Если подставить вместо y значение $-y$, то имеем $T_n(y^2) - yQ_n(y^2) = (1-y)^n$. Отсюда получаем формулы, которые можно использовать как альтернативное определение многочленов T_n, Q_n:

$$T_n(y^2) = \frac{1}{2}((1+y)^n + (1-y)^n),$$

$$Q_n(y^2) = \frac{1}{2y}((1+y)^n - (1-y)^n).$$

При любом $n \in \mathbb{N}$ многочлены $T_n(x)$ и $Q_n(x)$ взаимно просты и не имеют кратных корней.

Из (2) следует, что для любых $n, m \in \mathbb{N}$ справедливы тождества

$$\begin{aligned} T_{nm}(x) &= (T_n(x))^m \cdot T_m(z), \\ Q_{nm}(x) &= (T_n(x))^{m-1} \cdot Q_n(x) \cdot Q_m(z), \end{aligned} \tag{3}$$

где $z = x(Q_n(x)/T_n(x))^2$. В частности,

$$Q_{2n}(x) = 2T_n(c)\, Q_n(c). \tag{4}$$

Пусть K – числовое поле, и даны числа n, $m \in \mathbb{N}$. Из формул (3) следует, что, если у многочленов $T_n(x)$, $Q_n(x)$, $T_m(x)$ и $Q_m(x)$ нет корней в поле K, то у многочленов $T_{nm}(x)$ и $Q_{nm}(x)$ также нет корней в поле K.

3. МНОЖЕСТВО КОРНЕЙ $T_n(x)$ И $Q_n(x)$, НАД КВАДРАТИЧНЫМИ ПОЛЯМИ

В статье [9] были найдены все рациональные корни многочленов $T_n(x)$ и $Q_n(x)$, определенных в (1), при всех натуральных n: для многочленов $T_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-1, -1/3\}$, более точно, $T_{2(2k-1)}(-1) = 0$, $T_{3(2k-1)}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет; для многочленов $Q_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-3, -1, -1/3\}$, более точно, $Q_{3k}(-3) = 0$, $Q_{4k}(-1) = 0$, $Q_{6k}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет.

Исследуем последовательности многочленов $T_n(x)$ и $Q_n(x)$, на наличие корней в квадратичных полях. Запишем явные выражения для этих многочленов при $n \le 6$:

$$T_1(x) = 1, \quad Q_1(x) = 1, \quad T_2(x) = x + 1, \quad Q_2(x) = 2,$$

$$T_3(x) = 3x + 1, \quad Q_3(x) = x + 3,$$

$$T_4(x) = x^2 + 6x + 1, \quad Q_4(x) = 4(x + 1),$$

$$T_5(x) = 5x^2 + 10x + 1, \quad Q_5(x) = x^2 + 10x + 5,$$

$$T_6(x) = (x+1)(x^2 + 14x + 1),$$

$$Q_6(x) = 2(x+3)(3x+1).$$

По критерию Эйзенштейна из (1) при простых n многочлены $T_n(x)$ и $Q_n(x)$ неприводимы, причем при $n \ge 7$ степени многочленов $T_n(x)$ и $Q_n(x)$ больше 3, поэтому при простых n многочлены $T_n(x)$ и $Q_n(x)$ корней в квадратичных полях не имеют. Обозначим множество различных корней многочленов $T_n(x)$ и $Q_n(x)$ при $n \le 6$ через M. Имеем

$$\begin{gathered} M = \Big\{-1, -\frac{1}{3}, -3, -3 \pm 2\sqrt{2}, \\ \frac{-5 \pm 2\sqrt{5}}{5}, -5 \pm 2\sqrt{5}, -7 \pm 4\sqrt{3}\Big\}. \end{gathered} \tag{5}$$

Покажем, что других корней в квадратичных полях, кроме корней из множества M, многочлены $T_n(x)$ и $Q_n(x)$, $n \in \mathbb{N}$, не имеют.

Рассуждая по индукции по числу простых множителей числа n, с помощью формул (3) получаем следующее утверждение.

П р е д л о ж е н и е. При $n \in \mathbb{N}$ таких, что $n \not\equiv 0 \pmod 2$, $n \not\equiv 0 \pmod 3$, $n \not\equiv 0 \pmod 5$, многочлены $T_n(x)$ и $Q_n(x)$ в квадратичных полях корней не имеют.

Таким образом, корни многочленов $T_n(x)$ и $Q_n(x)$ из квадратичных полей могут быть только при n, кратных 2, 3 или 5.

Теорема 1. *Множество корней последовательностей многочленов $T_n(x)$ и $Q_n(x)$, принадлежащих квадратичным полям, исчерпывается множеством M, определенном в* (4).

Доказательство. Пусть для некоторого $n \in \mathbb{N}$ имеем $T_n(a) = 0$, причем $a \not\in M$ — элемент некоторого квадратичного поля. Представим $n = n_1 \cdot m_1$, где $n_1 = 2^\alpha 3^\beta 5^\gamma$, а число m_1 не имеет простых делителей меньше 7. Предположим, что $T_{n_1}(a) \neq 0$, тогда из (3) следует, что $T_{m_1}(b) = 0$, где $b = a(Q_{n_1}(a)/T_{n_1}(a))^2$. Но этого не может быть, так как b, как и a, принадлежит квадратичному полю. Значит, $T_{n_1}(a) = 0$ для $a \not\in M$.

Если n_1 четно, то представим $n_1 = 2m_1$. Так как $T_2(a) \neq 0$, ибо $a \not\in M$, то из (3) следует, что $T_{m_1}(b_1) = 0$, где $b_1 = a(Q_2(a)/T_2(a))^2$. Покажем, что из того, что $a \not\in M$ следует, что $b_1 \not\in M$. Предположим противное, т.е. $b_1 \in M$. Перебрав все возможные значения для $b_1 \in M$, видим, что значения a, удовлетворяющие уравнению $b_1 = a(Q_2(a)/T_2(a))^2$, либо принадлежат множеству M, либо не являются элементами квадратичных полей, что противоречит начальному предположению о корне a многочлена $T_n(x)$. Таким образом, $b_1 \not\in M$ и $T_{m_1}(b_1) = 0$. Если m_1 четно, то снова представим $m_1 = 2m_2$, и, рассуждая аналогично, придем к тому, что должно существовать число $b_2 \not\in M$ такое, что $T_{m_2}(b_2) = 0$. Повторяя эти рассуждения необходимое количество раз, получаем, что должен существовать элемент $b_\alpha \not\in M$ некоторого квадратичного поля такой, что $T_{m_\alpha}(b_\alpha) = 0$, причем $m_\alpha = 3^\beta 5^\gamma$. Далее, если $\beta > 0$, то представим $m_\alpha = 3k$. Так как $T_3(b_\alpha) \neq 0$, ибо $b_\alpha \not\in M$, то из (3) следует, что $T_k(c) = 0$, где $c = b_\alpha(Q_3(b_\alpha)/T_3(b_\alpha))^2$. Перебирая все возможные значения $c \in M$, приходим к выводу, что либо $b_\alpha \in M$, либо b_α не является элементом квадратичного поля, что противоречит нашему предположению об элементе b_α. Значит, $c \not\in M$ — такой элемент квадратичного расширения, что $T_k(c) = 0$. При необходимости рассуждая аналогично, можно считать, что $k = 5^\gamma$. Если $\gamma > 1$, то представим $k = 5k_1$. Так как $T_5(c) \neq 0$, ибо $c \not\in M$, то из (3) следует, что $T_{k_1}(c_1) = 0$, где $c_1 = c(Q_5(c)/T_5(c))^2$. Перебирая все возможные значения $c_1 \in M$, приходим к выводу, что либо $c \in M$, либо c не является элементом квадратичного поля, что противоречит нашему предположению об элементе c. Значит, $c_1 \not\in M$ — такой элемент квадратичного расширения, что $T_{k_1}(c_1) = 0$. При необходимости рассуждая аналогично, можно считать, что $k_1 = 5$. Но все корни $T_5(x)$ лежат в M, что приводит нас к противоречию. Таким образом, у многочлена $T_n(x)$ не может быть других корней из квадратичного поля, кроме корней, указанных в множестве M.

Для многочлена $Q_n(x)$ рассуждения полностью аналогичны.

Теорема 1 доказана.

4. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Обозначим через $\mathcal{U}_0$ множество пар $[K, f(x)]$, состоящих из числового поля K и свободного от квадратов многочлена $f \in K[x]$, $\deg f = 4$, имеющего периодическое разложение $\sqrt{f}$ в непрерывную дробь в поле $K((x))$. Множество пар $[K, f(x)]$ в $\mathcal{U}_0$ будем рассматривать с точностью до отношения эквивалентности, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx)$ для $a, b \in K^*$ и заменой $f(x)$ на $f^\sigma(x)$, где $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Для $[K, f(x)] \in \mathcal{U}_0$ в силу критерия из [1] (теорема 1) эллиптическое поле $L = K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени N, где множество $S = \{v_x^-, v_x^+\}$ состоит из двух сопряженных нормирований, являющихся продолжением нормирования v_x поля $K(x)$. Отсюда следует, что класс дивизора $v_x^- - v_x^+$ имеет конечный порядок N в группе классов дивизоров $\Delta^\circ(L)$, причем в случае $K = \mathbb{Q}$ из [10] следует, что $N \le 12$, $N \neq 11$, а в случае $[K : \mathbb{Q}] = 2$ из [11] следует, что $N \le 18$, $N \neq 17$.

Обозначим за $\mathcal{U}$ множество троек $[K, f(x), N]$, где $[K, f(x)] \in \mathcal{U}_0$ и N — степень соответствующей фундаментальной S-единицы поля $L = K(x)(\sqrt{f})$.

Теорема 2. *Пусть* $[K : \mathbb{Q}] \le 2$. *Множество троек* $[K, f(x), N]$, *входящих в множество* $\mathcal{U}$ *и определяющих эллиптическое поле* $L = K(x)(\sqrt{f})$, *содержащее фундаментальную S-единицу степени N*, $4 \le N \le 12$, $N \neq 11$, *описывается следующим образом*

$$\left[\mathbb{Q}, -\frac{3x^4}{4} - 3x^3 - 2x^2 - 2x + 1, 4\right],$$

$$\left[\mathbb{Q}(\sqrt{3}), \frac{36 - 21\sqrt{3}}{2}x^4 + (15 - 9\sqrt{3})x^3 + \right.$$
$$\left. + (4 - 3\sqrt{3})x^2 - 2x + 1, 4\right],$$

$$\left[\mathbb{Q}, -1280x^4 + 192x^3 - 28x^2 + 4x + 1, 5\right],$$

$$\left[\mathbb{Q}, \frac{128000x^4}{243} + \frac{1280x^3}{9} + \frac{368x^2}{27} - \frac{8x}{3} + 1, 6\right],$$

$$\left[\mathbb{Q}, -56000x^4 + 3360x^3 + 84x^2 + 4x + 1, 7\right],$$

$$\left[\mathbb{Q}(\sqrt{-7}), \frac{(35-9\sqrt{-7})x^4}{2} + \frac{(33-3\sqrt{-7})x^3}{2} + \right.$$
$$\left. + \frac{(41+5\sqrt{-7})x^2}{8} - \frac{(3+\sqrt{-7})x}{2} + 1, 7\right],$$

$$\left[\mathbb{Q}(\sqrt{21}), \frac{(34383\sqrt{21}-157563)x^4}{2} + \right.$$
$$+ (1938 - 423\sqrt{21})x^3 +$$
$$\left. + \frac{(567\sqrt{21}-2605)x^2}{8} + \frac{(11-3\sqrt{21})x}{2} + 1, 7\right].$$

Обозначим через $X_1(N)$ модулярную кривую, чьи K-точки отвечают с точностью до изоморфизма парам (E, P_N), где E — эллиптическая кривая, определенная над K, P_N — K-точка порядка N на E. Ограничение в теореме 2 на степень N фундаментальной S-единицы обусловлено тем фактом, что в случае $N \le 12$, $N \ne 11$ кривые $X_1(N)$ рациональны, и дают так называемую рациональную параметризацию множества пар (E, P_N) в зависимости от единственного параметра t (явное представление см. в [12]). Для $N = 11$ и $N \ge 13$ кривые $X_1(N)$ перестают быть рациональными, и эти случаи являются темой для дальнейших исследований.

Доказательство теоремы 2 является обобщением доказательства основных результатов статьи [5], проведенных над полем $\mathbb{Q}$, на случай квадратичных полей констант. Отметим, что рассуждения нельзя назвать аналогичными, поскольку при расширениях поля $\mathbb{Q}$ существенным образом изменяется множество M корней многочленов $T_n(x)$ и $Q_n(x)$, определенных в (1). Для квадратичных расширений в теореме 1 явно найдены элементы множества M — их конечное число, что дает конечное число вариантов уравнений, связывающих параметры семейств эллиптических кривых, имеющих точку порядка N, $N \le 12$, $N \ne 11$. Указанная связь возникает из условия периодичности разложения $\sqrt{f}$ в непрерывную дробь в поле $K((x))$, и явно представлена в теореме 4 [5].

Кроме того, ввиду необходимости объемных символьных компьютерных вычислений над квадратичными полями, была существенно изменена программная реализация используемых алгоритмов.

5. СХЕМА ДОКАЗАТЕЛЬСТВА

Пусть K – числовое поле. Для каждого $4 \le N \le 12$, $N \ne 11$, в [13, 14] явно выписано полное параметрическое семейство приведенных многочленов $F = F(X, c) \in \mathbb{Q}[X]$ четвертой степени с параметром $c \in K$ таких, что класс дивизора — имеет порядок N в группе классов дивизоров степени ноль $\Delta^\circ(\mathscr{L})$ поля $\mathscr{L} = K(X)(\sqrt{F(X,c)})$. Здесь приведенность многочлена F понимается в смысле дополнительных ограничений: коэффициент при X^3 равен нулю, свободный член равен 1. При всевозможных значениях параметра $c \in K$, для которых дискриминант $F(X,c)$ не обращается в ноль, указанные параметрические семейства содержат все приведенные многочлены F четвертой степени над полем K, такие, что выполнены равносильные условия:

- непрерывная дробь элемента $\sqrt{F}$ в в поле $K((1/X))$ периодическая;
- норменное уравнение

$$\Omega_1^2 - \Omega_2^2 F = b \tag{6}$$

имеет решение $\Omega_1, \Omega_2 \in K[X]$, $\Omega_2 \ne 0$, для некоторого $b \in K^*$.

Если пара многочленов Ω_1, Ω_2 является решением норменного уравнения (6) с минимальной степенью $\deg \Omega_1$, причем $\Omega_2 \ne 0$, то $\deg \Omega_1 = N$ и $\Omega_1 + \Omega_2\sqrt{F}$ является фундаментальной единицей поля $\mathscr{L} = K(X)(\sqrt{F})$. По теореме 4 [5] периодичность непрерывной дроби элемента $X^s\sqrt{F}$ равносильна разрешимости норменного уравнения вида (6) с дополнительными условиями на значения $v_X(\Omega_1)$ и $v_X(\Omega_2)$, но теперь $\Omega_1 + \Omega_2\sqrt{F}$ может не являться фундаментальной единицей, а может быть некоторой степенью k фундаментальной единицы, причем из теоремы 1 следует, что в случае $[K : \mathbb{Q}] \le 2$ степень k ограничена числом 6 (см. [15]).

Обозначим через p_j/q_j, $j \in \mathbb{N}_0$, подходящие дроби к $\sqrt{F(X,c)}$, причем $p_j = p_j(X,c)$, $q_j = q_j(X, c) \in \mathbb{Q}(c)[X]$. Положим $K = \mathbb{Q}(c)$. Тогда фундаментальная единица поля $\mathscr{L} = K(X)(\sqrt{F})$ имеет вид $p_n + q_n\sqrt{F}$ для некоторого минимального $n \in \mathbb{N}$ такого, что $p_n^2 - q_n^2 F \in K^*$ (см. [2]). Обозначим $\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{F} = (p_n + q_n\sqrt{F})^j$, где $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[X]$, $j \in \mathbb{N}$. Положим $r_j = v_X\left(\Omega_2^{(j)}\right)$, тогда согласно теореме 1 в силу (4) возможны только следующие 8 случаев: $r_n > 0$ при том, что $r_j = 0$, если $1 \le j < n$, для каждого $n \in \Lambda = \{1,3,4,5,6,8,10,12\}$. Отметим, что, если для некоторого $n \in \mathbb{N}$ выполнено

$r_n > 0$, то непрерывная дробь элемента $\sqrt{F}/X^{r_n}$, построенная в поле $K((1/X))$ периодическая.

Замена X на $X + t$ соответствует изоморфизму кривых $C : Y^2 = F(X)$ и $C_t : Y^2 = F(X + t)$. Тем самым, с точностью до отношения эквивалентности, определяемого допустимыми заменами $F(X)$ на $a^2F(bX)$ для некоторых $a, b \in K^*$, имеем полное описание всех многочленов $F = F(c,t) \in \mathbb{Q}[X]$, $\deg F = 4$, для которых разложение $\sqrt{F}$ в непрерывную дробь в поле $\mathbb{Q}(c,t)((1/X))$ периодично. Наша задача сводится к поиску всех значений параметров $c, t \in K$ для каждого из случаев $v_X\left(\Omega_2^{(j)}\right) > 0$, $n \in \Lambda$, причем мы ограничиваемся квадратичными расширениями, $K = \mathbb{Q}(c,t)$, $[K : \mathbb{Q}] \le 2$.

Необходимым и достаточным условием периодичности непрерывной дроби $\sqrt{F(X+t,c)}/X$ в $K((1/X))$ является $\Omega_2^{(n)}(t) = 0$ хотя бы для одно из $n \in \Lambda$. Для того, чтобы непрерывная дробь $\sqrt{F(X+t,c)}/X^2$ была периодической, необходимо и достаточно, чтобы $r_n = v_X\left(\Omega_2^{(n)}\right) \ge 2$ для некоторого $j \in \Lambda$, т.е. $\Omega_2^{(n)}(t) = 0$ и $\frac{\mathrm{d}}{\mathrm{d}t}\Omega_2^{(n)}(t) = 0$, что возможно только тогда, когда дискриминант $d = d^{(n)}(c)$ многочлена $\Omega_2^{(n)}(t) \in \mathbb{Q}(c)[t]$ равен нулю. То есть задача сводится к поиску корней c_0 дискриминанта $d^{(n)}(c)$ и соответствующих кратных корней t_0 многочлена $\Omega_2^{(n)}(t) \in \mathbb{Q}(c_0)[t]$ для каждого из $n \in \Lambda$, причем ограничиваемся значениями параметров c_0, t_0 из квадратичных полей и таких, что дискриминант многочлена $F(X + t_0, c_0) \in \mathbb{Q}(c_0, t_0)[X]$ отличен от нуля. Если найдены все подходящие значения параметров c_0, t_0, то для доказательства теоремы 2 достаточно положить $f(x) = x^4F(1/x + t_0, c_0) \in K[x]$ и отобрать представителей с точностью до указанного в определении множества $\mathcal{U}_0$ отношения эквивалентности.

Изложенная схема доказательства существенным образом опирается на большие символьные компьютерные вычисления. Программный код реализовывался на языке программирования Python с использоваем библиотеки Sympy. Без подобных вычислений получить заявленные результаты не представляется возможным.

6. ЗАКЛЮЧЕНИЕ

Приведем новые примеры непрерывных дробей, которые определены над полями K, $[K : \mathbb{Q}] = 2$.

Пример 1. *Рассмотрим* $K = \mathbb{Q}(\sqrt{3})$ *и*

$$f = \frac{36 - 21\sqrt{3}}{2}x^4 + (15 - 9\sqrt{3})x^3 + (4 - 3\sqrt{3})x^2 - 2x + 1.$$

Непрерывная дробь $\sqrt{f}$ *в поле* $\mathbb{Q}(\sqrt{3})((x))$ *имеет вид*

$$\Bigg[1, -x - \frac{3(1-\sqrt{3})}{2}; \overline{\frac{2x(12+7\sqrt{3})}{9} - 5 - 3\sqrt{3},}$$
$$\overline{\frac{2x^4(3-2\sqrt{3})}{9} - \frac{2x^3(3-2\sqrt{3})}{9} + \frac{x^2(9-5\sqrt{3})}{3} + 2x(7-4\sqrt{3}) + 3(7-4\sqrt{3}),}$$
$$\overline{\frac{2x(12+7\sqrt{3})}{9} - 5 - 3\sqrt{3}, -x - \frac{2-3\sqrt{3}}{2}, 4x + 2(2-3\sqrt{3})}^{-1/4}\Bigg].$$

Длина квазипериода равна 5, *коэффициент квазипериода равен* $-1/4$, *длина периода равна* 10. *Степень фундаментальной* S*-единицы равна* 4.

Пример 2. *Рассмотрим* $K = \mathbb{Q}(\sqrt{-7})$ *и*

$$f = \frac{(35 - 9\sqrt{-7})x^4}{2} + \frac{(33 - 3\sqrt{-7})x^3}{2} + \frac{(41 + 5\sqrt{-7})x^2}{8} - \frac{(3 + \sqrt{-7})x}{2} + 1.$$

Непрерывная дробь $\sqrt{f}$ *в поле* $\mathbb{Q}(\sqrt{-7})((x))$ *имеет вид*

$$\Bigg[1, -\frac{x(3+\sqrt{-7})}{4} + 1 - \sqrt{-7}; \overline{\frac{x(1+\sqrt{-7})}{32} + \frac{3(1-3\sqrt{-7})}{64},}$$

$$\overline{\frac{x^3(47+45\sqrt{-7})}{128}-\frac{x^2(67-23\sqrt{-7})}{32}-\frac{x(31-3\sqrt{-7})}{4}+11-\sqrt{-7},}$$
$$\overline{\frac{x(1+\sqrt{-7})}{32}+\frac{3(1-3\sqrt{-7})}{64},-\frac{x(3+\sqrt{-7})}{4}+\frac{(3-2\sqrt{-7})}{2},}$$
$$\left.\overline{x(3+\sqrt{-7})-2(3-2\sqrt{-7})}^{\,-1/4}\right].$$

Длина квазипериода равна 5, *коэффициент квазипериода равен* $-1/4$, *длина периода равна* 10. *Степень фундаментальной* S*-единицы равна* 7.

П р и м е р 3. *Рассмотрим* $K=\mathbb{Q}(\sqrt{21})$ *и*

$$f=\frac{(34383\sqrt{21}-157563)x^4}{2}+$$
$$+(1938-423\sqrt{21})x^3+$$
$$+\frac{(567\sqrt{21}-2605)x^2}{8}+\frac{(11-3\sqrt{21})x}{2}+1.$$

Непрерывная дробь $\sqrt{f}$ *в поле* $\mathbb{Q}(\sqrt{21})((x))$ *имеет вид*

$$\left[1,-\frac{x(11+3\sqrt{21})}{17}+\frac{60(25-4\sqrt{21})}{289};\overline{\frac{x(8807\sqrt{21}+40377)}{7200}-\frac{3(209+45\sqrt{21})}{64},}\right.$$
$$\overline{\frac{32x^3(2811+371\sqrt{21})}{3758445}+\frac{128x^2(1566-239\sqrt{21})}{1252815}+\frac{128x(961-200\sqrt{21})}{83521}+\frac{480(9005-1961\sqrt{21})}{83521},}$$
$$\overline{\frac{x(40377+8807\sqrt{21})}{7200}-\frac{3(209+45\sqrt{21})}{64},-\frac{x(11+3\sqrt{21})}{17}+\frac{3289-480\sqrt{21}}{578},}$$
$$\left.\overline{\frac{4x(11+3\sqrt{21})}{17}-\frac{2(3289-480\sqrt{21})}{289}}^{\,-1/4}\right].$$

Длина квазипериода равна 5, *коэффициент квазипериода равен* $-1/4$, *длина периода равна* 10. *Степень фундаментальной* S*-единицы равна* 7.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Финансирование проекта осуществлялось из средств Университета “Сириус” в рамках научного проекта FMF-RND-2125.

СПИСОК ЛИТЕРАТУРЫ

1. *Платонов В.П., Федоров Г.В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209. № 4. С. 54–94.
2. *Платонов В.П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. 2014. Т. 69. № 1 (415). С. 3–38.
3. *Adams W.W., Razar M.J.* Multiples of points on elliptic curves and continued fractions // Proc. London Math. Soc. 1980. V. 41. № 3. P. 481–498.
4. *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.
5. *Платонов В.П., Федоров Г.В.* О проблеме классификации многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в гиперэллиптических полях // Известия Российской академии наук. Серия математическая. 2021. Т. 85. № 5. С. 152–189.
6. *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.
7. *Платонов В.П., Петрунин М.М., Штейников Ю.Н.* О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // ДАН. 2019. Т. 488. № 3. С. 237–242.
8. *Платонов В.П., Петрунин М.М.* О конечности числа периодических разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над полями алгебраических чисел // Доклады РАН. Математика, информатика, процессы управления. 2020. Т. 495. № 1. С. 48–54.

9. *Платонов В.П., Федоров Г.В.* Критерий периодичности непрерывных дробей ключевых элементов гиперэллиптических полей // Чебышевский сборник. 2019. Т. 20. № 1. С. 246–258.
10. *Mazur B.* Rational points on modular curves // Modular funct. one Var. V, Proc. Int. Conf., Bonn 1976. Lect. Notes Math. 1977. V. 601. P. 107–148.
11. *Kenku M.A., Momose F.* Torsion points on elliptic curves defined over quadratic fields // Nagoya Mathematical Journal. 1988. V. 109. P. 125–149.
12. *Kubert D.S.* Universal bounds on the torsion of elliptic curves // Proc. London Math.Soc. (3). 1976. Vol. 33. № 2. P. 193–237.
13. *Van Der Poorten A.J., Tran X.C.* Periodic continued fractions in elliptic function fields // International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg. 2002. P. 390–404.
14. *Scherr Z.L.* Rational polynomial pell equations // Diss. The University of Michigan. 2013. P. 1–86.
15. *Федоров Г.В.* Об ограниченности длин периодов непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел // Чебышевский сборник. 2019. Т. 20. № 4. С. 321–334.

ON THE PROBLEM OF DESCRIBING ELEMENTS OF ELLIPTIC FIELDS WITH A PERIODIC EXPANSION INTO A CONTINUED FRACTION O VER QUADRATIC FIELDS

G. V. Fedorov[a]

[a] *"Sirius University", Sochi, Russian Federation*

Presented by Academician of the RAS V.P. Platonov

For all possible quadratic number fields K, we obtain a description of the square-free polynomials $f(x) \in K[x]$ of degree 4 such that $\sqrt{f}$ has a periodic expansion into a continued fraction in the field of formal power series $K((x))$, while the elliptic field $K(x)(\sqrt{f})$ has the fundamental S-unit degree m, $4 \le m \le 12$, $m \ne 11$, where the set S consists of two conjugate valuations defined on the field $\mathscr{L}$ and related to the uniformizing x of the field $K(x)$.

Keywords: continued fraction, fundamental S-unit, elliptic field, divisor class group, cyclotomic polynomials