ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2020, том 495, с. 48–54

МАТЕМАТИКА

УДК 511.6

О КОНЕЧНОСТИ ЧИСЛА ПЕРИОДИЧЕСКИХ РАЗЛОЖЕНИЙ В НЕПРЕРЫВНУЮ ДРОБЬ $\sqrt{f}$ ДЛЯ КУБИЧЕСКИХ МНОГОЧЛЕНОВ НАД ПОЛЯМИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

© 2020 г. Академик РАН В. П. Платонов[1,2,*], М. М. Петрунин[1,]**

Поступило 15.09.2020 г.
После доработки 15.09.2020 г.
Принято к публикации 21.09.2020 г.

Получено полное описание кубических многочленов f над полями алгебраических чисел $\mathbb{K}$ степени 3 над $\mathbb{Q}$, для которых разложение $\sqrt{f}$ в непрерывную дробь в поле формальных степенных рядов $\mathbb{K}((x))$ периодично. Доказана теорема конечности для кубических многочленов $f \in K[x]$ с периодическим разложением $\sqrt{f}$ для расширений $\mathbb{Q}$ степени, не превосходящей 6, и дано полное описание таких многочленов f над произвольным полем, соответствующих эллиптическим полям с точкой кручения порядка $N \geq 30$.

Ключевые слова: эллиптическое поле, S-единицы, непрерывные дроби, периодичность, модулярные кривые, точки конечного порядка

DOI: 10.31857/S2686954320060119

Рассмотрим свободный от квадратов многочлен $f(x) \in \mathbb{K}[x]$ степени $2g + 1$ над полем алгебраических чисел $\mathbb{K}$. Предположим, что $f(x)$ не делится на x, а его младший коэффициент является полным квадратом. Тогда нормирование ν_x, соответствующее линейному многочлену x, имеет два продолжения в поле $\mathbb{K}(x)(\sqrt{f(x)})$. Следовательно, существует вложение $\sqrt{f(x)}$ (и тем самым поля $\mathbb{K}(x)(\sqrt{f(x)})$) в поле формальных рядов Лорана $\mathbb{K}((x))$, что позволяет рассмотреть разложение этого элемента или любого другого элемента поля $\mathbb{K}(x)(\sqrt{f(x)})$ в непрерывную дробь (подробнее, см. [1]). Пусть $\mathscr{C}$ – гладкая компактификация гиперэллиптической кривой $y^2 = f(x)$. Рассмотрим вложение точки $P = (0, \sqrt{f(0)})$ в якобиан $\mathscr{C}$, переводящее P в класс $P - \infty$. В случае, когда класс $P - \infty$ имеет конечный порядок в якобиане, существуют элементы поля $\mathbb{K}(x)(\sqrt{f(x)})$, разложение которых в непрерывную дробь периодично. Эти разложения обладают интересными свойствами, которые описаны в работах [1–3].

Отметим, что некоторые элементы при указанных предположениях на пару $(\mathscr{C}, P)$ заведомо периодичны: например, $\sqrt{f(x)}/x^g$ и $\sqrt{f(x)}/x^{g+1}$. В свою очередь, сам элемент $\sqrt{f(x)}$ периодичен не всегда, что является существенным отличием от случая разложения в непрерывную дробь в $\mathbb{K}((1/x))$. В связи с этим в работе [3] была поставлена проблема описания всех многочленов $f(x) \in \mathbb{K}[x]$ степени $2g + 1$ для различных классов полей алгебраических чисел $\mathbb{K}$ с квазипериодическим разложением $\sqrt{f(x)}$ в непрерывную дробь (квазипериодичность $\sqrt{f}$ равносильна периодичности, см. [2]). Там же она была полностью решена для кубических многочленов над полем рациональных чисел с использованием теоремы об ограниченности кручения и рациональной параметризации пары эллиптическая кривая и точка кручения (см. [4]). В работе [5] аналогичный результат был получен для случая многочленов f степени 4, а в работе [6] был исследован случай алгебраических полей чисел в качестве поля констант, и было предложено обобщение метода работы [3]. Это позволило полностью решить проблему периодичности $\sqrt{f}$ для квадратичных числовых полей и кубических многочленов f, а именно, было получено полное описание

[1] *Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук, Москва, Россия*
[2] *Математический институт им. В.А. Стеклова Российской академии наук, Москва, Россия*
**E-mail: platonov@mi-ras.ru*
***E-mail: petrushkin@yandex.ru*

периодических разложений пар, состоящих из квадратичного числового поля и периодического элемента $\sqrt{f}$, а также была доказана теорема конечности для таких многочленов f над расширениями степени 3 и 4 над $\mathbb{Q}$. В работе [7] без использования параметризаций было исследовано на периодичность разложение $\sqrt{f(x)}$ в предположениях, ограничивающих его период, что достигалось ограничением порядка точки кручения (что эквивалентно ограничению степени фундаментальной S-единицы) и поиском решений сложной системы уравнений, условие разрешимости которой эквивалентно периодичности $\sqrt{f(x)}$.

Пусть E – эллиптическая кривая над полем алгебраических чисел $\mathbb{K}$. По теореме Морделла–Вейля множество $\mathbb{K}$-точек на E образует конечнопорожденную абелеву группу $E(\mathbb{K})$. В частности, ее подгруппа кручения $E(\mathbb{K})_{\mathrm{tors}}$ конечна. Мерель показал, что $\#E(\mathbb{K})_{\mathrm{tors}} \le B(d)$ для каждой эллиптической кривой E над полем $\mathbb{K}$ степени d над $\mathbb{Q}$. Однако оценка на $B(d)$, которую можно получить из результата Парента (см. [8]), более чем велика для текущего состояния вычислительных инструментов, и при попытке обобщения теоремы об описании периодических $\sqrt{f}$ для кубических многочленов над $\mathbb{Q}$ на более общие поля алгебраических чисел $\mathbb{K}$ ее использование неэффективно. Полное описание порядков точек кручения известно только для расширений $\mathbb{Q}$ степени не выше 3 (см. [9, 10]).

В настоящем сообщении мы, опираясь на новые результаты других авторов и результаты работы [6], получаем полное решение проблемы периодичности $\sqrt{f}$ для кубических числовых полей. Благодаря оптимизации алгоритмов и компьютерных вычислений, мы доказываем теорему конечности кубических многочленов f с периодическим разложением $\sqrt{f}$ над полями алгебраических чисел степени, не превосходящей 6, а также даем полное описание таких многочленов f над произвольным полем, соответствующих эллиптическим полям с точкой кручения порядка $N \le 30$.

Поскольку периодичность разложения $\sqrt{f(x)}$ в непрерывную дробь равносильна периодичности $\sqrt{f^{\sigma}(x)}$, где $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, а также периодичности $\sqrt{a^2 f(bx)}$ для любых $a, b \in \mathbb{K}^{\times}$, мы будем рассматривать многочлены с точностью до указанной эквивалентности.

Результаты работы мы сформулируем в виде следующих теорем.

Т е о р е м а 1. *Число классов эквивалентности свободных от квадратов кубических многочленов $f \in \mathbb{K}[x]$, отличных от вида $cx^3 + 1$, над полем алгебраических чисел $\mathbb{K}$ степени $d = 3$ над $\mathbb{Q}$, имеющих периодическое разложение $\sqrt{f(x)}$ в непрерывную дробь над $\mathbb{K}$, – конечно, и определяется следующими представителями:*

$$12x^3 - 8x^2 + 4x + 1, \quad 12x^3 - 5x^2 + 2x + 1,$$
$$-120x^3 + 25x^2 + 2x + 1,$$
$$x^3 + (-6z^2 - 6)x^2 + (249z^2 + 105z + 360)x +$$
$$+ \frac{2397}{2}z^2 + \frac{2055}{4}z + \frac{3495}{2},$$

где z – корень многочлена $t^3 - t^2 + \frac{1}{2}t - \frac{1}{12}$;

$$(x + 9z^2 - 6z + 2) \cdot (x^2 + (-48z^2 + 36z - 14)x +$$
$$+ 216z^2 - 156z + 65),$$

где z – корень многочлена $t^3 - 3t^2 - 5$;

$$x^3 + \frac{1}{84}(64z^2 - 40z - 123)x^2 +$$
$$+ \frac{1}{49}(-32z^2 + 32z + 39)x + \frac{1}{343}(216z - 369),$$

где z – корень многочлена $t^3 + t^2 - 2t - \frac{9}{2}$.

Эта теорема является следствием следующей более технической теоремы, дающей полное описание периодических $\sqrt{f}$, соответствующих эллиптической кривой с точкой кручения $(0, \sqrt{f(0)})$ порядка, не превосходящего 30.

Т е о р е м а 2. *Существует лишь конечное число классов эквивалентности свободных от квадратов кубических многочленов $f \in \mathbb{K}[x]$ над произвольным полем $\mathbb{K}$ таких, что*

1) *точка $P = (0, \sqrt{f(0)})$ соответствующей эллиптической кривой имеет порядок $5 \le N \le 30$,*

2) *разложение элемента $\sqrt{f(x)} \in \mathbb{K}((x))$ в непрерывную дробь периодично.*

Более того, для каждого порядка кручения $N \le 30$, $N \ne 6$ существует с точностью до эквивалентности один такой многочлен f, а для $N = 6$ такого многочлена не существует.

Степени расширения d полей констант $\mathbb{K}$ и длина периода Π разложения в непрерывную дробь $\sqrt{f}$ для многочленов f из теоремы 2 приведены в табл. 1. Отметим, что квазипериод $\sqrt{f}$ во всех приведенных выше случаях оказывается равен половине периода.

Теорема 2 позволяет сделать вывод о конечности числа периодических $\sqrt{f} \in \mathbb{K}[x]$ в случае, если $\mathbb{K}$ – поле алгебраических чисел степени не выше 6.

Т е о р е м а 3. *Число классов эквивалентности свободных от квадратов кубических многочленов*

$f \in \mathbb{K}[x]$, *отличных от вида* $cx^3 + 1$, *над полем алгебраических чисел* $\mathbb{K}$ *степени* $d \le 6$ *над* $\mathbb{Q}$, *имеющих периодическое разложение* $\sqrt{f(x)}$ *в непрерывную дробь над* $\mathbb{K}$, *– конечно*.

Приведем схему доказательства теоремы 2, базирующуюся на схеме доказательства основных теорем работы [6]. Зафиксируем N и рассмотрим определенную над $\mathbb{Q}$ модулярную кривую $X_1(N)$, $\mathbb{K}$-точки которой отвечают множествам пар $(\mathscr{C}, P)$, состоящих из эллиптической кривой $\mathscr{C}$ над $\mathbb{K}$ и $\mathbb{K}$-точки конечного P порядка N на ней. В работе [11] были приведены уравнения от двух переменных $g_N(t,u) = 0$, задающие кривые $X_1(N)$. За исключением пар $(t,u) \in X_1(N)$, отвечающим каспидальным точкам, каждой паре (t,u) отвечает эллиптическая кривая в форме Тейта:

$$y^2 + c(t,u)xy + b(t,u)y = x^3 + b(t,u)x^2. \qquad (1)$$

Для такой кривой точка (0, 0) является точкой кручения порядка N, если и только если выполнено соотношение $g_N(t,u) = 0$.

Для всех кривых коэффициенты b и c единообразно задаются формулами

$$\begin{aligned} c &= s - rs + 1, \\ b &= rs - r^2 s. \end{aligned} \qquad (2)$$

где $r := r_N(t,u)$ и $s := s_N(t,u)$ уже зависят от N. Заменяя y на $y - \dfrac{cx + b}{2}$, переходим к кривой $y^2 = f(x)$ с точкой кручения $\left(0, \dfrac{b}{2}\right)$, где

$$f = x^3 + \left(b + \frac{c^2}{4}\right)x^2 + \frac{bc}{2x} + \frac{b^2}{4}. \qquad (3)$$

Как было отмечено ранее, разложение элемента $\sqrt{f}/x^2$ в непрерывную дробь периодично. Шагу n этого разложения сопоставим многочлен $L_n = (-1)^{n+1}(x^4 P_n^2 - fQ_n^2)$, где P_n/Q_n – n-я подходящая дробь к элементу $\sqrt{f}/x^2$. В [2] показано, что точка $(0, \sqrt{f(0)})$ является точкой кручения тогда и только тогда, когда для некоторого n многочлен L_n пропорционален x^{2g+1} или x^{2g+2}. А степень S-единицы, равная порядку точки кручения, определяет четность степени многочлена L_n для такого минимального n, что L_n обладает указанным ранее свойством.

Итак, имеем уравнение $y^2 = f_N(x,t,u)$, у которого коэффициенты при x зависят от параметров (t,u), где t, u удовлетворяют соотношению $g_N(t,u) = 0$.

Разложим в непрерывную дробь элемент $\dfrac{\sqrt{f_N(x,t,u)}}{x^2}$ по переменной x^{-1}, воспринимая (t,u) как формальные переменные до шага, на котором L_n пропорционален либо x^3, либо x^4. Далее в соответствии с критерием периодичности элемента $\sqrt{f}$ из [6] на многочлены $P_n = p_0(t,u) + p_1(t,u)x^{-1} + \ldots$, $Q_n = q_0(t,u) + q_1(t,u)x^{-1} + \ldots$ накладываем соотношения либо $q_0(t,u) = 0$, либо $p_1(t,u) = 0$, в зависимости от четности степени L_n, что при выполнении соотношения $g_N(t,u) = 0$ повлечет периодичность $\sqrt{f}$. Наконец, мы решаем систему, состоящую из $g_N(t,u) = 0$ и одного из уравнений $q_0(t,u) = 0$ или $p_1(t,u) = 0$.

Отметим, что свободный коэффициент Q_n и коэффициент P_n при x^{-1} зависят только от свободных коэффициентов и коэффициентов при x^{-1} элементов P_m, Q_m, A_m для $m < n$. Это обстоятельство позволяет существенно снизить число арифмети-

Таблица 1. Значения порядков N и степени поля $\mathbb{K}$ над $\mathbb{Q}$, реализующие периодические разложения $\sqrt{f}$ с периодом П

N	П	$\deg \mathbb{K}$
5	6	1
6	–	–
7	10	2
8	6	1
9	14	3
10	10	1
11	18	5
12	10	3
13	22	7
14	14	3
15	26	8
16	14	6
17	30	12
18	18	6
19	34	15
20	18	10
21	38	16
22	22	10
23	42	22
24	22	14
25	46	25
26	26	15
27	50	27
28	26	21
29	54	35
30	30	20

ческих операций, необходимых для применения критерия периодичности $\sqrt{f}$. Снижение числа арифметических операций, а также оптимизация алгоритма и его программной реализации позволили завершить вычисление для $N \le 30$, что, в свою очередь, позволило завершить доказательство основных результатов.

В случаях кривых с точкой кручения порядка $N \ge 20$ мы воспользовались методом исключения переменной, основанным на базисах Гребнера и сводящим вопрос к одному уравнению от t.

Схема доказательства теорем 1 и 3. Если элемент $\sqrt{f}$ периодичен, то также периодичен и $\sqrt{f}/x^2$, а для кривой $y^2 = f(x)$ точка $(0, \sqrt{f(0)})$ имеет конечный порядок N (подробнее см. [2]). Воспользуемся следующими результатами о конечности возможных порядков N, сформулированными для удобства читателя в виде одной теоремы.

Теорема 4. *Пусть $\mathscr{C}$ – эллиптическая кривая над полем алгебраических чисел $\mathbb{K}$ степени $d \le 6$ над $\mathbb{Q}$, тогда для поля $\mathbb{K}$ и $\mathbb{K}$-точки кручения порядка N на кривой $\mathscr{C}$ имеют место следующие ограничения*:

(i) *В случае $\mathbb{K} = \mathbb{Q}$ имеем $N \le 12$, $N \ne 11$ (см.* [12]);

(ii) *В случае $d = 2$ имеем $N \le 18$, $N \ne 17$ (см.* [9]);

(iii) *В случае $d = 3$ имеем $N \le 21$, $N \ne 17,19$ (см.* [10]);

(iv) *В случае $d = 4$ число полей $\mathbb{K}$ и неизоморфных эллиптических кривых $\mathscr{C}_{\mathbb{K}}$ с порядком точки кручения, отличным от $N \le 24$, $N \ne 19, 23$ – конечно (см.* [13]);

(v) *В случае $d = 5$ число полей $\mathbb{K}$ и неизоморфных эллиптических кривых $\mathscr{C}_{\mathbb{K}}$ с порядком точки кручения, отличным от $N \le 25$, $N \ne 23$, – конечно (см.* [14]);

(vi) *В случае $d = 6$ число полей $\mathbb{K}$ и неизоморфных эллиптических кривых $\mathscr{C}_{\mathbb{K}}$ с порядком точки кручения, отличным от $N \le 30$, $N \ne 23, 25, 29$, – конечно (см.* [14]).

В формулировке теоремы 4 и доказательстве теоремы 1 мы используем результаты из только что появившегося препринта [10]. Как сообщил нам один из авторов, работа готовится к публикации. Отметим, что в более ранней работе [15] показано, что число кубических числовых полей $\mathbb{K}$ и неизоморфных эллиптических кривых $\mathscr{C}_{\mathbb{K}}$ с порядком точки кручения, отличным от $N \le 20$ $N \ne 17,19$, – конечно.

Из теоремы 4 следует, что для доказательства конечности числа классов многочленов f над полями алгебраических чисел степени ≤ 6 достаточно исследовать на периодичность элемента $\sqrt{f}$ лишь кривые с порядком кручения $N \le 30$, $N \ne 23$, 29, что и было сделано в теореме 2.

Доказательство теоремы 2. В силу ограничений объема и сложности результатов вычислений приведем здесь полное доказательство только для случая $N = 11$, который соответствует выражениям с не слишком большими коэффициентами и дает единственное решение над расширением степени 5, а также для случая $N = 20$, в котором существенно используется аппарат базисов Грёбнера. Отметим, что во всех случаях, кроме случая $N = 6$, система на (t, u) имеет ровно одно решение с точностью до выбора корня неприводимого над $\mathbb{Q}$ многочлена, не обнуляющее знаменатели коэффициентов f_N и свободный коэффициент f_N. Кроме того, следует отметить, что в работе [3] были разобраны случаи $N \le 12$, $N \ne 11$, для которых параметризация $X_1(N)$ рациональна. А случаи $N = 11,13,14,\ldots,22,24$ были анонсированы в работе [6], где было показано, что для $d = 2$ нетривиальный периодический корень реализуется только при $N = 7$.

Из теоремы 4 и табл. 1 видно, что нетривиальные случаи для $d = 3$ реализуются только для $N = 9,12,14$. Кроме того, показано что для $d = 5$ периодический корень реализуется при $N = 11$, а для $d = 6$ при $N = 16,18$.

Случай $N = 11$.

Кривая $X_1(11)$ задана соотношением $g_{11}(t, u) = u^2 - \frac{1}{4}t^4 - \frac{1}{2}t^2 + t - \frac{1}{4} = 0$, а формулы

$$r(t,u) = tu - \frac{1}{2}t^3 - \frac{1}{2}t + 1, s(t,u) = -t + 1, \qquad (4)$$

после подстановки в (2) и (3) определяют соответствующую эллиптическую кривую:

$$\begin{aligned} f_{11} = x^3 &+ \left(\frac{1}{8}(t^8 + 2t^7 - t^6 + 2t^5 - 15t^4 + 14t^3 - 9t^2 + 6t + 2) - \frac{1}{4}(t-1)t(t^4 + 3t^3 + t^2 + 3t - 6)u\right)x^2 \\ &+ \left(\frac{1}{2}(t-1)t(t^7 - t^6 + 2t^5 - 4t^4 + 2t^3 - 2t^2 + 1)u - \frac{1}{4}(t-1)^2t(t^8 + 3t^6 - 4t^5 + 2t^4 - 6t^3 - t - 1)\right)x \\ &+ \left(\frac{1}{8}(t-1)^3t^2(t^9 + t^8 + 5t^7 - t^6 + 5t^5 - 9t^4 + 4t^3 - 6t^2 + 3t - 1) - \frac{1}{4}(t-1)^3t^2(t^3 + t - 1)(t^4 + t^3 + 3t^2 + 1)u\right). \end{aligned} \qquad (5)$$

Рассмотрим разложение квадратичной иррациональности $\frac{\sqrt{f_{11}}}{x^2}$ в непрерывную дробь в $\mathbb{K}(t,u)((x))$. В этом случае

$$L_4 = t^{-2}\left((-t^4 + 2t^3 - 2t + 1)u + \frac{1}{2}t^6 - \right.$$
$$\left. - t^5 + \frac{1}{2}t^4 - t^3 + \frac{5}{2}t^2 - 2t + \frac{1}{2}\right)x^3,$$

причем L_n не пропорционален x^k при $0 \le n < 4$. Степень S-единицы гиперэллиптического поля, заданного многочленом f_{11}, совпадает с порядком точки кручения с $x = 0$ и равна 11.

Квазипериод разложения $\sqrt{f_{11}}/x^2$ в непрерывную дробь совпадает с периодом и равен 10. По критерию периодичности квадратного корня из [6], примененному в случае S-единицы нечетной степени, $\sqrt{f_{11}}$ периодичен, если и только если коэффициент многочлена Лорана P_n при x^{-1} обращается в нуль:

$$p_1(t,u) = \frac{2(t^5 - 3t^3 + 4t^2 - 9t + 7)u - (t^7 - 2t^5 + 2t^4 - 12t^3 + 13t^2 + 5t - 7)}{4t} = 0.$$

Выражая из предыдущего уравнения u через t и подставляя в $g_{11}(t,u) = 0$, получаем

$$(3t^5 - 3t^4 - 12t^3 + 9t^2 - 35t + 63)(t-1)^3 t = 0. \quad (6)$$

Найдем неприводимые множители (6), которым отвечают периодические разложения $\sqrt{f_{11}}$. Корни $z = 0$, $z = 1$ не отвечают f с периодическим разложением $\sqrt{f}$, поскольку подстановка $t = z$ влечет $f_{11}(0,z) = 0$, тем самым $P = (0,0)$ является точкой второго порядка.

Корню z неприводимого над $\mathbb{Q}$ многочлена $t^5 - t^4 - 4t^3 + 3t^2 - \frac{35}{3}t + 21$ соответствует $u = \frac{6}{55}z^4 + \frac{3}{11}z^3 - \frac{53}{110}z^2 - \frac{6}{55}z - \frac{127}{110}$, и этим значениям отвечает

$$f_{11}(x,z) = x^3 + \frac{1}{11}(-24z^4 + 72z^3 -$$
$$- 70z^2 + 112z - 76)x^2 + \frac{1}{11}(2877z^4 -$$
$$- 9984z^3 + 13080z^2 - 23436z + 24318)x + \quad (7)$$
$$+ \frac{1}{4}(10224z^4 - 35451z^3 +$$
$$+ 46509z^2 - 83811z + 87129).$$

Разложение элемента $\sqrt{f_{11}(x,z)}$ над полем алгебраических чисел степени 5 имеет период 18, квазипериод 9 и коэффициент квазипериодичности

$$-\frac{56419}{33075}z^4 - \frac{77114}{33075}z^3 + \frac{43201}{33075}z^2 -$$
$$- \frac{3181}{1575}z + \frac{1501463}{99225}.$$

Случай $N = 20$.

Кривая $X_1(20)$ задана соотношением $g_{20}(u, t) = u^3 + (t^2 + 3)u^2 + (t^3 + 4)u + 2$, а после подстановки выражений для $r(t,u)$ и $s(t,u)$ в (2) и (3) мы можем определить соответствующую эллиптическую кривую:

$$f_{20} = x^3 + \frac{1}{4}(t-1)^{-6}(t^2 - 2t + 2)^{-2}(t^2 - t - 1)^{-2} \times$$
$$\times ((t-1)^{-1}t(t^{13} + ...)u + (t^{14} + ...))x^2 + (t-1)^{-10} \times$$
$$\times t(t^2 - 2t + 2)^{-2}(t^2 - t - 1)^{-3}((t^{15} + ...)u - \quad (8)$$
$$- \frac{1}{2}(t^{18} + ...))x + \frac{1}{4}(t-1)^{-11}t^2(t^2 - 2t + 2)^{-2} \times$$
$$\times (t^2 - t - 1)^{-4}((t^{19} + ...) - 3(t-1)^{-1}(t^{17} + ...)u).$$

Рассмотрим разложение квадратичной иррациональности $\frac{\sqrt{f_{20}}}{x^2}$ в непрерывную дробь в $\mathbb{K}(t,u)((x))$. В этом случае L_8 пропорционален x^4, причем L_n не пропорционален x^k при $0 \le n < 8$. Степень S-единицы гиперэллиптического поля, заданного многочленом f_{20}, совпадает с порядком точки кручения с $x = 0$ и равна 20. Разложение элемента $\frac{\sqrt{f_{20}}}{x^2}$ квазипериодично с квазипериодом 9 и периодом разложения 18. По критерию периодичности элемента $\sqrt{f}$ из [6], примененному в случае S-единицы четной степени, $\sqrt{f_{20}}$ периодичен, если и только если свободный коэффициент Q_n обращается в нуль. Запишем это условие:

$$q_0(t,u) = -(t^{10} - 8t^9 + 30t^8 - 68t^7 + 101t^6 -$$
$$- 100t^5 + 64t^4 - 24t^3 + 4t^2)^{-1}(-(3t^{12} - 33t^{11} +$$
$$+ 177t^{10} - 606t^9 + 1453t^8 - 2555t^7 + 3362t^6 -$$
$$- 3340t^5 + 2505t^4 - 1413t^3 + 592t^2 - 174t +$$
$$+ 28)u^2 - (3t^{13} - 30t^{12} + 141t^{11} - 398t^{10} + 679t^9 -$$
$$- 529t^8 - 533t^7 + 2257t^6 - 3545t^5 + 3488t^4 -$$
$$- 2349t^3 + 1100t^2 - 342t + 56)u + 2t^{11} - 19t^{10} +$$
$$+ 111t^9 - 426t^8 + 1126t^7 - 2106t^6 + 2846t^5 -$$
$$- 2800t^4 + 1998t^3 - 1012t^2 + 336t - 56) = 0.$$

Базис Грёбнера системы из двух вышеприведенных условий состоит из трех уравнений и выглядит следующим образом:

$$u^2 + \frac{1}{2}(t^2+4)u + \frac{1788203968386774417}{1454626383087500}t^{31} + \ldots,$$
$$(t^5 - 4t^4 + 8t^3 - 8t^2 + 4t)u -$$
$$- \frac{1012274029378176552}{51950942253125}t^{31} + \ldots,$$
$$t\cdot(t-1)\cdot(t^2-2t+2)^2\cdot(t^4-2t^3+4t^2-3t+1)^4\times$$
$$\times(54t^{10} - 525t^9 + 2370t^8 - 6570t^7 + 12300t^6 -$$
$$- 16104t^5 + 14850t^4 - 9510t^3 + 4060t^2 -$$
$$- 1050t + 126).$$

Найдем неприводимые множители последнего уравнения из базиса Грёбнера, которым отвечают периодические разложения $\sqrt{f_{20}}$.

Случаи корней $z=0$, $z=1$ не отвечают $f_{20}(x,z)$ с периодическим разложением $\sqrt{f_{20}(x,z)}$, поскольку при подстановке $x=0$, $t=z$ получаем $f_{20}(0,z)=0$, тем самым $P=(0,0)$ – точка второго порядка. Случай, когда z является корнем многочлена t^2-2t+2 или многочлена $t^4-2t^3+4t^2-3t+1$, не отвечает $f_{20}(x,z)$ с периодическим разложением $\sqrt{f_{20}(x,z)}$, поскольку z также является корнем знаменателя одного из коэффициентов $f_{20}(x,t)$.

В свою очередь, корню z многочлена $t^{10} - \frac{175}{18}t^9 + \frac{395}{9}t^8 - \frac{365}{3}t^7 + \frac{2050}{9}t^6 - \frac{2684}{9}t^5 + 275t^4 - \frac{1585}{9}t^3 + \frac{2030}{27}t^2 - \frac{175}{9}t + \frac{7}{3}$ отвечает

$$f_{20}(x,z) = x^3 + \frac{1}{360020}(121532184z^9 + \ldots)x^2 +$$
$$+ \frac{1}{180010}(-3074046066z^9 + \ldots)x + \qquad (9)$$
$$+ \frac{1}{360020}(-40173695550z^9 + \ldots).$$

Разложение элемента $\sqrt{f_{20}}$ над числовым полем степени 10 имеет период 9 и квазипериод 18.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа выполнена в рамках государственного задания по проведению фундаментальных научных исследований по проекту № 0065-2019-0011.

СПИСОК ЛИТЕРАТУРЫ

1. *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.
2. *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.
3. *Платонов В.П., Федоров Г.В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209. № 4. С. 54–94.
4. *Kubert D.S.* Universal bounds on the torsion of elliptic curves // Proc. London Mathematical Society. 1976. V. 3. № 2. P. 193–237.
5. *Платонов В.П., Федоров Г.В.* О проблеме классификации периодических непрерывных дробей в гиперэллиптических полях // УМН. 2020. Т. 75. № 4 (454). С. 211–212.
6. *Платонов В.П., Жгун В.С., Петрунин М.М.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над числовыми полями // Доклады РАН. Математика, информатика, процессы управления. 2020. Т. 493. С. 32–37.
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. *Parent P.* Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres // Journal für die reine und angewandte Mathematik. 1999. V. 1999. № 506. P. 85–116.
9. *Kenku M.A., Momose F.* Torsion points on elliptic curves defined over quadratic fields // Nagoya Mathematical Journal. 1988. V. 109. P. 125–149.
10. *Derickx M., Etropolski A., van Hoeij M., Morrow J.S., Zureick-Brown D.* Sporadic cubic torsion // arXiv:2007.13929. 2020.
11. *Sutherland A.* Constructing elliptic curves over finite fields with prescribed torsion // Mathematics of Computation. 2012. V. 81. № 278. P. 1131–1147.
12. *Mazur B.* Rational points on modular curves // Modular Functions of one Variable V / ed. Serre J.-P., Zagier D.B. B.; Heidelberg, Springer, 1977. P. 107–148.
13. *Jeon D., Kim C.H., Park E.* On the torsion of elliptic curves over quartic number fields // J. London Math. Soc. 2006. V. 74. № 1. P. 1–12.
14. *Derickx M., Sutherland A.* Torsion subgroups of elliptic curves over quintic and sextic number fields // Proc. American Mathematical Society. 2017. V. 145. № 10. P. 4233–4245.
15. *Jeon D., Kim C.H., Schweizer A.* On the torsion of elliptic curves over cubic number fields // Acta Arithmetica. 2004. V. 113. P. 291–301.

ON THE FINITENESS OF THE NUMBER OF EXPANSIONS INTO A CONTINUED FRACTION OF $\sqrt{f}$ FOR CUBIC POLYNOMIALS OVER ALGEBRAIC NUMBER FIELDS

Academician of the RAS V. P. Platonov[a,b] and M. M. Petrunin[a]

[a] *Federal State Institution "Scientific Research Institute for System Analysis of the Russian Academy of Sciences", Moscow, Russian Federation*

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

We obtain a complete description of the cubic polynomials f over algebraic number fields $\mathbb{K}$ of degree 3 over $\mathbb{Q}$, for which the continued fraction expansion of $\sqrt{f}$ in the field of formal power series $\mathbb{K}((x))$ is periodic. We also prove the finiteness theorem for cubic polynomials $f \in K[x]$ with periodic expansion $\sqrt{f}$ for extensions of $\mathbb{Q}$ of degree at most 6, and give a complete description of such polynomials f over an arbitrary field corresponding to elliptic fields with a torsion point of order $N \leq 30$.

Keywords: elliptic field, S-units, continued fractions, periodicity, modular curves, torsion point