ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2020, том 493, с. 32–37

МАТЕМАТИКА

УДК 511.6

О ПРОБЛЕМЕ ПЕРИОДИЧНОСТИ РАЗЛОЖЕНИЙ В НЕПРЕРЫВНУЮ ДРОБЬ $\sqrt{f}$ ДЛЯ КУБИЧЕСКИХ МНОГОЧЛЕНОВ НАД ЧИСЛОВЫМИ ПОЛЯМИ

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

Поступило 17.06.2020 г.
После доработки 18.06.2020 г.
Принято к публикации 18.06.2020 г.

Получено полное описание полей $\mathbb{K}$, являющихся квадратичными расширениями $\mathbb{Q}$, и кубических многочленов $f \in \mathbb{K}[x]$, для которых разложение $\sqrt{f}$ в непрерывную дробь в поле формальных степенных рядов $\mathbb{K}((x))$ периодично. Также доказана теорема конечности для кубических многочленов $f \in \mathbb{K}[x]$ с периодическим разложением $\sqrt{f}$ для кубических и квартичных расширений $\mathbb{Q}$.

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

DOI: 10.31857/S2686954320040244

Рассмотрим свободный от квадратов многочлен $f(x) \in \mathbb{K}[x]$ степени $2g + 1$ над полем $\mathbb{K}$ характеристики, отличной от 2. Для нас особенный интерес представляет случай, когда $\mathbb{K}$ – поле алгебраических чисел. Предположим, что $f(x)$ не делится на x, и $f(0)$ – полный квадрат в поле $\mathbb{K}$, таким образом, нормирование ν_x, соответствующее униформизующей x, имеет два продолжения: ν_x^+, ν_x^- в поле $\mathbb{K}(x)(\sqrt{f(x)})$. При этих предположениях 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 кривой $\mathscr{C}$, переводящее P в класс $P - \infty$. В случае, когда класс $P - \infty$ имеет конечный порядок в якобиане, существует класс элементов поля $\mathbb{K}(x)(\sqrt{f})$, для которых разложение в непрерывную дробь периодично. Эти разложения обладают интересными свойствами, о которых можно узнать из работ [1–3].

Отметим, что некоторые элементы при указанных предположениях на пару $(\mathscr{C}, P)$ заведомо периодичны: например $\frac{\sqrt{f(x)}}{x^g}$ и $\frac{\sqrt{f(x)}}{x^{g+1}}$. В свою очередь, сам элемент $\sqrt{f(x)}$ периодичен не всегда, что является существенным отличием от случая разложения в непрерывную дробь в $\mathbb{K}((x^{-1}))$. 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. Там же она была полностью решена для кубических многочленов над полем рациональных чисел. Рассуждения основывались на следующих соображениях. Первое – ограниченность порядка точки эллиптической кривой (полученное Мазуром [4]), второе – рациональность соответствующих модулярных кривых $X_1(N)$, отвечающих порядкам N из теоремы Мазура. Напомним, что $\mathbb{K}$-точки аффинной кривой $Y_1(N)$, определенной над $\mathbb{Q}$, отвечают множествам пар $(\mathscr{C}, P)$, определенных над $\mathbb{K}$ и состоящих из эллиптической кривой $\mathscr{C}$ и точки P конечного порядка N на ней (через $X_1(N)$ обозначается гладкая компактификация $Y_1(N)$). Это дает для

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

данных значений N так называемую рациональную параметризацию множества таких пар $(\mathscr{C}, P)$ (см. [5]) в зависимости от параметра t, или, иными словами, многочленов $f(x, t)$, где P соответствует $x = 0$. И последний этап – вычисление непрерывной дроби для $\sqrt{f(x,t)}$ зависимости от параметра t, и применение критерия периодичности $\sqrt{f(x,t)}$, который формулируется в виде неравенства на нормирования для числителя и знаменателя дроби, представляющей наилучшее приближение, и по сути является обращением в нуль некоторого коэффициента при степени x (см. подробнее [2, 3]).

При попытке обобщения этого результата на более общие числовые поля $\mathbb{K}$ мы сразу сталкиваемся со следующими проблемами: полное описание порядков точек кручения (аналог теоремы Мазура) известно только для квадратичных полей (см. [6]), а оценка на кручение, полученная Мерелем (см. [7], а также [8]), более чем велика для текущего состояния вычислительных инструментов. Более того, кривые $X_1(N)$ перестают быть рациональными. В работе [9] были изучены конкретные квадратичные числовые поля, где текущие методы вычисления позволяли дать полный ответ, а в работах [10, 11] 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). В последних двух работах были исследованы многочлены f, соответствующие эллиптическим кривым с точками кручения порядка $N \le 12$, $N = 14$, 16, 18. Тем самым для полного описания периодических элементов $\sqrt{f}$ над квадратичными расширениями $\mathbb{Q}$ оставалось рассмотреть порядки кручения 13 и 15, что являлось нетривиальной вычислительной задачей. В [10, 11] периодичность $\sqrt{f(x)}$ переформулировалась в терминах решения сложной системы уравнений, включающей коэффициенты $\sqrt{f(x)}$ и дополнительные переменные. На самом деле, эта система отвечает за квазипериодичность, но для элементов вида $\sqrt{f}/x^n$ их периодичность является следствием квазипериодичности (см. [2]).

В настоящей работе мы предлагаем обобщение метода работы [3]. Наш метод позволяет полностью решить проблему периодичности $\sqrt{f}$ для квадратичных числовых полей, а именно, мы получаем полное описание периодических разложений пар, состоящих из квадратичного числового поля и периодического элемента $\sqrt{f}$ (что, в частности, доказывает гипотезу из работы [11]), а также доказываем теорему конечности для кубических и квартичных расширений $\mathbb{Q}$. Ключевым замечанием, позволившим добиться продвижения в решении этих задач, является то, что рациональность кривых $X_1(N)$ хоть и упрощает ситуацию, но не является существенной.

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 $\mathbb{K}$ степени $d \le 4$ над $\mathbb{Q}$, имеющих периодическое разложение $\sqrt{f(x)}$ в непрерывную дробь над $\mathbb{K}$, конечно, и в случае $d \le 2$ исчерпывается следующими представителями*:

$$12x^3 - 8x^2 + 4x + 1, \quad 12x^3 - 5x^2 + 2x + 1,$$
$$-120x^3 + 25x^2 + 2x + 1,$$
$$6(9\sqrt{21} - 41)x^3 - 4(3\sqrt{21} - 13)x^2 + 4x + 1$$
$$\text{для} \quad \mathbb{K} = \mathbb{Q}(\sqrt{21}).$$

Эта теорема является следствием следующей более технической теоремы.

Т е о р е м а 2. *Число классов эквивалентности свободных от квадратов кубических многочленов $f \in \mathbb{K}[x]$ над произвольным полем $\mathbb{K}$, отличных от вида $cx^3 + 1$, для которых точка $(0, \sqrt{f(0)})$ соответствующей эллиптической кривой имеет порядок $3 \le N \le 22$, $N = 24$, а разложение $\sqrt{f(x)}$ в непрерывную дробь периодично, конечно.*

Имеет место также следующее простое следствие нашего метода, которое было совершенно не очевидно с позиции работ [3, 10, 11]. Множество решений систем, аналогичных построенным в работах [10, 11], не более чем одномерно, поскольку пространство решений является алгебраическим подмножеством в модулярной кривой $Y_1(N)$.

Приведем схему доказательства теоремы 2. Зафиксируем N и рассмотрим модулярную кривую $Y_1(N)$, определенную над $\mathbb{Q}$, $\mathbb{K}$-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. Напомним, что точки $X_1(N) \setminus Y_1(N)$ называются каспидальными. В работе [12] были приведены уравнения от двух переменных $g_N(t, u) = 0$, задающие кривые $Y_1(N)$. Каждой паре $(t, u) \in Y_1(N)$ отвечает эллиптическая кривая в форме Тейта:

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

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

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

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

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

Как было отмечено ранее, разложение элемента $\dfrac{\sqrt{f}}{x^2}$ в непрерывную дробь периодично. Шагу n этого разложения сопоставим многочлен $L_n = (-1)^{n+1}(x^4 P_n^2 - fQ_n^2)$, где $\dfrac{P_n}{Q_n}$ – n-я подходящая дробь к элементу $\dfrac{\sqrt{f}}{x^2}$. В [2] показано, что точка $\left(0, \sqrt{f(0)}\right)$ 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 многочлена L_n, для такого минимального n, что L_n обладает указанным ранее свойством.

Сформулируем критерий периодичности элемента $\sqrt{f}$ из [2] в терминах подходящих дробей и многочлена L_n.

Теорема 3. *Пусть f – бесквадратный многочлен степени $2g+1$. Предположим, что для кривой $y^2 = f(x)$ точка $\left(0, \sqrt{f(0)}\right)$ является точкой кручения.*

(i) *Тогда найдется минимальное n, что на n-м шаге разложения $\dfrac{\sqrt{f}}{x^{g+1}}$ в непрерывную дробь многочлен L_n пропорционален x^{2g+1} или x^{2g+2}.*

(ii) *Обозначим через $\dfrac{P_n}{Q_n}$ подходящую дробь с номером n к элементу $\sqrt{f}$, где $P_n, Q_n \in \mathbb{K}[x^{-1}]$. Тогда в случае $L_n = cx^{2g+1}$ имеем $\nu_x(P_n) < 0$, а элемент $\sqrt{f}$ периодичен тогда и только тогда, когда $\nu_x(P_n) \le -(g+1)$. А в случае $L_n = cx^{2g+2}$ элемент $\sqrt{f}$ периодичен тогда и только тогда, когда $\nu_x(Q_n) \le -g$.*

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 (при выполнении соотношения $g_N(t,u) = 0$). Далее для

$$P_n = p_0(t,u) + p_1(t,u)x^{-1} + \ldots$$
$$\ldots, Q_n = q_0(t,u) + q_1(t,u)x^{-1} + \ldots$$

накладываем соотношения либо $q_0(t,u) = 0$, либо $p_1(t,u) = 0$, в зависимости от четности степени L_n, что по теореме 3 (при выполнении соотношения $g_N(t,u) = 0$) повлечет периодичность $\sqrt{f}$. Далее мы решаем систему, состоящую из $g_N(t,u) = 0$ и одного из уравнений $q_0(t,u) = 0$ или $p_1(t,u) = 0$.

Заметим, что в случае квадратичных числовых полей все модулярные кривые $g_N(t,u) = 0$ имеют род не больше 2 и либо отвечают рациональной параметризации, либо легко приводятся к виду $u^2 = h(t)$, и тем самым решение рассматриваемой системы полностью элементарно. В случае для кривых с точкой кручения порядка $N = 17, 19, 20, 21, 22, 24$ мы воспользовались методом исключения переменной, основанным на базисах Гребнера и сводящим вопрос к одному уравнению от t.

Доказательство теоремы 1. Как мы заметили ранее, если элемент $\sqrt{f}$ периодичен, то также периодичен и $\dfrac{\sqrt{f}}{x^2}$, 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 $\mathbb{K}$ степени $d \le 4$ 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. [4]).*

(ii) *В случае $d = 2$ имеем $N \le 18, N \ne 17$ (см. [6]).*

(iii) *В случае $d = 3$ число 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 (см. [13]).*

Таблица 1.

N	Период	F_d и g_N
11	18	$F_5 = t^5 - t^4 - 4t^3 + 3t^2 - \frac{35}{3}t + 21$
		$g_{11} = u^2 - \frac{1}{4}t^4 - \frac{1}{2}t^2 + t - \frac{1}{4}$
13	22	$F_7 = t^7 + 5t^6 + 7t^5 + 4t^4 + \frac{31}{5}t^3 + \frac{56}{5}t^2 + \frac{126}{5}t + \frac{63}{5}$
		$g_{13} = u^2 + (t^3 + t^2 + 1)u - t^2 - t$
14	14	$F_3 = t^3 + t^2 - 2t - \frac{9}{2}$
		$g_{14} = u^2 + (t^2 + t)u + t$
15	26	$F_8 = t^8 + 2t^7 + \frac{8}{11}t^6 - t^5 - \frac{5}{7}t^4 - \frac{47}{77}t^3 - \frac{64}{77}t^2 - \frac{8}{11}t - \frac{13}{77}$
		$g_{15} = u^2 + (t^2 + t + 1)u + t^2$
16	14	$F_6 = t^6 + \frac{2}{7}t^5 - \frac{9}{7}t^4 - \frac{12}{7}t^3 - \frac{15}{7}t^2 - \frac{30}{7}t - \frac{15}{7}$
		$g_{16} = u^2 + (t^3 + t^2 - t + 1)u + t^2$
18	18	$F_6 = t^6 - \frac{39}{7}t^5 + \frac{96}{7}t^4 - \frac{136}{7}t^3 + \frac{114}{7}t^2 - \frac{15}{2}t + \frac{10}{7}$
		$g_{18} = u^2 + (t^3 - 2t^2 + 3t + 1)u + 2t$

(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.* [14]).

Следует подчеркнуть, что для разложения в непрерывную дробь мы фиксируем нормирование, или, что равносильно, точку $P \in \mathscr{C}$ степени 1. И хотя для некоторого целого l кривая $\mathscr{C}$ с точкой порядка lN над $\mathbb{K}$ (соответствующая точке на $X_1(lN)$) встречается среди кривых, обладающих точками порядка N, параметризуемых точками $X_1(N)$, но там она соответствует другой паре. Более того, кривая $\mathscr{C}$ встречается несколько раз среди пар $(\mathscr{C}, P)$, параметризуемых точками $X_1(N)$, однако она появляется в паре с разными соответствующими точками кручения, и периодическое разложение $\sqrt{f}$ могут давать не все пары. Поэтому мы исследуем кривые $X_1(N)$, соответствующие всем натуральным числам из нашего диапазона, а не только те, которые соответствуют простым делителям чисел из него. Таким образом, для доказательства конечности числа классов достаточно исследовать на периодичность элемента $\sqrt{f}$ лишь кривые с порядком кручения $3 < N \le 24$, $N \ne 19$, 23, что и было сделано в теореме 2.

Доказательство. В силу ограничений объема и сложности результатов вычислений приведем здесь полное доказательство только одного случая $N = 14$, который дает нетривиальный периодический $\sqrt{f}$ над кубическим расширением $\mathbb{Q}$, а также сводную таблицу 1, содержащую данные о возможных периодических корнях в эллиптических полях, обладающих точкой кручения заданного порядка, а именно, уравнение модулярной кривой $g_N(t,u)$, многочлен $F_d(t)$ степени d, корни которого реализуют значение параметра t, при которых $\sqrt{f_N}$ периодичен (что определяет поле $\mathbb{K} = \mathbb{Q}[t]/(F_d)$, причем каждый раз u лежит в поле $\mathbb{K}$), период $\sqrt{f_N}$ (его квазипериод во всех случаях оказывается равен половине периода). Во всех случаях 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.

В табл. 1 из-за величины коэффициентов не вошли данные для $N = 17, 19, 20, 21, 22, 24$. Степени числовых полей, в которых реализуются периодические $\sqrt{f_N}$, равны, соответственно, 12, 15, 10, 16, 10, 14, а периоды разложения $\sqrt{f_N}$ в непрерывную дробь: 30, 34, 18, 38, 22, 22. Кроме того, следует отметить, что в работе [3] были разобраны случаи

$N \le 12$, $N \ne 11$, для которых параметризация $X_1(N)$ рациональна. Для $N = 7$ периодический $\sqrt{f_7}$ реализуется над квадратичным расширением, а для $N = 9$, 12 периодический $\sqrt{f_N}$ реализуется над кубическими расширениями $\mathbb{Q}$. В других случаях для $N \le 10$ периодический $\sqrt{f_N}$ либо не реализуется, либо реализуется над $\mathbb{Q}$.

Приведем вычисления только для случая $N = 14$, который приводит к выражениям с не слишком большими коэффициентами. Остальные случаи доказываются аналогично.

Порядок кручения 14.

Кривая $X_1(14)$ задана соотношением $g_{14}(t, u) = u^2 + (t^2 + t)u + t$, а формулы

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

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

$$f_{14} = x^3 + \left(\frac{1}{4}(t+1)^{-4}(t^3 + t^2 - 2t - 1)^{-2} \times (t^{10} + 3t^9 - 6t^8 - 28t^7 - 10t^6 + 66t^5 + 80t^4 - 28t^3 - 83t^2 - 17t + 6)u + \frac{1}{4}(t-1)(t+1)^{-4} \times (t^3 + t^2 - 2t - 1)^{-2}(t^{11} + 5t^{10} + 3t^9 - 26t^8 - 55t^7 + t^6 + 117t^5 + 115t^4 - 30t^3 - 98t^2 - 36t - 1)\right)x^2 + \left(\frac{1}{2}(t-1)(t+1)^{-5}(t^3 + t^2 - 2t - 1)^{-3}(t^{10} + 4t^9 - t^8 - 21t^7 - 7t^6 + 62t^5 + 48t^4 - 67t^3 - 66t^2 + 6t + 1)u + \frac{1}{2}(t-1)t(t+1)^{-5}(t^3 + t^2 - 2t - 1)^{-3}(t^{11} + 5t^{10} + 2t^9 - 29t^8 - 44t^7 + 50t^6 + 137t^5 - t^4 - 151t^3 - 45t^2 + 47t + 4)\right)x + \left(\frac{1}{4}(t-1)^2 t(t+1)^{-6}(t^3 + t^2 - 2t - 1)^{-4}(t^4 + t^3 - 5t^2 - 6t + 1)(t^5 + 4t^4 + 2t^3 - 7t^2 - t + 9)u + \frac{1}{4}(t-1)^2 t(t+1)^{-6}(t^3 + t^2 - 2t - 1)^{-4} \times (t^{11} + 6t^{10} + 7t^9 - 25t^8 - 61t^7 + 19t^6 + 139t^5 + 29t^4 - 143t^3 - 56t^2 + 37t - 1)\right). \qquad (5)$$

Рассмотрим разложение квадратичной иррациональности $\frac{\sqrt{f_{14}}}{x^2}$ в непрерывную дробь в $\mathbb{K}(t,u)((x))$. В этом случае $L_5 = x^4$, причем L_n не пропорционален x^k при $0 \le n < 5$. Степень S-единицы гиперэллиптического поля, заданного многочленом f_{14}, совпадает с порядком точки кручения с $x = 0$ и равна 14.

Квазипериод разложения $\frac{\sqrt{f_{14}}}{x^2}$ в непрерывную дробь совпадает с периодом и равен 6. По теореме 3, примененной в случае S-единицы четной степени, $\sqrt{f_{14}}$ периодичен, если и только если свободный коэффициент Q_n обращается в нуль. Запишем это условие:

$$q_0(t,u) = \frac{2(t^3 + t^2 + tu - 2t + 2u - 3)}{t^2 + 2t + 1} = 0.$$

Подставляя в него выражение для u из $g_{14}(t,u) = 0$, получаем

$$-4(2t^3 + 2t^2 - 4t - 9)(t+1)^2 = 0. \qquad (6)$$

Проверим реализуемость периодичного $\sqrt{f_{14}}$ для корня каждого неконстантного множителя (6).

Корень $t = -1$ не отвечает f_{14} с периодическим разложением $\sqrt{f_{14}}$, поскольку $t = -1$ является корнем знаменателя одного из коэффициентов f_{14}.

Пусть теперь z является корнем неприводимого над $\mathbb{Q}$ многочлена $t^3 + t^2 - 2t - \frac{9}{2}$. Тогда $u = -\frac{1}{3}z^2 + \frac{1}{3}z$, которому отвечает

$$f_{14}(x,z) = x^3 + \frac{1}{84}(64z^2 - 40z - 123)x^2 + \frac{1}{49}(-32z^2 + 32z + 39)x + \frac{1}{343}(216z - 369). \qquad (7)$$

Разложение $\sqrt{f_{14}(x,z)}$ над числовым полем степени 3 периодично с квазипериодом 7, периодом 14, коэффициентом квазипериодичности

$$-\frac{784}{25}z^2 - \frac{1274}{15}z - \frac{74137}{900}.$$

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. *Mazur B.* Rational points on modular curves // Modular Functions of one Variable V / Ed. by J.-P. Serre, Don B. Zagier. Lecture Notes in Mathematics. B.; Heidelberg: Springer, P. 107–148.
5. *Kubert Daniel Sion*. Universal bounds on the torsion of elliptic curves // Proc. London Math. Soc.(3). 1976. V. 33. № 2. P. 193–237.
6. *Kenku Monsur A.* Momose Fumiyuki. Torsion Points on Elliptic Curves Defined over Quadratic Fields // Nagoya Math. J. 1988. V. 109. P. 125–149.
7. *Merel Loïc*. Bornes pour la torsion des courbes elliptiques sur les corps de nombres // Invent Math. 1996. V. 124. № 1. P. 437–449.
8. *Mazur B.* (with an appendix by Goldfeld D.). Rational isogenies of prime degree // Invent Math. 1978. V. 44. P. 129–162.
9. *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.
10. *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.
11. *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. 9–14.
12. *Sutherland Andrew*. Constructing Elliptic Curves over Finite Fields with Prescribed Torsion // Mathematics of Computation. 2012. V. 81. № 278. P. 1131–1147.
13. *Jeon Daeyeol, Kim Chang Heon, Schweizer Andreas*. On the Torsion of Elliptic Curves over Cubic Number Fields // Acta Arithmetica. 2004. V. 113. P. 291–301.
14. *Jeon Daeyeol, Kim Chang Heon, Park Euisung*. On the Torsion of Elliptic Curves over Quartic Number Fields // J. London Math. Society. 2006. V. 74. № 1. P. 1–12.

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

Academician of the RAS V. P. Platonov[a,b], V. S. Zhgoon[a], 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 fields $\mathbb{K}$, that are quadratic extensions of $\mathbb{Q}$, and of cubic polynomials $f \in \mathbb{K}[x]$, for which a 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 $f \in \mathbb{K}[x]$ with periodic decomposition $\sqrt{f}$ over cubic and quartic extensions of $\mathbb{Q}$.

Keywords: elliptic field, S-units, continued fractions, periodicity, modular curves, points of finite order