Г. В. Федоров, О длине периода функциональной непрерывной дроби над числовым полем, *Докл. РАН. Матем., информ., проц. упр.*, 2020, том 495, 78–81

DOI: 10.31857/S2686954320060089

ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2020, том 495, с. 78–83

МАТЕМАТИКА

УДК 511.6

О ДЛИНЕ ПЕРИОДА ФУНКЦИОНАЛЬНОЙ НЕПРЕРЫВНОЙ ДРОБИ НАД ЧИСЛОВЫМ ПОЛЕМ

Г. В. Федоров[1,*]

Представлено академиком РАН В.П. Платоновым 08.10.2020 г.
Поступило 09.10.2020 г.
После доработки 09.10.2020 г.
Принято к публикации 14.10.2020 г.

В классическом случае давно известна связь между условием периодичности непрерывной дроби элемента $\sqrt{f}$ и условием существования фундаментальной единицы соответствующего гиперэллиптического поля $\mathcal{L} = K(x)(\sqrt{f})$, где K – поле характеристики, отличной от 2. Для элемента $\sqrt{f}$ длина периода непрерывной дроби, построенной в поле формальных степенных рядов $K((1/x))$, может быть тривиальным образом оценена сверху удвоенной степенью фундаментальной единицы. Значительно более сложной и интересной является задача о верхней оценке длин периодов других элементов гиперэллиптического поля $\mathcal{L}$, обладающих периодической непрерывной дробью. Среди таких элементов ключевую роль играют элементы вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$. Для таких элементов длина периода может многократно превосходить удвоенную степень фундаментальной единицы. Найдены верхние оценки на длины периодов некоторых ключевых элементов гиперэллиптических полей $\mathcal{L}$ над числовыми полями K. Найден пример, демонстрирующий точность доказанных верхних оценок.

Ключевые слова: непрерывная дробь, длина периода, фундаментальная единица, гиперэллиптическое поле, циклотомические многочлены, критерий Эйзенштейна

DOI: 10.31857/S2686954320060089

За последние 20 лет теория функциональных непрерывных дробей стала важным арифметическим инструментом в проблеме поиска и построения фундаментальных единиц гиперэллиптического поля. С развитием современных алгебраических и теоретико-числовых методов появился новый взгляд на ряд классических проблем, идущих от обыкновенных числовых непрерывных дробей. Одной из таких проблем является проблема о верхней оценке длин периодов функциональных непрерывных дробей элементов гиперэллиптического поля.

Проблема периодичности функциональных непрерывных дробей, построенных в поле формальных степенных рядов $K((1/x))$ для элементов гиперэллиптического поля $\mathcal{L} = K(x)(\sqrt{f})$, тесно связана с проблемой поиска и построения фундаментальных единиц кольца $D_f = K[x](\sqrt{f}) = \{\omega_1 + \omega_2\sqrt{f} \mid \omega_1, \omega_2 \in K[x]\}$ и проблемой кручения в якобиане J_f соответствующей гиперэллиптической кривой (подробнее см. [1–5]). Символом $\mathcal{L}$ (или L) мы обозначаем гиперэллиптическое поле, которое вкладывается в поле формальных степенных рядов $K((1/x))$ (соответственно $K((1/x)))$), и, тем самым, элементы поля $\mathcal{L}$ (поля L) могут быть разложены в непрерывную дробь, связанную с бесконечным нормированием v_∞ (конечным нормированием v_x). Для эллиптических кривых над полем рациональных чисел проблема кручения была решена Б. Мазуром в 1978 г. Для гиперэллиптических кривых рода 2 и выше над полем рациональных чисел и соответствующих им гиперэллиптических полей приведенные три проблемы остаются открытыми.

Для эллиптических полей над полем констант $K = \mathbb{Q}$ рациональных чисел, заданных свободными от квадратов многочленами f четвертой степени, в [6] был поставлен вопрос о возможной дли-

[1] *Московский государственный университет имени М.В. Ломоносова, Москва, Россия*
[*] *E-mail: fedorov@mech.math.msu.su*

не периода непрерывной дроби $\sqrt{f}$. Используя параметризацию из [7], в статье [8] показано, что длина периода n непрерывной дроби $\sqrt{f}$, построенной в $\mathbb{Q}((1/x))$, принимает одно из значений $\{1, ..., 8, 10, 12, 14, 18, 22\}$, причем для каждого значения длины периода из этого множества существует бесконечная серия соответствующих примеров неизоморфных эллиптических полей (см. [9]). Для эллиптических полей над квадратичными полями констант K в [10] доказано, что длина периода непрерывной дроби $\sqrt{f}$ в $\mathbb{Q}((1/x))$ может принимать одно из значений $\{1, ..., 15, 17, 18, 22, 26, 30, 34\}$.

В эллиптическом случае над полем $\mathbb{Q}$ рациональных чисел в статьях [11, 12] полностью решена проблема классификации многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в поле формальных степенных рядов $\mathbb{Q}((x))$. В частности, найдено полное описание многочленов $f \in \mathbb{Q}[x]$, $3 \le \deg f \le 4$, с периодическим разложением $\sqrt{f}$ в непрерывную дробь в $\mathbb{Q}((x))$, которое при $\deg f = 3$ с точностью до естественного отношения эквивалентности, заданного допустимыми заменами вида $a^2 f(bx)$, $a, b \in \mathbb{Q}^*$, состоит из одного бесконечного семейства многочленов и еще трех отдельных многочленов, а в случае $\deg f = 4$ – из четырех бесконечных семейств и еще семи отдельных многочленов. Из этого описания явно следуют возможные длины периодов непрерывных дробей элементов $\sqrt{f}$, построенных в $\mathbb{Q}((x))$.

Для получения верхних оценкок на длины периодов ключевых элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$, гиперэллиптического поля $L = K(x)(\sqrt{f})$ важным промежуточным этапом стала теорема 2 [3] о достаточных условия одновременной квазипериодичности непрерывных дробей элементов α, $\alpha \cdot x^s \in L\backslash K(x)$, заданных в поле формальных степенных рядов $K((x))$. Для гиперэллиптических полей $L = K(x)(\sqrt{f})$, построенных с помощью свободных от квадратов многочленов $f \in K[x]$ нечетной степени $2g+1$ достаточные условия также являются необходимыми. В случае $\deg f = 2g + 2$ найденные достаточные условия не являются необходимыми, что подтверждается примерами 1–3 в статье [3]. Одно из наглядных следствий этого случая – значительное отличие длин квазипериодов непрерывных дробей элементов α и $\alpha \cdot x^s$. Так, в примере 4 статьи [3] найден свободный от квадратов многочлен $f \in \mathbb{Q}$ степени 6, для которого в $\mathbb{Q}((x))$ длина периода непрерывной дроби элемента $\alpha = \sqrt{f}/x^3$ равна 2, а длина периода непрерывной дроби элемента $\alpha \cdot x^3 = \sqrt{f}$ равна 18.

В теореме 2 [13] найдено уточнение теоремы 2 [3] над полем рациональных чисел $\mathbb{Q}$, а именно, для гиперэллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, $\deg f = 2g + 2$, найден точный промежуток значений $s \in \mathbb{Z}$ таких, что непрерывные дроби элементов вида $\sqrt{f}/x^s \in L\backslash\mathbb{Q}(x)$ периодические. Ключевым этапом доказательства было определение рациональных корней последовательности многочленов $T_n, Q_n \in \mathbb{Z}[x]$, заданных для $n \in \mathbb{N}$ следующим образом:

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

С использованием этих результатов в статье [14] найдены оценки сверху на периоды непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел.

В данном сообщении полностью изучена мультипликативная структура над полем $\mathbb{Q}$ последовательности многочленов T_n, Q_n, и тем самым дано описание всех возможных корней многочленов T_n, Q_n для $n \in \mathbb{N}$. На основании этого найдены точные оценки сверху на длины периодов функциональных непрерывных дробей в $K((1/x))$ ключевых элементов $\sqrt{f}/x^s$, $s \in \mathbb{Z}$, гиперэллиптических полей над числовыми полями K. Аналогичные оценки справедливы для длин периодов непрерывных дробей ключевых элементов, построенных в поле формальных степенных рядов $K((x))$.

Мы высказываем предположение, что для периодических элементов гиперэллиптических полей $\mathscr{L}$ над произвольными полями K характеристики 0 длины периодов непрерывных дробей, построенных в $K((1/x))$, ограничены сверху постоянной, зависящей только от рода гиперэллиптического поля $\mathscr{L}$, порядка группы кручения якобиана соответствующей гиперэллиптической кривой и степени расширения $[K_0 : \mathbb{Q}]$, где K_0 – некоторое числовое подполе поля K.

Приведем ряд вспомогательных утверждений, необходимых для поиска корней многочленов T_n, Q_n. Из (1) следует равенство $T_n(x^2) + xQ_n(x^2) = (1 + x)^n$. Отсюда для $n, m \in \mathbb{N}$ и $a \in \mathbb{Q}$ таких, что $T_n(a) \ne 0$, справедливы тождества

$$\begin{gathered} T_{nm}(a) = (T_n(a))^m \cdot T_m(b), \\ Q_{nm}(a) = (T_n(a))^{m-1} \cdot Q_n(a) \cdot Q_m(b), \end{gathered} \quad (2)$$

где $b = a(Q_n(a)/T_n(a))^2$.

П р е д л о ж е н и е 1. 1. *Пусть n нечетно. Тогда*

а) $T_n(x) = x^{\deg Q_n} Q_n(1/x)$;

б) *если* $q|n$, *то* $T_q(x)|T_n(x)$, $Q_q(x)|Q_n(x)$.

2. *Пусть n четно. Тогда*

а) $T_n(x) = x^{\deg T_n} T_n(1/x)$;

б) *если* $n = qd$, q *— нечетное, то* $T_d(x)|T_n(x)$, $Q_q(x)|Q_n(x)$;

в) *если* $n = qd$, d *— четное, то* $T_q(x)|Q_n(x)$.

Доказательство предложения 1 следует из формул (2).

Положим $L(T_n)$ — наименьшее общее кратное многочленов T_d, где $n = qd$ и $q > 1$ нечетное. Положим $P(T_n) = T_n/L(T_n)$ и $\tilde{P}(T_n)(x) = x^d P(T_n)(1/x)$, где $d = \deg P(T_n)(x)$. Отметим, что по предложению 1 при нечетном n справедливо соотношение $\tilde{P}(T_n)|Q_n$, а при четном n справедливо равенство $\tilde{P}(T_n)(x) = P(T_n)(x)$.

П р е д л о ж е н и е 2. *Пусть* $n \in \mathbb{N}$, $n \geq 2$, *тогда многочлены* $P(T_n)$ *и* $\tilde{P}(T_n)$ *неприводимы.*

Доказательство предложения 2 следует из представлений

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

соответствующих разложений на циклотомические многочлены и критерия Эйзенштейна неприводимости многочленов с целыми коэффициентами.

П р е д л о ж е н и е 3. *Пусть* $n = 2^t q$, *где* q *нечетно. Тогда справедливы формулы*

$$T_n(x) = \prod_{d|q} P(T_{2^t d})(x),$$

$$Q_n(x) = 2^t \prod_{d|q} \tilde{P}(T_d)(x) \cdot \prod_{r|n}{}' P(T_r)(x),$$

где последнее произведение берется по всем делителям r числа n таким, что n/r четное.

Предложение (3) доказывается по индукции.

Пусть многочлен $f \in K[x]$ свободен от квадратов, $\deg f = 2g+2$ и $D = \omega^2 f$ является дискриминантом квадратного уравнения $\Lambda_2 y^2 + 2\Lambda_1 y + \Lambda_0 = 0$, где $\Lambda_0, \Lambda_1, \Lambda_2 \in K[x]$ в совокупности взаимно простые многочлены. Пусть элемент $\beta \in \mathcal{L} = K(x)(\sqrt{f})$ является корнем этого квадратного уравнения. Тогда по теореме 2 [15] квазипериодичность непрерывной дроби $\beta = [a_0; a_1, \ldots]$ в $K((1/x))$ эквивалентна наличию решения $\Theta_1, \Theta_2 \in K[x]$, $\Theta_2 \neq 0$, уравнения

$$\Theta_1^2 - \Theta_2^2 D = \gamma \in K^*. \tag{3}$$

Следующая теорема была доказана в статье [14].

Т е о р е м а 1. *Пусть существует решение* Θ_1, $\Theta_2 \in K[x]$, $\Theta_2 \neq 0$, *уравнения* (3). *Тогда длина квазипериода непрерывной дроби элемента* β *не превосходит*

$$\deg \Theta_2 + \max\left(\deg \Lambda_1, \frac{1}{2}(\deg \Lambda_0 + \deg \Lambda_2)\right).$$

Перейдем к основным результатам сообщения.

Т е о р е м а 2. *Элемент* $\beta = \sqrt{f}/x^s \in \mathcal{L}$ *для некоторого* $s \in \mathbb{Z}$ *имеет периодическое разложение в непрерывную дробь тогда и только тогда, когда существуют многочлены* $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, *которые удовлетворяют условиям*

$$f_2\Omega_4^2 - f_1\Omega_3^2 = 1, \quad f_1 \cdot f_2 = b^2 f,$$
$$\deg f_2 > 0, \quad v_x(f_2) = v_x(\Omega_4) = 0,$$

для некоторого $b \in K^*$ *и* $-v_x(\Omega_3) \leq s \leq v_x(\Omega_3) + v_x(f_1)$. *В случае периодичности непрерывной дроби элемента* β *для длины квазипериода N справедливы оценки*

$$N \leq 2\deg(\Omega_3 + s + 1), \quad \text{если} \quad s + g + 1 \leq \deg f_1,$$
$$N \leq 2\deg(\Omega_3 + \deg f_1 - g),$$
$$\text{если} \quad \deg f_1 < s + g + 1 \leq 2g + 2,$$
$$N \leq 2\deg(\Omega_3 + \deg f_1 + 1 - s), \quad \text{если} \quad g + 1 < s,$$
$$N < 2\deg(\Omega_3 + \deg f_1 - g), \ldots$$

Доказательство теоремы 2 опирается на теорему 1, а также на предложение 2 [3].

Обозначим

$$\begin{aligned} \delta = \max(0, |g + 1 - s| - 1) + \\ + \max(0, |s + g + 1 - \deg f_1| - 1), \end{aligned} \tag{4}$$

тогда оценку теоремы 2 можно записать следующим образом:

$$N \leq 2\deg \Omega_3 + \deg f_1 - \delta.$$

Пусть в поле $\mathcal{L} = K(x)(\sqrt{f})$ существует фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$, где $\Psi1$,

$\Psi_2 \in K[x]$. Для $n \in \mathbb{N}$ определим многочлены $\Omega_1^{(n)}, \Omega_2^{(n)} \in K[x]$ так, что

$$\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{f} = (\Psi_1 + \Psi_2\sqrt{f})^n. \tag{5}$$

Положим $z = \Psi_2^2 f/\Psi_1^2$, тогда

$$\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{f} = \Psi_1^n(T_n(z) + Q_n(z)\sqrt{z}), \tag{6}$$

где многочлены $T_n(z), Q_n(z) \in \mathbb{Z}[z]$ определены в (1).

Для доказательства следующей теоремы нам понадобится еще один вспомогательный результат.

П р е д л о ж е н и е 4. *Пусть $\beta \in \mathcal{L}$ — квадратичная иррациональность с дискриминантом $D(\beta) = \omega^2 f \in K[x]$. Для того чтобы разложение элемента β в непрерывную дробь в поле $K((1/x))$ было квазипериодично, необходимо и достаточно, чтобы нашелся номер $n \in \mathbb{N}$ такой, что $\omega | \Omega_2^{(n)}$.*

Главный результат работы получен в следующей теореме.

Т е о р е м а 3. *Пусть K — расширение поля рациональных чисел $\mathbb{Q}$ степени k. Пусть $f \in K[x]$ — свободный от квадратов многочлен, и в поле $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $u = \Psi_1 + \Psi_2\sqrt{f}$ степени m, где $\Psi_1, \Psi_2 \in K[x]$. Пусть для $n \in \mathbb{N}$ многочлены $\Omega_1^{(n)}, \Omega_2^{(n)} \in K[x]$ определены соотношениями (5).*

1. *Если хотя бы одно из значений $v_x(f)$, $v_x(\Psi_1)$, $v_x(\Psi_2)$ отлично от нуля, то непрерывная дробь элемента $\sqrt{f}/x^s$, построенная в $K((1/x))$, периодическая тогда и только тогда, когда*

$$-v_x(\Psi_1) - v_x(\Psi_2) \le s \le v_x(\Psi_1) + v_x(\Psi_2) + v_x(f).$$

В случае периодичности непрерывной дроби $\sqrt{f}/x^s$ длина квазипериода N не превосходит $m - \delta$, где значение δ определено в (4) при некотором $f_1 | f$, $\deg f_1 < \deg f$.

2. *Если $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$, то непрерывная дробь элемента $\sqrt{f}/x^s$, построенная в $K((1/x))$, периодическая тогда и только тогда, когда найдется такой номер j, что $v_x(\Omega_2^{(1)}) = \ldots = v_x(\Omega_2^{(j-1)}) = 0$, $|s| \le v_x(\Omega_2^{(j)})$ и $\phi(j) | 2k$. В случае периодичности непрерывной дроби $\sqrt{f}/x^s$, длина квазипериода N не превосходит $jm - \delta$, где значение δ определено в (4) при некотором $f_1 | f$, $\deg f_1 < \deg f$.*

Д о к а з а т е л ь с т в о. Пункт 1 следует из результатов статьи [14]. Предположим, что $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$. Положим $z = z(x) = \Psi_2^2 f/\Psi_1^2$, тогда для $n \in \mathbb{N}$ имеем (6). Отметим, что $z(0)$ определено корректно, поскольку $\Psi_1(0) \ne 0$. Согласно предложению 4, для периодичности элемента $\sqrt{f}/x^s$, $s \ne 0$, необходимо, чтобы для некоторого минимального $j \in \mathbb{N}$ было выполнено равенство $Q_j(z)\big|_{x=0} = 0$, т.е. число $z(0)$ должно быть корнем многочлена $Q_j(x)$. В силу минимальности j, число $z(0)$ не должно быть корнем многочленов $Q_1(x)$, ..., $Q_{j-1}(x)$. Число $z(0)$ должно быть корнем либо многочлена $P(T_{j/2})$ при четном j, либо многочлена $\tilde{P}(T_j)$ при нечетном j. Имеем $\deg P(T_{j/2}) = \phi(j)/4$, $\deg \tilde{P}(T_j) = \phi(j)/2$, откуда и получаем условие $\phi(j) | 2k$. Более того, поле K в качестве подполя должно содержать поле разложения соответственно многочлена $P(T_{j/2})$ или многочлена $\tilde{P}(T_j)$.

Из оценок на длину квазипериода в теоремах 1 и 2 следует, что $N \le \deg \Theta_1 - \delta = \deg \Omega_1^{(j)} - \delta = jm - \delta$.

Теорема 3 доказана.

Из условия $\phi(j) | 2k$ теоремы 3 следует, что, например, при $k = 6$ возможно $j \in \{1, \ldots, 10, 12, 13, 14, 18, 21, 26, 28, 36, 42\}$, а при $k = 7$ возможны только случаи $j \in \{1, 2, 3, 4, 6\}$, такие же, как при $k = 1$.

С л е д с т в и е 1. *Пусть справедливы обозначения теоремы 3, непрерывная дробь элемента $\sqrt{f}/x^s$ периодическая. Пусть дополнительно либо в пункте 1 теоремы 3 имеем $j = 1$, либо в пункте 2 теоремы 3 многочлен f неприводим, либо j четно. Тогда справедливо неравенство $N \le jm - 2g$.*

Если многочлен f неприводим или j четно, то $f_1 \in K^*$, откуда и следует утверждение следствия 1.

Еще одним интересным следствием теоремы 3 является утверждение о конечности числа нормированных дискриминантов ограниченной степени, для которых соответствующие квадратичные иррациональности имеют квазипериодическое разложение в непрерывную дробь.

С л е д с т в и е 2. *Пусть $\mathcal{L} = K(x)(\sqrt{f})$ — гиперэллиптическое поле и C — некоторая постоянная, $\deg f \le C$. Пусть $M = M(C)$ — множество дискриминантов D со старшим коэффициентом 1 и $\deg D \le C$, таких, что $f \mid D$ и элементы поля $\mathcal{L}$ с дискриминантом $D \in M$ обладают квазипериодическим разложением в непрерывную дробь. Тогда множество M конечно.*

Из предложения 3 следует, что множество корней многочленов $T_n(x)$ и $Q_n(x)$ при $n \in \mathbb{N}$, ле-