

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 16. Выпуск 4.

УДК 511.6.

ВЫЧИСЛЕНИЕ ФУНДАМЕНТАЛЬНЫХ S -ЕДИНИЦ В ГИПЕРЭЛЛИПТИЧЕСКИХ ПОЛЯХ РОДА 2 И ПРОБЛЕМА КРУЧЕНИЯ В ЯКОБИАНАХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ¹

М. М. Петрунин (г. Москва)

Посвящается 75-летию
академика В. П. Платонова

Аннотация

В 2010 г. В. П. Платоновым был предложен принципиально новый подход к проблеме кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел. Этот новый подход базируется на вычислении фундаментальных единиц в гиперэллиптических полях. С помощью указанного подхода было доказано существование точек кручения новых порядков. Полное изложение нового метода и полученных на его основе результатов содержится в [2].

В. П. Платонов высказал гипотезу, что если рассмотреть S , состоящее из конечного и бесконечного нормирования, и изменить соответствующим образом определение степени S -единицы, то порядки $\mathbb{Q}$ -точек кручения, как правило, будут определяться степенями фундаментальных S -единиц.

Основным результатом настоящего сообщения является построение фундаментальных S -единиц больших степеней методами, основанными на подходе В. П. Платонова. Вычисление базируется на методах непрерывных дробей и матричной линеаризации.

В настоящей статье получили развитие эффективные алгоритмы вычисления S -единиц методом непрерывных дробей. Улучшенные алгоритмы позволили построить упомянутые выше фундаментальные S -единицы больших степеней.

В качестве следствия получено альтернативное доказательство существования $\mathbb{Q}$ -точек кручения некоторых больших порядков в соответствующих якобианах гиперэллиптических кривых.

¹Работа была выполнена при поддержке грантами РФФИ 13-01-12402 и 15-01-02094-а.

Ключевые слова: фундаментальные единицы, S -единицы, гиперэллиптические поля, якобиевы многообразия, гиперэллиптические кривые, проблема кручения в якобианах, быстрые алгоритмы, непрерывные дроби, матричная линеаризация, $\mathbb{Q}$ -точки кручения.

Библиография: 19 названий.

CALCULATION OF THE FUNDAMENTAL S -UNITS IN HYPERELLIPTIC FIELDS OF GENUS 2 AND THE TORSION PROBLEM IN THE JACOBIANS OF HYPERELLIPTIC CURVES

M. M. Petrunin (Moscow)

Abstract

A new approach to the torsion problem in the Jacobians of hyperelliptic curves over the field of rational numbers was offered by Platonov. This new approach is based on the calculation of fundamental units in hyperelliptic fields. The existence of torsion points of new orders was proved with the help of this approach. The full details of the new method and related results are contained in [2].

Platonov conjectured that if we consider the S consisting of finite and infinite valuation and change accordingly definition of the degree of S -unit, the orders of torsion $\mathbb{Q}$ -points tend to be determined by the degree of fundamental S -units.

The main result of this article is the proof of existence of the fundamental S -units of large degrees. The proof is based on the methods of continued fractions and matrix linearization based on Platonov's approach.

Efficient algorithms for computing S -units using method of continued fractions have been developed. Improved algorithms have allowed to construct the above-mentioned fundamental S -units of large degrees.

As a corollary, alternative proof of the existence of torsion $\mathbb{Q}$ -points of some large orders in corresponding Jacobians of hyperelliptic curves was obtained.

Keywords: fundamental unit, S -unit, hyperelliptic fields, Jacobian, hyperelliptic curves, torsion problem in Jacobians, fast algorithms, continued fractions, matrix linearization, torsion $\mathbb{Q}$ -points.

Bibliography: 19 titles.

1. Введение

В последние 25 лет усилиями целого ряда математиков (Flynn, Leprevost, Howe, Roonen, Ogawa, Elkies и других, см. [8]–[18]) было доказано существование $\mathbb{Q}$ -точек кручения якобианов гиперэллиптических кривых рода 2, определённых над $\mathbb{Q}$, следующих порядков: 11, 13, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29,

30, 32, 34, 35, 39, 40, 45, 60, 63, 70. Эти точки были получены с использованием различных методов, индивидуальных для отдельных порядков.

В. П. Платоновым в работе [1] был предложен принципиально новый подход к проблеме кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел. Этот новый подход базируется на вычислении фундаментальных единиц в гиперэллиптических полях.

С помощью указанного подхода в работах В. П. Платонова и М. М. Петрунина [3], [4] было завершено доказательство гипотезы существования $\mathbb{Q}$ -точек любого порядка ≤ 30 , были единообразно построены все $\mathbb{Q}$ -точки простых порядков $p \leq 29$, а также было доказано существование $\mathbb{Q}$ -точек порядков 33, 36 и 48 в якобианах соответствующих кривых рода 2. Полное изложение нового метода и полученных на его основе результатов содержится в [2].

Для формулировки результатов настоящей статьи нам понадобятся некоторые определения из [2].

Пусть $f(x) = a_{2s}x^{2s} + \dots + a_0 \in \mathbb{Q}[x]$, многочлен $f(x)$ является свободным от квадратов и $a_{2s} = \gamma^2$, $\gamma \in \mathbb{Q}^*$.

Обозначим

$$D_f = \mathbb{Q}[x](\sqrt{f}) = \{\alpha + \beta\sqrt{f} \mid \alpha, \beta \in \mathbb{Q}[x]\}$$

Предположим, что D_f обладает нетривиальными единицами. Тогда мультипликативная группа $D_f^* = \mathbb{Q}^* \times \langle u \rangle$, где $\langle u \rangle$ — бесконечная циклическая группа. Элемент u называется фундаментальной единицей кольца D_f . Поле $L = \mathbb{Q}(x)(\sqrt{f})$ имеет два бесконечных нормирования $w_1(\infty)$, $w_2(\infty)$.

Пусть $S = \{w_1(\infty), w_2(\infty)\}$, тогда u является фундаментальной S -единицей, причём степень $\deg u$ равна порядку класса дивизора $w_1(\infty) - w_2(\infty)$ в $\Delta^\circ(L)$, группе классов дивизоров степени 0 поля L .

В. П. Платонов высказал гипотезу, что если рассмотреть S , состоящее из конечного и бесконечного нормирования, и изменить соответствующим образом определение степени фундаментальной S -единицы, то порядки $\mathbb{Q}$ -точек кручения, как правило, будут определяться степенями фундаментальных S -единиц.

Основным результатом настоящего сообщения является построение фундаментальных S -единиц больших степеней методами, основанными на подходе В. П. Платонова. Вычисление базируется на методах непрерывных дробей и матричной линеаризации из работы [6]. Были построены фундаментальные S -единицы в гиперэллиптических полях рода 2 степеней 20, 21, 22, 24, 25, 26, 27, 30, 32, 34, 40.

В работе [6] была установлена связь проблемы построения S -единиц и теории непрерывных дробей в функциональных полях. Более того, в работе приведён алгоритм построения S -единицы с помощью аппарата непрерывных дробей. В формулировке упомянутого алгоритма использовалось утверждение, доказательство которого было опущено. А именно, в описании алгоритма утверждается, что если для некоторого d , делителя многочлена f , мы нашли первую

подходящую дробь $\frac{p_n}{q_n}$ к $\frac{\sqrt{f}}{d}$, для которой выполняется соответствующий аналог норменного равенства, то это означает, что мы нашли фундаментальную S -единицу, для некоторого S . Априори это равенство может выполняться для нескольких делителей, и тогда мы не можем утверждать, что найденная S -единица фундаментальная. В настоящей статье показано, что алгоритм позволяет построить фундаментальную S -единицу по первой найденной паре $d, \frac{p_n}{q_n}$. Более того, будет доказано, что если такой делитель многочлена f существует, то он единственен с точностью до константы.

В качестве следствия получено доказательство следующего факта, связанного с вычислением S -единиц. В случае, если группа S -единиц нетривиальна, упомянутый алгоритм позволяет построить u — фундаментальную S -единицу, зафиксировав некоторый делитель d многочлена f степени строго меньше $\frac{1}{2} \deg f$. При использовании матричного метода поиска и построения S -единицы из [6] каждой S -единице u^n можно сопоставить минор соответствующей бесконечной ганкелевой матрицы, ранг которого будет меньше максимального. Иными словами, если продолжить выполнять шаги матричного алгоритма после нахождения фундаментальной S -единицы, алгоритм позволит построить все S -единицы вида u^n , $n > 1$. Алгоритм, основанный на использовании непрерывных дробей, ведет себя несколько иначе. В данной работе показано, что при любом d — делителе f — никакому u^{2r} не соответствует (в смысле теоремы 5.8, [6]) никакая подходящая дробь к $\frac{\sqrt{f}}{d}$, в то время как при единственном с точностью до константы d для всякой u^{2r+1} соответствует некоторая подходящая дробь к $\frac{\sqrt{f}}{d}$.

В настоящей статье получили развитие эффективные алгоритмы вычисления S -единиц методом непрерывных дробей. Существенное уменьшение числа вычисляемых коэффициентов и, как следствие, числа арифметических операций позволило значительно сократить время работы алгоритма и построить упомянутые выше фундаментальные S -единицы больших степеней.

В качестве следствия из существования S -единиц больших степеней получено альтернативное доказательство существования $\mathbb{Q}$ -точек кручения некоторых больших порядков в якобианах кривых рода 2. А именно, порядков 20, 21 ..., 30 и 32, 34, 36, 39, 40, 48. Существование S -единицы степени 39 было доказано в неопубликованной работе В. П. Платонова и В. В. Беньш-Кривеца, а доказательство существования в гиперэллиптических полях рода 2 фундаментальных S -единиц степеней 23, 28, 29, 36, 48 было получено в работах [3], [4], [5], и здесь приведено для полноты изложения.

2. Предварительные сведения

Для дальнейшего изложения нам понадобится напомнить некоторые факты и понятия.

Для неприводимого многочлена $h(x) \in \mathbb{Q}[x]$ через v_h будем обозначать нор-

мирование поля $\mathbb{Q}(x)$, задаваемое равенством

$$v_h \left(h(x)^m \frac{P(x)}{Q(x)} \right) = m,$$

где $P(x), Q(x) \in \mathbb{Q}[x]$, $h(x) \nmid P(x)$, $h(x) \nmid Q(x)$, $m \in \mathbb{Z}$. Через v_∞ будем обозначать бесконечное нормирование поля $\mathbb{Q}(x)$

$$v_\infty \left(\frac{P(x)}{Q(x)} \right) = \deg Q(x) - \deg P(x).$$

Пусть теперь $f = a_{2s+1}x^{2s+1} + \dots + a_0 \in \mathbb{Q}[x]$, $a_{2s+1} \neq 0$ — многочлен нечётной степени, свободный от квадратов. Тогда поле $L = \mathbb{Q}(x)(\sqrt{f})$ обладает одним бесконечным нормированием v_∞ . Предположим, что v_h обладает двумя неэквивалентными продолжениями v'_h и v''_h на поле L . Положим далее $S = \{v_\infty, v'_h\}$. Для конечного поля констант проблема построения S -единиц была решена в [6]. Большинство результатов из §2, [6] остаются верны и в случае, когда $\mathbb{Q}$ является полем констант. В частности, верен следующий факт: нетривиальная S -единица существует тогда и только тогда, когда существует фундаментальная S -единица $u = \alpha + \beta\sqrt{f}$, где $\alpha, \beta \in \mathbb{Q}[x]$. Иными словами, вид такой фундаментальной S -единицы остаётся таким же, как и в случае двух бесконечных нормирований.

Норма нетривиальной S -единицы $u = \alpha + \beta\sqrt{f}$ при указанном S принимает вид $N(u) = \alpha^2 - \beta^2 f = bh^m$. Это позволяет определить понятие степени S -единицы следующим образом (см. [5]).

ОПРЕДЕЛЕНИЕ 1. *Степенью S -единицы $u = \alpha + \beta\sqrt{f}$ называется число $\deg u = m$, где m — показатель степени многочлена h в норменном уравнении*

$$\alpha^2 - \beta^2 f = bh^m. \quad (1)$$

Существование нетривиальной S -единицы при указанном S равносильно наличию решения норменного уравнения $\alpha^2 - \beta^2 f = bh^m$ для некоторого $m > 0$ в многочленах $\alpha, \beta \in \mathbb{Q}[x]$, $b \in \mathbb{Q}^*$. Далее без ограничения общности будем рассматривать только S -единицы положительной степени, заменив при необходимости u на u^{-1} .

ПРЕДЛОЖЕНИЕ 1. ([5]) *Поле $L = \mathbb{Q}(x)(\sqrt{f})$ имеет нетривиальную S -единицу тогда и только тогда, когда класс дивизора $v'_h - lv_\infty$, где $l = \deg h$, имеет конечный порядок в группе классов дивизоров $\Delta^\circ(L)$. При этом степень фундаментальной S -единицы равна порядку класса дивизора $v'_h - lv_\infty$ в $\Delta^\circ(L)$.*

Из предложения следует, что степень фундаментальной S -единицы равна порядку соответствующей $\mathbb{Q}$ -точки кручения в якобиане J_f .

3. S -единицы и нормирование первой степени

Здесь и далее по тексту §3 будем считать, что $\deg h = 1$, $h \in \mathbb{Q}[x]$. В этом случае мы будем применять метод непрерывных дробей для построения S -единиц из [6]. В оригинальной работе авторами были сформулированы и доказаны результаты для случая $\mathbb{F}_q$ в качестве поля констант. Однако, большая часть утверждений и теорем справедлива и для случая $\mathbb{Q}$ в качестве поля констант. Приведем адаптированные для поля $\mathbb{Q}$ результаты работы [6], относящиеся к указанному методу, а также утверждения, которые необходимы для понимания основных результатов настоящей статьи.

3.1. Разложение в непрерывную дробь элемента квадратичного поля

Пусть $\xi \in \overline{\mathbb{Q}(x)}$, $v_h(\xi) = 0$, и пусть Σ – выбранная в $\mathbb{Q}[x]$ фиксированная система представителей смежных классов по идеалу (h) , состоящая из всех многочленов степени меньшей, чем $\deg h$. Представим ξ в виде формального степенного ряда

$$\xi = \sum_{j=0}^{\infty} d_j h^j,$$

где $d_j \in \Sigma$. Для произвольного степенного ряда

$$\psi = \sum_{j=e}^{\infty} b_j h^j, \quad \psi \in \overline{\mathbb{Q}(x)}$$

введем обозначение

$$[\psi] = \begin{cases} \sum_{i=e}^0 b_i h^i, & \text{если } e \leq 0, \\ 0, & \text{если } e > 0. \end{cases}$$

Положим $a_0 = [\xi] = d_0$. Если $\xi - a_0 \neq 0$, то положим

$$\xi_1 = \frac{1}{\xi - a_0} \in \overline{\mathbb{Q}(x)}, \quad a_1 = [\xi_1].$$

Далее по индукции определяем элементы a_i, ξ_i : если $\xi_{i-1} - a_{i-1} \neq 0$, то

$$\xi_i = \frac{1}{\xi_{i-1} - a_{i-1}} \in \overline{\mathbb{Q}(x)}, \quad a_i = [\xi_i].$$

В результате мы получим *непрерывную дробь*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}. \quad (2)$$

Справедливо утверждение, что непрерывная дробь вида (2) произвольного элемента $\psi \in \overline{\mathbb{Q}(x)}$ конечна тогда и только тогда, когда $\psi \in \mathbb{Q}(x)$.

Будем использовать стандартную сокращенную запись $[a_0, a_1, a_2, \dots]$ для непрерывной дроби (2). По построению, $\xi_n = [a_n, a_{n+1}, \dots]$.

Определим по индукции элементы $p_i, q_i \in \mathbb{Q}(x)$. Положим

$$p_{-2} = 0, \quad p_{-1} = 1, \quad q_{-2} = 1, \quad q_{-1} = 0$$

и если $n \geq 0$, то

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}. \quad (3)$$

Тогда $p_n/q_n = [a_0, a_1, a_2, \dots, a_n]$ при $n \geq 0$. Стандартным образом можно показать (см. [7]), что для $n \geq -1$ справедливы соотношения

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \quad (4)$$

$$q_n \xi - p_n = \frac{(-1)^n}{q_n \xi_{n+1} + q_{n-1}}, \quad (5)$$

$$\xi = \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}}. \quad (6)$$

Дробь p_n/q_n назовем n -й *подходящей дробью* к ξ . По построению, $v_h(a_n) = v_h(\xi_n) < 0$ для $n \geq 1$.

3.2. Квадратичная иррациональность

Пусть $\xi \in \mathbb{Q}((h))$ является корнем квадратного многочлена

$$H(X) = \lambda_2 X^2 + \lambda_1 X + \lambda_0, \quad \text{где } \lambda_0, \lambda_1, \lambda_2 \in \mathbb{Q}[h]. \quad (7)$$

Тогда элемент ξ называется *квадратичной иррациональностью*. Пусть $\xi = [a_0, a_1, \dots]$ — разложение ξ в непрерывную дробь. Положим

$$D = \lambda_1^2 - 4\lambda_0\lambda_2, \quad H(X, Y) = \lambda_2 X^2 + \lambda_1 XY + \lambda_0 Y^2.$$

Тогда из (6) получаем

$$\xi_{n+1} = \frac{B_n + \lambda_2 \xi}{A_n}, \quad (8)$$

где

$$A_n = (-1)^{n+1} H(p_n, q_n), \\ B_n = (-1)^n (\lambda_2 p_{n-1} p_n + \lambda_1 p_{n-1} q_n + \lambda_0 q_{n-1} q_n).$$

По аналогии с рассуждениями из [6] можно показать, что A_n, B_n являются многочленами из $\mathbb{Q}[x]$, причем их степени не превосходят

$$\Lambda = \max\{\deg \lambda_0, \deg \lambda_1, \deg \lambda_2\}.$$

Пусть $\xi = \frac{\sqrt{f}}{d}$ для некоторого делителя d многочлена f , $0 \leq \deg d < \frac{1}{2} \deg f$. В этом случае

$$H(X) = dX^2 - \frac{f}{d}.$$

Выражение (8) в нашем случае имеет вид

$$\xi_{n+1} = \frac{B_n + \sqrt{f}}{A_n}. \quad (9)$$

Стандартным образом можно вывести следующие рекуррентные формулы:

$$B_n = a_n A_{n-1} - B_{n-1}, \quad (10)$$

$$A_n = A_{n-2} + a_n (B_{n-1} - B_n). \quad (11)$$

3.3. Наилучшие приближения

В дальнейшем нам потребуется понятие наилучшего приближения к элементу $\psi \in \mathbb{Q}(x)$. Если $a/b \in \mathbb{Q}(x)$, где $a, b \in \mathbb{Q}[x]$ — взаимно простые многочлены, то разложим a и b по степеням h :

$$a = a_0 + a_1 h + \dots + a_e h^e, \quad b = b_0 + b_1 h + \dots + b_t h^t,$$

где $a_i, b_i \in \Sigma$, $a_e \neq 0$, $b_t \neq 0$. Тогда, разделив a и b на h^r , где $r = \max\{e, t\}$, мы представим дробь a/b в виде

$$\frac{a}{b} = \frac{c_{-k} h^{-k} + \dots + c_0}{d_{-l} h^{-l} + \dots + d_0}, \quad (12)$$

где $c_i, d_i \in \Sigma$, $c_{-k} \neq 0$, $d_{-l} \neq 0$, $r = \max\{k, l\}$, c_0 и d_0 одновременно не равны нулю. Будем в дальнейшем предполагать, что все элементы из $\mathbb{Q}(x)$ записаны в виде (12).

ОПРЕДЕЛЕНИЕ 2. Несократимая дробь $p/q \in \mathbb{Q}(x)$ является наилучшим приближением к $\psi \in \overline{\mathbb{Q}(x)}$, если для любой другой несократимой дроби $a/b \neq p/q$, такой, что $v_h(b) \geq v_h(q)$, справедливо неравенство

$$v_h(\psi - \frac{p}{q}) > v_h(\psi - \frac{a}{b}).$$

Приведем здесь без доказательства некоторые важные для изложения результаты из [6], относящиеся к понятию наилучшего приближения.

ТЕОРЕМА 1 ([6]). Дробь p/q является наилучшим приближением к ψ тогда и только тогда, когда $v_h(\psi - p/q) > -2v_h(q)$.

ПРЕДЛОЖЕНИЕ 2 ([6]). Если дроби a/b и c/d — такие наилучшие приближения к ψ , что $v_h(b) = v_h(d)$, то найдется константа $\gamma \in \mathbb{Q}^*$ такая, что $a = \gamma c$, $b = \gamma d$.

ТЕОРЕМА 2 ([6]). Справедливы следующие утверждения:

1. n -я подходящая дробь p_n/q_n к ψ является наилучшим приближением к ψ ;
2. Если дробь a/b является наилучшим приближением к ψ , то найдется такая подходящая дробь p_n/q_n к ψ и такая константа $c \in \mathbb{Q}^*$, что $a = cp_n$, $b = cq_n$.

3.4. Теорема о вычислении фундаментальной S -единицы

Сформулируем аналог теоремы 5.8 из работы [6] для поля $\mathbb{Q}$.

ТЕОРЕМА 3. Предположим, что для некоторого минимального натурального t уравнение

$$\alpha^2 - \beta^2 f = ch^m \quad (13)$$

имеет решение в многочленах $\alpha, \beta \in \mathbb{Q}[x]$, $\beta \neq 0$ для некоторой константы $c \in \mathbb{Q}$. Справедливы следующие утверждения

1. Если $m = 2t + 1$, то $\frac{\alpha}{\beta}$ является наилучшим приближением к $\sqrt{f}$. Таким образом, $\frac{\alpha}{\beta} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\sqrt{f}$.
2. Если $m = 2t$, то найдется делитель d многочлена f , $\deg d < \frac{1}{2} \deg f$, такой что уравнение

$$\frac{f}{d} \beta_1^2 - d \alpha_1^2 = bh^t, \quad (14)$$

где $b \in \mathbb{Q}$, имеем решение в многочленах $\alpha_1, \beta_1 \in \mathbb{Q}[x]$. При этом $\frac{\alpha_1}{\beta_1}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$ и, следовательно, $\frac{\alpha_1}{\beta_1} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{f}}{d}$.

Наоборот, если $\alpha_1, \beta_1 \in \mathbb{Q}[x]$ — решение (14), то $\frac{\alpha_1}{\beta_1}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$, $\frac{\alpha_1}{\beta_1} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{f}}{d}$ и многочлены α и β , определяемые по формулам

$$\alpha = \frac{1}{2} \left(d \alpha_1^2 + \frac{f}{d} \beta_1^2 \right), \quad \beta = \alpha_1 \beta_1, \quad (15)$$

являются решением уравнения (13) для $m = 2t$.

Отметим, что теорема 3 становится неверной в случае $\deg h > 1$. Контрпример приведён в [6] (примеры 3.7 и 5.7).

3.5. Единственность делителя и полугруппа монарных S -единиц

Как отмечалось во введении, утверждение о единственности делителя d , упомянутого в теореме 3 требует доказательства. Без него, в частности, нельзя дать ответ на следующий вопрос. Если для некоторого d , делителя многочлена f , мы нашли $\frac{p_n}{q_n}$ — первую подходящую дробь к $\frac{\sqrt{f}}{d}$, для которой выполняется равенство $dp_n^2 - \frac{f}{d}q_n^2 = bh^m$, где $b \in \mathbb{Q}$, означает ли это, что мы нашли фундаментальную S -единицу? В этом параграфе мы докажем, что ответ положительный. Мы покажем, что алгоритм позволяет построить фундаментальную S -единицу по первой найденной паре $d, \frac{p_n}{q_n}$. Более того, мы докажем, что если такой делитель многочлена f существует, то он в единственен с точностью до константы.

Прежде чем перейти к формулировке основного результата параграфа нам потребуется ввести понятие монарной S -единицы и показать, что без ограничения общности многочлены f и h можно считать монарными, т.е. многочленами, старшие коэффициенты которых равны 1. Напомним, что здесь, как и на протяжении всего §3 мы считаем, что $\deg h = 1$.

Пусть $f(x) = c_{2s+1}x^{2s+1} + \dots + c_0$, $c_{2s+1} \neq 0$. Для $a \neq 0, a \in \mathbb{Q}$ замена

$$(x, y) \rightarrow (x/a, y/a^s)$$

переводит $\mathbb{Q}$ -точки кривой C_f , заданной уравнением $y^2 = f(x)$, в $\mathbb{Q}$ -точки кривой $(y/a^s)^2 = f(x/a)$. Такая замена является изоморфизмом кривых. При этом, если положить $a = c_{2s+1}$, то многочлен $f(x)$ перейдет в монарный той же степени, поэтому далее без ограничения общности будем считать, что $f(x)$ монарный.

Мы будем считать, что наибольший общий делитель (α, β) двух многочленов $\alpha, \beta \in \mathbb{Q}[x]$ всегда является монарным многочленом. В этом случае утверждение: «степень (α, β) равна 0» можно равносильно записать следующим образом: « $(\alpha, \beta) = 1$ ».

Существование двух продолжений нормирования v_h на поле L влечет $(h, f) = 1$. Без ограничения общности многочлен $h(x)$ также положить монарным, поскольку для изучения подгруппы кручения якобиана $J_f(\mathbb{Q})$ нас в первую очередь интересуют корни многочлена $h(x)$. В силу нечетности степени многочлена $f(x)$ коэффициент b норменного уравнения (1) по абсолютной величине является квадратом старшего коэффициента одного из многочленов α или β . Значит можно поделить обе части (1) на $|b|$ и далее рассматривать норменное уравнение вида

$$\alpha^2 - \beta^2 f = (-1)^m h^m, \quad (16)$$

где старшие коэффициенты многочленов f и h удовлетворяют следующим соотношениям: $\text{lc}(f) = 1$, $\text{lc}(h) = 1$. Кроме того, хотя бы один из многочленов α^2 или β^2 в (16) также монарный.

Если уравнение (16) имеет решение α, β и $u = \alpha + \beta\sqrt{f}$ — S -единица, то $-u = -\alpha - \beta\sqrt{f}$ также является S -единицей, а пара $-\alpha, -\beta$ является решением (16). Чтобы устранить эту неопределённость, введём следующее понятие.

ОПРЕДЕЛЕНИЕ 3. Будем называть S -единицу $u = \alpha + \beta\sqrt{f}$, $\alpha, \beta \in \mathbb{Q}[x]$, мо-
нарной, если $lc(\alpha) = 1$ в случае, когда степень S -единицы u является чётным
числом, и $lc(\beta) = 1$ в противном случае.

Заметим, что в случае мо-
нарной S -единицы выполняется $(\alpha, h) = 1$ и $N(u) = h^m$ для некоторого натурального m , то есть многочлены α и β удовле-
творяют мо-
нарному норменному уравнению (16). Легко видеть, что если u_1, u_2 —
мо-
нарные S -единицы, то произведение $u_1 u_2$ также является мо-
нарной S -едини-
цей.

Существование S -единицы положительной степени влечет существование
мо-
нарной S -единицы той же степени, так как разрешимость норменных уравне-
ний (1) и (16) эквивалентна. Кроме того, возведение в степень мо-
нарной фунда-
ментальной S -единицы порождает также мо-
нарную S -единицу. Поэтому мно-
жество всех мо-
нарных S -единиц образует полугруппу. Пусть u_1 — фунда-
ментальная мо-
нарная S -единица. Элемент $u \in \mathcal{U}_S$ также назовем мо-
нарным, если
 $u = u_1^k$ для некоторого целого k . Тогда множество мо-
нарных элементов $\mathcal{U}_S$ обра-
зует группу обратимых мо-
нарных элементов кольца $\mathcal{O}_h$ — S -целых элементов
поля L . Эта группа изоморфна $\mathcal{U}_S/\mathbb{Q}$.

Рассмотрим уравнение

$$d\Phi^2 - \frac{f}{d}\Gamma^2 = h^t, \quad (17)$$

с параметром $t \in \mathbb{N}$ и неизвестными $d, \Phi, \Gamma \in \mathbb{Q}[x]$, причем $(\Phi, h) = 1$ и d — неко-
торый мо-
нарный делитель многочлена f . Это уравнение более общего вида, чем
норменное уравнение (16). Далее мы покажем, что из разрешимости уравнения
(17) следует разрешимость (16) и обратно. Также покажем, что при фиксиро-
ванных параметрах t и m каждое из уравнений имеет не более одного решения.
В частности, отсюда будет следовать, что решение (17) может существовать
только для одного конкретного мо-
нарного делителя d многочлена f .

ЛЕММА 1. Пусть фиксировано $t = t_0$ и уравнение (17) имеет решение,
тогда это решение единственное. Кроме того, $d = (\alpha + h^t, f)$, где многочлен
 $\alpha = d\Phi^2 + \frac{f}{d}\Gamma^2$.

ДОКАЗАТЕЛЬСТВО. Пусть для некоторого $t = t_0 \in \mathbb{N}$ и собственного мо-
нарного делителя d многочлена f , уравнение (17) имеет решение Φ, Γ . Тогда
многочлены α, β , определенные по формулам

$$\alpha = d\Phi^2 + \frac{f}{d}\Gamma^2, \quad \beta = 2\Phi\Gamma, \quad (18)$$

являются решением диофантового уравнения

$$\alpha^2 - f\beta^2 = h^{2t}. \quad (19)$$

Из (18) и (17) следует, что

$$\alpha + h^t = 2d\Phi^2, \quad \alpha - h^t = 2\frac{f}{d}\Gamma^2.$$

С другой стороны, из (19) имеем

$$(\alpha - h^t)(\alpha + h^t) = f\beta^2. \quad (20)$$

Учитывая, что многочлен f бесквадратный, получаем $d = (\alpha + h^t, f)$.

Так как по условию леммы полугруппа монарных S -единиц нетривиальна, то существует единственная монарная S -единица степени $2t_0$, следовательно пара многочленов α, β однозначно определена. По α, β мы можем однозначно восстановить многочлены d, Φ, Γ , удовлетворяющие условиям леммы. Действительно, положим

$$d = (\alpha + h^t, f), \quad \alpha + h^t = 2dw_1, \quad \alpha - h^t = 2\frac{f}{d}w_2. \quad (21)$$

Заметим, что $(w_1, w_2) = 1$, так как иначе многочлен α делился бы на h и $\alpha + \beta\sqrt{f}$ не была бы монарной S -единицей. С другой стороны, из (20) следует, что $4w_1w_2 = \beta^2$, а значит можем положить

$$w_1 = \Phi^2, \quad w_2 = \Gamma^2, \quad (22)$$

причем Φ — монарный, если t четно и Γ — монарный в противном случае. Следовательно, набор (d, Φ, Γ) является решением (17) и совпадает с решением, данным в условии леммы.

Если в условии леммы решение (17) существует при $d = 1$, то $\Phi + \Gamma\sqrt{f}$ является монарной S -единицей степени t_0 , и в полугруппе монарных S -единиц она единственная. Кроме того, $\alpha + h^t = 2\Phi^2$, значит $(\alpha + h^t, f) = 1$. $\square$

Отметим, что уравнение (17) имеет решение для некоторого монарного делителя d многочлена f тогда и только тогда, когда уравнение

$$\hat{d}\hat{\Phi}^2 - \frac{f}{\hat{d}}\hat{\Gamma}^2 = bh^t \quad (23)$$

имеет решение для делителя $\hat{d}$ многочлена f с произвольным старшим коэффициентом и некоторой постоянной $b \in \mathbb{Q}$. Действительно, необходимость очевидна. Для доказательства достаточности преобразуем (23) к виду

$$\frac{\hat{d}}{b}\hat{\Phi}^2 - \frac{f}{b\hat{d}}\hat{\Gamma}^2 = h^t,$$

причем в силу нечетности степени f имеем $\gamma_1 \neq \gamma_2$, где

$$\gamma_1 = \deg \frac{f}{b\hat{d}}\hat{\Gamma}^2, \quad \gamma_2 = \deg \frac{\hat{d}}{b}\hat{\Phi}^2, \quad t = \max(\gamma_1, \gamma_2).$$

Если $t = \gamma_1$, то в силу монарности многочленов f и h имеем $\text{lc}(\hat{\Gamma})^2 = -b \cdot \text{lc}(\hat{d})$, и число $-\frac{\text{lc}(\hat{d})}{b}$ является полным квадратом, то есть $-\frac{\text{lc}(\hat{d})}{b} = \kappa^2$, $\kappa = \frac{\text{lc}(\hat{\Gamma})}{b} \in \mathbb{Q}$. Тогда

$$d = \frac{\text{lc}(\hat{d}) \cdot f}{\hat{d}}, \quad \frac{f}{d} = \frac{\hat{d}}{\text{lc}(\hat{d})}, \quad \Phi = \frac{\hat{\Gamma}}{\text{lc}(\hat{\Gamma})}, \quad \Gamma = \kappa \cdot \hat{\Phi}$$

и справедливо (17). Если $t = \gamma_2$, то

$$\text{lc}(\hat{\Phi})^2 = \frac{b}{\text{lc}(\hat{d})}, \quad \kappa^2 = b \cdot \text{lc}(\hat{d}), \quad \kappa = \frac{b}{\text{lc}(\hat{\Phi})},$$

$$d = \frac{\hat{d}}{\text{lc}(\hat{d})}, \quad \Phi = \frac{\hat{\Phi}}{\text{lc}(\hat{\Phi})}, \quad \Gamma = \frac{\hat{\Gamma}}{\kappa}$$

и также выполнено (17).

Таким образом, справедливо предложение.

ПРЕДЛОЖЕНИЕ 3. *Норменные уравнения (1), (16), (23), (17) одновременно либо имеют либо не имеют нетривиальное решение.*

Далее мы покажем, какие из решений уравнений (16), (17) могут соответствовать наилучшему приближению к $\sqrt{f}$ или $\frac{\sqrt{f}}{d}$, и тем самым выясним, какие S -единицы могут быть вычислены с помощью аппарата непрерывных дробей.

Напомним, что если $u = u_1$ — фундаментальная монарная S -единица, то полугруппу всех монарных S -единиц можно записать следующим образом:

$$\mathbb{U}_S = \{u_j = u^j, j = 1, 2, \dots\},$$

$$u_j = \alpha_j + \beta_j \sqrt{f}, \quad \alpha_j, \beta_j \in \mathbb{Q}[x], \quad (\alpha_j, h) = 1, \quad j \in \mathbb{N}.$$

Из доказательства леммы 1 следует, что любой монарной S -единице $u_j = \alpha_j + \beta_j \sqrt{f}$ степени $m_j = 2t$ можно по формулам (21) и (22) взаимно однозначно сопоставить набор d_j, Φ_j, Γ_j , удовлетворяющий (17) и (18), причем $\Phi_{2j} = \alpha_j$ и $\Gamma_{2j} = \beta_j$. Теперь результаты этого параграфа можно сформулировать в одной теореме.

ТЕОРЕМА 4. *Пусть $u = u_1$ — фундаментальная монарная S -единица степени t .*

Если t четно, то существует собственный монарный делитель d многочлена f такой, что $d_{2j} = 1$, $d_{2j-1} = d$ для любого $j \in \mathbb{N}$. При этом $\frac{\Phi_{2j-1}}{\Gamma_{2j-1}}$ — наилучшее приближение к $\frac{\sqrt{f}}{d}$, а отношение $\frac{\Phi_{2j}}{\Gamma_{2j}} = \frac{\alpha_j}{\beta_j}$ не является наилучшим приближением к $\sqrt{f}$.

Если t нечетно, то для любого чётного $j \in \mathbb{N}$: $d_{2j} = 1$, а для нечётного j : $d_{2j} = f$. Многочлены d_{2j-1} не определены. При этом $\frac{\alpha_{2j-1}}{\beta_{2j-1}}$ — наилучшее приближение к $\sqrt{f}$, а отношение $\frac{\alpha_{2j}}{\beta_{2j}}$ не является наилучшим приближением к $\sqrt{f}$.

Доказательство теоремы 4 разобьем на четыре леммы. Пусть u — монарная фундаментальная S -единица степени m .

ЛЕММА 2. *Если $m = 2t$, то существует собственный монарный делитель d многочлена f такой, что $d_{2j-1} = d$ для любого $j \in \mathbb{N}$.*

ДОКАЗАТЕЛЬСТВО. Пусть $u = \alpha + \beta\sqrt{f}$, тогда

$$u_{2j-1} = u^{2j-1}, \quad \alpha_{2j-1} = \alpha^{2j-1} + fR,$$

где $R \in \mathbb{Q}[x]$. Следовательно,

$$\alpha_{2j-1} - h^{t(2j-1)} = (\alpha - h^t)(\alpha^{2j-2} + \dots + h^{(2j-2)t}) + fR, \quad (24)$$

$$\alpha_{2j-1} + h^{t(2j-1)} = (\alpha + h^t)(\alpha^{2j-2} - \dots + h^{(2j-2)t}) + fR. \quad (25)$$

Положим $d = (\alpha + h^t, f)$, тогда в силу монарности f , α и d из (20) получаем

$$(\alpha - h^t, \alpha + h^t) = 1, \quad (\alpha - h^t, f) = \frac{f}{d},$$

и аналогично

$$d_{2j-1} = (\alpha_{2j-1} + h^t, f), \quad (\alpha_{2j-1} - h^{t(2j-1)}, f) = \frac{f}{d_{2j-1}},$$

$$(\alpha_{2j-1} - h^{t(2j-1)}, \alpha_{2j-1} + h^{t(2j-1)}) = 1.$$

Из равенства (25) следует, что d_{2j-1} делится на d , а из равенства (24) следует $\frac{f}{d_{2j-1}}$ делится на $\frac{f}{d}$, откуда с неизбежностью заключаем $d_{2j-1} = d$.

Отметим, что если $d = 1$, то уравнение (17) имеет вид (16) что противоречит минимальности $m = 2t$ в условии леммы. $\square$

ЛЕММА 3. $d_{2j} = 1$ при чётном jm , и $d_{2j} = f$ при нечётном jm , $j \in \mathbb{N}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим монарную фундаментальную S -единицу u степени m , возведенную в четную степень

$$\alpha_{2j} + \beta_{2j}\sqrt{f} = u_{2j} = u^{2j} = (u^j)^2 = (\alpha_j + \beta_j\sqrt{f})^2. \quad (26)$$

Тогда по лемме 1 при $t = jm$ и формуле

$$\alpha_j^2 - f\beta_j^2 = (-h)^{jm},$$

а также формулам (26), (21), (22) при чётном jm получаем, что

$$2f\beta_j^2 = \alpha_{2j} - h^{jm} = 2\frac{f}{d_{2j}}\Gamma_{2j}^2,$$

поскольку уравнение (17) имеет единственное решение. Следовательно,

$$(\alpha_{2j} - h^{jm}, f) = f, \quad d_{2j} = (\alpha_{2j} + h^{jm}, f) = 1.$$

При чётном jm получаем

$$2f\beta_j^2 = \alpha_{2j} + h^{jm} = 2d_{2j}\Phi_{2j}^2,$$

Следовательно,

$$d_{2j} = (\alpha_{2j} + h^{jm}, f) = f.$$

□

ЛЕММА 4. Если t чётно, то $\frac{\alpha_j}{\beta_j} = \frac{\Phi_{2j}}{\Gamma_{2j}}$ не является наилучшим приближением к $\frac{\sqrt{f}}{d_{2j}} = \sqrt{f}$ для любого $j \in \mathbb{N}$. Если t нечётно, то $\frac{\alpha_j}{\beta_j}$ не является наилучшим приближением к $\sqrt{f}$ для любого чётного $j = 2k$, $k \in \mathbb{N}$.

ДОКАЗАТЕЛЬСТВО. Так как хотя бы одно из чисел t или j чётно, мы можем записать $mj = 2t$ для некоторого $t \in \mathbb{N}$. Тогда в силу предложения 2.1, [6] мы можем считать, что $v'_h(\alpha_j - \beta_j\sqrt{f}) = 0$, $v'_h(\alpha_j + \beta_j\sqrt{f}) = 2t$. Разложим α_j и β_j по степеням h :

$$\alpha_j = b_0 + b_1h + \dots + b_{e-1}h^{e-1} + h^e, \quad \beta_j = c_0 + c_1h + \dots + c_rh^r,$$

причем из вида норменного уравнения (16) в силу нечётности $\deg f$ и чётности $\deg u_j = 2t$, многочлен α_j монарен, $e = t$ и $r < e$, а также $c_0 \neq 0$, $b_0 \neq 0$, так как иначе $h \mid (\alpha_j, \beta_j)$, а это не так.

Рассмотрим элемент $\bar{\alpha}_j + \bar{\beta}_j\sqrt{f}$, где

$$\bar{\alpha}_j = \frac{\alpha_j}{h^e} = b_0h^{-e} + \dots + 1, \quad \bar{\beta}_j = \frac{\beta_j}{h^e} = c_0h^{-e} + \dots + c_rh^{r-e}.$$

Так как $\frac{\bar{\alpha}_j}{\bar{\beta}_j}$ имеет вид (12) и

$$v'_h(\bar{\alpha}_j + \bar{\beta}_j\sqrt{f}) = 2t - e = e = -v'_h(\bar{\beta}_j),$$

то по теореме 1 дробь $\frac{\bar{\alpha}_j}{\bar{\beta}_j} = \frac{\alpha_j}{\beta_j}$ не может являться наилучшим приближением к $\sqrt{f}$. Тогда по теореме 2 отношение $\frac{\alpha_j}{\beta_j} \neq \frac{p_n}{q_n}$ ни для какой подходящей дроби $\frac{p_n}{q_n}$ к $\sqrt{f}$. □

Из леммы 4 и теоремы 1 о наилучшем приближении следует, что

- среди подходящих дробей $\frac{p_n}{q_n}$ к $\sqrt{f}$ не найдётся такой дроби, для которой $\frac{\alpha}{\beta} = \frac{p_n}{q_n}$ и для многочленов α и β выполнено (16) для какого-либо чётного $m \in \mathbb{N}$;

- если существует фундаментальная S -единица и её степень – чётное число, то среди подходящих дробей $\frac{p_n}{q_n}$ к $\sqrt{f}$ не найдётся такой дроби, что для многочленов Φ и Γ , для которых $\frac{\Phi}{\Gamma} = \frac{p_n}{q_n}$, $\frac{\Phi}{\Gamma} = \frac{\Phi_{2j}}{\Gamma_{2j}}$ для некоторого $j \in \mathbb{N}$ и выполнено (17) для какого-либо $t \in \mathbb{N}$ и d – монарного делителя f .

Далее в лемме 5 мы докажем, что при условии существования S -единицы

- перебирая различные подходящие дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{f}}{d}$ при всевозможных монарных делителях d многочлена f , мы найдем многочлены d , Φ и Γ , для которых $\frac{\Phi}{\Gamma} = \frac{p_n}{q_n}$ и выполнено (17) для некоторого четного $t \in \mathbb{N}$ тогда и только тогда, когда $\frac{\Phi}{\Gamma} = \frac{\Phi_{2j-1}}{\Gamma_{2j-1}}$ для некоторого $j \in \mathbb{N}$;
- перебирая различные подходящие дроби $\frac{p_n}{q_n}$ к $\sqrt{f}$, мы найдем многочлены α и β , для которых $\frac{\alpha}{\beta} = \frac{p_n}{q_n}$ и выполнено (16) для некоторого нечетного $t \in \mathbb{N}$ тогда и только тогда, когда $\frac{\alpha}{\beta} = \frac{\alpha_{2j-1}}{\beta_{2j-1}}$ для некоторого $j \in \mathbb{N}$.

ЛЕММА 5. Если t чётно, то $\frac{\Phi_{2j-1}}{\Gamma_{2j-1}}$ – наилучшее приближение к $\frac{\sqrt{f}}{d_{2j-1}} = \frac{\sqrt{f}}{d}$ для любого $j \in \mathbb{N}$. Если t нечётно, то $\frac{\alpha_{2j-1}}{\beta_{2j-1}}$ – наилучшее приближение к $\sqrt{f}$ для любого $j \in \mathbb{N}$.

ДОКАЗАТЕЛЬСТВО. В силу того, что при $d = 1$ вид уравнений (16) и (17) совпадает, то без ограничения общности для доказательства леммы мы можем рассматривать только уравнение (17) с разделением случаев $d = 1$ при нечетном t и $\deg d > 1$ при четном t . Покажем, что в каждом из этих случаев отношение $\frac{\Phi}{\Gamma}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$.

Запишем (17) в виде

$$d \left(\Phi - \frac{\sqrt{f}}{d} \Gamma \right) \left(\Phi + \frac{\sqrt{f}}{d} \Gamma \right) = h^t. \quad (27)$$

Так как $v'_h(d) = 0$, $v'_h(\sqrt{f}) = 0$, то в силу предложения 2.1, [6] мы можем считать, что

$$v'_h \left(\Phi - \frac{\sqrt{f}}{d} \Gamma \right) = 0, \quad v'_h \left(\Phi + \frac{\sqrt{f}}{d} \Gamma \right) = t.$$

Разложим Φ и Γ по степеням h :

$$\Phi = b_0 + b_1 h + \dots + b_e h^e, \quad \Gamma = c_0 + c_1 h + \dots + c_r h^r,$$

где $b_i, c_i \in \mathbb{Q}$, $b_e \neq 0$, $c_r \neq 0$. Сравнивая степени в левой и правой части (27) имеем

$$t = \max(\deg d + 2e, \deg f - \deg d + 2r),$$

откуда в каждом из двух рассматриваемых случаев получаем $e < t/2$, $r < t/2$.

Пусть $l = \max(r, e)$. Рассмотрим элемент $\bar{\Phi} + \frac{\sqrt{f}}{d} \bar{\Gamma}$, где

$$\bar{\Phi} = \frac{\Phi}{h^l}, \quad \bar{\Gamma} = \frac{\Gamma}{h^l}.$$

Так как $\frac{\bar{\Phi}}{\bar{\Gamma}}$ имеет вид (12) и

$$v'_h(\bar{\Phi} + \frac{\sqrt{f}}{d}\bar{\Gamma}) = t - l > l = -v'_h(\bar{\Gamma}),$$

то по теореме 1 дробь $\frac{\bar{\Phi}}{\bar{\Gamma}} = \frac{\Phi}{\Gamma}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$. Тогда по теореме 2 получаем $\frac{\Phi}{\Gamma} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{f}}{d}$.

Теорема 4 доказана. $\square$

3.6. Базовый алгоритм метода непрерывных дробей

В [6] отмечено, что теорема 3 дает алгоритм для вычисления фундаментальной S -единицы в случае $\deg h = 1$. Пусть $d_1, \dots, d_r$ — все делители многочлена f степени, не превосходящей $1/2 \deg f$. Будем последовательно вычислять подходящие дроби к $\sqrt{f}$, $\sqrt{f}/d_1, \dots, \sqrt{f}/d_r$ и для каждой подходящей дроби p_n/q_n проверять, выполняется ли равенство (14):

$$\frac{f}{d_i} \beta_1^2 - d_i \alpha_1^2 = bh^t, \quad \frac{p_n}{q_n} = \frac{\alpha_1}{\beta_1}.$$

Алгоритм заканчивает работу, как только мы найдем подходящую дробь p_n/q_n , удовлетворяющую (14). Тогда по формулам (15) находим решение α, β нормального уравнения (13). В этом случае либо $\alpha + \beta\sqrt{f}$, либо $\alpha - \beta\sqrt{f}$ будет фундаментальной S -единицей.

Выше было показано, что в случае существования фундаментальной S -единицы существует единственный делитель $d \in \{1, d_1, \dots, d_r\}$, для которого в приведенном алгоритме найдется соответствующая подходящая дробь p_n/q_n , дающая решение (14).

С вычислительной точки зрения алгоритм имеет следующие особенности. Во-первых, на предварительном этапе нам потребуется вычислить $O(n^2)$ коэффициентов каждого $\sqrt{f}/d$ для нахождения подходящей дроби p_n/q_n . Во-вторых, количество коэффициентов, вычисляемых при проверке равенства (14) и нахождении дробно-рациональных функций p_n, q_n на каждом шаге, растет линейным образом, а следовательно, общее количество коэффициентов растет квадратичным образом относительно текущего шага алгоритма. Кроме того, существенным этапом является этап разложения многочлена f на множители, и поиск делителей. На эту тему имеется большое количество работ (см., например, [19] и цитируемую там литературу), и обсуждение этого вопроса выходит за рамки настоящей статьи.

На практике реализация этого алгоритма с полем $\mathbb{Q}$ в качестве поля констант не позволяет вычислить p_n, q_n для достаточно больших n за разумное время.

Ниже будут приведены два алгоритма, каждый из которых с вычислительной точки зрения существенно превосходит указанный алгоритм. В частности,

оба алгоритма требуют вычисления фиксированного количества коэффициентов на каждом шаге, включая предварительные вычисления.

3.7. Алгоритм с вычислением коэффициентов подходящих дробей

В основе нижеприведенного алгоритма лежит следующее замечание. Оказывается, функция $A_n = A_n(p_n, q_n)$ имеет вид (14). Как показано выше, A_n — многочлен, и его степень не превосходит $\deg f$. В этом случае, наша задача сводится к вычислению и проверке того, что A_n имеет вид bh^t , $b \in k, t \in \mathbb{N}$, на каждом шаге с номером n . Для этого нам достаточно вычислять ограниченное число коэффициентов у каждой из функций A_n, B_n, a_n, q_n и p_n .

В этом параграфе запись $g(h)$ для произвольной рациональной функции g подчеркивает, что функция g разложена по степеням многочлена h . И когда речь идёт о коэффициентах функции g подразумеваются коэффициенты именно в этом разложении, если не указано иное.

Рассмотрим данный алгоритм подробнее. Для каждого делителя $d = d_j$ многочлена f , $0 \leq \deg d_j \leq s$, $\deg f = 2s + 1$ достаточно вычислить разложения

$$\frac{f}{d} = c_\gamma h^\gamma + \dots + c_0, \quad d = b_\kappa h^\kappa + \dots + b_0,$$

где $\gamma = \deg f - \deg d > \deg d = \kappa$, а также необходимо знать $2(s + 1)$ коэффициентов степенного ряда $\sqrt{f}$.

На каждом шаге вычисляем коэффициенты многочленов

$$A_n = A_n(h) = (-1)^n \left(dp_n^2 - \frac{f}{d} q_n^2 \right), \quad 0 < \deg A_n(h) \leq \gamma, \quad A_n(0) = 0,$$

$$B_n = B_n(h) = (-1)^{n+1} \left(dp_n p_{n-1} - \frac{f}{d} q_n q_{n-1} \right), \quad 0 \leq \deg B_n(h) \leq \gamma,$$

причем достаточно знать $\kappa + 1$ “старших” коэффициентов числителя дробно-рациональных функций $p_{n-1} = p_{n-1}(h)$, $p_n = p_n(h)$ и $\gamma + 1$ “старших” коэффициентов числителя дробно-рациональных функций $q_{n-1} = q_{n-1}(h)$ и $q_n = q_n(h)$, где функции p_n и q_n имеют вид

$$p_n = \frac{p_{n,t_n} h^{t_n} + p_{n,t_n-1} h^{t_n-1} + \dots + p_{n,0}}{h^{t_n}},$$

$$q_n = \frac{q_{n,t_n} h^{t_n} + q_{n,t_n-1} h^{t_n-1} + \dots + q_{n,0}}{h^{t_n}},$$

$$t_n = v_h(p_n) = v_h(q_n) = \sum_{j=1}^n v_h(a_j).$$

Если $v_h(A_n) = \deg A_n(h)$, то подходящая дробь p_n/q_n дает решение (14), тем самым алгоритм завершает работу.

Формула (9) дает возможность вычислить коэффициенты a_{n+1} , причем $s_{n+1} = v_h(A_n)$,

$$\begin{aligned}\xi_{n+1}A_n &= B_n + \sqrt{f}, & a_{n+1} &= [\xi_{n+1}], \\ a_{n+1} &= a_{n+1,s_{n+1}}h^{-s_{n+1}} + \dots + a_{n+1,0}.\end{aligned}$$

Далее из рекуррентных формул

$$p_{n+1} = a_{n+1}p_n + p_{n-1}, \quad q_{n+1} = a_{n+1}q_n + q_{n-1}$$

находим соответственно $\kappa + 1$ и $\gamma + 1$ “старших” коэффициентов числителей дробно-рациональных функций $p_{n+1} = p_{n+1}(h)$ и $q_{n+1} = q_{n+1}(h)$.

Суммарно к n -ому шагу в данном алгоритме будет вычислено не более $5n(2s + 2) + O(1)$ коэффициентов.

С вычислительной точки зрения, приведённый алгоритм значительно повысил скорость работы его программной реализации. Однако, на практике скорости работы всё ещё не достаточно для вычисления S -единиц больших степеней с $\mathbb{Q}$ в качестве поля констант.

3.8. Алгоритм без вычисления коэффициентов подходящих дробей

Следующим этапом развития данного подхода являлось использование рекуррентных равенств для вычисления коэффициентов многочленов A_n и B_n , что позволило не вычислять p_n и q_n явно. В настоящем параграфе мы сформулируем улучшенный алгоритм.

На очередном шаге с номером $n + 1$ вычислим коэффициенты a_{n+1} по формуле (9). Далее вычисляем коэффициенты многочленов A_{n+1} и B_{n+1} по рекуррентным формулам (10), (11)

$$B_{n+1} = a_{n+1}A_n - B_n, \quad A_{n+1} = A_{n-1} + a_{n+1}(B_n - B_{n+1}).$$

Если $v_h(A_n) = \deg A_n(v)$, то подходящая дробь p_n/q_n дает решение (14), тем самым алгоритм завершает работу.

Суммарно к n -ому шагу в данном алгоритме будет вычислено не более $3n(2s + 2) + O(1)$ коэффициентов.

Существенное уменьшение числа вычисляемых коэффициентов и, как следствие, числа арифметических операций, а также отсутствие необходимости вычислять p_n, q_n позволило значительно сократить время работы алгоритма и построить S -единицы больших степеней с $\mathbb{Q}$ в качестве поля констант.

3.9. S -единицы больших степеней

С помощью вышеуказанного алгоритма метода непрерывных дробей удаётся построить S -единицы больших порядков, где $S = \{v'_h, v_\infty\}$, $\deg h = 1$.

Рассмотрим многочлены

$$\begin{aligned} f'_{20} &= (x^4 - 2x^3 + 4)(x + 2)x \\ f_{20} &= (4x^4 - 2x + 1)(2x + 1) \\ h_{20} &= x - 1. \end{aligned}$$

ЛЕММА 6. Кривая $C_{f'_{20}}$ бирационально эквивалентна кривой $C_{f_{20}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 5. Пусть $S_{20} = \{v'_{h_{20}}, v_\infty\}$, тогда поле $L_{20} = \mathbb{Q}(x)(\sqrt{f_{20}})$ обладает фундаментальной S_{20} -единицей, степень которой равна 20 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{20}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{20} = \alpha_{20} - \beta_{20}\sqrt{f_{20}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{20} &= -\frac{1}{4}h_{20}^{10} - 16h_{20}^9 - 172h_{20}^8 - \frac{3009}{4}h_{20}^7 - \frac{14087}{8}h_{20}^6 - \frac{4925}{2}h_{20}^5 - \\ &\quad - \frac{17349}{8}h_{20}^4 - \frac{9765}{8}h_{20}^3 - \frac{3429}{8}h_{20}^2 - \frac{1377}{16}h_{20} - \frac{243}{32}, \\ \beta_{20} &= h_{20}^7 + \frac{149}{8}h_{20}^6 + \frac{685}{8}h_{20}^5 + \frac{1273}{8}h_{20}^4 + \frac{303}{2}h_{20}^3 + \frac{1269}{16}h_{20}^2 + \frac{351}{16}h_{20} + \frac{81}{32}, \\ \alpha_{20}^2 - f_{20}\beta_{20}^2 &= \frac{1}{16}h_{20}^{20}. \end{aligned}$$

$\square$

Рассмотрим многочлены

$$\begin{aligned} f'_{21} &= (x^5 + 2x^4 - x^3 + 6x^2 - 7x + 8)x \\ f_{21} &= 8x^5 - 7x^4 + 6x^3 - x^2 + 2x + 1 \\ h_{21} &= x - 1. \end{aligned}$$

ЛЕММА 7. Кривая $C_{f'_{21}}$ бирационально эквивалентна кривой $C_{f_{21}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 6. Пусть $S_{21} = \{v'_{h_{21}}, v_\infty\}$, тогда поле $L_{21} = \mathbb{Q}(x)(\sqrt{f_{21}})$ обладает фундаментальной S_{21} -единицей, степень которой равна 21 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{21}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{21} = \alpha_{21} - \beta_{21}\sqrt{f_{21}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{21} &= -25h_{21}^{10} - 332h_{21}^9 - \frac{6087}{4}h_{21}^8 - \frac{31711}{8}h_{21}^7 - \frac{110055}{16}h_{21}^6 - \frac{135999}{16}h_{21}^5 - \\ &\quad - \frac{61749}{8}h_{21}^4 - \frac{82215}{16}h_{21}^3 - \frac{19683}{8}h_{21}^2 - \frac{12393}{16}h_{21} - \frac{2187}{16}, \\ \beta_{21} &= h_{21}^8 + 37h_{21}^7 + \frac{787}{4}h_{21}^6 + \frac{3663}{8}h_{21}^5 + \frac{10881}{16}h_{21}^4 + \frac{2619}{4}h_{21}^3 + \frac{7047}{16}h_{21}^2 + \\ &\quad + \frac{729}{4}h_{21} + \frac{729}{16}, \\ \alpha_{21}^2 - f_{21}\beta_{21}^2 &= -8h_{21}^{21}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f'_{22} &= (x^4 + x^3 - 16x + 16)(x + 1)x \\ f_{22} &= (16x^4 - 16x^3 + x + 1)(x + 1) \\ h_{22} &= x - 1.\end{aligned}$$

ЛЕММА 8. Кривая $C_{f'_{22}}$ бирационально эквивалентна кривой $C_{f_{22}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 7. Пусть $S_{22} = \{v'_{h_{22}}, v_\infty\}$, тогда поле $L_{22} = \mathbb{Q}(x)(\sqrt{f_{22}})$ обладает фундаментальной S_{22} -единицей, степень которой равна 22 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{22}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{22} = \alpha_{22} - \beta_{22}\sqrt{f_{22}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{22} &= -\frac{1}{3}h_{22}^{11} - 24h_{22}^{10} - 284h_{22}^9 - \frac{7729}{6}h_{22}^8 - \frac{8738}{3}h_{22}^7 - \frac{44425}{12}h_{22}^6 - \\ &\quad - \frac{270361}{96}h_{22}^5 - \frac{64021}{48}h_{22}^4 - \frac{1591}{4}h_{22}^3 - \frac{437}{6}h_{22}^2 - \frac{15}{2}h_{22} - \frac{1}{3}, \\ \beta_{22} &= h_{22}^8 + \frac{257}{12}h_{22}^7 + \frac{1343}{12}h_{22}^6 + 214h_{22}^5 + \frac{17969}{96}h_{22}^4 + \frac{347}{4}h_{22}^3 + \\ &\quad + \frac{89}{4}h_{22}^2 + 3h_{22} + \frac{1}{6}, \\ \alpha_{22}^2 - f_{22}\beta_{22}^2 &= \frac{1}{9}h_{22}^{22}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f'_{23} &= (4x^5 + 12x^4 - 68x^2 + 45x + 81)(x + 1) \\ f_{23} &= -24x^5 + 153x^4 - 36x^3 - 8x^2 - 8x + 4 \\ h_{23} &= x - 1.\end{aligned}$$

ЛЕММА 9. Кривая $C_{f'_{23}}$ бирационально эквивалентна кривой $C_{f_{23}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{X+1}{X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 8. Пусть $S_{23} = \{v'_{h_{23}}, v_{\infty}\}$, тогда поле $L_{23} = \mathbb{Q}(x)(\sqrt{f_{23}})$ обладает фундаментальной S_{23} -единицей, степень которой равна 23 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{23}}$.

К сожалению, предъявить здесь S -единицы степеней 23 и выше не представляется возможным, ввиду величины и количества коэффициентов. Однако, для того, чтобы у читателя возникло представление о значениях коэффициентов указанной единицы, приведём их частично.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{23} = \alpha_{23} - \beta_{23}\sqrt{f_{23}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{23} &= -63 h_{23}^{11} + 1626 h_{23}^{10} - \frac{10809}{2} h_{23}^9 - \frac{156621}{4} h_{23}^8 + \frac{1280743}{48} h_{23}^7 + \dots, \\ \beta_{23} &= h_{23}^9 - 82 h_{23}^8 + \frac{1601}{2} h_{23}^7 + \frac{11527}{12} h_{23}^6 - \frac{173331}{16} h_{23}^5 - \frac{558495}{16} h_{23}^4 - \\ &\quad - \frac{2899719}{64} h_{23}^3 - \frac{3851307}{128} h_{23}^2 - \frac{649539}{64} h_{23} - \frac{177147}{128}, \\ \alpha_{23}^2 - f_{23}\beta_{23}^2 &= 24 h_{23}^{23}.\end{aligned}$$

$\square$

Рассмотрим многочлены

$$\begin{aligned}f'_{24} &= (2x^4 + x^3 + 2x^2 + x + 2)(2x + 1)(x + 2) \\ f_{24} &= (8x^4 - 5x^3 + 14x^2 - 12x + 8)(3x + 2) \\ h_{24} &= x - 2.\end{aligned}$$

ЛЕММА 10. Кривая $C_{f'_{24}}$ бирационально эквивалентна кривой $C_{f_{24}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{X+2}{2X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 9. Пусть $S_{24} = \{v'_{h_{24}}, v_{\infty}\}$, тогда поле $L_{24} = \mathbb{Q}(x)(\sqrt{f_{24}})$ обладает фундаментальной S_{24} -единицей, степень которой равна 24 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{24}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{24} = \alpha_{24} - \beta_{24}\sqrt{f_{24}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{24} &= -\frac{4}{19} h_{24}^{12} - 57 h_{24}^{11} - 2576 h_{24}^{10} - \frac{887888}{19} h_{24}^9 - \frac{8633472}{19} h_{24}^8 - \dots, \\ \beta_{24} &= h_{24}^9 + \frac{1620}{19} h_{24}^8 + 2016 h_{24}^7 + \frac{398720}{19} h_{24}^6 + \frac{2234112}{19} h_{24}^5 + \dots, \\ \alpha_{24}^2 - f_{24}\beta_{24}^2 &= \frac{16}{361} h_{24}^{24}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{25} &= (x^5 + 30x^4 + 165x^3 - 900x^2 + 900x + 972)x \\ f_{25} &= 972x^5 + 900x^4 - 900x^3 + 165x^2 + 30x + 1 \\ h_{25} &= x - \frac{1}{3}. \end{aligned}$$

ЛЕММА 11. Кривая $C_{f'_{25}}$ бирационально эквивалентна кривой $C_{f_{25}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 10. Пусть $S_{25} = \{v'_{h_{25}}, v_{\infty}\}$, тогда поле $L_{25} = \mathbb{Q}(x)(\sqrt{f_{25}})$ обладает фундаментальной S_{25} -единицей, степень которой равна 25 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{25}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{25} = \alpha_{25} - \beta_{25}\sqrt{f_{25}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{25} &= -\frac{175}{3}h_{25}^{11} + \frac{775}{27}h_{25}^{10} - \frac{7250}{243}h_{25}^9 + \frac{648125}{177147}h_{25}^8 - \frac{880625}{531441}h_{25}^7 - \dots, \\ \beta_{25} &= h_{25}^{10} - \frac{35}{27}h_{25}^9 + \frac{440}{243}h_{25}^8 - \frac{20675}{19683}h_{25}^7 + \frac{321175}{531441}h_{25}^6 - \frac{105475}{531441}h_{25}^5 + \dots, \\ \alpha_{25}^2 - f_{25}\beta_{25}^2 &= -972h_{25}^{25}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{26} &= (18x^4 - 9x^3 - 24x^2 + 21x - 4)(2x + 3)x \\ f_{26} &= -(4x^4 - 21x^3 + 24x^2 + 9x - 18)(3x + 2) \\ h_{26} &= x - 2. \end{aligned}$$

ЛЕММА 12. Кривая $C_{f'_{26}}$ бирационально эквивалентна кривой $C_{f_{26}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 11. Пусть $S_{26} = \{v'_{h_{26}}, v_{\infty}\}$, тогда поле $L_{26} = \mathbb{Q}(x)(\sqrt{f_{26}})$ обладает фундаментальной S_{26} -единицей, степень которой равна 26 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{26}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{26} = \alpha_{26} - \beta_{26}\sqrt{f_{26}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{26} &= \frac{3}{8}h_{26}^{13} - 16h_{26}^{12} + \frac{236}{3}h_{26}^{11} + \frac{1504}{9}h_{26}^{10} - \frac{26945}{27}h_{26}^9 - \frac{49780}{81}h_{26}^8 + \dots, \\ \beta_{26} &= h_{26}^{10} - \frac{95}{6}h_{26}^9 + \frac{343}{6}h_{26}^8 + \frac{254}{27}h_{26}^7 - \frac{19114}{81}h_{26}^6 - \frac{11}{9}h_{26}^5 + \frac{11269}{27}h_{26}^4 + \dots, \\ \alpha_{26}^2 - f_{26}\beta_{26}^2 &= \frac{9}{64}h_{26}^{26}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{27} &= (x^5 + 5x^4 + 9x^3 + 3x^2 - x - 1)(x - 1) \\ f_{27} &= 16x^5 + 57x^4 + 70x^3 + 39x^2 + 10x + 1 \\ h_{27} &= x. \end{aligned}$$

ЛЕММА 13. Кривая $C_{f'_{27}}$ бирационально эквивалентна кривой $C_{f_{27}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = -\frac{X-1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 12. Пусть $S_{27} = \{v'_{h_{27}}, v_\infty\}$, тогда поле $L_{27} = \mathbb{Q}(x)(\sqrt{f_{27}})$ обладает фундаментальной S_{27} -единицей, степень которой равна 27 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{27}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{27} = \alpha_{27} - \beta_{27}\sqrt{f_{27}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{27} &= -49h_{27}^{13} - \frac{4891}{4}h_{27}^{12} - \frac{17981}{2}h_{27}^{11} - \frac{121825}{4}h_{27}^{10} - 57842h_{27}^9 - 69044h_{27}^8 - \dots, \\ \beta_{27} &= h_{27}^{11} + \frac{293}{4}h_{27}^{10} + \frac{3195}{4}h_{27}^9 + \frac{12091}{4}h_{27}^8 + \frac{10621}{2}h_{27}^7 + \frac{21089}{4}h_{27}^6 + \dots, \\ \alpha_{27}^2 - f_{27}\beta_{27}^2 &= -16h_{27}^{27}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{28} &= (16x^3 + 20x^2 - 8x + 9)(4x^2 + x + 4)x \\ f_{28} &= (9x^3 - 8x^2 + 20x + 16)(4x^2 + x + 4) \\ h_{28} &= x - \frac{4}{3}. \end{aligned}$$

ЛЕММА 14. Кривая $C_{f'_{28}}$ бирационально эквивалентна кривой $C_{f_{28}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 13. Пусть $S_{28} = \{v'_{h_{28}}, v_\infty\}$, тогда поле $L_{28} = \mathbb{Q}(x)(\sqrt{f_{28}})$ обладает фундаментальной S_{28} -единицей, степень которой равна 28 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{28}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{28} = \alpha_{28} - \beta_{28}\sqrt{f_{28}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{28} &= -\frac{18}{49}h_{28}^{14} - 49h_{28}^{13} - \frac{3430}{3}h_{28}^{12} - \frac{325703}{27}h_{28}^{11} - \frac{19033756}{243}h_{28}^{10} - \dots, \\ \beta_{28} &= h_{28}^{11} + 42h_{28}^{10} + \frac{4819}{9}h_{28}^9 + \frac{874006}{243}h_{28}^8 + \frac{103701248}{6561}h_{28}^7 + \dots, \\ \alpha_{28}^2 - f_{28}\beta_{28}^2 &= \frac{324}{2401}h_{28}^{28}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{29} &= (x^5 + x^4 - 4x^3 + 12x^2 - 12x + 4)(x + 1) \\ f_{29} &= 32x^5 - 47x^4 + 20x^3 + 2x^2 - 4x + 1 \\ h_{29} &= x - 1. \end{aligned}$$

ЛЕММА 15. Кривая $C_{f'_{29}}$ бирационально эквивалентна кривой $C_{f_{29}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{X+1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 14. Пусть $S_{29} = \{v'_{h_{29}}, v_{\infty}\}$, тогда поле $L_{29} = \mathbb{Q}(x)(\sqrt{f_{29}})$ обладает фундаментальной S_{29} -единицей, степень которой равна 29 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{29}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{29} = \alpha_{29} - \beta_{29}\sqrt{f_{29}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{29} &= -89h_{29}^{14} - 3670h_{29}^{13} - 45230h_{29}^{12} - 263316h_{29}^{11} - 882052h_{29}^{10} - \dots, \\ \beta_{29} &= h_{29}^{12} + 122h_{29}^{11} + 2332h_{29}^{10} + 16648h_{29}^9 + 59244h_{29}^8 + 121872h_{29}^7 + \dots, \\ \alpha_{29}^2 - f_{29}\beta_{29}^2 &= -32h_{29}^{29}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{30} &= (9x^4 + 27x^3 - 12x^2 - 60x + 4)(x - 1)x \\ f_{30} &= -(32x^4 - 33x^3 - 123x^2 - 63x - 9)(x + 1) \\ h_{30} &= x + \frac{3}{4}. \end{aligned}$$

ЛЕММА 16. Кривая $C_{f'_{30}}$ бирационально эквивалентна кривой $C_{f_{30}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = -\frac{X-1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 15. Пусть $S_{30} = \{v'_{h_{30}}, v_{\infty}\}$, тогда поле $L_{30} = \mathbb{Q}(x)(\sqrt{f_{30}})$ обладает фундаментальной S_{30} -единицей, степень которой равна 30 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{30}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{30} = \alpha_{30} - \beta_{30}\sqrt{f_{30}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{30} &= -\frac{8}{21}h_{30}^{15} + 42h_{30}^{14} - \frac{11525}{16}h_{30}^{13} + \frac{5202887}{1344}h_{30}^{12} - \frac{20529531}{3584}h_{30}^{11} - \dots, \\ \beta_{30} &= h_{30}^{12} - \frac{11507}{336}h_{30}^{11} + \frac{369799}{1344}h_{30}^{10} - \frac{489975}{896}h_{30}^9 - \frac{1502455}{4096}h_{30}^8 + \dots, \\ \alpha_{30}^2 - f_{30}\beta_{30}^2 &= \frac{64}{441}h_{30}^{30}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{32} &= (18x^4 + 63x^3 - 69x^2 - 24x - 4)(2x + 1)(x - 1) \\ f_{32} &= -(16x^4 - 99x^3 - 228x^2 - 135x - 18)(3x + 2) \\ h_{32} &= x. \end{aligned}$$

ЛЕММА 17. Кривая $C_{f'_{32}}$ бирационально эквивалентна кривой $C_{f_{32}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = -\frac{X-1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 16. Пусть $S_{32} = \{v'_{h_{32}}, v_{\infty}\}$, тогда поле $L_{32} = \mathbb{Q}(x)(\sqrt{f_{32}})$ обладает фундаментальной S_{32} -единицей, степень которой равна 32 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{32}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{32} = \alpha_{32} - \beta_{32}\sqrt{f_{32}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{32} &= \frac{24}{53} h_{32}^{16} - 53 h_{32}^{15} + \frac{2467}{3} h_{32}^{14} - \frac{2631595}{3816} h_{32}^{13} - \frac{766708927}{45792} h_{32}^{12} - \dots, \\ \beta_{32} &= h_{32}^{13} - \frac{5447}{159} h_{32}^{12} + \frac{187943}{1272} h_{32}^{11} + \frac{4859569}{5724} h_{32}^{10} + \frac{64444735}{40704} h_{32}^9 + \dots, \\ \alpha_{32}^2 - f_{32}\beta_{32}^2 &= \frac{576}{2809} h_{32}^{32}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{34} &= (4x^3 + 2x^2 - 6x + 3)(2x^2 + 1)(2x + 5) \\ f_{34} &= -(32x^3 - 59x^2 + 28x - 4)(27x^2 - 20x + 4) \\ h_{34} &= x. \end{aligned}$$

ЛЕММА 18. Кривая $C_{f'_{34}}$ бирационально эквивалентна кривой $C_{f_{34}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{5X+2}{2X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 17. Пусть $S_{34} = \{v'_{h_{34}}, v_{\infty}\}$, тогда поле $L_{34} = \mathbb{Q}(x)(\sqrt{f_{34}})$ обладает фундаментальной S_{34} -единицей, степень которой равна 34 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{34}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{34} = \alpha_{34} - \beta_{34}\sqrt{f_{34}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{34} &= \frac{432}{277} h_{34}^{17} - 277 h_{34}^{16} + \frac{220136}{27} h_{34}^{15} - \frac{235233784}{2493} h_{34}^{14} + \frac{472487072}{831} h_{34}^{13} - \dots, \\ \beta_{34} &= h_{34}^{14} - \frac{432496}{7479} h_{34}^{13} + \frac{799052}{831} h_{34}^{12} - \frac{53823040}{7479} h_{34}^{11} + \frac{24331952}{831} h_{34}^{10} - \dots, \\ \alpha_{34}^2 - f_{34}\beta_{34}^2 &= \frac{186624}{76729} h_{34}^{34}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{36} &= (12x^4 - 8x^3 - 8x^2 + 28x + 3)(3x + 4)x \\ f_{36} &= (3x^4 + 28x^3 - 8x^2 - 8x + 12)(4x + 3) \\ h_{36} &= x + 2. \end{aligned}$$

ЛЕММА 19. Кривая $C_{f'_{36}}$ бирационально эквивалентна кривой $C_{f_{36}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 18. Пусть $S_{36} = \{v'_{h_{36}}, v_{\infty}\}$, тогда поле $L_{36} = \mathbb{Q}(x)(\sqrt{f_{36}})$ обладает фундаментальной S_{36} -единицей, степень которой равна 36 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{36}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{36} = \alpha_{36} - \beta_{36}\sqrt{f_{36}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{36} &= -\frac{1}{9}h_{36}^{18} - 54h_{36}^{17} - \frac{24491}{6}h_{36}^{16} - \frac{23181596}{243}h_{36}^{15} - \frac{108463667}{243}h_{36}^{14} + \dots, \\ \beta_{36} &= h_{36}^{15} + \frac{25799}{162}h_{36}^{14} + \frac{1597891}{243}h_{36}^{13} + \frac{6849617}{81}h_{36}^{12} - \frac{1056283}{9}h_{36}^{11} - \dots, \\ \alpha_{36}^2 - f_{36}\beta_{36}^2 &= \frac{1}{81}h_{36}^{36}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f'_{39} &= (36x^5 + 72x^4 - 12x^3 + 24x^2 + x + 2)(x + 2) \\ f_{39} &= 192x^5 + 337x^4 - 1056x^3 + 852x^2 - 288x + 36 \\ h_{39} &= x - \frac{3}{4}. \end{aligned}$$

ЛЕММА 20. Кривая $C_{f'_{39}}$ бирационально эквивалентна кривой $C_{f_{39}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = \frac{2X+1}{X}$, $y = \frac{Y}{X^3}$. □

ТЕОРЕМА 19. Пусть $S_{39} = \{v'_{h_{39}}, v_{\infty}\}$, тогда поле $L_{39} = \mathbb{Q}(x)(\sqrt{f_{39}})$ обладает фундаментальной S_{39} -единицей, степень которой равна 39 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{39}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{39} = \alpha_{39} - \beta_{39}\sqrt{f_{39}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{39} &= -345h_{39}^{19} - \frac{851171}{24}h_{39}^{18} - \frac{268660479}{256}h_{39}^{17} - \frac{55600732287}{4096}h_{39}^{16} - \dots, \\ \beta_{39} &= h_{39}^{17} + \frac{7373}{24}h_{39}^{16} + \frac{3800211}{256}h_{39}^{15} + \frac{1055613113}{4096}h_{39}^{14} + \frac{132974896587}{65536}h_{39}^{13} + \dots, \\ \alpha_{39}^2 - f_{39}\beta_{39}^2 &= -192h_{39}^{39}. \end{aligned}$$

□

4. S -единицы и нелинейное нормирование

Метод непрерывных дробей является эффективным методом вычисления S -единиц, для S указанного выше вида. Однако, как отмечалось ранее, он работает только в случае $\deg h = 1$. Следовательно, для некоторых кривых его применение невозможно. Для более общего случая необходимо использовать метод матричной линеаризации из [6]. Точно также как и в случае метода непрерывных дробей авторами метода были доказаны результаты для случая поля $\mathbb{F}_q$ в качестве поля констант. Приведём основные результаты, относящиеся к данному методу для случая поля $\mathbb{Q}$ в качестве поля констант.

4.1. Метод матричной линеаризации

Напомним, что каждый элемент из пополнения $\overline{\mathbb{Q}(x)}$ можно представить в виде формального степенного ряда с коэффициентами из Σ , где Σ – выбранная в $\mathbb{Q}[x]$ фиксированная система представителей смежных классов по идеалу (h) , состоящая из всех многочленов степени меньшей, чем $\deg h$.

Введем следующее обозначение. Если $\alpha(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_r x^r \in \mathbb{Q}[x]$, то через $\hat{\alpha} = (\alpha_0, \dots, \alpha_r)^t$ будем обозначать вектор-столбец коэффициентов α .

Для дальнейшего изложения необходимо привести здесь аналоги некоторых важных утверждений из [6] для случая $\mathbb{Q}$ в качестве поля констант.

ПРЕДЛОЖЕНИЕ 4 ([6]). Пусть $h(x) = h_0 + h_1 x + \dots + h_l x^l$, $h_l \neq 0$, – фиксированный неприводимый многочлен и пусть $a(x) = a_0 + a_1 x + \dots + a_{l-1} x^{l-1}$, $b(x) = b_0 + b_1 x + \dots + b_{l-1} x^{l-1}$ – многочлены из $\mathbb{Q}[x]$. Разделим ab на h с остатком: $ab = gv + r$, где $g = g_0 + g_1 x + \dots + g_{l-2} x^{l-2}$, $r = r_0 + r_1 x + \dots + r_{l-1} x^{l-1}$. Тогда существуют $(l \times l)$ -матрицы $A_h(a)$ и $B_h(a)$, коэффициенты которых являются линейными функциями от $a_0, \dots, a_{l-1}$ с коэффициентами из $\mathbb{Q}$, такие, что

$$\hat{r} = A_h(a)\hat{b}, \quad \begin{pmatrix} \hat{g} \\ 0 \end{pmatrix} = B_h(a)\hat{b}.$$

ПРЕДЛОЖЕНИЕ 5 ([6]). Пусть $u_1 = \sum_{i=s_1}^{\infty} a_i v^i$, $u_2 = \sum_{i=s_2}^{\infty} b_i v^i$ – два элемента из пополнения $\overline{\mathbb{Q}(x)}$. Положим $C_h(a_{s_1}) = A_h(a_{s_1})$ и $C_h(a_i) = A_h(a_i) + B_h(a_{i-1})$ при $i > s_1$. Тогда $u_1 u_2 = \sum_{j=s_1+s_2}^{\infty} L_j v^j$, где

$$\hat{L}_j = \sum_{i+s=j} C_h(a_i)\hat{b}_s.$$

Предположим, что для заданного m норменное уравнение (1) имеет решение в многочленах $\alpha, \beta \in \mathbb{Q}[x]$, $\beta \neq 0$. Поскольку нормирование v_h имеет два продолжения на L , то $\sqrt{f} \in \overline{\mathbb{Q}(x)}$. Представим $\alpha, \beta, \sqrt{f}$ в виде формальных степенных рядов:

$$\alpha = \alpha_0 + \alpha_1 v + \dots + \alpha_r h^r, \quad \beta = \beta_0 + \beta_1 h + \dots + \beta_e h^e, \quad \sqrt{f} = \sum_{i=0}^{\infty} f_i v^i,$$

где $\alpha_i, \beta_i, f_i \in \Sigma$. Сравнение степеней левой и правой части в (1) показывает, что

$$m \geq \frac{\deg f}{\deg h}, \quad r = \left\lfloor \frac{m}{2} \right\rfloor, \quad e = \left\lfloor \frac{m \deg h - \deg f}{2 \deg h} \right\rfloor,$$

где $[z]$ означает целую часть числа z . Кроме того, степени многочленов α_r и β_e должны удовлетворять следующим соотношениям:

$$r_1 = \deg \alpha_r = \left\lfloor \left(\frac{m}{2} - r \right) \deg h \right\rfloor = \begin{cases} 0, & \text{если } m \text{ чётно,} \\ \left\lfloor \frac{\deg h}{2} \right\rfloor, & \text{если } m \text{ нечётно,} \end{cases}$$

$$e_1 = \deg \beta_e = \left\lfloor \frac{1}{2} R \right\rfloor,$$

где R — остаток от деления $m \deg h - \deg f$ на $2 \deg h$. Положим $C_h(f_i) = C_i$ и рассмотрим матрицу

$$\overline{D}_m = \begin{pmatrix} C_{r-e} & C_{r-e+1} & \dots & C_r \\ C_{r-e+1} & C_{r-e+2} & \dots & C_{r+1} \\ \dots & \dots & \dots & \dots \\ C_{m-e-1} & C_{m-e} & \dots & C_{m-1} \end{pmatrix}.$$

Пусть D_m — матрица, которая получается из $\overline{D}_m$ вычеркиванием первых $r_1 + 1$ строк и столбцов с номерами $e_1 + 2, \dots, \deg h$ (если $e_1 + 2 > \deg h$, то столбцы не вычеркиваются).

Следующая теорема является основой для матричного алгоритма нахождения фундаментальной S -единицы.

ТЕОРЕМА 20 ([6]). *Для натурального $m \geq \deg f / \deg h$ норменное уравнение (1) имеет решение в многочленах $\alpha, \beta \in \mathbb{Q}[x]$, $\beta \neq 0$, тогда и только тогда, когда ранг матрицы D_m меньше, чем $e \deg h + e_1 + 1$.*

5. Алгоритм метода матричной линеаризации

Приведём здесь алгоритм, основанный на методе матричной линеаризации из [6].

Чтобы найти фундаментальную S -единицу поля L , вначале нужно разложить $\sqrt{f}$ в формальный степенной ряд. Затем, вычисляя последовательно ранг матрицы D_m , начиная с $m \geq \deg f / \deg h$, находим минимальное натуральное m такое, что ранг D_m меньше, чем $e \deg h + e_1 + 1$. После этого, решая однородную систему линейных уравнений с матрицей D_m , находим ненулевой многочлен β , а по формулам

$$\hat{\alpha}_i = - \sum_{j+j'=i, j' \leq e} C_j \hat{\beta}_{j'}, \quad 0 \leq i < r, \quad \tilde{\alpha}_r = - \sum_{p=0}^e \tilde{C}_{r-p} \hat{\beta}_p,$$

где $\tilde{C}_i$ — матрица, которая состоит из первых $r_1 + 1$ строк матрицы C_i , находим многочлен α . Искомая фундаментальная S -единица имеет вид $\alpha + \beta\sqrt{f}$.

5.1. S -единицы больших степеней

С помощью метода матричной линеаризации удаётся построить S -единицы больших порядков, где $S = \{v'_h, v_\infty\}$, в том случае, когда для данной кривой подходящего нормирования первой степени не существует.

Рассмотрим многочлены

$$\begin{aligned} f'_{40} &= (32x^4 + 32x^3 - 38x^2 - 23x - 67)(2x + 3)(x - 1) \\ f_{40} &= -(64x^4 - 125x^3 - 250x^2 - 160x - 32)(5x + 2) \\ h_{40} &= x^2 - \frac{14}{5}x - \frac{8}{5}. \end{aligned}$$

ЛЕММА 21. Кривая $C_{f'_{40}}$ бирационально эквивалентна кривой $C_{f_{40}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = -\frac{X-1}{X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 21. Пусть $S_{40} = \{v'_{h_{40}}, v_\infty\}$, тогда поле $L_{40} = \mathbb{Q}(x)(\sqrt{f_{40}})$ обладает фундаментальной S_{40} -единицей, степень которой равна 40 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{40}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{40} = \alpha_{40} - \beta_{40}\sqrt{f_{40}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{40} &= -\frac{128}{913}h_{40}^{20} + \frac{75}{1826}h_{40}^{19}(120x - 721) + \frac{(8390045x - 160114702)}{1460800}h_{40}^{18} + \dots, \\ \beta_{40} &= -\frac{1}{913}h_{40}^{18}(60x - 913) - \frac{17}{36520000}h_{40}^{17}(7475085x - 26535266) - \dots, \\ \alpha_{40}^2 - f_{40}\beta_{40}^2 &= \frac{16384}{833569}h_{40}^{40}. \end{aligned}$$

$\square$

Рассмотрим многочлены

$$\begin{aligned} f'_{48} &= (18x^4 + 45x^3 + 21x^2 - 24x + 4)(2x - 1)(x - 1) \\ f_{48} &= (64x^4 + 225x^3 + 264x^2 + 117x + 18)(x + 2) \\ h_{48} &= x^2 + \frac{1}{4}x - \frac{3}{2}. \end{aligned}$$

ЛЕММА 22. Кривая $C_{f'_{48}}$ бирационально эквивалентна кривой $C_{f_{48}}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим замену $x = -\frac{X-1}{X}$, $y = \frac{Y}{X^3}$. $\square$

ТЕОРЕМА 22. Пусть $S_{48} = \{v'_{h_{48}}, v_{\infty}\}$, тогда поле $L_{48} = \mathbb{Q}(x)(\sqrt{f_{48}})$ обладает фундаментальной S_{48} -единицей, степень которой равна 48 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{48}}$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $u_{48} = \alpha_{48} - \beta_{48}\sqrt{f_{48}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{48} &= -\frac{64}{344387} h_{48}^{24} - \frac{255}{688774} h_{48}^{23}(1020x + 346073) - \dots, \\ \beta_{48} &= \frac{1}{344387} h_{48}^{22}(510x + 344387) + \frac{(4454762690x + 429814442277)}{22040768} h_{48}^{21} + \dots, \\ \alpha_{48}^2 - f_{48}\beta_{48}^2 &= \frac{4096}{118602405769} h_{48}^{48}.\end{aligned}$$

□

6. Заключение

В настоящей статье получили развитие эффективные алгоритмы вычисления S -единиц методом непрерывных дробей в случае S , состоящего из бесконечного и конечного нормирования первой степени. Также в работе приведено доказательство корректности условия остановки алгоритмов, основанных на методе непрерывных дробей, и в качестве следствия получено необходимое и достаточно условие соответствия S -единицы вида u^n , где u — фундаментальная S -единица, и подходящей дроби к $\sqrt{f}/d$ для некоторого d , делителя f .

Улучшенные алгоритмы позволили построить фундаментальные S -единицы больших степеней, а именно 20, 21, 22, 24, 25, 26, 27, 30, 32, 34.

Кроме того, методом матричной линеаризации была построена фундаментальная S -единица степени 40 для S , состоящего из бесконечного и конечного нормирования второй степени.

В качестве следствия из существования упомянутых S -единиц больших степеней, а также S -единиц степеней 23, 28, 29, 36, 48, существование которых было доказано ранее, получено альтернативное доказательство существования $\mathbb{Q}$ -точек кручения больших порядков в якобианах кривых рода 2. А именно, порядков 20, 21, ..., 30 и 32, 34, 36, 39, 40, 48.

Указанные выше результаты доказывают верность гипотезы Платонова для перечисленных порядков $\mathbb{Q}$ -точек кручения о том, что рассмотреть S , состоящее из конечного и бесконечного нормирования, то порядки $\mathbb{Q}$ -точек кручения, как правило, будут определяться степенями фундаментальных S -единиц.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Платонов В. П. Арифметика квадратичных полей и кручение в якобианах // Доклады РАН. 2010. Т. 430, №3. С. 318–320.

2. Платонов В. П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. 2014. Т. 69, вып.1 (415). С. 3–38.
3. Платонов В. П., Петрунин М.М. Новые порядки точек кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады РАН. 2012. Т. 443, №6. С. 664–667.
4. Платонов В. П., Петрунин М. М. О проблеме кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады РАН. 2012. Т. 446. №3. С. 263–264.
5. Платонов В. П., Петрунин М. М. Фундаментальные S -единицы в гиперэллиптических полях и проблема кручения в якобианах гиперэллиптических кривых // Доклады РАН. 2015. Т. 465, №1. С. 23–25.
6. Бенияш-Кривец В. В., Платонов В. П. Группы S -единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. 2009. Т. 200, №11. С. 15–44.
7. Ленг С. Введение в теорию диофантовых приближений. М.: Мир, 1970.
8. Flynn E. V. Large rational torsion on abelian varieties // J. Number Theory. 1990. P. 257–265.
9. Leprevost F. Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13 // C. R. Acad. Sci. Paris Ser. I Math. 1991. Vol. 313, №7. P. 451–454.
10. Leprevost F. Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre // C. R. Acad. Sci. Paris Ser. I Math. 1991. Vol. 313, №11. P. 771–774.
11. Leprevost F. Points rationnels de torsion de jacobiniennes de certaines courbes de genre 2 // C.R. Acad. Sci. Paris. 1993. Vol. 316, №8. P. 819–821.
12. Ogawa H. Curves of genus 2 with a rational torsion divisor of order 23 // Proc. Japan Acad. Ser. A Math. Sci. 1994. Vol. 70, №9. P. 295–298.
13. Leprevost F. Jacobiniennes de certaines courbes de genre 2: torsion et simplicite // Journal de Theorie des Nombres de Bordeaux. 1995. Vol. 7, №1. P. 283–306.
14. W. S. Cassels E. V. F. Prolegomena to a middlebrow arithmetic of curves of genus 2. Cambridge Univ. Press, 1996.
15. E. W. Howe F. L., Poonen B. Large torsion subgroups of split Jacobians of curves of genus two or three // Forum Mathematicum. 2000. Vol. 12. P. 315–364.

16. Nicolas B., Leprevost F., Pohst M. Jacobians of genus-2 curves with a rational point of order 11 // Experiment. Math. 2009. Vol. 18, №1. P. 65–70.
17. Elkies N. D. Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order // preprint, Harvard University. 2010.
18. Howe E. W. Genus-2 Jacobians with torsion points of large order // Bulletin of the London Mathematical Society. 2015. Vol. 47, №1. P. 127–135.
19. Hart W., Van Hoeij M., Novocin A. Practical polynomial factoring in polynomial time // Proceedings of the 36th international symposium on Symbolic and algebraic computation. – ACM, 2011. P. 163-170.

REFERENCES

1. Platonov, V. P. 2010, "Arithmetic of quadratic fields and torsion in Jacobians", Dokl. Math, 81, 1, pp. 55–57
2. Platonov, V. P. 2014, "Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field", Russian Math. Surveys 69, 1, pp. 1–34.
3. Platonov, V. P. & Petrunin, M. M. 2012, "New orders of torsion points in Jacobians of curves of genus 2 over the rational number field", Dokl. Math, 85, 2, pp. 286–288.
4. Platonov, V. P. & Petrunin, M. M. 2012, "On the torsion problem in jacobians of curves of genus 2 over the rational number field", Dokl. Math, 86, 2, pp. 642–643.
5. Platonov, V. P. & Petrunin, M. M. 2015, "Fundamental S-units in hyperelliptic fields and the torsion problem in jacobians of hyperelliptic curves", Dokl. Math, 92, 3, pp. 23–25.
6. Benyash-Krivets, V. V. & Platonov, V. P. 2009, "Groups of S-units in hyperelliptic fields and continued fractions", Sb. Math, 200, 11, pp. 1587-1615.
7. Lang, S. 1966, "Introduction to diophantine approximations", Reading, Mass., Addison-Wesley Pub. Co.
8. Flynn, E. V. 1990. "Large rational torsion on abelian varieties", J. Number Theory, pp. 257–265.
9. Leprevost, F. 1991. "Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13", C. R. Acad. Sci. Paris Ser. I Math, 313, 7, pp. 451–454.

10. Leprevost, F. 1991b. Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre. C. R. Acad. Sci. Paris Ser. I Math, 313, 11, pp. 771–774.
11. Leprevost, F. 1993. "Points rationnels de torsion de jacobienes de certaines courbes de genre 2", C. R. Acad. Sci. Paris, 316, 8, pp. 819–821.
12. Ogawa, H. 1994. "Curves of genus 2 with a rational torsion divisor of order 23", Proc. Japan Acad. Ser. A Math. Sci, 70, 9, pp. 295–298.
13. Leprevost, F. 1995. "Jacobienes de certaines courbes de genre 2: torsion et simplicite", Journal de Theorie des Nombres de Bordeaux, 7, 1, pp. 283–306.
14. W. S. Cassels, E. V. F. 1996. "Prolegomena to a middlebrow arithmetic of curves of genus 2", Cambridge Univ. Press.
15. E. W. Howe, F. L. and Poonen, B. 2000. "Large torsion subgroups of split Jacobians of curves of genus two or three", Forum Mathematicum, 12, pp. 315–364.
16. Nicolas, B. et al. 2009. "Jacobians of genus-2 curves with a rational point of order 11", Experiment. Math, 18, 1, pp. 65–70.
17. Elkies, N. D. 2010. "Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order", preprint Harvard University.
18. Howe, E. W. 2015. "Genus-2 Jacobians with torsion points of large order", Bulletin of the London Mathematical Society, 47, 1, pp. 127–135.
19. Hart W., Van Hoeij M. & Novocin A. 2011. "Practical polynomial factoring in polynomial time", Proceedings of the 36th international symposium on Symbolic and algebraic computation, ACM, pp. 163–170.

Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук (ФГУ ФНЦ НИИСИ РАН).

Поступило 10.03.2015.