ЧЕБЫШЕВСКИЙ СБОРНИК
Том 21. Выпуск 1.

УДК 511.6 DOI 10.22405/2226-8383-2020-21-1-322-340

О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков [1]

Г. В. Федоров

Посвящается 80-летию академика РАН В. П. Платонова

Федоров Глеб Владимирович — кандидат физико-математических наук, механико-математический факультет, Московский государственный университет имени М. В. Ломоносова (г. Москва).
e-mail: fedorov@mech.math.msu.su

Аннотация

Одной из актуальных современных проблем алгебры и теории чисел является проблема существования и поиска фундаментальных S-единиц в гиперэллиптических полях. Проблема существования и поиска S-единиц в гиперэллиптических полях эквивалентна разрешимости норменного уравнения — функционального уравнения Пелля — с некоторыми дополнительными условиями на вид этого уравнения и его решения. Существует глубокая связь между точками конечного порядка в якобиевом многообразии (якобиане) гиперэллиптической кривой и нетривиальными S-единицами соответствующего гиперэллиптического поля. Эта связь легла в основу предложенного В. П. Платоновым алгебраического подхода к известной фундаментальной проблеме об ограниченности кручения в якобиевых многообразиях гиперэллиптических кривых. Для эллиптических кривых над полем рациональных чисел проблема кручения была решена Мазуром в 1970-ых годах. Для кривых рода 2 и выше над полем рациональных чисел проблема кручения оказалась значительно сложнее, и пока далека от своего полного решения. Основные результаты, полученные к настоящему времени в этом направлении, относятся к описанию подгрупп кручения якобиевых многообразий конкретных гиперэллиптических кривых, а также к описанию некоторых семейств гиперэллиптических кривых рода $g \geqslant 2$.

В данной статье нами найден новый метод исследования разрешимости функциональных норменных уравнений, дающий полное описание гиперэллиптических кривых над полем рациональных чисел, якобиевы многообразия которых обладают точками кручения данных порядков. Наш метод основан на аналитическом изучении представителей дивизоров конечного порядка в группе классов дивизоров степени ноль и их представлений Мамфорда. В качестве иллюстрации работы нашего метода в данной статье непосредственно найдены все параметрические семейства гиперэллиптических кривых рода два над полем рациональных чисел, якобиевы многообразия которых обладают рациональными точками кручения порядков не превосходящих пяти. Более того, наш метод позволяет определить, какому найденному параметрическому семейству принадлежит данная кривая, якобиан которой обладает точкой кручения порядка, не превосходящего пяти.

Ключевые слова: непрерывные дроби, фундаментальные единицы, S-единицы, кручение в якобианах, гиперэллиптические поля, дивизоры, группа классов дивизоров.

Библиография: 30 названий.

[1] Работа выполнена при поддержке РНФ (грант №19-71-00029).

Для цитирования:
Г. В. Федоров. О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков // Чебышевский сборник, 2020, т. 21, вып. 1, с. 322–340.

CHEBYSHEVSKII SBORNIK
Vol. 21. No. 1.

UDC 511.6 DOI 10.22405/2226-8383-2020-21-1-322-340

On families of hyperelliptic curves over the field of rational numbers, whose jacobian contains torsion points of given orders [2]

G. V. Fedorov (Moscow)

Dedicated to the 80–year anniversary of academician RAS V. P. Platonov

Fedorov Gleb Vladimirovich — candidate of physical and mathematical Sciences, faculty of mechanics and mathematics, Lomonosov Moscow state University (Moscow).
e-mail: fedorov@mech.math.msu.su

Abstract

One of the pressing contemporary problems of algebra and number theory is the problem of the existence and searching for fundamental S-units in hyperelliptic fields. The problem of the existence and searching of S-units in hyperelliptic fields is equivalent the solvability of the norm equation — the functional Pell equation — with some additional conditions on the form of this equation and its solution. There is a deep connection between points of finite order in Jacobian variety (Jacobian) of hyperelliptic curve and nontrivial S-units of hyperelliptic field. This connection formed the basis of the algebraic approach proposed by V.P. Platonov to the well-known fundamental problem of boundedness of torsion in Jacobian varieties of hyperelliptic curves. For elliptic curves over a field of rational numbers, the torsion problem was solved by Mazur in the 1970s. For curves of genus 2 and higher over the field of rational numbers, the torsion problem turned out to be much more complicated, and it is far from its complete solution. The main results obtained in this direction include to the description of torsion subgroups of Jacobian varieties of specific hyperelliptic curves, and also to the description of some families of hyperelliptic curves of the genus $g \geqslant 2$.

In this article, we have found a new method for studying solvability. functional norm equations giving a full description hyperelliptic curves over the field of rational numbers, whose Jacobian varieties possess torsion points of given orders. Our method is based on an analytical study of representatives finite order divisors in a divisor class group of degree zero and their Mumford representations. As an illustration of the operation of our method in this article, we directly found all parametric families of hyperelliptic curves of genus two over the field of rational numbers, whose Jacobian varieties have rational torsion points of orders not exceeding five. Moreover, our method allows us to determine which parametric family found this curve belongs, whose Jacobian has a torsion point of order not exceeding five.

Keywords: continued fractions, fundamental units, S-units, torsion in the Jacobians, hyperelliptic fields, divisors, divisor class group.

Bibliography: 30 titles.

For citation:
G. V. Fedorov, 2020, "On families of hyperelliptic curves over the field of rational numbers whose Jacobian contains torsion points of given orders" , *Chebyshevskii sbornik*, vol. 21, no. 1, pp. 322–340.

[2]The work was supported by RSF (grant №19-71-00029).

1. Введение

Путь A — абелево многообразие размерности g над числовым полем K. По теореме Мордела-Вейля множество $A(K)$ K-точек многообразия A является конечно порожденной абелевой группой изоморфной $\mathbb{Z}^r \oplus A(K)_{tors}$, где $A(K)_{tors}$ — группа кручения K-точек многообразия A. Естественным образом возникают две проблемы: проблема полного описания конечных групп, реализуемых как группа кручения многообразия A над числовыми полями, и проблема полного перечисления многообразий A над числовым полем K, реализующих данную группу кручения. Для случая $g = 1$ эллиптических кривых над полем $\mathbb{Q}$ рациональных чисел первая проблема была решена Б. Мазуром в 1977 году [1]. С учетом результата Б. Мазура, в статьях Д. Куберта [2] и [3] была дана полная параметризация кубических эллиптических кривых для каждой из возможных групп точек конечного порядка, тем самым была решена вторая проблема для кубических эллиптических кривых над полем рациональных чисел. Для эллиптических кривых четвертой степени над полем рациональных чисел первая проблема эквивалентна кубическому случаю (см., например, [4]), а вторая проблема была решена в [5] с помощью формул [4], устанавливающих бирациональную эквивалентность кривых третей и четвертой степени. Более подробно эллиптический случай над полем рациональных чисел с помощью теории функциональных непрерывных дробей исследован в [6], [7] для кривых третей степени и в [8], [9] для кривых четвертой степени.

Для случая $g = 1$ эллиптических кривых над квадратичным полем констант проблема описания групп точек конечного порядка была решена в 1986 году С. Каменни [10]. Проблема описания эллиптических кривых над квадратичным полем констант реализующих данную группу кручения была решена в 1988 году М. Кенку и Ф. Момозем [11]. Исследование элементов кубических эллиптических полей над квадратичным полем констант, имеющих периодическое разложение в функциональную дробь, и связь с проблемой перечисления эллиптических кривых над квадратичным полем констант имеющих точку кручения заданного порядка проведены в статьях [12], [13] и [14].

В 1996 году Л. Мерел [15] доказал для каждого $d \geqslant 1$ существование постоянной $B(d)$, зависящей только от d, такой, что для любой эллиптической кривой E, определенной над числовым полем K степени d, справедливо неравенство $|E(K)_{tors}| \leqslant B(d)$. В случае $g \geqslant 2$ проблема ограниченности порядка подгруппы кручения даже для гиперэллиптических кривых над полем $\mathbb{Q}$ остается открытой. Тем более не решены проблема описания возможных групп кручения над числовыми полями и проблема перечисления гиперэллиптических кривых рода g над числовым полем K, реализующих данную группу кручения. Основные результаты, полученные к настоящему времени в этом направлении, относятся к описанию подгрупп кручения якобиевых многообразий определенного вида гиперэллиптических кривых рода $g \geqslant 2$, а также к описанию некоторых семейств гиперэллиптических кривых рода $g \geqslant 2$, якобианы которых обладают точками кручения определенного порядка (подробнее см. [16]). На основе нового подхода, предложенного В.П. Платоновым, доказана гипотеза о существовании $\mathbb{Q}$-точек любого порядка, не превосходящего 30, в якобианах гиперэллиптических кривых рода 2 над полем рациональных чисел (см. [17]). В статье [18] приведено доказательство существования рациональных точек кручения некоторых порядков больших 30 в соответствующих якобианах гиперэллиптических кривых над полем рациональных чисел. С помощью метода Флина-Лепровоста В.П. Платонов и автор [19] построили бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28.

Глубокие идеи, высказанные В.П. Платоновым, позволили установить связь среди четырех самостоятельных фундаментальных проблем: проблемы существования в гиперэллиптическом поле L нетривиальных S-единиц специального вида, где $S = \{v_x^-, v_x^+\}$, проблемы квазипериодичности непрерывной дроби квадратичной иррациональности $\alpha \in L$, проблемы существова-

ния решения определенного вида у норменного уравнения (функционального уравнения типа Пелля) и проблемы кручения у класса дивизора $v_x^- - v_x^+$ в группе классов дивизоров $\Delta^\circ(L)$. Последняя проблема эквивалентна наличию точки конечного порядка в якобиевом многообразии гиперэллиптической кривой, соответствующей гиперэллиптическому полю L. Более подробно об указанных связях и развитии идей В.П. Платонова читатель может ознакомиться в статьях [21]-[25]. Фундаментальные наблюдения В.П. Платонова оказали важное и существенное влияние на современное развитие описанных проблем, являясь основой для многих настоящих и будущих исследований.

В данной статье нами найден новый метод исследования разрешимости функциональных норменных уравнений (функционального уравнения типа Пелля), дающий полную параметризацию гиперэллиптических кривых над полем рациональных чисел, якобиевы многообразия которых обладают точками кручения данных порядков. Наш метод основан на аналитическом изучении представителей дивизоров конечного порядка в группе классов дивизоров степени ноль и их представлений Мамфорда, и частично опирается на результаты статей [26]-[29]. Отметим, что в статье [30] путем изучения функциональных непрерывных дробей с малыми длинами периодов найдены необходимые условия на вид гиперэллиптических полей, но не даны исчерпывающие описания соответствующих кривых, якобиевы многообразия которых обладают рациональными точками кручения малых порядков. В качестве иллюстрации работы нашего метода в данной статье непосредственно найдены все параметрические семейства гиперэллиптических кривых рода два над полем рациональных чисел, якобиевы многообразия которых обладают рациональными точками кручения порядков не превосходящих 5. Более того, наш метод позволяет определить, какому найденному параметрическому семейству принадлежит данная кривая, якобиан которой обладает точкой кручения порядка, не превосходящего 5.

2. Вспомогательные сведения

Пусть K — поле характеристики отличной от 2, $h \in K[x]$ — неприводимый многочлен, многочлен $f \in K[x]$ свободен от квадратов, $\deg f \geqslant 3$, нормирование v_h поля $K(x)$ имеет два продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Положим $S_h = \{v_h^-,\ v_h^+\}$. Мультипликативная группа S_h-целых элементов поля L называется *группой S_h-единиц.* Если группа S_h-единиц U_h нетривиальна, то для данного S_h она является прямым произведением K^* и бесконечной циклической группы. Образующая бесконечной циклической группы называется *фундаментальной S_h-единицей.* Любая нетривиальная S_h-единица $u \in U_h$ поля L имеет вид

$$u_h = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}, \quad v_h(\mu_2) = 0, \quad \max\big(\deg(\mu_1^2), \deg(\mu_2^2 f)\big) = 2m\deg h, \tag{1}$$

где $\mu_1, \mu_2 \in K[x]$ и $m \in \mathbb{N}$ (см. лемму 2.2 [7]). *Степенью* нетривиальной S_h-единицы $u_h \in U_h$, записанной в виде (1), называется число $\deg u_h = m \in \mathbb{N}$.

Предложение 1. *Следующие утверждения эквивалентны*

1. *m — минимальное натуральное число такое, что уравнение*

$$\omega_1^2 - \omega_2^2 f = bh^{2m}, \quad \max\big(2\deg\omega_1,\ 2\deg\omega_2 + \deg f\big) = 2m\deg h \tag{2}$$

имеет решение $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$, для некоторого $b \in K^*$;

2. *в поле $L = K(x)(\sqrt{f})$ существует фундаментальная S_h-единица $u_h = (\omega_1 + \omega_2\sqrt{f})/h^m$ степени m;*

3. m — минимальное натуральное число, для которого существует функция $\beta \in L$ такая, что ее главный дивизор имеет вид $(\beta) = m((h)^- - (h)^+)$.

Доказательство. Доказательство легко получается по аналогии с предложением 3.1 [20], или леммой 2.3 [7], или теореме 3 [25]. □

Если выполнены эквивалентные условия предложения 1, то с точностью до постоянного множителя элемент β совпадает с u_h или $bu_h^{-1} = (\omega_1 - \omega_2\sqrt{f})/h^m$. При этом в случае, когда m нечетно и существует такое $\gamma \in K^*$, что $b = \gamma^2$ и $f \mid \omega_1 - \gamma h^m$, выполняется тождество $\mu_1^2 - \mu_2^2 f = \gamma h^m$ для некоторых $\mu_1, \mu_2 \in K[x]$. Таким образом, для нечетного m показатель $2m$ степени h в норменном уравнении (2) может оказаться не минимальным.

Пусть $g \in \mathbb{N}$, $f, h \in \mathbb{Q}[x]$, причем многочлен f свободен от квадратов, $2g+1 \leqslant \deg f \leqslant 2g+2$, $(f,\ h) \in \mathbb{Q}^*$, $\deg h \leqslant g$. Бесконечное нормирование поля $\mathbb{Q}(x)$ может иметь два неэквивалентных продолжения v_∞^- и v_∞^+ или два эквивалентных продолжения $v_\infty = v_\infty^- = v_\infty^+$ на поле $L = \mathbb{Q}(x)(\sqrt{f})$.

Предложение 2. *Для описания с точностью до изоморфизма всех гиперэллиптических кривых $C : y^2 = f(x)$ рода два над полем рациональных чисел, якобиевы многообразия которых обладают точкой с кручением заданного порядка m достаточно решить уравнение вида*

$$\omega_1^2 - \omega_2^2 f = \gamma h^m, \quad \max(2\deg\omega_1,\ 2\deg\omega_2 + \deg f) = m \cdot \deg h, \tag{3}$$

где $h, f, \omega_1, \omega_2 \in \mathbb{Q}[x]$, $1 \leqslant \deg h \leqslant 2$, $(h, \omega_1) \in \mathbb{Q}^*$, $\operatorname{lc}(h) = \operatorname{lc}(\omega_2) = 1$, многочлен f свободен от квадратов, $5 \leqslant \deg f \leqslant 6$, $\gamma \in \mathbb{Q}^*$.

Доказательство. В группе классов дивизоров степени ноль $\Delta^\circ(L)$ гиперэллиптического поля L, соответствующего гиперэллиптической кривой C рода два, достаточно рассмотреть канонические представители вида $D-(\infty^- + \infty^+)$, где D — некоторый эффективный дивизор степени два, определенный над полем $\mathbb{Q}$. Пусть класс дивизора $D-(\infty^- + \infty^+) = P_1 + P_2 - (\infty^- + \infty^+)$ имеет порядок m в группе классов дивизоров $\Delta^\circ(L)$. Если $P_1 + P_2 \neq 2\infty^-$ и $P_1 + P_2 \neq 2\infty^+$, то существует функция $\omega_1 + \omega_2\sqrt{f} \in \mathbb{Q}[x][\sqrt{f}]$, дивизор которой имеет вид

$$\left(\omega_1 + \omega_2\sqrt{f}\right) = m\big(P_1 + P_2 - (\infty^- + \infty^+)\big),$$

а также существует многочлен $h \in \mathbb{Q}[x]$, $1 \leqslant \deg h \leqslant 2$, дивизор которого имеет вид

$$(h) = (P_1 + P_2) + \iota(P_1 + P_2) - 2\big(\infty^- + \infty^+\big).$$

Это означает, что

$$\left(\omega_1 + \omega_2\sqrt{f}\right) = m\big((h)^- - (\infty^- + \infty^+)\big).$$

Последнее соотношение эквивалентно разрешимости уравнения (3).

Если $P_1 + P_2 = 2\infty^-$, то можно рассмотреть изоморфную кривую $C_1 : Y^2 = F(X)$, где $X = 1/x$, $Y = yX^{g+1}$, $F = X^{2g+2} f(1/X)$. В группе классов дивизоров для этой кривой класс дивизора $v_X^- - v_X^+$ имеет порядок m. Тогда существует функция $\omega_1 + \omega_2\sqrt{F} \in \mathbb{Q}[X][\sqrt{F}]$, дивизор которой имеет вид

$$\left(\omega_1 + \omega_2\sqrt{F}\right) = m\big(2\,(X)^- - (\infty^- + \infty^+)\big). \tag{4}$$

Если положить $h = X^2$, то равенство (4) равносильно разрешимости уравнения вида (3). □

3. Основные результаты

Нашей целью является явное параметрическое описание всех свободных от квадратов многочленов f, удовлетворяющих (3) для некоторых $h, f, \omega_1, \omega_2 \in \mathbb{Q}[x]$, $\gamma \in \mathbb{Q}^*$, и приведенным выше условиям. Из уравнения (3) видно, что в зависимости от четности $\deg f$ и $\deg h^m$ число γ может принимать одно из трех значений $\operatorname{lc}(\omega_1)^2$, $-\operatorname{lc}(f)$, $\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$. Более точная связь степеней многочленов ω_1, ω_2, h, f и значений для числа γ представлена в таблице 1 для различных значений $m, n, k \in \mathbb{N}$. Таким образом, в любом случае значение γ в (3) однозначно восстанавливается по данным многочленам f и ω_1.

Далее штрихом будем обозначать производную по переменной x, например, $h' = \mathrm{d}h/\mathrm{d}x$.

Таблица 1: возможные значения параметра γ

$\deg h$	m	$\deg \omega_1$	$\deg f$	γ
$2n-1$	$2k$	$k(2n-1)$	$< 2k(2n-1) - 2\deg\omega_2$	$\operatorname{lc}(\omega_1)^2$
$2n-1$	$2k$	$k(2n-1)$	$2k(2n-1) - 2\deg\omega_2$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
$2n-1$	$2k$	$< k(2n-1)$	$2k(2n-1) - 2\deg\omega_2$	$-\operatorname{lc}(f)$
$2n-1$	$2k-1$	$\leqslant 2nk - n - k$	$(2k-1)(2n-1) - 2\deg\omega_2$	$-\operatorname{lc}(f)$
$2n$	m	mn	$< 2mn - 2\deg\omega_2$	$\operatorname{lc}(\omega_1)^2$
$2n$	m	mn	$2mn - 2\deg\omega_2$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
$2n$	m	$< mn$	$2mn - 2\deg\omega_2$	$-\operatorname{lc}(f)$

3.1. Общий подход

Теорема 1. *Пусть даны некоторые многочлены $h, \omega_2 \in \mathbb{Q}[x]$, причем $\operatorname{lc}(h) = \operatorname{lc}(\omega_2) = 1$ и ω_2 свободен от квадратов. Уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ таких, что $(\omega_1,\ h) \in \mathbb{Q}^*$, тогда и только тогда, когда разрешима система сравнений*

$$\begin{cases} q_0^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2h(q_1\omega_2' + q_0') \equiv m q_0 h' \pmod{\omega_2} \end{cases} \tag{5}$$

в многочленах $q_0, q_1 \in \mathbb{Q}[x]$ таких, что $\deg q_0, \deg q_1 < \deg\omega_2$, $(q_0,\ h) \in \mathbb{Q}^*$, $2(\deg q_1 + \deg\omega_2) \leqslant \leqslant m\deg h$.

Доказательство. Предположим, что уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ таких, что $(\omega_1,\ h) \in \mathbb{Q}^*$. Запишем $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2, и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2. Тогда $(q_0,\ h) \in \mathbb{Q}^*$, так как $(\omega_1,\ h) \in \mathbb{Q}^*$. Кроме того, $\deg q_0, \deg q_1 < \deg\omega_2$, и $2(\deg q_1 + \deg\omega_2) \leqslant 2\deg\omega_1 \leqslant m\deg h$. Из (3) следует, что $\omega_2^2 \mid \omega_1^2 - \gamma h^m$. Так как многочлен ω_2 свободен от квадратов, то последнее условие равносильно системе сравнений

$$\begin{cases} \omega_1^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2\omega_1'\omega_1 \equiv \gamma m h^{m-1} h' \pmod{\omega_2}. \end{cases} \tag{6}$$

Из $(\omega_1,\ h) \in \mathbb{Q}^*$ следует $(\omega_2,\ h) \in \mathbb{Q}^*$, поэтому домножим второе сравнение на h и воспользуемся первым сравнением. Тогда рассматриваемая система сравнений будет равносильна

$$\begin{cases} \omega_1^2 \equiv \gamma h^m \pmod{\omega_2}, \\ 2\omega_1' h \equiv m\omega_1 h' \pmod{\omega_2}. \end{cases} \tag{7}$$

Подставляя выражение для ω_1, получаем искомую систему (5).

Пусть теперь система сравнений (5) разрешима в многочленах $q_0, q_1 \in \mathbb{Q}[x]$ таких, что $\deg q_0, \deg q_1 < \deg \omega_2$, $(q_0,\ h) \in \mathbb{Q}^*$, $2(\deg q_1 + \deg \omega_2) \leqslant m \deg h$. Положим $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, где $q_2 \in \mathbb{Q}[x]$ — произвольный многочлен такой, что $\deg \omega_1 \leqslant [\deg h \cdot m/2]$. Так как $2(\deg q_1 + \deg \omega_2) \leqslant m \deg h$, то действительно такой многочлен q_2 можно подобрать (возможно нулевой). Таким образом, справедлива система (7), причем ввиду $(q_0,\ h) \in \mathbb{Q}^*$ имеем $(q_0,\ \omega_2) \in \mathbb{Q}^*$ и $(\omega_1,\ \omega_2) \in \mathbb{Q}^*$, а также $(\omega_1,\ h) \in \mathbb{Q}^*$. Домножая второе уравнение (7) на ω_1 и подставляя первое уравнение (7), приходим к системе (6), из которой следует условие $\omega_2^2 \mid \omega_1^2 - \gamma h^m$, поскольку многочлен ω_2 свободен от квадратов. Отсюда получаем многочлен f, для которого выполнено (3). $\square$

Теорема 2. *Пусть дано $m \in \mathbb{N}$ и многочлены $\omega_2, h \in \mathbb{Q}[x]$ такие, что $4 \deg \omega_2 \leqslant m \deg h + 2$, $(\omega_2,\ h) \in \mathbb{Q}^*$ и ω_2 свободен от квадратов. Уравнение (3) разрешимо в многочленах $\omega_1, f \in \mathbb{Q}[x]$ тогда и только тогда, когда γh^m является квадратичным вычетом по модулю ω_2, то есть найдется многочлен $q_0 \in \mathbb{Q}[x]$, $\deg q_0 \leqslant \deg \omega_2$, такой, что $q_0^2 \equiv \gamma h^m \pmod{\omega_2}$.*

Доказательство. По предложению 1 из разрешимости уравнения (3) следует разрешимость системы сравнений (5). Остается показать только, что сравнение $2h(q_1\omega_2' + q_0') \equiv mq_0h' \pmod{\omega_2}$ всегда разрешимо относительно многочлена $q_1 \in \mathbb{Q}[x]$. Так как многочлен ω_2 свободен от квадратов, то $(\omega_2',\ \omega_2) \in \mathbb{Q}^*$, следовательно, ω_2' обратим по модулю ω_2. Кроме того, $(h,\ \omega_2) \in \mathbb{Q}^*$, значит многочлен h также обратим по модулю ω_2. Значит, $q_1 \equiv (mq_0h'h^{-1}/2 - q_0')(\omega_2')^{-1} \pmod{\omega_2}$, причем $\deg q_1 < \deg \omega_2$.

Заметим, что, если для некоторого q_0 выполнено сравнение $q_0^2 \equiv \gamma h^m \pmod{\omega_2}$, то можно положить q_1 равным остатку от деления $(mq_0h'h^{-1}/2 - q_0')(\omega_2')^{-1}$ на ω_2. Из условия $4 \deg \omega_2 \leqslant m \deg h + 2$ следует, что можно положить $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, для некоторого (возможно нулевого) многочлена $q_2 \in \mathbb{Q}[x]$, причем $\deg \omega_1 \leqslant [\deg h \cdot m/2]$. Далее доказательство в точности как у теоремы 1. $\square$

В некоторых частных случаях для описанного выше общего подхода к решению уравнения (3) можно увеличить продуктивность. Например, предположим, что в (3) порядок $m = 2k$ и число $\gamma = \tau^2$ является полным квадратом в $\mathbb{Q}^*$. Тогда $\omega_2^2 f = (\omega_1 - \tau h^k)(\omega_1 + \tau h^k)$. Так как множители в правой части последнего равенства взаимнопросты, то можно представить $\omega_2 = \omega_3 \cdot \omega_4$ так, что разрешимость (3) равносильна системе условий

$$\begin{cases} \omega_3^2 \mid \omega_1 - \tau h^k, \\ \omega_4^2 \mid \omega_1 + \tau h^k. \end{cases} \tag{8}$$

Следовательно, $\omega_1 = f_1\omega_3^2 + \tau h^k = f_2\omega_4^2 - \tau h^k$, где $f = f_1 \cdot f_2$, причем $\deg f_1, \deg f_2 \geqslant 1$, поскольку иначе порядок будет равен k, а не $2k$, как мы желаем. Если дополнительно предположить, что многочлен ω_2 свободен от квадратов, то система (8) равносильна системе сравнений

$$\begin{cases} f_2\omega_4^2 \equiv 2h^k \pmod{\omega_3}, \\ \frac{f_2'}{f_2} + 2\frac{\omega_4'}{\omega_4} \equiv k\frac{h'}{h} \pmod{\omega_3}, \\ f_1\omega_3^2 \equiv -2h^k \pmod{\omega_4}, \\ \frac{f_1'}{f_1} + 2\frac{\omega_3'}{\omega_3} \equiv k\frac{h'}{h} \pmod{\omega_4}. \end{cases} \tag{9}$$

Чтобы найти решение задачи (3) в рассматриваемом частном случае можно, положить $\omega_1 = f_1\omega_3^2 + \tau h^k$ и найти многочлены $\omega_3, \omega_4, f_1, f_2$ с неопределенными коэффициентами, удовлетворяющими последним двум условиям системы (9).

Далее для каждого значения $0 \leqslant \deg \omega_2 \leqslant 2$ рассмотрим решение задачи (3) согласно подходу, описанному в теоремах 1 и 2.

3.2. Случай $\deg\omega_2 = 0$

В этом случае решить задачу (3) не составляет труда:

$$F = \omega_1^2 - \gamma h^m,$$

где $h, \omega_1 \in \mathbb{Q}[x]$ — произвольные многочлены такие, что $\deg h \geqslant 1$, $\operatorname{lc}(\omega_1) = \operatorname{lc}(h) = 1$, $(h, \omega_1) \in \mathbb{Q}^*$, $m \in \mathbb{N}$ такое, что $2\deg\omega_1 \leqslant m\deg h$, $\gamma \in \mathbb{Q}^*$ — любое. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов. Возможные значения $\deg F \leqslant 6$, $\deg h \leqslant 2$, m, $\deg\omega_1$ и γ приведены в таблице 2.

Таблица 2: значения параметров для случая $\deg\omega_2 = 0$

$\deg F$	$\deg h$	m	$\deg\omega_1$	γ
3	1	3	$\leqslant 1$	$-\operatorname{lc}(f)$
3	1	4	2	$\operatorname{lc}(\omega_1)^2$
4	1	4	$\leqslant 2$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
5	1	5	$\leqslant 2$	$-\operatorname{lc}(f)$
5	1	6	3	$\operatorname{lc}(\omega_1)^2$
5	2	3	3	$\operatorname{lc}(\omega_1)^2$
6	1	6	$\leqslant 3$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
6	2	3	$\leqslant 3$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$

3.3. Случай $\deg\omega_2 = 1$

Воспользуемся теоремой 1. Для этого случая $q_0, q_1 \in \mathbb{Q}$ и $\omega_2 = x - a$ для некоторого $a \in \mathbb{Q}$. Система (5) имеет решение

$$q_0 = \sqrt{\gamma h^m(a)}, \quad q_1 = \frac{mh'(a)\cdot q_0}{2h(a)}$$

для любых $a \in \mathbb{Q}$, $h \in \mathbb{Q}[x]$, $\deg h \geqslant 1$, $\operatorname{lc}(h) = 1$, $h(a) \neq 0$, $\gamma \in \mathbb{Q}^*$, $m \in \mathbb{N}$, $m \geqslant 2$. Тогда имеем

$$\omega_1 = q_2(x-a)^2 + q_1(x-a) + q_0, \quad F = \frac{\omega_1^2 - \gamma h^m}{(x-a)^2},$$

где q_2 — произвольный многочлен, $2\deg q_2 \leqslant m\deg h - 4$, такой, что $(\omega_1,\ h) \in \mathbb{Q}^*$. При $m\deg h < 4$ имеем $q_2 = 0$. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов. Возможные значения $\deg F \leqslant 6$, $\deg h \leqslant 2$, m, $\deg\omega_1$ и γ приведены в таблице 3.

3.4. Случай $\deg\omega_2 = 2$

Воспользуемся теоремой 2. Для этого случая $\deg q_0 = \deg q_1 = 1$ и с помощью сдвига можно считать, что $\omega_2 = x^2 + b$ для некоторого $b \in \mathbb{Q}$. Кроме того, с помощью растяжения можно считать, что $h = q\omega_2 + c$ или $h = q\omega_2 + x + c$, где $q \in \mathbb{Q}[x]$, $\operatorname{lc}(q) = 1$. Остается найти значения параметров, при которых сравнение $q_0^2 \equiv \gamma h^m \pmod{x^2+b}$ разрешимо.

Пусть $h = q\omega_2 + c$ для некоторого многочлена $q \in \mathbb{Q}[x]$, $\operatorname{lc}(q) = 1$. Тогда необходимо решить сравнение $q_0^2 \equiv \gamma c^m \pmod{x^2+b}$. Положим $q_0 = a_0 + a_1 x$, тогда получаем систему

$$\begin{cases} 2a_0a_1 = 0, \\ a_0^2 - ba_1^2 = \gamma c^m. \end{cases} \tag{10}$$

Таблица 3: значения параметров для случая $\deg\omega_2 = 1$

$\deg F$	$\deg h$	m	$\deg\omega_1$	γ
3	1	5	$\leqslant 2$	$-\operatorname{lc}(f)$
3	1	6	3	$\operatorname{lc}(\omega_1)^2$
4	1	6	$\leqslant 3$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
5	1	7	$\leqslant 3$	$-\operatorname{lc}(f)$
5	1	8	4	$\operatorname{lc}(\omega_1)^2$
5	2	4	4	$\operatorname{lc}(\omega_1)^2$
6	1	8	$\leqslant 4$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
6	2	4	$\leqslant 4$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$

Если $a_0 = 0$, то $b = -\gamma c^m/a_1^2$ для любых $a_1, c \in \mathbb{Q}^*$. Если $a_1 = 0$ и $2\deg\omega_1 \leqslant 2\deg\omega_2 + \deg f$, то $\gamma = a_0^2/c^m$ для любых $a_0, b, c \in \mathbb{Q}^*$. Если $a_1 = 0$ и $2\deg\omega_1 > 2\deg\omega_2 + \deg f$, то $\gamma = 1$, $a_0 = t^m$, $c = t^2$ для любых $b, t \in \mathbb{Q}^*$. Как отмечалось в теореме 2, многочлен q_1 восстанавливается из сравнения $2h(q_1\omega_2' + q_0') \equiv mq_0h' \pmod{\omega_2}$. Тогда имеем

$$\omega_1 = q_2(x^2+b)^2 + q_1(x^2+b) + q_0, \quad F = \frac{\omega_1^2 - \gamma h^m}{\omega_2^2},$$

где q_2 — произвольный многочлен подходящей степени, $\operatorname{lc}(q_2) = 1$. Далее останется только выделить полный квадрат $F = \omega^2 f$ так, чтобы многочлен f был свободен от квадратов.

Таблица 4: значения параметров для случая $\deg\omega_2 = 2$

$\deg F$	$\deg h$	m	$\deg\omega_1$	γ
3	1	8	4	$\operatorname{lc}(\omega_1)^2$
4	1	8	$\leqslant 4$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
5	1	9	$\leqslant 4$	$-\operatorname{lc}(f)$
5	1	10	5	$\operatorname{lc}(\omega_1)^2$
5	2	5	5	$\operatorname{lc}(\omega_1)^2$
6	1	10	$\leqslant 5$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$
6	2	5	$\leqslant 5$	$\operatorname{lc}(\omega_1)^2 - \operatorname{lc}(f)$

Пусть $h = q\omega_2 + x + c$ для некоторого многочлена $q \in \mathbb{Q}[x]$, $\operatorname{lc}(q) = 1$. Тогда необходимо решить сравнение $q_0^2 \equiv \gamma(x+c)^m \pmod{x^2+b}$. Положим $\gamma(x+c)^m \equiv Cx + B \pmod{x^2+b}$ и $q_0 = a_0 + a_1x$, тогда получаем систему

$$\begin{cases} 2a_0a_1 = C, \\ a_0^2 - ba_1^2 = B, \end{cases} \tag{11}$$

причем $B = B(\gamma, b, c)$ и $C = C(\gamma, b, c)$ Из первого уравнения при условии, что $C \neq 0$, имеем $a_1 = C/2a_0$, тогда из второго получаем

$$a_0^2 = \frac{B \pm \sqrt{B^2 + bC^2}}{2}. \tag{12}$$

Если представить $(x+c)^m = (x^2+b)Q(x) + Cx + B$ для некоторого $Q(x) \in \mathbb{Q}[x]$, то

$$B^2 + bC^2 = (B + \sqrt{-b}C)(B - \sqrt{-b}C) = \prod_{x=\pm\sqrt{-b}} \big((x^2+b)Q(x) + Cx + B\big) =$$
$$= (\sqrt{-b}+c)^m(-\sqrt{-b}+c)^m = (b+c^2)^m.$$

Остается подобрать значения параметров γ, b, c так, чтобы $(b+c^2)^m$ и выражение в правой части равенства (12) являлись полными квадратами над $\mathbb{Q}$.

Случай $C = 0$ необходимо рассматривать отдельно.

Далее многочлены q_1 и f восстанавливаются также, как было указано выше. Возможные значения $\deg F \leqslant 6$, $\deg h \leqslant 2$, m, $\deg \omega_1$ и γ приведены в таблице 4.

4. Параметрические семейства кривых рода два

В качестве иллюстрации приведенных методов приведем параметризацию для гиперэллиптических кривых рода два над полем $\mathbb{Q}$, имеющих рациональную точку. Такие кривые могут быть заданы уравнением $C:\ y^2 = f(x)$, где $f(x) \in [x]$ — свободный от квадратов многочлен, $5 \leqslant \deg f \leqslant 6$.

Напомним, что в любом классе дивизоров степени ноль содержится единственный представитель вида $D - (\infty^- + \infty^+)$, где D — эффективный дивизор степени 2, не содержащий самосопряженных точек с кратностью 2. Такой представитель будем называть *каноническим*. Мы будем использовать буквами $P, P_1, P_2, \ldots$ для обозначения некоторых плейсов степени один. Путем домножения многочлена f на $\mathrm{lc}\,(\omega_2)^2$, можно без ограничения общности считать, что $\mathrm{lc}\,(\omega_2) = 1$. Также без ограничения общности в норменном уравнении мы можем делать линейные замены вида $X = ax + b$, поскольку "сдвиг" и "растяжение" по координате x соответствует изоморфизму гиперэллиптических кривых. Например, с помощью "сдвига" и "растяжения" без ограничения общности можно считать, что многочлен ω степени $k \geqslant 2$ имеет вид $\omega = a_k x^k + a_{k-2}x^{k-2} + \ldots + a_2x^2 + x + a_0$ или $\omega = a_k x^k + a_{k-2}x^{k-2} + \ldots + a_2x^2 + a_0$. В различных ситуациях с помощью "сдвига" и "растяжения" мы будем фиксировать разные коэффициенты многочленов ω_1 и ω_2. Кроме того, умножая норменное уравнение на полный квадрат, можно без ограничения общности считать, что зафиксирован еще один из коэффициентов многочленов ω_1 или ω_2. Например, таким образом можно зафиксировать старший коэффициент многочлена ω_1, $\mathrm{lc}\,(\omega_1) = 1$.

Далее рассмотрим по-очереди возможные порядки $3 \leqslant m \leqslant 5$ в якобиевых многообразиях гиперэллиптической кривой рода 2, как в предложении 2. Отметим, что случай $m = 2$ возможен только для дивизора вида $2(P - \infty) \sim 0$, который является главным дивизором для функции $x - x_P$ в поле $L = \mathbb{Q}(x)(\sqrt{f})$, где $f = (x - x_P)\omega$, $\omega \in \mathbb{Q}[x]$, $\deg \omega = 4$. Основы теории дивизоров в гиперэллиптических полях в наших обозначениях описаны в статье [26].

4.1. Порядок 3

Рассмотрим в классе дивизоров порядка 3 канонический представитель $D - (\infty^- + \infty^+)$. Если $v_\infty^+(D) > 0$, то $v_\infty^+(D) = 2$, поскольку по лемме Мамфорда (см. лемму 2.2 [26]) дивизор вида $3(P - \infty^-)$ не может быть главным в поле L. Если $v_\infty^+(D) = 2$, то соотношение $3(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega^2 - f = \gamma,$$

где $\deg \omega = 3$, $\mathrm{lc}\,(\omega) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига и растяжения мы можем считать, что $\omega_1 = x^3 + x + c_0$ или $\omega_1 = x^3 + c_0$, где $c_0, \gamma \in \mathbb{Q}$. Таким

образом, искомая параметризация имеет вид

$$f = \omega_1^2 - \gamma,$$

где $\omega_1 \in \mathbb{Q}[x]$ и $\gamma \neq 0$ такие, что многочлен f свободен от квадратов.

Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то соотношение $3\big(D - (\infty^- + \infty^+)\big) \sim 0$ эквивалентно существованию многочлена $\omega \in \mathbb{Q}[x]$, $\deg\omega \leqslant 3$, $\operatorname{lc}(\omega) = 1$, такого, что $\omega^2 - f = \gamma h^3$, где $\gamma \in \mathbb{Q}^*$ и $h = \operatorname{Pol}(D) \in \mathbb{Q}[x]$ — такой многочлен, что $\operatorname{lc}(h) = 1$, $\deg h = 2$, главный дивизор $(h) = D + \iota D - 2(\infty^- + \infty^+)$. Без ограничения общности путем сдвига мы можем считать, что $\omega_1 = x^3 + x + c_0$ или $\omega_1 = x^3 + c_0$, где $c_0, \gamma \in \mathbb{Q}$. Таким образом, искомая параметризация имеет вид

$$f = \omega^2 - \gamma h^3,$$

где $\gamma \in \mathbb{Q}^*$, $\omega, h \in \mathbb{Q}[x]$ такие, что многочлен f свободен от квадратов, $5 \leqslant \deg f \leqslant 6$.

4.2. Порядок 4

Рассмотрим в классе дивизоров порядка 4 канонический представитель $D - (\infty^- + \infty^+)$. Если $v_\infty^+(D) > 0$, то $v_\infty^+(D) = 2$, поскольку по лемме Мамфорда (см. лемму 2.2 [26]) дивизор вида $4(P - \infty^-)$ не может быть главным в поле L. Если $v_\infty^+(D) = 2$, то соотношение $4(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega_1^2 - \omega_2^2 f = \gamma, \tag{13}$$

где $\deg\omega_1 = 4$, $\deg\omega_2 = 1$, $\operatorname{lc}(\omega_1) = \operatorname{lc}(\omega_2) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига мы можем считать, что $\omega_2 = x$. Тогда уравнение (13) равносильно системе

$$\begin{cases} \omega_1^2(0) = \gamma, \\ 2\omega_1(0)\omega_1'(0) = 0. \end{cases}$$

Таким образом, искомая параметризация имеет вид

$$f = \frac{\omega_1^2 - \gamma}{x^2},$$

где $\gamma = \omega_1^2(0)$, $\omega_1 = x^4 + c_3x^3 + c_2x^2 + c_0 \in \mathbb{Q}[x]$ такой, что f — свободен от квадратов.

Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то соотношение $4(D - (\infty^- + \infty^+)) \sim 0$ эквивалентно существованию многочленов $\omega_1, \omega_2 \in \mathbb{Q}[x]$, $\deg\omega_1 \leqslant 4$, $\deg\omega_2 \leqslant 1$, таких, что

$$\omega_1^2 - \omega_2^2 f = \gamma h^4, \quad \max(2\deg\omega_1,\ 2\deg\omega_2 + \deg f) = 8, \quad 5 \leqslant \deg f \leqslant 6,$$

где $h = \operatorname{Pol}(D)$, $\operatorname{lc}(h) = 1$, $\deg h = 2$, $\operatorname{lc}(\omega_2) = 1$. С помощью сдвига всегда можно считать, что $h = x^2 + b$ для некоторой постоянной $b \in \mathbb{Q}^*$.

Рассмотрим случай, когда $\deg\omega_2 = 1$. Тогда путем растяжения можно считать, что $\omega_2 = x$ или $\omega_2 = x - 1$. Как в теореме 1 запишем $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2, и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2.

Пусть $\omega_2 = x$, тогда $b \neq 0$, и по пункту 3.3 имеем $q_1 = 0$, $q_0 = b^2t$, $\gamma = t^2$, где $t \in \mathbb{Q}^*$. Отсюда для произвольного $q_2 \in \mathbb{Q}[x]$, $\deg q_2 \leqslant 2$, $b, t \in \mathbb{Q}^*$, находим

$$f = \big(q_2 - t(x^2 + 2b)\big)\big(q_2x^2 + b^2t + t(x^2 + b)^2\big).$$

Мы можем без ограничения общности предполагать, что $\operatorname{lc}(q_2) = 1$, поскольку, умножая норменное уравнение на полный квадрат, можно зафиксировать один из коэффициентов многочлена ω_1.

Пусть $\omega_2 = x-1$, тогда по пункту 3.4 имеем $q_1 = 4t(b+1)$, $q_0 = t(b+1)^2$, $\gamma = t^2$, где $t \in \mathbb{Q}^*$. Отсюда для произвольного $q_2 \in \mathbb{Q}[x]$, $\deg q_2 \leqslant 2$, $\operatorname{lc}(q_2) = 1$, $b, t \in \mathbb{Q}^*$, находим

$$f = \big(q_2 - t((x+1)^2 + 2(b+1))\big)\big(q_2(x-1)^2 + 4t(b+1)(x-1) + t(b+1)^2 + t(x^2+b)^2\big).$$

Если $\deg \omega_2 < 1$, то $\omega_2 = 1$ и $f = \omega_1^2 - \gamma h^4$, причем $\deg \omega_1 = 4$, $\operatorname{lc}(\omega_1) = 1$, $5 \leqslant \deg f \leqslant 6$. Значит, должно быть $\gamma = 1$ и $1 \leqslant \deg(\omega - h^2) \leqslant 2$, то есть $\omega = h^2 + a_2x^2 + a_1x + a_0$, где $a_0, a_1, a_2 \in \mathbb{Q}^*$ — произвольные числа, $a_2^2 + a_1^2 \neq 0$, откуда

$$f = (a_2x^2 + a_1x + a_0)\big(2h^2 + a_2x^2 + a_1x + a_0\big).$$

За счет растяжения и сдвига можно считать, что $h = x^2 + b$ для некоторой постоянной $b \in \mathbb{Q}^*$, и $a_1 = 1$ или $a_1 = 0$.

4.3. Порядок 5

Рассмотрим в классе дивизоров порядка 5 канонический представитель $D - (\infty^- + \infty^+)$. Необходимо рассмотреть три случая: $v_\infty^+(D) = 2$, $v_\infty^+(D) = 1$ и $v_\infty^-(D) = v_\infty^+(D) = 0$.

Если $v_\infty^+(D) = 2$, то соотношение $5(\infty^+ - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega_1^2 - \omega_2^2 f = \gamma, \tag{14}$$

где $\deg \omega_1 = 5$, $\deg \omega_2 = 2$, $\operatorname{lc}(\omega_1) = \operatorname{lc}(\omega_2) = 1$, $\deg f = 6$, $\gamma \in \mathbb{Q}^*$. Без ограничения общности путем сдвига мы можем считать, что $\omega_2 = x^2 + b$. Тогда уравнение (14) равносильно системе сравнений

$$\begin{cases} \omega_1^2 \equiv \gamma \pmod{\omega_2}, \\ 2\omega_1\omega_1' \equiv 0 \pmod{\omega_2}. \end{cases}$$

Как в теореме 1 запишем $\omega_1 = q_2\omega_2^2 + q_1\omega_2 + q_0$, где $q_0, q_1, q_2 \in \mathbb{Q}[x]$ такие, что q_0 есть остаток от деления ω_1 на ω_2, и q_1 есть остаток от деления $(\omega_1 - q_0)/\omega_2$ на ω_2. Тогда последняя система сравнений равносильна системе

$$\begin{cases} q_0^2 \equiv \gamma \pmod{\omega_2}, \\ q_0\big(\omega_2'q_1 + q_0'\big) \equiv 0 \pmod{\omega_2}. \end{cases}$$

Без ограничения общности путем растяжения мы можем считать, что $q_0 = x + a_0$ или $q_0 = a_0$. Если $q_0 = x + a_0$, то из первого сравнения системы имеем $a_0 = 0$, $\gamma = -b \neq 0$, и второе сравнение системы имеет вид

$$x\big(2x(a_2x + a_1) + 1\big) \equiv 0 \pmod{x^2 + b}.$$

Отсюда получаем, что $a_1 = 0$, $a_2 = 1/2b$. Положим $q_2 = x + a$, тогда искомая параметризация имеет вид

$$f = x^6 + 2ax^5 + x^4\frac{\big(a^2b + 2b^2 + 1\big)}{b} + x^3\frac{a\left(4b^2+1\right)}{b} + \\ + x^2\frac{\big(8a^2b^3 + 4b^4 + 12b^2 + 1\big)}{4b^2} + xa\left(2b^2 + 3\right) + \frac{a^2b^3 + 1}{b},$$

где $a, b \in \mathbb{Q}$ такие, что $b \neq 0$, многочлен f свободен от квадратов.

Если $v_\infty^+(D) = 1$, то соотношение $5(P - \infty^-) \sim 0$ эквивалентно разрешимости уравнения

$$\omega^2 - f = \gamma h^5, \tag{15}$$

где $h, \omega \in \mathbb{Q}[x]$, $\deg \omega \leqslant 2$, $\deg h = 1$. Без ограничения общности с помощью сдвига можно считать, что $h = x$. С помощью растяжения по x и домножения норменного уравнения на постоянную, являющуюся полным квадратом в $\mathbb{Q}^*$, можно считать, что $\omega = ax^2 + x + 1$ или $\omega = ax^2 + 1$, где $a, \gamma \in \mathbb{Q}$, $\gamma \neq 0$. Тогда при $\omega = ax^2 + x + 1$ искомая параметризация имеет вид

$$f = -\gamma x^5 + a^2 x^4 + 2ax^3 + x^2 (2a + 1) + 2x + 1,$$

а при $\omega = ax^2 + 1$ искомая параметризация имеет вид

$$f = -\gamma x^5 + a^2 x^4 + 2ax^2 + 1.$$

Пусть теперь $v_\infty^-(D) = v_\infty^+(D) = 0$, $h = \mathrm{Pol}(D)$, $\mathrm{lc}(h) = 1$, $\deg h = 2$. Соотношение $5\big(D - (\infty^- + \infty^+)\big) \sim 0$ эквивалентно существованию многочленов $\omega_1, \omega_2 \in \mathbb{Q}[x]$, $\deg \omega_1 \leqslant 5$, $\deg \omega_1 \leqslant 2$, таких, что

$$\omega_1^2 - \omega_2^2 f = \gamma h^5, \quad \max(2 \deg \omega_1,\ 2 \deg \omega_2 + \deg f) = 10.$$

За счет сдвига и растяжения по x не ограничивая общности достаточно рассмотреть следующие случаи

- $\deg \omega_2 = 2$, $\deg \omega_1 \leqslant 5$, $\omega_2 = x^2 + b$, $h = \omega_2 + x + c$;
- $\deg \omega_2 = 2$, $\deg \omega_1 \leqslant 5$, $\omega_2 = x^2 + b$, $h = \omega_2 + c$;
- $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\mathrm{lc}(\omega_1) = 1$, $h = x^2 + c$, $\gamma = 1$, $\omega_2 = x$;
- $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\mathrm{lc}(\omega_1) = 1$, $h = x^2 + x + c$, $\gamma = 1$, $\omega_2 = x$;
- $\deg \omega_2 = 0$, $\deg \omega_1 = 5$, $\mathrm{lc}(\omega_1) = 1$, $h = x^2 + c$, $\gamma = 1$, $\omega_2 = 1$,

где $b, c \in \mathbb{Q}$.

Случай $\omega_2 = x^2 + b$, $h = \omega_2 + x + c$.

По пункту 3.4 имеем $\omega_1 = q_2 \omega_2^2 + q_1 \omega_2 + q_0$, $\deg q_0, \deg q_1, \deg q_2 \leqslant 1$, $q_0 = a_0 + a_1 x$, $q_1 = a_2 + a_3 x$, и $q_2 = ex + a$, $a, e \in \mathbb{Q}$. Как в 3.4 запишем

$$\gamma(x + c)^5 \equiv Cx + B \pmod{x^2 + b}, \qquad B = \gamma\big(5b^2 c - 10bc^3 + c^5\big), \quad C = \gamma\big(b^2 - 10bc^2 + 5c^4\big).$$

Получаем систему (11), из которой при условии, что $C \neq 0$, находим выражение (12) для a_0^2, причем $B^2 + bC^2 = \gamma^2 (b + c^2)^5$. Сделаем замену $b = s^2 - c^2$, тогда

$$a_0^2 = \frac{\gamma(c + s)}{2}(-4c^2 + 2cs + s^2)^2.$$

Сделаем замену $c = -s + 2t^2/\gamma$, тогда

$$a_0 = \frac{t\left(5\gamma^2 s^2 - 20\gamma s t^2 + 16t^4\right)}{\gamma^2}, \qquad a_1 = \frac{\gamma^2 s^2 - 12\gamma s t^2 + 16t^4}{2\gamma t}. \tag{16}$$

Далее из сравнения $2h(q_1 \omega_2' + q_0') \equiv m q_0 h' \pmod{\omega_2}$ находим коэффициенты многочлена q_1:

$$a_2 = \frac{-5\gamma^2 s - 60\gamma s t^2 + 20\gamma t^2 + 80t^4}{8\gamma t}, \qquad a_3 = \frac{\gamma^2 s - 20\gamma s t^2 + 4\gamma t^2 + 80t^4}{16t^3}. \tag{17}$$

В итоге получаем параметризацию

$$f = f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$
$$f_6 = -\gamma + e^2, \quad f_5 = -5\gamma + 2ae,$$
$$f_4 = e^2\left(\frac{8st^2}{\gamma} - \frac{8t^4}{\gamma^2}\right) + e\left(-\frac{\gamma s\left(-\gamma + 20t^2\right)}{8t^3} + \frac{\gamma + 20t^2}{2t}\right) +$$
$$+s\left(5\gamma - 12t^2\right) + \frac{-10\gamma^2 + \gamma a^2 - 10\gamma t^2 + 12t^4}{\gamma},$$
$$f_3 = e\left(\frac{s\left(-5\gamma^2 - 60\gamma t^2 + 64at^3\right)}{4\gamma t} - \frac{t\left(-5\gamma^2 - 20\gamma t^2 + 16at^3\right)}{\gamma^2}\right) -$$
$$-\frac{s\left(-\gamma^2 a + 20\gamma at^2 - 160\gamma t^3 + 320t^5\right)}{8t^3} + \frac{\gamma^2 a - 20\gamma^2 t + 20\gamma at^2 - 80\gamma t^3 + 80t^5}{2\gamma t},$$
$$f_2 = e^2\left(\frac{16s^2t^4}{\gamma^2} - \frac{32st^6}{\gamma^3} + \frac{16t^8}{\gamma^4}\right) +$$
$$+e\left(-\frac{s^2\left(-3\gamma + 20t^2\right)}{2t} + \frac{st\left(-21\gamma + 100t^2\right)}{2\gamma} - \frac{2t^3\left(-7\gamma + 20t^2\right)}{\gamma^2}\right) -$$
$$-\frac{s^2\left(-\gamma^5 + 40\gamma^4t^2 - 400\gamma^3t^4 + 2560\gamma^2t^6 - 10240\gamma t^8 + 12288t^{10}\right)}{256\gamma t^6} +$$
$$+\frac{s\left(\gamma^5 - 40\gamma^3at^3 + 560\gamma^3t^4 - 480\gamma^2at^5 + 256\gamma a^2t^6 - 3840\gamma t^8 + 3072t^{10}\right)}{32\gamma^2t^4} -$$
$$-\frac{-\gamma^5 + 40\gamma^4t^2 - 80\gamma^3at^3 + 560\gamma^3t^4 - 320\gamma^2at^5 + 128\gamma a^2t^6 - 1280\gamma t^8 + 768t^{10}}{16\gamma^3t^2},$$
$$f_1 = e\left(\frac{s^2t\left(5\gamma^2 - 60\gamma t^2 + 32at^3\right)}{\gamma^2} - \frac{st^3\left(15\gamma^2 - 140\gamma t^2 + 64at^3\right)}{\gamma^3} + \frac{4t^5\left(3\gamma^2 - 20\gamma t^2 + 8at^3\right)}{\gamma^4}\right) -$$
$$-\frac{s^2\left(5\gamma^4 - 40\gamma^3t^2 - 96\gamma^2at^3 + 720\gamma^2t^4 + 640\gamma at^5 - 5120\gamma t^6 + 5120t^8\right)}{64\gamma t^4} +$$
$$+\frac{s\left(10\gamma^3 - 21\gamma^2at + 40\gamma^2t^2 + 100\gamma at^3 - 480\gamma t^4 + 320t^6\right)}{2\gamma^2} -$$
$$-\frac{-\gamma^4 + 40\gamma^3t^2 - 56\gamma^2at^3 + 80\gamma^2t^4 + 160\gamma at^5 - 640\gamma t^6 + 320t^8}{4\gamma^3},$$
$$f_0 = -\frac{s^3\left(-\gamma + 4t^2\right)^5}{16\gamma^2t^4} + \frac{s^2\left(-7\gamma^5 - 40\gamma^4t^2 + 320\gamma^3at^3\right)}{64\gamma^3t^2} +$$
$$+\frac{s^2\left(-240\gamma^3t^4 - 3840\gamma^2at^5 + 12800\gamma^2t^6 + 1024\gamma a^2t^6 - 20480\gamma t^8 + 12288t^{10}\right)}{64\gamma^3t^2} -$$
$$-\frac{s\left(\gamma^5 - 80\gamma^4t^2 + 120\gamma^3at^3 + 240\gamma^3t^4 - 1120\gamma^2at^5 + 2560\gamma^2t^6 + 256\gamma a^2t^6 - 3200\gamma t^8 + 1536t^{10}\right)}{8\gamma^4} +$$
$$+\frac{t^2\left(\gamma^5 - 40\gamma^4t^2 + 48\gamma^3at^3 + 80\gamma^3t^4 - 320\gamma^2at^5 + 640\gamma^2t^6 + 64\gamma a^2t^6 - 640\gamma t^8 + 256t^{10}\right)}{4\gamma^5},$$

где параметры $a, e \in \mathbb{Q}$, $t, s, \gamma \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $C = 0$ возможен только, если $c = 0$, но тогда $b = 0$, чего не может быть, так как в этом случае $(\omega_2, h) = x \notin \mathbb{Q}^*$.

Также отметим, что многочлен ω_2 должен быть свободен от квадратов, поскольку иначе $b = 0$, что влечет $c = 0$, а это невозможно.

Случай $\omega_2 = x^2 + b$, $h = \omega_2 + c$.

Аналогично действуя по пункту 3.4, имеем два варианта, когда $a_0 = 0$ или $a_1 = 0$.

При $a_0 = 0$ получаем

$$q_2 = ex + a, \quad a_1 = t, \quad a_2 = 0, \quad a_3 = \frac{5c^4tv - t^3}{2c^5v}.$$

Отсюда получаем параметризацию

$$f = (e^2 - \gamma)x^6 + 2aex^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$
$$f_4 = -\frac{2\gamma c^5e^2}{t^2} + \frac{3\gamma^2c^5 - 5\gamma ct^2 + a^2t^2}{t^2} - \frac{et\left(-5\gamma c^4 + t^2\right)}{\gamma c^5},$$
$$f_3 = -\frac{4\gamma ac^5e}{t^2} - \frac{at\left(-5\gamma c^4 + t^2\right)}{\gamma c^5},$$
$$f_2 = \frac{\gamma^2c^{10}e^2}{t^4} + \frac{e\left(-5\gamma c^4 + 3t^2\right)}{t} +$$
$$+\frac{-12\gamma^5c^{20} + 40\gamma^4c^{16}t^2 - 8\gamma^3a^2c^{15}t^2 - 40\gamma^3c^{12}t^4 + 25\gamma^2c^8t^6 - 10\gamma c^4t^8 + t^{10}}{4\gamma^2c^{10}t^4},$$
$$f_1 = \frac{2\gamma^2ac^{10}e}{t^4} + \frac{a\left(-5\gamma c^4 + 3t^2\right)}{t},$$
$$f_0 = -\frac{-\gamma^5c^{20} + 5\gamma^4c^{16}t^2 - \gamma^3a^2c^{15}t^2 - 10\gamma^3c^{12}t^4 + 10\gamma^2c^8t^6 - 5\gamma c^4t^8 + t^{10}}{\gamma c^5t^6},$$

где параметры $a, e \in \mathbb{Q}$, $c, t, \gamma \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

При $a_1 = 0$ необходимо рассмотреть два случая: $\deg f = 6$ или $\deg f = 5$. Пусть $\deg f = 6$, тогда можно положить

$$q_2 = ex + a, \quad a_0 = t, \quad a_2 = 5t/(2c), \quad a_3 = 0.$$

Отсюда получаем параметризацию

$$f = e^2 - \frac{t^2}{c^5}x^6 + 2aex^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$
$$f_4 = 2be^2 - \frac{-a^2c^5 + 3bt^2 + 5ct^2}{c^5}, \quad f_3 = \frac{e\left(4abc + 5t\right)}{c},$$
$$f_2 = b^2e^2 - \frac{-2a^2bc^5 - 5ac^4t + 3b^2t^2 + 10bct^2 + 10c^2t^2}{c^5},$$
$$f_1 = \frac{e\left(2ab^2c + 5bt + 2ct\right)}{c},$$
$$f_0 = -\frac{-4a^2b^2c^5 - 20abc^4t - 8ac^5t + 4b^3t^2 + 20b^2ct^2 + 40bc^2t^2 + 15c^3t^2}{4c^5},$$

где параметры $a, b, c, e, t \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

В случае, когда $\deg f = 5$ имеем $\deg \omega_1 = 6$, $\operatorname{lc}(\omega_1) = 1$, $q_2 = x + a$,

$$\gamma = 1, \quad a_0 = t^5, \quad c = t^2, \quad a_2 = \frac{5t^3}{2}, \quad a_3 = 0.$$

Отсюда получаем параметризацию

$$f = 2ax^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$
$$f_5 = 2a, \quad f_4 = a^2 - b - 5t^2, \quad f_3 = 4ab + 5t^3,$$
$$f_2 = 2a^2b + 5at^3 - 2b^2 - 10bt^2 - 10t^4, \quad f_1 = 2ab^2 + 5bt^3 + 2t^5,$$
$$f_0 = -\frac{-4a^2b^2 - 20abt^3 - 8at^5 + 4b^3 + 20b^2t^2 + 40bt^4 + 15t^6}{4},$$

где параметры $a, b, t \in \mathbb{Q}^*$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg \omega_2 = 1$, $\deg \omega_1 = 5$, $\operatorname{lc}(\omega_1) = 1$, $h = x^2 + c$, $\omega_2 = x$

Так как в этом случае $\deg(\omega_1^2) > \deg(\omega_2^2 f)$ и $\operatorname{lc}(\omega_1) = 1$, то в норменном уравнении $\gamma = 1$. Таким образом, норменное уравнение (3) эквивалентно системе

$$\deg(\omega_1^2 - h^5) \leqslant 8,$$
$$\omega_1^2 \equiv h^5 \pmod{x^2}.$$

Положим $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, тогда первое условие системе равносильно условию $a_4 = 0$, а второе условие системы равносильно условиям $a_1 = 0$ и $a_0^2 = c^5$. Значит, можно положить $a_0 = t^5$, $c = t^2$, $a_2 = e$, $a_3 = s$, откуда получается параметризация

$$f = \left(2s - 5t^2\right)x^6 + 2ex^5 + \left(s^2 - 10t^4\right)x^4 + \left(2es + 2t^5\right)x^3 + \left(e^2 - 10t^6\right)x^2 + 2st^5x + 2et^5 - 5t^8,$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg\omega_2 = 1$, $\deg\omega_1 = 5$, $\operatorname{lc}(\omega_1) = 1$, $h = x^2 + x + c$, $\omega_2 = x$

Аналогично предыдущему случаю $\gamma = 1$ и можно положить $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, где $c = t^2$, $a_0 = t^5$, $a_1 = 5c^3/2$, $a_2 = e$, $a_3 = s$, $a_4 = 5/2$. Отсюда получается параметризация

$$f = x^6\left(2s - \frac{5\left(4t^2+3\right)}{4}\right) + x^5\left(5s - 2\left(-e + 10t^2 + 5\right)\right) +$$
$$+x^4\left(s^2 - 5\left(-e + 2t^4 - t^3 + 6t^2 + 1\right)\right) + x^3\left(2es + \frac{4t^5 - 60t^4 + 25t^3 - 40t^2 - 2}{2}\right) +$$
$$+x^2\left(e^2 + 5st^3 - 10t^6 + 5t^5 - 30t^4 - 5t^2\right) +$$
$$+x\left(2st^5 - 5t^3\left(-e + 4t^3 + 2t\right)\right) - \frac{t^5\left(-8e + 20t^3 + 15t\right)}{4},$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

Случай $\deg\omega_2 = 0$, $\deg\omega_1 = 5$, $\operatorname{lc}(\omega_1) = 1$, $h = x^2 + c$, $\omega_2 = 1$

Если положить $\omega_1 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, то норменное уравнение (3) дает условие $\deg(\omega_1^2 - h^5) \leqslant 6$, откуда $a_0 = e$, $a_1 = s$, $a_2 = 0$, $a_3 = 5t/2$, $a_4 = 0$, $c = t$. Отсюда получается параметризация

$$f = x^6\left(2s - \frac{15t^2}{4}\right) + 2ex^5 + x^4\left(5st - 10t^3\right) + 5etx^3 + x^2\left(s^2 - 5t^4\right) + 2esx + e^2 - t^5,$$

где $e, s, t \in \mathbb{Q}$, $t \neq 0$ такие, что многочлен f свободен от квадратов и $(f, h) \in \mathbb{Q}^*$.

5. Заключение

Автор выражает большую благодарность академику В. П. Платонову за многолетнюю поддержку, постановку задач и активное участие в совместных математических исследованиях.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Mazur B. Rational points on modular curves // Modular Funct. one Var. V, Proc. Int. Conf., Bonn 1976. Lect. Notes Math. 1977. Vol. 601. P. 107-148.
2. Kubert D. S. Universal bounds on the torsion of elliptic curves // Proc. London Math.Soc. (3). 1976. Vol. 33, № 2. P. 193-237.
3. Kubert D. S. Universal bounds on the torsion of elliptic curves // Compositio Mathematica. 1979. Vol. 38, № 1. P. 121-128.
4. Adams W. W., Razar M. J. Multiples of points on elliptic curves and continued fractions // Proc. London Math. Soc. 1980. Vol. 41, № 3. P. 481-498.
5. Van Der Poorten A. J., Tran X. C. Periodic continued fractions in elliptic function fields // International Algorithmic Number Theory Symposium. – Springer, Berlin, Heidelberg, 2002. P. 390-404.

6. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в эллиптических полях // ДАН. 2017. Т. 475, № 2. С. 133-136.

7. Платонов В. П., Федоров Г. В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209, № 4. С. 54-94.

8. Платонов В. П., Федоров Г. В. Критерий периодичности непрерывных дробей ключевых элементов гиперэллиптических полей // Чебышевский сборник. 2019. Т. 20, № 1. С. 246-258.

9. Федоров Г. В. Об ограниченности длин периодов непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел // Чебышевский сборник. 2019. Т. 20, № 4. С. 321-334.

10. Kamienny S. Torsion points on elliptic curves over all quadratic fields // Duke Math. J. 1986. Vol. 53, № 1. P. 157-162.

11. Kenku M. A, Momose F. Torsion points on elliptic curves defined over quadratic fields // Nagoya Math. J. 1988. Vol. 109. P. 125-149.

12. Платонов В. П., Жгун В. С., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант // ДАН. 2018. Т. 482, № 2. С. 137-141.

13. Платонов В. П., Жгун В. С., Петрунин М. М., Штейников Ю. Н. О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // ДАН. 2018. Т. 483, № 6. С. 603-608.

14. Платонов В. П., Петрунин М. М., Штейников Ю. Н. О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // ДАН. 2019. Т. 488, № 3. С. 237-242.

15. Merel L. Bornes pour la torsion des courbes ellipticques sur les corps de nombers // Invent. Math. 1996. Vol. 124, № 1-3. P. 437-449.

16. Howe E. W. Genus-2 Jacobians with torsion points of large order // Bull. London Math. Soc. 2015. Vol. 47. P. 127-135.

17. Платонов В. П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. 2014. Т. 69, № 1(415). С. 3-38.

18. Петрунин М. М. Вычисление фундаментальных S-единиц в гиперэллиптических полях рода 2 и проблема кручения в якобианах гиперэллиптических кривых // Чебышевский сборник. 2015. Т. 16, № 4. С. 250-283.

19. Платонов В. П., Федоров Г. В. Бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28 // ДАН. 2018. Т. 482, № 4. С. 385-388.

20. Беняш-Кривец В. В., Платонов В. П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Матем. сб. 2009. Т. 200, № 1. С. 15-44.

21. Платонов В. П., Федоров Г. В. S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // ДАН. 2015. Т. 465, № 5. С. 537-541.

22. Платонов В. П., Петрунин М. М. S-единицы и периодичность в квадратичных функциональных полях // УМН. 2016. Т. 71, № 5. С. 181-182.

23. Платонов В. П., Петрунин М. М. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // ДАН. 2016. Т. 470, № 3. С. 260-265.

24. Платонов В. П., Федоров Г. В. О периодичности непрерывных дробей в гиперэллиптических полях // ДАН. 2017. Т. 474, № 5. С. 540-544.

25. Платонов В. П., Петрунин М. М. Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Тр. МИАН. 2018. Т. 302. С. 354-376.

26. Федоров Г. В. Об S-единицах для нормирований второй степени в гиперэллиптических полях // Известия РАН. 2020. Т. 84, № 2 (в печати).

27. Федоров Г. В. Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях // Чебышевский сборник. 2018. Т. 19, № 3. С. 283-298.

28. Жгун В. С. Обобщенные якобианы и непрерывные дроби в гиперэллиптических полях // Чебышевский сборник. 2017. Т. 18, № 4. С. 208-220.

29. Платонов В. П., Жгун В. С., Федоров Г. В. Непрерывные дроби в гиперэллиптических полях и многочлены Мамфорда // ДАН. 2016. Т. 471, № 6. С. 640-644.

30. Кузнецов Ю. В., Штейников Ю. Н. О некоторых свойствах непрерывных периодических дробей с небольшой длиной периода, связанных с гиперэллиптическими полями и S-единицами // Чебышевский сборник. 2017. Т. 18, № 4. С. 260-267.

REFERENCES

1. Mazur, B. 1977, "Rational points on modular curves" *Modular Funct. one Var. V, Proc. Int. Conf., Bonn 1976* Lect. Notes Math., vol. 601, pp. 107-148.

2. Kubert, D. S. 1976, "Universal bounds on the torsion of elliptic curves" *Proc. London Math.Soc. (3)*, vol. 33, no. 2, pp. 193-237.

3. Kubert, D. S. 1979, "Universal bounds on the torsion of elliptic curves" *Compositio Mathematica*, vol. 38, no. 1, pp. 121-128.

4. Adams W. W., Razar M. J. 1980, "Multiples of points on elliptic curves and continued fractions", *Proc. London Math. Soc.*, vol. 41, no. 3, pp. 481-498.

5. Van Der Poorten A. J., Tran X. C. 2002, "Periodic continued fractions in elliptic function fields", *International Algorithmic Number Theory Symposium.* – Springer, Berlin, Heidelberg, pp. 390-404.

6. Platonov, V. P., Fedorov, G. V. 2017, "On the periodicity of continued fractions in elliptic fields", *Dokl. Math.*, vol. 96, no. 1, pp. 332-335.

7. Platonov, V. P., Fedorov, G. V. 2018, "On the problem of periodicity of continued fractions in hyperelliptic fields", *Sb. Math.*, vol. 209, no. 4, pp. 519-559.

8. Platonov, V. P., Fedorov, G. V. 2019, "The criterion of the periodicity of continued fractions of key elements in hyperelliptic fields", *Chebyshevskii Sbornik*, vol. 20, no. 1, pp. 246-258 (In Russ.)

9. Fedorov, G. V. 2019, "On boundedness of period lengths of continued fractions of key elements hyperelliptic fields over the field of rational numbers", *Chebyshevskii Sbornik*, vol. 20, no. 4, pp. 321-334 (In Russ.)

10. Kamienny, S. 1986, "Torsion points on elliptic curves over all quadratic fields" *Duke Math. J.*, vol. 53, no. 1, pp. 157-162.

11. Kenku, M. A, Momose, F. 1988, "Torsion points on elliptic curves defined over quadratic fields" *Nagoya Math. J.*, vol. 109, pp. 125-149.

12. Platonov, V. P., Zhgoon, V. S., Fedorov, G. V. 2016, "On the Periodicity of Continued Fractions in Hyperelliptic Fields over Quadratic Constant Field", *Dokl. Math.*, vol. 98, no. 2, pp. 430-434.

13. Platonov, V. P., Zhgoon, V. S., Petrunin, M. M., Shteinikov, Yu. N. 2018, "On the Finiteness of Hyperelliptic Fields with Special Properties and Periodic Expansion of $\sqrt{f}$", *Dokl. Math.*, vol. 98, no. 3, pp. 641-645.

14. Platonov, V. P., Petrunin, M. M., Shteinikov, Yu. N. 2019, "On the Finiteness of the Number of Elliptic Fields with Given Degrees of S-Units and Periodic Expansion of $\sqrt{f}$", *Dokl. Math.*, vol. 100, no. 2, pp. 1-5.

15. Merel, L. 1996, "Bornes pour la torsion des courbes ellipticques sur les corps de nombers" *Invent. Math.*, vol. 124, no. 1-3, pp. 437-449.

16. Howe, E. W. 2015, “Genus-2 Jacobians with torsion points of large order” *Bull. London Math. Soc.*, vol. 47, pp. 127-135.

17. 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*, vol. 69, no. 1, pp. 1-34.

18. Petrunin, M. M. 2015, “Calculation of the fndamental S-units in hyperelliptic fields of genus 2 and the torsion problem in the jacobians of hyperelliptic curves”, *Chebyshevskii Sbornik*, vol. 16, no. 4, pp. 250-283 (In Russ.)

19. Platonov, V. P., Fedorov, G. V. 2018, “An infinite family of curves of genus 2 over the field of rational numbers whose jacobian varieties contain rational points of order 28”, *Dokl. Math.*, vol. 98, no. 2, pp. 468-471.

20. Benyash-Krivets, V. V., Platonov, V. P. 2009, “Groups of S-units in hyperelliptic fields and continued fractions”, *Sb. Math.*, vol. 200, no. 11, pp. 1587-1615.

21. Platonov, V. P., Fedorov, G. V. 2015, “S-Units and Periodicity of Continued Fractions in Hyperelliptic Fields”, *Dokl. Math.*, vol. 92, no. 3, pp. 752-756.

22. Platonov, V. P., Petrunin, M. M. 2016, “S-Units and periodicity in quadratic function fields”, *Russian Math. Surveys*, vol. 71, no. 5, pp. 973-975.

23. Platonov, V. P., Petrunin, M. M. 2016, “S-units in hyperelliptic fields and periodicity of continued fractions”, *Dokl. Math.*, vol. 94, no. 2, pp. 532-537.

24. Platonov, V. P., Fedorov, G. V. 2017, “On the periodicity of continued fractions in hyperelliptic fields”, *Dokl. Math.*, vol. 95, no. 3, pp. 254-258.

25. Platonov, V. P., Petrunin, M. M. 2018, “Groups of S-units and the problem of periodicity of continued fractions in hyperelliptic fields”, *Proc. Steklov Inst. Math.*, vol. 302, pp. 336-357.

26. Fedorov, G.V. 2020, "On S-units for second degree valuations in hyperelliptic fields Izv. Ross. Akad. Nauk Ser. Mat., vol. 84, no. 2 (in press).

27. Fedorov, G. V. 2018, “Periodic continued fractions and S-units with second degree valuations in hyperelliptic fields”, *Chebyshevskii Sbornik*, vol. 19, no. 3., pp. 283-298 (In Russ.)

28. Zhgoon V. S. 2017, “On generalized jacobians and rational continued fractions in the hyperelliptic fields”, *Chebyshevskii Sbornik*, vol. 18, no. 4, pp. 208-220. (In Russ.)

29. Platonov, V. P., Zhgoon, V. S., Fedorov, G. V. 2016, “Continued Rational Fractions in Hyperelliptic Fields and the Mumford Representation”, *Dokl. Math.*, vol. 94, no. 3, pp. 692-696.

30. Kuznetsov, Y. V., Shteinikov, Y. N. 2017, “On some properties of continued periodic fractions with small length of period related with hyperelliptic fields and S-units”, *Chebyshevskii Sbornik*, vol. 18, no. 4, pp. 260-267 (In Russ.)

Получено 16.01.2019 г.
Принято в печать 20.03.2020 г.