ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2024, том 518, с. 10–17

МАТЕМАТИКА

УДК 511.6

О ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ НЕЧЕТНОЙ СТЕПЕНИ И РОДА g С 6 ТОЧКАМИ КРУЧЕНИЯ ПОРЯДКА 2g + 1

© 2024 г. Г. В. Федоров[1, *]

Представлено академиком РАН В. П. Платоновым
Поступило 10.03.2024 г.
После доработки 05.07.2024 г.
Принято к публикации 05.07.2024 г.

Пусть гиперэллиптическая кривая $\mathcal{C}$ рода g, определенная над алгебраически замкнутым полем K характеристики 0, задана уравнением $y^2 = f(x)$, где многочлен $f(x) \in K[x]$ свободен от квадратов и имеет нечетную степень $2g+1$. Кривая $\mathcal{C}$ содержит единственную "бесконечную" точку $\mathcal{O}$, которая является точкой Вейерштрасса. Существует классическое вложение $\mathcal{C}(K)$ в группу K-точек $J(K)$ якобиева многообразия J кривой $\mathcal{C}$, отождествляющее точку $\mathcal{O}$ с единичным элементом группы $J(K)$. При $2 \le g \le 5$ в статье явно найдены представители классов бирациональной эквивалентности таких гиперэллиптических кривых $\mathcal{C}$ с отмеченной единственной точкой на бесконечности $\mathcal{O}$, что множество $\mathcal{C}(K) \cap J(K)$ содержит не менее 6 точек кручения порядка $2g+1$. Ранее было известно, что при $g = 2$ таких классов эквивалентности ровно 5, а при $g \ge 3$ была известна верхняя оценка, зависящая только от рода g. Мы улучшаем ранее известную верхнюю оценку почти в 36 раз.

Ключевые слова: гиперэллиптическая кривая, якобиево многообразие, точки кручения, метод Флина-Лепревоста

DOI: 10.31857/S2686954324040028, **EDN:** YZPDFK

1. ВВЕДЕНИЕ

Пусть K — алгебраически замкнутое поле характеристики 0 и K^* — мультипликативная группа поля K. Пусть $f(x) \in K[x]$ — многочлен степени $2g+1$, не имеющий кратных корней. Гладкой плоской афинной кривой $C_f^\circ : y^2 = f(x)$ соответствует неособая проективная кривая C_f, являющаяся гиперэллиптической кривой рода g с единственной точкой "на бесконечности", которую обозначим ∞. Множество K-точек кривой C_f имеет вид $C_f(K) = \{(x_0, y_0) \in K^2 : y_0^2 = f(x_0)\} \cup \{\infty\}$. Точки вида $(x_j, 0) \in C_f(K)$ и ∞ являются точками Вейерштрасса кривой C_f, где x_j — нули многочлена $f(x)$. *Отмеченной гиперэллиптической кривой нечетной степени и рода* g, определенной над полем K, будем называть пару (C_f, ∞).

Известно (см. [1]), что для определенной над полем K отмеченной гиперэллиптической кривой $(\mathcal{C}, \mathcal{O})$ нечетной степени и рода g найдется многочлен $f(x) \in K[x]$ степени $2g+1$, не имеющий кратных корней, для которого $(\mathcal{C}, \mathcal{O})$ бирационально эквивалентна (C_f, ∞) над K.

Пусть $(\mathcal{C}, \mathcal{O})$ — определенная над полем K отмеченная гиперэллиптическая кривая нечетной степени и рода g. Рассмотрим классическое отображение Альбанезе, сопоставляющее каждой точке $P \in \mathcal{C}(K)$ класс дивизора $P - \mathcal{O}$ в группе классов дивизоров степени ноль $\Delta_K^\circ(C)$ кривой $\mathcal{C}$. Над алгебраически замкнутым полем K характеристики 0 группу $\Delta_K^\circ(C)$ можно отождествить с группой K-точек многообразия Якоби (якобиана) $J(K)$ кривой $\mathcal{C}$. Поэтому существует вложение $\mathcal{C} \rightarrowtail J$, при котором мы можем рассматривать K-точки кривой $\mathcal{C}$ как их образы в $J(K)$, и, в частности, будем говорить, что точка $P \in \mathcal{C}(K)$ является точкой кручения порядка n в якобиане J, если соответствующий класс дивизора имеет порядок n в якобиане J.

В [2] доказано, что если $(\mathcal{C}, \mathcal{O})$ — определенная над полем K отмеченная гиперэллиптическая кривая нечетной степени и рода g, то не существует точек кручения $P \in \mathcal{C}(K)$ порядка n для $3 \le n \le 2g$. Если точка $P \in \mathcal{C}(K)$ является точкой кручения порядка $n \ge 2g+1$, то точка $\iota P \ne P$ также является точкой кручения порядка n, где ι — гиперэллиптическая инволюция.

В недавней статье [3] рассмотрена задача об описании множества пар $(\mathcal{C}, \mathcal{O})$ таких, что $(\mathcal{C}, \mathcal{O})$ — определенная над полем K отмеченная гипер-

[1] *Научно-технологический университет "Сириус", пгт Сириус, Краснодарский край, Россия*

[*] *E-mail: fedorov.gv@talantiuspeh.ru*

эллиптическая кривая нечетной степени и рода g, и существует $d = 2,4,6$ или более точек кручения $P \in \mathcal{C}(K)$ порядка $2g+1$ в якобиане J. Множество пар $(\mathcal{C},\mathcal{O})$ можно рассматривать с точностью до бирациональной эквивалентности, определенной над полем K. При $g = 2$ эта задача решена в [4], а именно при $d = 2,4,6$ описано множество классов бирациональной эквивалентности пар $(\mathcal{C},\mathcal{O})$ путем сопоставления их точкам на определенной поверхности.

При $g \geq 2$ обозначим S_g множество классов бирациональной эквивалентности пар $(\mathcal{C},\mathcal{O})$ таких, что определенная над полем K отмеченная гиперэллиптическая кривая $(\mathcal{C},\mathcal{O})$ содержит не менее 6 K-точек кручения порядка $2g+1$ в ее якобиане J. В [3] доказано, что $\#S_g \leq 9(4g-1)\binom{2g}{g}^2$.

Цель этой работы — ответить на вопрос из статьи [3] о явном виде представителей классов бирациональной эквивалентности, входящих в множество S_g, или доказательстве, что множество S_g пусто. В теоремах 1-4 найдены соответствующие результаты для $2 \leq g \leq 5$. Отдельно отметим теорему 3, в которой доказано, что $\#S_4 = 1$, и явно выписан представитель единственного класса бирациональной эквивалентности. Этот результат очень неожиданный, поскольку для нахождения сооответствующей отмеченной гиперэллиптической кривой необходимо было решить систему полиномиальных уравнений, в которой количество неизвестных больше, чем количество переменных (см. предложение 2). При $g \geq 6$ мы высказываем предположение, что множество S_g пусто. В теореме 5 мы несколько улучшаем результат [3] об оценке $\#S_g$, но все же мы пока далеки от указанного предположения.

Найденные результаты в теоремах 1-4 можно отнести к теоремам о конечности классов определенных кривых с явным описанием представителей этих классов (см. [5], [6], [7], [8]). Развитые в этой статье исследования являются продолжением [3], [9] с применением метода Флина-Лепревоста (см. [10], [11], [12]).

2. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

При $g = 2$ в [4] выделены 5 классов бирациональной эквивалентности пар $(\mathcal{C},\mathcal{O})$ над алгебраически замкнутым полем характеристики 0, удовлетворяющих указанным выше условиям. В теореме 1 мы еще раз независимо доказываем этот результат и явно находим представителей всех 5 классов.

Теорема 1. *Пусть* $S_2 = \{(C_{2,j},\infty) : y^2 = f_{2,j}(x), j = 1,\ldots,5\}$ *— множество из пяти отмеченных гиперэллиптических кривых нечетной степени и рода 2, где*

$$f_{2,1}(x) = 1 - 4x^5, \quad b_1 = -\frac{\sqrt{5}}{4} - \frac{1}{4} - \frac{i\sqrt{2}\sqrt{5-\sqrt{5}}}{4},$$

$$\begin{aligned} f_{2,2}(x) = {} & 4x^5(2b_2-1)\left(2b_2^2-6b_2+5\right) + \\ & + 20x^4(b_2+1)\left(2b_2^2-6b_2+5\right) + \\ & + 40x^3(b_2+1)\left(2b_2^2-6b_2+5\right) + \\ & + 4x^2\left(16b_2^3-35b_2^2+b_2+37\right) + \\ & + 12x\left(2b_2^3-5b_2^2+2b_2+4\right) + 9, \end{aligned}$$

$$b_2 = \frac{1}{2} - \frac{\sqrt{3-2\sqrt{5}}}{2},$$

$$\begin{aligned} f_{2,3}(x) = {} & -4x^5\left(79b_3^3-201b_3^2+144b_3-170\right) - \\ & - 100x^4\left(7b_3^3-18b_3^2+13b_3-15\right) - \\ & - 40x^3\left(14b_3^3-37b_3^2+28b_3-31\right) - \\ & - 20x^2\left(9b_3^3-25b_3^2+21b_3-23\right) - \\ & - 20x\left(b_3^3-3b_3^2+3b_3-4\right) + 5, \end{aligned}$$

$$b_3 = -\frac{\sqrt{5}}{4} + \frac{3}{4} - \frac{i\sqrt{2}\sqrt{1+3\sqrt{5}}}{4},$$

$$\begin{aligned} f_{2,4}(x) = {} & -8x^5\left(\sqrt{15}i+\sqrt{5}\right) - \\ & - 25x^4\left(-\sqrt{3}i+\sqrt{15}i+3\sqrt{5}+1\right) + \\ & + 20x^3\left(5\sqrt{3}i-7\sqrt{5}\right) + \\ & + 5x^2\left(5\sqrt{15}i+21\sqrt{3}i+21-15\sqrt{5}\right) + \\ & + 10x\left(\sqrt{15}i+3\sqrt{3}i+9-\sqrt{5}\right) + 20, \end{aligned}$$

$$b_4 = \frac{1}{2} - \frac{\sqrt{3}i}{2},$$

$$\begin{aligned} f_{2,5}(x) = {} & -4x^5\left(-3\sqrt{3}i+\sqrt{15}i+\sqrt{5}-7\right) - \\ & - 5x^4\left(-7\sqrt{3}i+\sqrt{15}i-3\sqrt{5}-7\right) - \\ & - 10x^3\left(-7\sqrt{3}i+\sqrt{15}i-3\sqrt{5}-7\right) - \\ & - x^2\left(-55\sqrt{3}i+9\sqrt{15}i-19\sqrt{5}-95\right) - \\ & - 4x\left(-5\sqrt{3}i+\sqrt{15}i-\sqrt{5}-15\right) + 16, \end{aligned}$$

$$b_5 = \frac{1}{2} - \frac{\sqrt{3}i}{2}.$$

Тогда

• *для каждого* $j = 1,\dots,5$ *точки* $P \in C_{2,j}$ *такие, что* $x(P) \in \{0,-1,-b_j\}$, *являются точками кручения порядка* 5 *в якобиане* $J_{2,j}(K)$ *соответствующей кривой* $(C_{2,j},\infty)$;

• *кривые* $(C_{2,j},\infty)$ *попарно бирационально неэквивалентны над* K;

• *если* $(\mathcal{C},\mathcal{O})$ — *определенная над полем* K *отмеченная гиперэллиптическая кривая нечетной степени и рода* 2, *содержащая не менее 6 точек кручения порядка* 5 *в ее якобиане* J, *то* $(\mathcal{C},\mathcal{O})$ *бирационально эквивалентна над* K *одной из кривых в* S_2.

В ходе доказательства теоремы 1 при $g = 2$ была найдена единственная с точностью до бирациональной эквивалентности пара $(\mathcal{C},\mathcal{O})$, для которой кривая $\mathcal{C}$ является особой. В связи с этим, для формулировки следующего результата мы используем понятие обобщенного якобиана в терминологии [13], [14], [15].

Теорема 2. *Пусть* $(C_1,\infty): y^2 = f_1(x)$ — *кубическая эллиптическая кривая с отмеченной точкой на бесконечности, где* $f_1(x) = 20x^3 + 25x^2 + 10x + 1$. *Тогда*

• *две точки* $P \in C_1(K)$ *такие, что* $x(P) = 0$, *имеют порядок* 3 *на эллиптической кривой* (C_1,∞);

• *четыре точки* $P \in C_1(K)$ *такие, что* $x(P)$ — *корень* $5x^2 + 5x + 1 = 0$, *являются точками кручения порядка* 5 *в обобщенном якобиане* $J_{\mathfrak{m}_1}(K)$ *кривой* (C_1,∞), *где* $\mathfrak{m}_1 = \{P \in C_1 : x(P) = 0\}$;

• *если* $(\mathcal{C},\mathcal{O})$ — *определенная над полем* K *кубическая эллиптическая кривая с отмеченной точкой Вейерштрасса* $\mathcal{O}$, *на которой существуют не менее* 4 *точек кручения порядка* 5 *в ее обобщенном якобиане* $J_{\mathfrak{m}}$, *где* $\mathfrak{m} = \{P, \iota P\}$ *для некоторой точки* $P \in \mathcal{C}$, $P \neq \mathcal{O}$, $P \neq \iota P$, *порядка* 3 *на эллиптической кривой* $(\mathcal{C},\mathcal{O})$, *то* $(\mathcal{C},\mathcal{O})$ *бирационально эквивалентна над* K *отмеченной эллиптической кривой нечетной степени* (C_1,∞).

Следующие две теоремы отвечают на вопрос из статьи [3] о явном виде представителей классов бирациональной эквивалентности, входящих в множество S_g при $3 \le g \le 5$.

Теорема 3. *Пусть* $(C_4,\infty): y^2 = f_4(x)$ — *отмеченная гиперэллиптическая кривая нечетной степени и рода* 4, *где*

$$f_4(x) = x^9 - 3x^8(b-2) - 12x^7(b-3) - 2x^6(10b-47) - 18x^5(b-8) - 2x^4(4b-71) + 92x^3 + 2x^2(b+19) + x(b+9) + \frac{2b+11}{12},$$

и b — *любой из корней* $x^2 - x + 1 = 0$. *Тогда*

• *точки* $P, \iota P \in C_4(K)$ *такие, что* $x(P) \in \{0,-1,-b\}$, *являются точками кручения порядка* 9 *в якобиане* $J_4(K)$ *кривой* (C_4,∞);

• *если* $(\mathcal{C},\mathcal{O})$ — *определенная над полем* K *отмеченная гиперэллиптическая кривая нечетной степени и рода* 4, *содержащая не менее 6 точек кручения порядка* 9 *в ее якобиане* J, *то* $(\mathcal{C},\mathcal{O})$ *бирационально эквивалентна над* K *кривой* (C_4,∞).

Теорема 4. *При* $g = 3$ *и* $g = 5$ *не существует определенных над полем* K *отмеченных гиперэллиптических кривых* (C_g,∞) *нечетной степени и рода* g, *содержащих* 6 *точек кручения порядка* $2g+1$ *в соответствующем якобиане* $J_g(K)$.

Доказательство теорем 1-4 опирается на алгоритмический подход, который мы описываем в § 4, а также на символьные компьютерные вычисления, реализованные на языке программирования Python с применением системы компьютерной алгебры Sympy и выполненные на персональном компьютере. При $g \ge 6$ в связи с большим объемом вычислений для получения подобных результатов необходимы более серьезные компьютерные мощности.

3. ВЕРХНЯЯ ОЦЕНКА

Пусть K — алгебраически замкнутое поле характеристики 0 и $g \ge 2$. Пусть определенная над полем K отмеченная гиперэллиптическая кривая $(\mathcal{C},\mathcal{O})$ нечетной степени и рода g содержит три пары $(P_j, \iota P_j)$, $j = 1,2,3$, точек кручения порядка $2g+1$ в ее якобиане J. Без ограничения общности (см. [1]), можем считать, что $(\mathcal{C},\mathcal{O}) = (C_f,\infty)$ и $x(P_1) = 0$, $x(P_2) = -1$, $x(P_1) = -b$, где $b \in K^*$, $b \neq 1$.

По теореме 1 [4] существуют такие многочлены $v_1, v_2, v_3 \in K[x]$, что $\deg v_j \le g$, $j = 1,2,3$, и справедлива система уравнений

$$\begin{aligned} v_1^2(x) - f(x) &= -x^{2g+1}, \\ v_2^2(x) - f(x) &= -(x+1)^{2g+1}, \\ v_3^2(x) - f(x) &= -(x+b)^{2g+1}. \end{aligned} \tag{1}$$

Верно и обратное утверждение: если для некоторого значения параметра b существуют многочлены $v_1, v_2, v_3, f \in K[x]$, $\deg v_j \le g$, $j = 1,2,3$, $\deg f = 2g+1$, являющиеся решением системы (1), и многочлен f свободен от квадратов, то отмеченная гиперэллиптическая кривая $(C_f,\infty): y^2 = f(x)$ нечетной степени и рода g содержит не менее 6 различных точек кручения порядка $2g+1$ в якобиане J кривой (C,∞).

Обозначим K_{2n+1} — круговое поле степени $2n+1$ и $M_{2g+1} \subset K_{2g+1} \subset K$ — множество всех корней степени $2g+1$ из 1, где $g \geq 2$. Обозначим $M^*_{2g+1} = M_{2g+1} \setminus \{1\}$. Для некоторого множества M обозначим $\#M$ количество элементов в M. Для двух многочленов $A(x)$ и $B(x)$ будем писать $A(x) \equiv B(x)$, если все соответствующие коэффициенты этих многочленов попарно совпадают.

Предложение 1. *Для некоторого фиксированного значения параметра $b \in K^*$, $b \neq 1$, существует решение системы* (1) *относительно неизвестных многочленов $v_1, v_2, v_3, f \in K[x]$ тогда и только тогда, когда для некоторого выбора $I, L \subset M^*_{2g+1}$, $\#I = \#L = g$, существуют значения параметров $\kappa, \tau \in K^*$ такие, что соотношение*

$$\kappa\tau\Phi(1+t) + \overline{\Phi}(1+t) = \kappa\Psi(1+bt) + \tau b\overline{\Psi}(1+bt) \quad (2)$$

справедливо для любого $t \in K$, где многочлены $\Phi(z), \overline{\Phi}(z), \Psi(z), \overline{\Psi}(z) \in K_{2g+1}[z]$ имеют вид

$$\Phi(z) = \prod_{\varepsilon \in I}(z-\varepsilon), \quad \overline{\Phi}(z) = \frac{z^{2g+1}-1}{(z-1)\Phi(z)},$$
$$\Psi(z) = \prod_{\varepsilon \in L}(z-\varepsilon), \quad \overline{\Psi}(z) = \frac{z^{2g+1}-1}{(z-1)\Psi(z)}. \quad (3)$$

Доказательство. Докажем необходимость. Исключим из системы (1) многочлен f, тогда

$$v_1^2 - v_2^2 = (x+1)^{2g+1} - x^{2g+1},$$
$$v_1^2 - v_3^2 = (x+b)^{2g+1} - x^{2g+1}.$$

Первое и второе уравнение разделим на x^{2g+1} и сделаем замену $t = 1/x$, при которой $v_j(x)/x^g = u_j(t) \in K[t]$, $j = 1,2,3$. Тогда система примет вид

$$u_1^2(t) - u_2^2(t) = \frac{1}{t}\left((1+t)^{2g+1} - 1\right),$$
$$u_1^2(t) - u_3^2(t) = \frac{1}{t}\left((1+bt)^{2g+1} - 1\right). \quad (4)$$

В правых частях стоят многочлены от t степени $2g$, поэтому степени многочленов $u_1(t) \pm u_2(t)$ и $u_1(t) \pm u_3(t)$ равны g. Выберем $I, L \subset M^*_{2g+1}$, $\#I = \#L = g$, и $\mu, \nu \in K^*$ так, что

$$2u_1(t) = \frac{1}{\mu}\overline{\Phi}(1+t) + \mu\Phi(1+t),$$
$$2u_2(t) = \frac{1}{\mu}\overline{\Phi}(1+t) - \mu\Phi(1+t),$$
$$2u_1(t) = \frac{b}{\nu}\overline{\Psi}(1+bt) + \nu\Psi(1+bt),$$
$$2u_3(t) = \frac{b}{\nu}\overline{\Psi}(1+bt) - \nu\Psi(1+bt), \quad (5)$$

где многочлены $\Phi(z), \overline{\Phi}(z), \Psi(z), \overline{\Psi}(z) \in K_{2g+1}[z]$ определены как в (3). Приравнивая правые части первого и третьего равенств, получаем следующее условие

$$\mu\Phi(1+t) + \frac{1}{\mu}\overline{\Phi}(1+t) = \nu\Psi(1+bt) + \frac{b}{\nu}\overline{\Psi}(1+bt), \quad (6)$$

которое должно быть справедливо для всех $t \in K$. Поскольку $\mu \neq 0$, то можно уравнение (6) умножить на μ и сделать замену $\kappa = \mu\nu$, $\tau = \mu/\nu$, тогда $\mu^2 = \kappa\tau$ и справедливо соотношение (2) для всех $t \in K$.

Докажем достаточность. По известным значениям параметров $\kappa, \tau \in K^*$, исходя из равенств $\kappa = \mu\nu$, $\tau = \mu/\nu$, значения $\mu, \nu \in K^*$ восстанавливаются однозначно с точностью до замены (μ, ν) на $(-\mu, -\nu)$, поэтому из (2) получаем (6). Если значения $b, \mu, \nu \in K^*$, $b \neq 1$, такие, что соотношение (6) справедливо для всех $t \in K$, то можно однозначно восстановить $u_1, u_2, u_3 \in K[t]$, далее $v_1, v_2, v_3 \in K[x]$, и, наконец, многочлен $f \in K[x]$. Замена (μ, ν) на $(-\mu, -\nu)$ меняет знак у многочленов u_1, u_2, u_3 и v_1, v_2, v_3, а многочлен f при этом не меняется.

Пусть $g \geq 2$ и многочлены $\Phi(z), \overline{\Phi}(z), \Psi(z), \overline{\Psi}(z) \in K_{2g+1}[z]$ определены как в (3) для фиксированного выбора $I, L \subset M^*_{2g+1}$, $\#I = \#L = g$. Обозначим $\Phi_k = \Phi^{(k)}(1)$, $\overline{\Phi}_k = \overline{\Phi}^{(k)}(1)$, $\Psi_k = \Psi^{(k)}(1)$, $\overline{\Psi}_k = \overline{\Psi}^{(k)}(1)$, при $k = 0, \ldots, g$. Определим матрицу $A(b)$ следующим образом:

$$A(b) = \begin{pmatrix} \Phi_k & \overline{\Phi}_k & b^k\Psi_k & b^k\overline{\Psi}_k \\ & & 0 \leq k \leq g & \end{pmatrix}. \quad (7)$$

Лемма 1. *Пусть $b = b_0 \in K^*$, $b_0 \neq 1$. Если ранг матрицы $A(b_0)$ равен 2, то существует не более 2 значений (κ, τ), для которых соотношение* (2) *справедливо для любого $t \in K$. Если ранг матрицы $A(b_0)$ равен 1, то таких значений (κ, τ) не существует.*

Доказательство. Элементы k-ой строки матрицы $A(b_0)$, умноженные на $t^k/k!$, в точности совпадают с соответствующими k-ыми слагаемыми разложения в ряд Маклорена многочленов

$$\Phi(1+t), \quad \overline{\Phi}(1+t), \quad \Psi(1+b_0t), \quad \overline{\Psi}(1+b_0t). \quad (8)$$

Поэтому линейная зависимость каких-то столбцов матрицы $A(b_0)$ равносильна линейной зависимости соответствующих многочленов (8) с теми же коэффициентами. Следовательно, из

справедливости соотношения (2) при некоторых значениях $b = b_0, \kappa, \tau$ следует, что ранг матрицы $A(b_0)$ не превосходит 3.

Предположим, что ранг матрицы $A(b_0)$ равен 1. Значит, $\Phi(1+t) \equiv \overline{\Phi}(1+t)$ и $\Psi(1+b_0t) \equiv \overline{\Psi}(1+b_0t)$, но это противоречит соотношениям

$$\begin{aligned} &\Phi(1+t)\overline{\Phi}(1+t) = ((1+t)^{2g+1} - 1)/t, \\ &\Psi(1+b_0t)\overline{\Psi}(1+b_0t) = ((1+b_0t)^{2g+1} - 1)/t. \end{aligned} \tag{9}$$

Предположим, что ранг матрицы $A(b_0)$ равен 2, то есть любые три столбца матрицы $A(b_0)$ линейно зависимы. Рассмотрим последнюю строку матрицы $A(b_0)$: $(1,1,b_0^g,b_0^g)$. Из (9) имеем $\Phi(1+t) \not\equiv \overline{\Phi}(1+t)$ и $\Psi(1+b_0t) \not\equiv \overline{\Phi}(1+b_0t)$. Значит, существует номер $0 \le k \le g-1$ такой, что $\Phi_k \ne \overline{\Phi}_k$, и существуют единственные $\alpha, \beta \in K$, $\alpha \ne \beta$, такие, что

$$\begin{cases} \alpha b_0^g \Phi(1+t) + (1-\alpha) b_0^g \overline{\Phi}(1+t) = \Psi(1+b_0t), \\ \beta b_0^g \Phi(1+t) + (1-\beta) b_0^g \overline{\Phi}(1+t) = \overline{\Psi}(1+b_0t). \end{cases}$$

Для того, чтобы при $b = b_0$ выполнялось (2) для некоторых значений κ_0, τ_0 параметров κ, τ необходимо и достаточно

$$\begin{cases} b_0^g(\alpha\kappa_0 + \beta b_0 \tau_0) = \kappa_0 \tau_0, \\ b_0^g((1-\alpha)\kappa_0 + (1-\beta) b_0 \tau_0) = 1. \end{cases}$$

Эта система уравнений относительно κ_0, τ_0 имеет не более 2 решений. □

Положим

$$A_k(b) = \begin{pmatrix} \Phi_0 & \overline{\Phi}_0 & \Psi_0 & \overline{\Psi}_0 \\ \Phi_k & \overline{\Phi}_k & b^k \Psi_k & b^k \overline{\Psi}_k \\ 1 & 1 & b^g & b^g \end{pmatrix}, \tag{10}$$

$$k = 1,2,\ldots,g-1,$$

Обозначим за $A_{j,k}(b)$ матрицу, полученную из матрицы $A_k(b)$ вычеркиванием j-го столбца, $j = 1,2,3,4$. При $k = 1,\ldots,g-1$, $j = 1,2,3,4$ определим многочлены $P_{j,k}(b) = \det A_{j,k}(b) \in K_{2g+1}[b]$.

В следующем предложении мы считаем, что любое число является корнем многочлена, тождественно равного нулю.

Предложение 2. *1. Для $b = b_0 \in K^*$, $b_0 \ne 1$, существуют значения $\kappa_0, \tau_0 \in K^*$ параметров κ, τ, для которых соотношение (2) справедливо для любого $t \in K$ тогда и только тогда, когда ранг матрицы $A(b_0)$ не превосходит 3, и значение b_0 является общим корнем многочленов*

$$\begin{aligned} R_k(b) = bP_{1,k}(b)P_{2,k}(b) - \\ -P_{3,k}(b)P_{4,k}(b), \quad k = 1,\ldots,g-1. \end{aligned} \tag{11}$$

2. При фиксированном $b = b_0$ существует не более δ значений (κ, τ), для которых соотношение (2) справедливо для любого $t \in K$, где $\delta = 0$, если ранг матрицы $A(b_0)$ равен 1, $\delta = 2$, если ранг матрицы $A(b_0)$ равен 2, $\delta = 1$, если ранг матрицы $A(b_0)$ равен 3.

Доказательство. Докажем необходимость в пункте 1. Пусть значения $b_0, \kappa_0, \tau_0 \in K^*$, $b_0 \ne 1$, параметров b, κ, τ такие, что соотношение (2) справедливо для любого $t \in K$. Продифференцируем k раз соотношение (2) и подставим $t = 0$, $b = b_0$, $\kappa = \kappa_0$, $\tau = \tau_0$: $\kappa_0\tau_0\Phi_k + \overline{\Phi}_k = \kappa_0 b_0^k \Psi_k + \tau_0 b_0^{k+1} \overline{\Psi}_k$. Отсюда получаем линейную зависимость столбцов матрицы $A(b_0)$ с набором коэффициентов $(\kappa_0\tau_0, 1, \kappa_0, \tau_0 b_0)$. Значит, ранг матрицы $A(b_0)$ не превосходит 3, и каждая однородная система линейных уравнений с матрицей $A_k(b_0)$ имеет общее ненулевое решение $(\kappa_0\tau_0, 1, -\kappa_0, -\tau_0 b_0)$. Заметим, что набор

$$(P_{1,k}(b), -P_{2,k}(b), P_{3,k}(b), -P_{4,k}(b)) \tag{12}$$

принадлежит множеству решений однородной системы линейных уравнений с матрицей $A_k(b)$, поскольку линейная комбинация каждой строки матрицы $A_k(b)$ с коэффициентами из этого набора есть разложение определителя матрицы, составленной из матрицы $A_k(b)$, дополненной соответствующей повторной строкой.

Если при фиксированном k хотя бы одно из значений $P_{j,k}(b_0)$, $1 \le j \le 4$, отлично от нуля, то ранг матрицы $A_k(b_0)$ равен 3, и, следовательно, размерность пространства решений однородной системы линейных уравнений с матрицей $A_k(b_0)$ равна 1. В этом случае при $b = b_0$ набор (12) должен быть пропорционален $(\kappa_0\tau_0, 1, -\kappa_0, -\tau_0 b_0)$, откуда получаем, что b_0 является корнем $R_k(b)$. Если же при фиксированном k все значения $P_{j,k}(b_0)$, $1 \le j \le 4$, равны нулю, то при $b = b_0$ многочлен $R_k(b)$ также обращается в ноль.

Докажем достаточность в пункте 1. Пусть b_0 является общим корнем всех многочленов (11) при $k = 1,\ldots,g-1$ и ранг матрицы $A(b_0)$ не превосходит 3. Если при некотором $1 \le k \le g-1$ имеем $P_{1,k}(b_0) = 0$, то в силу $R_k(b_0) = 0$ либо $P_{3,k}(b_0) = 0$, либо $P_{4,k}(b_0) = 0$, следовательно любые три столбца матрицы $A(b_0)$ линейно зависимы, то есть $P_{j,k}(b_0) = 0$ для любого $1 \le j \le 4$. Аналогично, если предположить, что $P_{j,k}(b_0) = 0$ при не-

которых $1 \le j \le 4$, $1 \le k \le g-1$, то $P_{j,k}(b_0) = 0$ для любого $1 \le j \le 4$.

Предположим, что ранг матрицы $A(b_0)$ равен 3. Тогда существует номер k, $k = 1,\dots,g-1$, для которого все значения $P_{j,k}(b_0)$, $1 \le j \le 4$, не обращаются в ноль, а набор (12) при $b = b_0$ с точностью до умножения на ненулевой коэффициент является единственным решением однородной системы линейных уравнений с матрицей $A(b_0)$. Обозначим $\kappa_0 = P_{3,k}(b_0) / P_{2,k}(b_0)$, $\tau_0 = -b_0^{-1} P_{4,k}(b_0) / P_{2,k}(b_0)$, тогда в силу $R_k(b_0) = 0$ столбцы матрицы $A(b_0)$ линейно зависимы с коэффициентами $(\kappa_0\tau_0, 1, -\kappa_0, -\tau_0 b_0)$. А, следовательно и многочлены (8) линейно зависимы с этими же коэффициентами.

Случаи, когда ранг матрицы $A(b_0)$ меньше 3 разобраны в лемме 1. Предложение 2 доказано. □

Предположим, что найдены подходящие значения $b_0, \kappa_0, \tau_0 \in K^*$, $b_0 \ne 1$, параметров b, κ, τ, для которых соотношение (2) справедливо для всех $t \in K$. Опишем, как по этой тройке значений (b_0, κ_0, τ_0) однозначно восстановить многочлен $f(x)$, удовлетворяющий системе (1).

Возведем первое соотношение (5) в квадрат, и используя $\kappa\tau = \mu^2$, $\kappa / \tau = \nu^2$, запишем

$$4u_1^2(t) = \frac{1}{\kappa_0\tau_0}\overline{\Phi}^2(1+t) + 2\frac{(1+t)^{2g+1}-1}{t} + \kappa_0\tau_0\Phi^2(1+t). \tag{13}$$

Аналогичным образом однозначно восстанавливаются u_2^2, u_3^2. Обозначим $F(t) = tu_1^2 + 1 = tu_2^2 + (1+t)^{2g+1} = tu_3^2 + (1-b_0 t)^{2g+1}$, причем последние два равенства тождественны ввиду (4) и дальнейших построений. Отсюда имеем

$$f(x) = x^{2g+1}F(1/x) = \frac{x^{2g}}{4\kappa_0\tau_0}\overline{\Phi}^2\left(1+\frac{1}{x}\right) + \frac{(x+1)^{2g+1} + x^{2g+1}}{2} + \frac{\kappa_0\tau_0 x^{2g}}{4}\Phi^2\left(1+\frac{1}{x}\right). \tag{14}$$

Если полученный многочлен $f(x)$ свободен от квадратов, то уравнение $y^2 = f(x)$ задает определенную над K отмеченную гиперэллиптическую кривую (C, ∞) нечетной степени и рода g, которая обладает не менее 6 K-точками кручения порядка $2g+1$ в ее якобиане J.

Предложение 3. *Пусть для* $(I, L) = (I_0, L_0)$, $I_0, L_0 \subset M^*_{2g+1}$, $\#I = \#J = g$, *существуют значения* $b_0, \kappa_0, \tau_0 \in K^*$, $b_0 \ne 1$, *параметров* b, κ, τ, *для которых соотношение* (2) *справедливо для любых* $t \in K^*$. *Пусть* (C, ∞) — *соответствующая отмеченная гиперэллиптическая кривая нечетной степени и рода* g, *которая содержит не менее 6 точек кручения порядка* $2g+1$. *Обозначим* $\hat{I}_0 = M^*_{2g+1} \setminus I_0$, $\hat{L}_0 = M^*_{2g+1} \setminus L_0$. *Тогда если в качестве набора* (I, L) *взять любой из наборов* $(\hat{I}_0, L_0)$, $(I_0, \hat{L}_0)$, $(\hat{I}_0, \hat{L}_0)$, (L_0, I_0), $(\hat{L}_0, I_0)$, $(L_0, \hat{I}_0)$, $(\hat{L}_0, \hat{I}_0)$, *то найдутся значения* $\tilde{b}_0, \tilde{\kappa}_0, \tilde{\tau}_0 \in K^*$, $\tilde{b}_0 \ne 1$, *параметров* b, κ, τ, *для которых соотношение* (2) *справедливо для любых* $t \in K^*$, *и при этом соответствующая отмеченная гиперэллиптическая кривая* $(\tilde{C}, \infty)$ *нечетной степени и рода* g *бирационально эквивалентна* (C, ∞).

Доказательство. Достаточно проверить утверждение предложения только для $(I, L) = (\hat{I}_0, L_0)$ и $(I, L) = (L_0, I_0)$, поскольку остальные варианты получаются из этих путем их композиции.

Если вместо $(I, L) = (I_0, L_0)$ положить $(I, L) = (\hat{I}_0, L_0)$, то в системе (5) многочлены $\Phi(1+t)$ и $\Phi(1+t)$ поменяются местами, при этом можно положить $\tilde{\mu} = 1/\mu$ и $\tilde{u}_2 = -u_2$, а остальные обозначения оставить прежними. Тогда тройка $(\tilde{b}_0, \tilde{\kappa}_0, \tilde{\tau}_0) = (b_0, \tau_0, \kappa_0)$ подходит под условия предложения.

Если вместо $(I, L) = (I_0, L_0)$ положить $(I, L) = (L_0, I_0)$, то в системе (5) многочлены Φ и Ψ, $\overline{\Phi}$ и $\overline{\Psi}$ поменяются местами, причем для соответствия виду системы (5) необходимо сделать следующие подстановки $\tilde{t} = b_0 t$, $\tilde{b}_0 = 1/b_0$, $\tilde{u}_j = u_j / \sqrt{b_0}$, $j = 1,2,3$, $\tilde{\mu} = \mu / \sqrt{b_0}$, $\tilde{\nu} = \nu / \sqrt{b_0}$. Тогда тройка $(\tilde{b}_0, \tilde{\kappa}_0, \tilde{\tau}_0) = (1/b_0, \kappa_0 / b_0, \tau_0)$ подходит под условия предложения.

Теорема 5. *Пусть* K — *алгебраически замкнутое поле характеристики* 0 *и* $g \ge 2$. *Тогда существует конечное множество* S_g *определенных над* K *отмеченных гиперэллиптических кривых нечетной степени и рода* g *таких, что*

- $\#S_g \le \frac{4g-1}{4}\binom{2g}{g}\left(\binom{2g}{g}+2\right)$;
- *если* $(C, \mathcal{O})$ — *определенная над полем* K *отмеченная гиперэллиптическая кривая нечетной степени и рода* g, *на которой существуют не менее 6 точек кручения порядка* $2g+1$ *в ее якобиане* J, *то* $(C, \mathcal{O})$ *бирационально эквивалентна одной из кривых в* S_g.

Доказательство. По предложению 3 необходимо рассмотреть $\frac{1}{2}\binom{2g}{g} + \frac{1}{8}\left(\binom{2g}{g}^2 - 2\binom{2g}{g}\right)$

вариантов для пары множеств (I, L), $I, L \subset M^*_{2g+1}$, $\#I = \#L = g$. По предложению 2 для каждой пары множеств (I, L) существует не более $\max_{1\le k\le g-1}\deg R_k(b) = 4g-1$ значений b_0 для параметра b, а для каждого b_0 существует не более 2 значений (κ_0, τ_0) для параметров (κ, τ). По набору I, κ_0, τ_0 с помощью (14) однозначно восстанавливается многочлен $f(x)$.

4. АЛГОРИТМИЧЕСКИЙ ПОДХОД

Используя результаты теоремы 5 и предложения 2 можно сформулировать алгоритм для поиска подходящих значений параметров b, κ, τ, с помощью которых восстанавливается многочлен $f(x)$, задающий искомую отмеченную гиперэллиптическую кривую нечетной степени и рода g. Дадим некоторые комментарии, относящиеся к эффективной реализации этого алгоритма.

Для каждой пары (I, L) вместо уравнений вида (11) будем в первую очередь рассматривать однородную систему уравнений с матрицей, состоящей из первых трех строк матрицы $A(b)$. Для того, чтобы соотношение (2) было справедливо для любого $t \in K$, необходимо, чтобы решение $(\lambda_1(b), \lambda_2(b), \lambda_3(b), \lambda_4(b))$ этой системы уравнений было таким, что $R(b) = b\lambda_1(b)\lambda_2(b) - \lambda_3(b)\lambda_4(b) = 0$. Отсюда уже можно найти значения b_0, которых в случае $R(b) \not\equiv 0$ будет не более $\deg R(b) \le 7$.

Для поиска корней многочлена $R(b) \in K_{2g+1}[b]$ выислим его норму $N(R) \in \mathbb{Q}[b]$, равную произведению сопряженных многочленов R^σ относительно автоморфизмов Галуа $\sigma \in Gal(K_{2n+1} / \mathbb{Q})$. Если $g \ge 3$, то дополнительно вычислим определитель $D(b)$ матрицы, составленной из первых четырех строк матрицы $A(b)$. Поскольку ранг матрицы $A(b)$ должен быть меньше 4, то подходящие значения b_0 являются также и корнями $D(b)$, причем $\deg D(b) \le 7$. Вычислим $T(b) = \gcd(N(R), N(D)) \in \mathbb{Q}[b]$. Вычислим корни b_0 многочлена $T(b)$ и подставим их в $R(b) = 0$ и $D(b) = 0$ для проверки. Если $R(b_0) = D(b_0) = 0$, то в соответствии с предложением 2 находим значения параметров κ_0, τ_0 и по формуле (14) восстанавливаем многочлен $f(x)$. Остается только проверить, что $f(x)$ свободен от квадратов.

Вообще говоря, может возникнуть сложность с вычислением корней многочлена $T(b) \in \mathbb{Q}$, но на практике при $g \le 5$ во всех случаях получаем, что многочлен $T(b)$ раскладывается на неприводимые над $\mathbb{Q}$ множители не более 4 -ой степени, то есть все корни b_0 могут быть выписаны явно в радикалах.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Исследование выполнено за счет гранта Российского научного фонда (проект № 22-71-00101) в Научно-технологическом университете “Сириус”.

СПИСОК ЛИТЕРАТЫ

1. *Lockhart P.* On the discriminant of a hyperelliptic curve. // Trans. Amer. Math. Soc. 1994. V. 342(2). P. 729–752.
2. *Зархин Ю.Г.* Деление на 2 в гиперэллиптических кривых нечетной степени и их якобианах // Изв. РАН. Сер. матем. 2019. Т. 83. № 3. С. 93–112.
3. *Bekker B.M., Zarhin Y.G.* Torsion points of small order on hyperelliptic curves. // European Journal of Mathematics. 2022. V. 8. № 2. P. 611–624.
4. *Boxall J., Grant D., Leprévost F.* 5-torsion points on curves of genus 2 // J. London Math. Soc. 2001. V. 64(1). P. 29–43.
5. *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.
6. *Платонов В.П., Федоров Г.В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. 2018. Т. 209. № 4. С. 54–94.
7. *Платонов В.П., Федоров Г.В.* О проблеме классификации многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в гиперэллиптических полях // Известия РАН. Серия математическая. 2021. Т. 85. № 5. С. 152–189.
8. *Федоров Г.В.* Непрерывные дроби и проблема классификации эллиптических полей над квадратичными полями констант // Матем. заметки. 2023. Т. 114. № 6. С. 873–893.
9. *Bekker B.M., Zarhin Y.G.* Torsion points of order 2g+1 on odd degree hyperelliptic curves of genus g. // Trans. Amer. Math. Soc. 2020. V. 373. № 11. P. 8059–8094.
10. *Flynn E.V.* Large Rational Torsion on Abelian Varieties // J. Number Theory. 1990. V. 36. P. 257–265.
11. *Leprévost F.* Torsion sur des familles de courbes de genre g // Manuscripta mathematica. 1992. V. 75. P. 303–326.
12. *Платонов В.П., Федоров Г.В.* Бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28 // Докл. РАН. 2018. Т. 482. № 4. С. 385–388.
13. *Rosenlicht M.* Generalized Jacobian varieties // Ann. Math. 1954. V. 59. P. 505–530.
14. *Serre J.-P.* Algebraic Groups and Class Fields (Springer, New York, 1988).
15. *Платонов В.П., Жгун В.С., Федоров Г.В.* О конечности множества обобщенных якобианов с нетривиальным кручением над полями алгебраических чисел, // Докл. РАН. Матем., информ., проц. упр. 2023. Т. 513. С. 66–70.

ON HYPERELLIPTIC CURVES OF ODD DEGREE AND GENUS g WITH 6 TORSION POINTS OF ORDER 2g + 1

G. V. Fedorov[a]

Presented by Academician of the RAS V. P. Platonov

[a] *Sirius University of Science and Technology, Sirius, Krasnodar region, Russia*

Let a hyperelliptic curve $\mathcal{C}$ of genus g defined over an algebraically closed field K of characteristic 0, given by the equation $y^2 = f(x)$, where the polynomial $f(x) \in K[x]$ is square-free and has odd degree $2g + 1$. The curve $\mathcal{C}$ contains a single "infinite" point $\mathcal{O}$, which is the Weierstrass point. There is a classical embedding of $\mathcal{C}(K)$ into the group of K-points $J(K)$ of the Jacobian variety J of the curve $\mathcal{C}$, identifying the point $\mathcal{O}$ with the unit element of the group $J(K)$. For $2 \le g \le 5$, the article explicitly found representatives of birational equivalence classes such hyperelliptic curves $\mathcal{C}$ with a marked unique point at infinity $\mathcal{O}$ that the set $\mathcal{C}(K) \cap J(K)$ contains at least 6 torsion points of order $2g + 1$. It was previously known that for $g = 2$ there are exactly 5 such equivalence classes, and for $g \ge 3$ an upper bound was known that depended only on the genus of g. We improve the previously known upper bound by almost 36 times.

Keywords: hyperelliptic curve, Jacobian variety, torsion points, Flynn-Leprevost method