Неприводимость кубоидного полинома $P_{a,u}(t)$ через эллиптическую кривую нулевого ранга

Valery Asiryan

asiryanvalery@gmail.com

13 октября 2025

Аннотация

Для взаимно простых целых $a \neq u > 0$ положим $\Delta := u^2 - a^2 \neq 0$ и $A_0 := a^2u^2$. Рассмотрим

$$P_{a,u}(t) = t^8 + 6\Delta\, t^6 + (\Delta^2 - 2A_0)\, t^4 - 6\Delta A_0\, t^2 + A_0^2 \in \mathbb{Z}[t].$$

Мы доказываем, что $P_{a,u}(t)$ неприводим над $\mathbb{Z}$. Доказательство таково: (1) над $K = \mathbb{Q}(\sqrt{2})$ многочлен $P_{a,u}$ раскладывается как H_-H_+ с взаимно простыми сопряжёнными квартиками $H_\pm$; (2) любая гипотетическая K–факторизация $H_\pm$ влечёт существование рациональной точки на фиксированной квартике рода 1 $\mathcal{C} : v^2 = 16y^4 + 136y^2 + 1$ со структурным ограничением $\tau = y^2 = (au/\Delta)^2$; (3) якобиан $\mathcal{C}$ допускает вейерштрассову модель $E/\mathbb{Q}$, на которой вычисление в Magma подтверждает $\operatorname{rank} E(\mathbb{Q}) = 0$ и $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; (4) единственные рациональные τ, возникающие из $\mathcal{C}(\mathbb{Q})$, это $\tau \in \{0, 1/4\}$, что несовместимо с взаимно простыми целыми $a \neq u > 0$. Следовательно, $H_\pm$ неприводимы в $K[t]$, откуда $P_{a,u}$ неприводим в $\mathbb{Q}[t]$ и в $\mathbb{Z}[t]$ по Гауссу.

Ключевые слова Неприводимость; совершенный кубоид; квадратические расширения; квартики рода 1; якобианы; эллиптические кривые; нулевой ранг; кручение.

MSC 2020 Основные: 12E05. Дополнительные: 11D09, 11G05, 11R09.

1 Разложение над $K = \mathbb{Q}(\sqrt{2})$ и взаимная простота

Пусть $a, u \in \mathbb{Z}_{>0}$ взаимно просты и $a \neq u$ [1, 2], и положим

$$\Delta := u^2 - a^2 \neq 0, \qquad A_0 := a^2u^2.$$

Запишем (ср. [3])

$$P_{a,u}(t) = t^8 + At^6 + Bt^4 + Ct^2 + D, \quad A = 6\Delta,\ B = \Delta^2 - 2A_0,\ C = -6\Delta A_0,\ D = A_0^2.$$

Пусть $K := \mathbb{Q}(\sqrt{2})$.

Лемма 1 (Явное разложение над K). В $K[t]$ верно

$$P_{a,u}(t) = H_-(t)\,H_+(t), \qquad H_\pm(t) := t^4 + (3 \mp 2\sqrt{2})\Delta\, t^2 - A_0.$$

Доказательство. Положив $s = t^2$, получаем

$$\begin{aligned} H_-(t)H_+(t) &= (s^2 + \left(3 - 2\sqrt{2}\right)\Delta s - A_0)\,(s^2 + \left(3 + 2\sqrt{2}\right)\Delta s - A_0) \\ &= s^4 + As^3 + Bs^2 + Cs + D. \end{aligned}$$

□

Лемма 2 (Взаимная простота). $\gcd(H_-, H_+) = 1$ в $K[t]$.

Доказательство. Общий корень t_0 даёт $s_0 = t_0^2$, удовлетворяющий обоим уравнениям $s^2 + (3 \mp 2\sqrt{2})\Delta s - A_0 = 0$; вычитая, получаем $4\sqrt{2}\,\Delta\, s_0 = 0 \Rightarrow s_0 = 0 \Rightarrow A_0 = 0$, что невозможно. □

2 Редукция к фиксированной квартике рода 1

Положим $S := t^2$ и

$$h_-(S) := S^2 + (3 - 2\sqrt{2})\Delta\, S - A_0 \in K[S], \qquad \Delta_S = (17 - 12\sqrt{2})\Delta^2 + 4A_0. \quad (1)$$

Если h_- раскладывается в $K[S]$, то $\Delta_S = (r + s\sqrt{2})^2$ при некоторых $r, s \in \mathbb{Q}$. Сравнивая части, получаем

$$2rs = -12\Delta^2, \qquad r^2 + 2s^2 = 17\Delta^2 + 4A_0. \quad (2)$$

Исключая r и полагая $T := s^2$, имеем

$$2T^2 - (17\Delta^2 + 4A_0)T + 36\Delta^4 = 0, \quad (3)$$

так что дискриминант

$$Z^2 = \Delta_T = (17\Delta^2 + 4A_0)^2 - 288\Delta^4 = \Delta^4 + 136\Delta^2 A_0 + 16A_0^2 \quad (4)$$

должен быть рациональным квадратом.

Введём обозначения

$$X := \Delta^2, \quad Y := A_0 = a^2u^2, \quad v := \frac{Z}{X}, \quad \tau := \frac{Y}{X} = \left(\frac{au}{\Delta}\right)^2 \in \mathbb{Q}_{>0}.$$

Деление (4) на X^2 даёт конику

$$v^2 = 16\tau^2 + 136\tau + 1. \quad (5)$$

Структурное ограничение $\tau = (au/\Delta)^2$ заставляет τ быть рациональным квадратом, скажем $\tau = y^2$, и мы приходим к фиксированной квартике рода 1

$$\mathcal{C}: \quad v^2 = 16y^4 + 136y^2 + 1. \quad (6)$$

3 Якобиан $\mathcal{C}$ и удобная эллиптическая модель

Пусть $F(Y) = 16Y^4 + 136Y^2 + 1$ с коэффициентами $(a, b, c, d, e) = (16, 0, 136, 0, 1)$. Классические инварианты (см., например, Касселс или Ланг [4, 5]) равны

$$I = 12ae - 3bd + c^2 = 18688, \ J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 = -4\,874\,240.$$

Вейерштрассова модель $\mathrm{Jac}(\mathcal{C})$ имеет вид

$$E_0 : \ Y^2 = X^3 - 27\,I\,X - 27\,J = Y^2 = X^3 - 504\,576\,X + 131\,604\,480. \quad (7)$$

Её j–инвариант равен $j(E_0) = \frac{1\,556\,068}{81}$.

Для арифметического удобства мы работаем с эквивалентной моделью

$$E : \quad Y^2 = X(X-8)(X-9) = X^3 - 17X^2 + 72X, \quad (8)$$

которая имеет тот же j и три рациональные точки порядка 2: $(0, 0), (8, 0), (9, 0)$. Поскольку у $\mathcal{C}$ есть рациональная точка $(y, v) = (0, 1)$, стандартная конструкция, основанная на ней, отождествляет $\mathcal{C}$ бирационально с её якобианом (см. Касселс, гл. 1–2 [4]); далее мы рассматриваем E как удобную вейерштрассову модель $\mathrm{Jac}(\mathcal{C})$ для вычислений.

Замечание 1 (Явный изоморфизм $E_0 \simeq E$). На $E_0 : \ y^2 = x^3 - 504576\,x + 131604480$ положим

$$(X, Y) = \Big((x + 816)/12^2, \ y/12^3\Big)$$

(эквивалентно, $x = 12^2X - 816, \ y = 12^3Y$). Прямая подстановка даёт $Y^2 = X^3 - 17X^2 + 72X$. Кроме того, $\Delta(E_0) = 12^{12}\Delta(E)$ и $j(E_0) = j(E)$.

Замечание 2 (Кручение на E). Для E из (8) точки $(0, 0), (8, 0), (9, 0)$ являются рациональными точками порядка 2. Более того, точки $(6, \pm6)$ и $(12, \pm12)$ имеют порядок 4 (действительно, $2(6, 6) = (9, 0)$ и $2(12, 12) = (9, 0)$). Вместе с O это даёт

$$E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \ \oplus \ \mathbb{Z}/4\mathbb{Z}.$$

4 Ранг и кручение E (по вычислениям)

Предложение 1 (Ранг 0 и кручение). Для кривой $E/\mathbb{Q}$, заданной в (8), выполнено

$$\mathrm{rank}\,E(\mathbb{Q}) = 0, \qquad E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \qquad \mathrm{Cond}(E) = 48.$$

Вычислительное доказательство. Сеанс Magma (Приложение) [6] на модели $E : Y^2 = X(X-8)(X-9)$ возвращает

$$\mathrm{Cond}(E) = 48, \qquad E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \qquad \mathrm{rank}\,E(\mathbb{Q}) = 0.$$

Он также перечисляет целые точки $(0, 0), (8, 0), (9, 0), (6, \pm6), (12, \pm12)$ (отрицательные значения ненулевых Y симметричны), которые порождают подгруппу кручения. Это доказывает утверждение. $\square$

5 Рациональные точки на $\mathcal{C}$

Пусть $\overline{\mathcal{C}}$ — гладкая проективная модель $\mathcal{C}$. Для чётной квартики с ведущим и свободным коэффициентами, являющимися полными квадратами (16 и 1), у $\overline{\mathcal{C}}$ имеется две рациональные бесконечно удалённые точки (две ветви $v = \pm 4y^2$ при $y \to \infty$). Аффинная карта содержит точки $(0, \pm 1)$, и кривая имеет род 1.

Предложение 2. Существует бирациональное соответствие $\phi : \overline{\mathcal{C}} \dashrightarrow E$ над $\mathbb{Q}$, отправляющее одну из бесконечно удалённых точек в $O \in E(\mathbb{Q})$. Поскольку обе кривые являются гладкими проективными кривыми рода 1 над $\mathbb{Q}$, любое бирационное отображение над $\mathbb{Q}$ является изоморфизмом; следовательно, $\overline{\mathcal{C}}(\mathbb{Q})$ и $E(\mathbb{Q})$ находятся в естественной биекции. В частности,

$$|\overline{\mathcal{C}}(\mathbb{Q})| = |E(\mathbb{Q})| = 8.$$

Среди восьми точек две — бесконечно удалённые на $\overline{\mathcal{C}}$, а шесть аффинных — это ровно

$$(y, v) = (0, \pm 1), \qquad \left(\pm\tfrac{1}{2},\ \pm 6\right).$$

Доказательство. Так как $\operatorname{rank} E(\mathbb{Q}) = 0$ по предложениию 1, имеем $|E(\mathbb{Q})| = |E(\mathbb{Q})_{\text{tors}}| = 8$ (см. замечание 2). Указанный изоморфизм тогда даёт $|\overline{\mathcal{C}}(\mathbb{Q})| = 8$. Мы предъявляем восемь рациональных точек на $\overline{\mathcal{C}}$: две бесконечно удалённые и шесть перечисленных аффинных (прямая подстановка в $v^2 = 16y^4 + 136y^2 + 1$ показывает, что они лежат на $\mathcal{C}$). Следовательно, это все рациональные точки. □

Следствие 1. Единственные рациональные значения $\tau = y^2$, возникающие из $\mathcal{C}(\mathbb{Q})$, это

$$\tau \in \{0,\ 1/4\}.$$

6 Исключение структурных значений τ

Напомним, $\tau = (au/\Delta)^2$ при $\Delta = u^2 - a^2 \neq 0$.

Лемма 3. Для взаимно простых целых $a \neq u > 0$ выполнено $\tau \notin \{0, 1/4\}$.

Доказательство. $\tau = 0$ влекло бы $au = 0$, что невозможно. Если $\tau = 1/4$, то

$$|u^2 - a^2| = 2au.$$

Если $u^2 - a^2 = 2au$, то $(u - a)^2 = 2a^2$, т.е. $u/a = 1 \pm \sqrt{2}$ (иррационально), что невозможно. Если $a^2 - u^2 = 2au$, то $(a - u)^2 = 2u^2$, т.е. $a/u = 1 \pm \sqrt{2}$ (иррационально), что также невозможно. Обе возможности исключены. □

Замечание 3 (Критерий чётного разложения над полностью вещественным K). Так как $K = \mathbb{Q}(\sqrt{2})$ полностью вещественно и $A_0 > 0$, любое разложение $t^4 + \alpha t^2 - A_0$ в $K[t]$ должно быть чётным по t. Действительно, записывая $(t^2 + pt + q)(t^2 - pt + r)$ и сравнивая коэффициент при t, получаем $(r - q)p = 0$;

случай $r = q$ приводит к $q^2 = -A_0$, что невозможно в полностью вещественном поле. Значит, $p = 0$ и задача сводится к квадратичному уравнению $S^2+\alpha S-A_0$ по $S = t^2$ (т.е. к (1)).

Следствие 2 (Отсутствие разложения $h_\pm$ в K). При наших предположениях дискриминант (1) никогда не является квадратом в $K = \mathbb{Q}(\sqrt{2})$. Следовательно, $h_-(S)$ и $h_+(S)$ не раскладываются в $K[S]$, и каждый $H_\pm(t)$ неприводим в $K[t]$.

Доказательство. Предположим противное, что Δ_S — квадрат в K (что эквивалентно разложению $h_-(S)$ в $K[S]$). Тогда, по алгебре раздела 2, существуют $v, \tau \in \mathbb{Q}$ с $v^2 = 16\tau^2 + 136\tau + 1$ и $\tau = (au/\Delta)^2 = y^2$, т.е. у $\mathcal{C}$ есть рациональная точка с $y^2 = \tau$. По следствию 1 и лемме 3 это невозможно. Тот же аргумент применим к $h_+(S)$.

Наконец, по замечанию 3, любое разложение $H_\pm(t)$ в $K[t]$ было бы чётным по t и влекло бы разложение $h_\pm(S)$ в $K[S]$, что мы только что исключили. Следовательно, каждый $H_\pm$ неприводим в $K[t]$. □

7 Неприводимость $P_{a,u}(t)$ над $\mathbb{Z}$

Теорема 1. Для любых взаимно простых целых $a \neq u > 0$ многочлен $P_{a,u}(t) \in \mathbb{Z}[t]$ неприводим.

Доказательство. По леммам ??, $P_{a,u} = H_- H_+$ в $K[t]$ и $\gcd(H_-, H_+) = 1$. По следствию 2 оба $H_\pm$ неприводимы в $K[t]$. Любая факторизация в $\mathbb{Q}[t]$ дала бы в $K[t]$ произведение подмножества из $\{H_-, H_+\}$; поскольку ни один из $H_\pm$ не лежит в $\mathbb{Q}[t]$, остаётся только тривиальная факторизация. Поэтому $P_{a,u}$ неприводим в $\mathbb{Q}[t]$, а по лемме Гаусса (примитивность) [5, Ch. VIII] — и в $\mathbb{Z}[t]$. □

Приложение: проверка в Magma для разделов 4 и 5

Код.

```
Q := Rationals();
E := EllipticCurve([0,-17,0,72,0]); // Y^2 = X^3 - 17 X^2 + 72 X
Emin, mp := MinimalModel(E); Emin;
CremonaReference(Emin);
Conductor(E);
T := TorsionSubgroup(E); T; AbelianInvariants(T);
Rank(E);
IntegralPoints(E);

P<x> := PolynomialRing(Q);
C := HyperellipticCurve(16*x^4 + 136*x^2 + 1);
EfromC, phi := EllipticCurve(C);
IsIsomorphic(EfromC, E);
RationalPoints(C : Bound := 1000);
```

Транскрипт.

```
Elliptic Curve defined by y^2 = x^3 + x^2 - 24*x + 36 over Rational Field
48a3
48
Abelian Group isomorphic to Z/2 + Z/4
Defined on 2 generators
Relations:
    2*T.1 = 0
    4*T.2 = 0
[ 2, 4 ]
0 true
[ (0 : 0 : 1), (6 : -6 : 1), (8 : 0 : 1), (9 : 0 : 1), (12 : 12 : 1) ]
[ <(0 : 0 : 1), 1>, <(6 : -6 : 1), 1>, <(8 : 0 : 1), 1>, <(9 : 0 : 1), 1>, <(12
: 12 : 1), 1> ]
true
{@ (1 : -4 : 0), (1 : 4 : 0), (0 : -1 : 1), (0 : 1 : 1), (-1 : -24 : 2), (-1 :
24 : 2), (1 : -24 : 2), (1 : 24 : 2) @}
```

Последнее множество перечисляет восемь рациональных точек на $\overline{\mathcal{C}}$ в взвешенных проективных координатах $(X : Y : Z)$ пространства $\mathbb{P}(1,2,1)$ (веса $1,2,1$). На аффинной карте $Z \neq 0$ имеем тождество

$$(y,v) = \Big(X/Z,\ Y/Z^2\Big).$$

Отсюда $(1 : \pm 24 : 2)$ соответствует $(y,v) = (\frac{1}{2}, \pm 6)$, а восемь рациональных точек — это две бесконечно удалённые точки $(1 : \pm 4 : 0)$ вместе с шестью аффинными точками $(0, \pm 1)$ и $(\pm\frac{1}{2}, \pm 6)$, использованными в предложении 2.

Список литературы

[1] R. Sharipov, Perfect Cuboids and Irreducible Polynomials, arXiv:1108.5348 [math.NT], 2011.

[2] R. Sharipov, A note on a perfect Euler cuboid, arXiv:1104.1716 [math.NT], 2011.

[3] V. Asiryan, On the Irreducibility of the Cuboid Polynomial $P_{a,u}(t)$, arXiv:2510.07643 [math.GM], 2025.

[4] J. W. S. Cassels, Lectures on Elliptic Curves, London Mathematical Society Student Texts 24, Cambridge Univ. Press, 1991.

[5] S. Lang, Algebra, Rev. 3rd ed., Springer, 2002.

[6] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra System I: The User Language, J. Symbolic Computation 24 (1997), 235–265.