О неприводимости кубоидного многочлена $P_{a,u}(t)$

Валерий Асирян

asiryanvalery@gmail.com

9 октября 2025 г.

Аннотация

В данной работе рассматривается чётный унитарный многочлен степени 8 $P_{a,u}(t)$ при взаимно простых целых $a \neq u > 0$. Мы доказываем неприводимость над $\mathbb{Z}$, исключая все разложения степени 8. Во-первых, любая предполагаемая факторизация типа 4+4 приводит к специфическому диофантову условию, не имеющему целых решений, что показывается коротким 2- и 3-адическим анализом. Во-вторых, мы исключаем каждую факторизацию 2+6 с помощью точного критерия делимости и препятствия по дискриминанту. Наконец, после исключения 2+6 шаблоны 2+2+4, 2+2+2+2 и 3+3+2 тривиально перегруппируются в 2+6 и потому невозможны. Следовательно, $P_{a,u}(t)$ не допускает нетривиальной факторизации в $\mathbb{Z}[t]$.

Ключевые слова Неприводимость над $\mathbb{Z}$; чётные унитарные многочлены; кубоидный (эйлеров) многочлен $P_{a,u}(t)$; типы факторизаций 4+4, 2+6, 2+2+4, 2+2+2+2, 3+3+2; диофантовы ограничения; p-адические оценки (2-адические, 3-адические); препятствие по дискриминанту; лемма Гаусса; перегруппировка по чётности/инволюции; эллиптические кривые.

MSC 2020 Основная: 12E05 (Многочлены: неприводимость). Дополнительные: 11D72 (Уравнения во многих переменных; диофантовы уравнения), 11S05 (Локальные и p-адические поля), 11Y05 (Факторизация; простота).

1 Постановка задачи и обозначения

Пусть $a, u \in \mathbb{Z}_{>0}$ взаимно просты и $a \neq u$. Рассматривается чётный унитарный многочлен [1, 2, 3]

$$P_{a,u}(t) = t^8 + At^6 + Bt^4 + Ct^2 + D,$$

$$A = 6\Delta,\ \Delta := u^2 - a^2 \neq 0,\ B = \Delta^2 - 2a^2u^2,\ C = -a^2u^2A,\ D = a^4u^4.$$

Мы работаем в $\mathbb{Z}[t]$. Многочлен $P_{a,u}$ чётный, унитарный и примитивный: $\mathrm{cont}(P_{a,u}) = 1$ [5, 13, 6]. Стандартные критерии неприводимости, такие как критерий Эйзенштейна (включая сдвиг $t \mapsto t + c$), в общем случае неприменимы к $P_{a,u}$; ср. [14].

Теорема 1 (Цель). Для любых взаимно простых $a, u \in \mathbb{Z}_{>0}$ с $a \neq u$ многочлен $P_{a,u}(t)$ не раскладывается в $\mathbb{Z}[t]$ в произведение двух унитарных многочленов степени 4 (случай 4+4).

2 Нормальная форма факторизации 4+4 и необходимое условие ($\star$)

Лемма 1 (Гаусс + инволюция). Если $P_{a,u} = FG$ с унитарными $F, G \in \mathbb{Z}[t]$ и $\deg F = \deg G = 4$, то, при необходимости переупорядочив множители, верно одно из следующих:

(E) оба множителя чётны: $F = t^4 + pt^2 + q$, $G = t^4 + rt^2 + s$ ($p, q, r, s \in \mathbb{Z}$);

(C) сопряжённая пара: $G(t) = F(-t)$, где $F = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$.

Идея. Примитивность и лемма Гаусса дают примитивность и унитарность множителей [5, 13, 6]. Инволюция $\tau : t \mapsto -t$ фиксирует $P_{a,u}$; либо оба множителя инвариантны (чётные), либо τ их меняет местами (сопряжённая пара). □

Подробный вывод для случая (E)

Пусть $F = t^4 + pt^2 + q$, $G = t^4 + rt^2 + s$. Из $FG = P_{a,u}$ получаем систему

$$p + r = A, \tag{1}$$
$$pr + q + s = B, \tag{2}$$
$$ps + rq = C, \tag{3}$$
$$qs = D. \tag{4}$$

Из (1) имеем $r = A - p$. Введём

$$M := B + p^2 - Ap.$$

Тогда (2) и (4) переписываются как

$$q + s = M, \qquad qs = D. \tag{5}$$

Следовательно, q, s — целочисленные корни квадратного уравнения $X^2 - MX + D = 0$. Обозначим (дискриминант данного квадратного)

$$T^2 := M^2 - 4D \; [5,\; 6].$$

Тогда

$$q = \frac{M + \sigma T}{2}, \quad s = \frac{M - \sigma T}{2}, \qquad \sigma \in \{\pm 1\}. \tag{6}$$

Подставим (6) в (3). Левая часть (3) равна

$$ps + rq = p\frac{M - \sigma T}{2} + (A - p)\frac{M + \sigma T}{2} = \frac{AM + \sigma T(A - 2p)}{2}.$$

Отсюда из (3) получаем

$$\frac{AM + \sigma T(A - 2p)}{2} = C \quad \Longleftrightarrow \quad \sigma\, T\, (A - 2p) = 2C - AM. \tag{7}$$

Положим

$$X := p - 3\Delta \qquad (\text{то есть } p = X + 3\Delta,\; A = 6\Delta).$$

Далее следуют прямые вычисления.

<u>Вычисление M.</u>

$$\begin{aligned} M &= B + p^2 - Ap = (\Delta^2 - 2a^2u^2) + (X + 3\Delta)^2 - 6\Delta(X + 3\Delta) \\ &= (\Delta^2 - 2a^2u^2) + \Big(X^2 + 6\Delta X + 9\Delta^2\Big) - 6\Delta X - 18\Delta^2 \\ &= X^2 - 8\Delta^2 - 2a^2u^2. \end{aligned}$$

<u>Вычисление $2C - AM$.</u> Так как $C = -a^2u^2A = -6\Delta\, a^2u^2$, имеем

$$2C = -12\Delta\, a^2u^2, \qquad AM = 6\Delta\,(X^2 - 8\Delta^2 - 2a^2u^2).$$

Следовательно,

$$2C - AM = -12\Delta a^2u^2 - 6\Delta(X^2 - 8\Delta^2 - 2a^2u^2) = -6\Delta X^2 + 48\Delta^3.$$

Таким образом, (7) принимает вид

$$\begin{aligned} \sigma\, T\, (A - 2p) &= \sigma\, T\, (6\Delta - 2X - 6\Delta) = -2\sigma X T \\ &= 2C - AM = -6\Delta X^2 + 48\Delta^3. \end{aligned}$$

Делим на -2 и получаем основное соотношение

$$\sigma\, T\, X = 3\Delta\,(X^2 - 8\Delta^2). \tag{8}$$

Вычисление T^2. По определению,

$$\begin{aligned} T^2 = M^2 - 4D &= \Big(X^2 - 8\Delta^2 - 2a^2u^2\Big)^2 - 4a^4u^4 \\ &= (X^2 - 8\Delta^2)^2 - 4a^2u^2(X^2 - 8\Delta^2) \\ &= (X^2 - 8\Delta^2)\Big(X^2 - 8\Delta^2 - 4a^2u^2\Big). \end{aligned}$$

Вывод «звёздного» уравнения. Возводим (8) в квадрат и подставляем выражение для T^2:

$$T^2X^2 = 9\Delta^2\,(X^2 - 8\Delta^2)^2.$$

Так как $X^2 \neq 8\Delta^2$ (см. ниже), можно сократить $(X^2 - 8\Delta^2)$ и получить

$$\Big(X^2 - 8\Delta^2 - 4a^2u^2\Big)X^2 = 9\Delta^2\,(X^2 - 8\Delta^2).$$

Переносим всё влево и группируем, приходим к диофантову уравнению

$$\boxed{(X^2 - 8\Delta^2)(X^2 - 9\Delta^2) = 4\,a^2u^2\,X^2} \qquad (\star)$$

(см. замечание ниже о допустимости сокращения).

Замечание 1 (Допустимость сокращения и следствие). Если $X^2 = 8\Delta^2$, то сравнение 2-адических оценок даёт $2\,\nu_2(X) = 3 + 2\,\nu_2(\Delta)$, что невозможно (левая часть чётна, правая нечётна). Значит, при $\Delta \neq 0$ равенство $X^2 = 8\Delta^2$ не имеет целых решений, и сокращение на множитель $X^2 - 8\Delta^2$ корректно [8, 10, 9]. Следовательно, из (1)–(4) вытекает $(\star)$. В обратную сторону в общем случае ничего не утверждается: требуется дополнительно, чтобы $T^2 = M^2 - 4D$ было полным квадратом и $q = \frac{M \pm T}{2} \in \mathbb{Z}$.

Случай (C): сопряжённая пара

Предположим

$$F(t) = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta, \qquad G(t) = F(-t),$$

так что $F(t)F(-t) = P_{a,u}(t)$. Приравнивание коэффициентов даёт систему

$$2\beta - \alpha^2 = A = 6\Delta, \tag{9}$$

$$\beta^2 + 2\delta - 2\alpha\gamma = B = \Delta^2 - 2A_0, \tag{10}$$

$$2\beta\delta - \gamma^2 = C = -6\Delta A_0, \tag{11}$$

$$\delta^2 = D = A_0^2, \tag{12}$$

где $\Delta = u^2 - a^2 \neq 0$ и $A_0 = a^2u^2 = (au)^2$.

Шаг 1: знак δ фиксирован. Из (12) имеем $\delta = \pm A_0$. Если $\delta = -A_0$, то (11) превращается в

$$-2\beta A_0 - \gamma^2 = -6\Delta A_0 \quad \Longrightarrow \quad \gamma^2 = A_0\,(6\Delta - 2\beta).$$

Используя (9), $2\beta = \alpha^2 + 6\Delta$, получаем $\gamma^2 = -A_0\alpha^2$. Следовательно, $\gamma = \alpha = 0$. Тогда (9) даёт $\beta = 3\Delta$, а (10) — $9\Delta^2 + 2(-A_0) = \Delta^2 - 2A_0$, т.е. $8\Delta^2 = 0$, что противоречит $\Delta \neq 0$. Поэтому обязательно

$$\boxed{\delta = +A_0}.$$

Шаг 2: удобная репараметризация. Положим $m := au$, тогда $A_0 = m^2$. При $\delta = A_0 = m^2$ из (11) следует

$$\gamma^2 = m^2(2\beta + 6\Delta),$$

откуда $m \mid \gamma$. Запишем $\gamma = m\kappa$ с $\kappa \in \mathbb{Z}$. Используя (9) (то есть $2\beta = \alpha^2 + 6\Delta$) получаем

$$\boxed{\kappa^2 = \alpha^2 + 12\Delta}. \tag{13}$$

Введём

$$s := \kappa + \alpha, \qquad t := \kappa - \alpha \qquad (\text{значит } s, t \in \mathbb{Z},\ \ s + t = 2\kappa,\ s - t = 2\alpha).$$

Тогда из (13)

$$st = \kappa^2 - \alpha^2 = 12\Delta. \tag{†}$$

В терминах s, t легко проверить, что

$$\begin{aligned} \beta &= \frac{\alpha^2 + 6\Delta}{2} = \frac{(s-t)^2}{8} + \frac{st}{4} = \boxed{\frac{s^2 + t^2}{8}}, \\ \alpha\gamma &= m\alpha\kappa = m\,\frac{(s+t)(s-t)}{4} = \boxed{m\,\frac{s^2 - t^2}{4}}. \end{aligned} \tag{14}$$

Шаг 3: устранение α, β, γ из (10). Подставим (14) и $\delta = m^2$ в (10):

$$\left(\frac{s^2 + t^2}{8}\right)^2 + 2m^2 - 2 \cdot m\,\frac{s^2 - t^2}{4} = \Delta^2 - 2m^2.$$

Умножив на $576 = \mathrm{lcm}(64, 2, 144)$ и используя (†), т.е. $\Delta^2 = (st)^2/144$, уничтожим знаменатели:

$$9(s^2 + t^2)^2 - 288m(s^2 - t^2) + 2304m^2 = 4s^2t^2.$$

Переставляя, получаем

$$9(s^2+t^2)^2 - 288m(s^2-t^2) + 2304m^2 - 4s^2t^2 = 0. \tag{15}$$

Положим $U := s^2$, $V := t^2$ (неотрицательные целые). Тогда (15) принимает вид

$$9U^2 + 14UV + 9V^2 - 288mU + 288mV + 2304m^2 = 0.$$

Дополняя до квадрата, получаем тождество

$$(3U - 3V - 48m)^2 + 32\,UV = 0.$$

Значит, оба слагаемых равны нулю:

$$UV = 0 \quad \text{и} \quad 3U - 3V - 48m = 0.$$

Первое равенство $UV = 0$ означает $s\,t = 0$, откуда по (†) $\Delta = 0$, что противоречит нашему предположению $\Delta \neq 0$.

Вывод. Таким образом, система (9)–(12) не имеет целых решений при $\Delta \neq 0$. Эквивалентно, факторизация $P_{a,u}(t) = F(t)F(-t)$ с унитарным квартником $F \in \mathbb{Z}[t]$ невозможна.

Теорема 2 (Случай (C) невозможен). Для взаимно простых целых $a \neq u > 0$ (поэтому $\Delta = u^2 - a^2 \neq 0$) не существуют целые $\alpha, \beta, \gamma, \delta$ с $\delta^2 = A_0^2$ такие, что

$$P_{a,u}(t) = \Big(t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta\Big)\Big(t^4 - \alpha t^3 + \beta t^2 - \gamma t + \delta\Big).$$

В частности, факторизации 4+4 типа (C) (сопряжённая пара) не существует.

Замечание 2. Этот довод независим от анализа случая чётный–чётный (E) и не использует вспомогательных факторизаций устраняемого многочлена. Он опирается лишь на (9)–(12), определение знака $\delta = A_0$, репараметризацию (s,t) через соотношение $\kappa^2 = \alpha^2 + 12\Delta$ и элементарную тождественность

$$(3s^2 - 3t^2 - 48m)^2 + 32s^2t^2 = 0,$$

которая вынуждает $st = 0$, следовательно, $\Delta = 0$, что невозможно.

Теорема 3 (Необходимое условие для 4+4). Пусть $\Delta = u^2 - a^2 \neq 0$. Если $P_{a,u}(t)$ раскладывается в $\mathbb{Z}[t]$ в произведение двух унитарных квартников, то существует $X \in \mathbb{Z}$, удовлетворяющий $(\star)$.

Доказательство. По лемме 1 любая факторизация 4+4 имеет тип (E) или (C). По теореме 2 случай (C) исключён; значит мы в (E): $F = t^4 + pt^2 + q$, $G = t^4 + rt^2 + s$. Как показано при выводе $(\star)$, положив $X := p - 3\Delta$ и устраняя q, s через (1)–(4), получаем именно $(\star)$. □

3 Ключевая лемма: $\gcd(X, \Delta) = 1$

Лемма 2. Если $X \in \mathbb{Z}$ удовлетворяет $(\star)$, то $\gcd(X, \Delta) = 1$.

Доказательство. Предположим противное: простое p делит и X, и Δ [7, 9, 10, 11, 12]. Пишем

$$X = p^x X_0, \quad \Delta = p^d \Delta_0, \qquad x, d \geq 1, \;\; \gcd(X_0, p) = \gcd(\Delta_0, p) = 1.$$

Случай $p \geq 3$. Как обычно:

$$\begin{aligned} X^2 - 8\Delta^2 &= p^{2x}\Big(X_0^2 - 8p^{2(d-x)}\Delta_0^2\Big), \\ X^2 - 9\Delta^2 &= p^{2x}\Big(X_0^2 - 9p^{2(d-x)}\Delta_0^2\Big). \end{aligned}$$

Если $d > x$, обе скобки $\not\equiv 0 \pmod p$, и $\nu_p(\text{ЛЧ}) = 4x$. Правая часть имеет $\nu_p(\text{ПЧ}) = 2x + \nu_p(4a^2u^2) = 2x$ (так как $\gcd(a, u) = 1 \Rightarrow p \nmid au$). Противоречие. Если $d = x$, обе скобки не могут быть кратны p (иначе $\Delta_0^2 \equiv 0$), значит $\nu_p(\text{ЛЧ}) \geq 4x + 1 > 2x = \nu_p(\text{ПЧ})$. Противоречие [9, 11].

Добавление: нечётное простое p, гипотетический подслучай $d < x$. Для полноты предположим, что p — нечётное простое, $p \mid \Delta$ и $x := \nu_p(X) > d := \nu_p(\Delta) \geq 1$. Тогда обязательно

$$\nu_p(X^2 - 8\Delta^2) = 2d, \qquad \nu_p(X^2 - 9\Delta^2) = 2d,$$

так что

$$\nu_p\Big((X^2 - 8\Delta^2)(X^2 - 9\Delta^2)\Big) = 4d.$$

В правой части $(\star)$ $\nu_p(4a^2u^2X^2) = 2x$, поскольку $p \mid (u^2 - a^2)$ влечёт $p \nmid a$ и $p \nmid u$. Отсюда $4d = 2x$ и, следовательно,

$$x = 2d. \tag{16}$$

Сократив p^{4d} в $(\star)$, получаем

$$\Big(p^{2(x-d)}X_0^2 - 8\Delta_0^2\Big)\Big(p^{2(x-d)}X_0^2 - 9\Delta_0^2\Big) = 4a^2u^2X_0^2,$$

а с учётом (16)

$$\Big(p^{2d}X_0^2 - 8\Delta_0^2\Big)\Big(p^{2d}X_0^2 - 9\Delta_0^2\Big) = 4a^2u^2X_0^2.$$

Редуцируя по модулю p (так как $d \geq 1$), имеем

$$(-8\Delta_0^2) \cdot (-9\Delta_0^2) \equiv 4a^2u^2X_0^2 \pmod p,$$

т.е.

$$72\,\Delta_0^4 \equiv 4\,a^2u^2X_0^2 \pmod p \quad \Longleftrightarrow \quad 18 \equiv \left(\frac{auX_0}{\Delta_0^2}\right)^2 \pmod p. \qquad (17)$$

Значит, 18 — квадратичный вычет по модулю p. Так как $\left(\frac{3^2}{p}\right) = 1$, это равносильно

$$\left(\frac{18}{p}\right) = \left(\frac{2}{p}\right) = 1,$$

и по классическому описанию знака символа Лежандра $(2/p)$ (см., напр., [4]) получаем

$$p \equiv 1 \text{ или } 7 \pmod 8. \qquad (18)$$

Пишем $X_0 = h\,\xi$ и $\Delta_0 = h\,\Delta_1$ при $h := \gcd(X_0, \Delta_0)$ и $\gcd(\xi, \Delta_1) = 1$. Положим

$$A' := p^{2d}\xi^2 - 8\Delta_1^2, \qquad B' := p^{2d}\xi^2 - 9\Delta_1^2.$$

Из вычисления $\gcd(A, B)$ в основном тексте имеем $\gcd(A', B') = 1$ и

$$A'B' = \left(\frac{2au\,\xi}{h}\right)^2.$$

Так как $A'B' \in \mathbb{Z}$, получаем $\frac{2au\,\xi}{h} \in \mathbb{Z}$. Следовательно, существуют $\varepsilon \in \{\pm 1\}$ и взаимно простые целые m, n такие, что

$$A' = \varepsilon\, m^2, \qquad B' = \varepsilon\, n^2, \qquad \gcd(m, n) = 1. \qquad (19)$$

Утверждение (определение знака). $\varepsilon = +1$.
Доказательство. Редуцируем (19) по модулю 3. Так как $p \geq 5$, $p^{2d} \equiv 1 \pmod 3$, откуда

$$B' \equiv \xi^2 \pmod 3, \qquad A' \equiv \xi^2 - 2\Delta_1^2 \equiv \xi^2 + \Delta_1^2 \pmod 3.$$

Если $\varepsilon = -1$, то $A' = -m^2$ и $B' = -n^2$, так что $A', B' \in \{0, 2\} \pmod 3$. Из $B' \equiv \xi^2$ следует $\xi \equiv 0 \pmod 3$, затем $A' \equiv -2\Delta_1^2 \equiv \Delta_1^2 \pmod 3$ даёт $\Delta_1 \equiv 0 \pmod 3$, что влечёт $3 \mid m$ и $3 \mid n$ — противоречие $\gcd(m, n) = 1$. $\square$

При $\varepsilon = +1$, редуцируя $B' = n^2$ по модулю p, получаем $n^2 \equiv -9\Delta_1^2 \pmod p$, откуда $(-1/p) = 1$ и, значит, $p \equiv 1 \pmod 4$. Вместе с (18) (т.е. $(2/p) = 1$) это даёт более строгую конгруэнцию

$$p \equiv 1 \pmod 8. \qquad (20)$$

В частности, ветка $p \equiv 7 \pmod 8$ исключается.

Остаточный подслучай и текущий статус. В остающейся конфигурации $p \equiv 1 \pmod 8$ приходим к системе

$$m^2 = p^{2d}\xi^2 - 8\Delta_1^2, \qquad n^2 = p^{2d}\xi^2 - 9\Delta_1^2, \qquad m^2 - n^2 = \Delta_1^2,$$

с $\gcd(m,n) = 1$ и $\gcd(\xi, \Delta_1) = 1$. Используя стандартные факторизации $(m \mp n)$ и соответствующие параметризации при нечётной/чётной Δ_1, проверяется, что обе формулы для $p^{2d}\xi^2$ сводятся к одному выражению; т.е. данными (элементарными) методами остаточный случай не приводит к противоречию.

Сохраняя остаточную нечётно-простую установку $p \geq 5$, $p \mid \Delta$, $d := \nu_p(\Delta) \geq 1$, $x := \nu_p(X) > d$, для которой $x = 2d$, после удаления общих множителей система

$$m^2 = p^{2d}\xi^2 - 8\Delta_1^2, \qquad n^2 = p^{2d}\xi^2 - 9\Delta_1^2, \qquad \gcd(\xi, p\Delta_1) = 1,$$

задаёт кривую рода 1

$$\mathcal{C}: \quad \begin{cases} m^2 = u^2 - 8w^2, \\ n^2 = u^2 - 9w^2, \end{cases} \qquad (m : n : w : u) \in \mathbb{P}^3,$$

и пучок квадрик показывает, что $\mathrm{Jac}(\mathcal{C})$ — эллиптическая кривая

$$E_0: \quad y^2 = x(x+1)(x+9). \tag{21}$$

Далее, дополнительное ограничение из остаточной системы состоит ровно в том, что X-координата на E_0 есть рациональный квадрат: полагая $u := n/\Delta_1$, соотношения «$u^2 + 1$ и $u^2 + 9$ — квадраты» переписываются как

$$(x, y) \in E_0(\mathbb{Q}) \qquad \text{с} \qquad x = u^2 \in (\mathbb{Q}^\times)^2.$$

Иными словами, нужно понять, содержит ли $E_0(\mathbb{Q})$ точку с x — ненулевым квадратом. Сейчас мы безусловно вычислим $E_0(\mathbb{Q})$.

Предложение 1 (Торсионная подгруппа). Для эллиптической кривой

$$E_0: \quad y^2 = x(x+1)(x+9),$$

торсионная подгруппа равна

$$\begin{aligned} E_0(\mathbb{Q})_{\mathrm{tors}} &= \big\{ O,\ (0,0),\ (-1,0),\ (-9,0),\ (3, \pm 12),\ (-3, \pm 6) \big\} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \ \times\ \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

В частности, $2(3,12) = (0,0)$ и $2(-3,6) = (-1,0)$, так что $(3,12)$ и $(-3,6)$ — точки порядка 4.

Доказательство. По теореме Нагелла–Лутца [17, 18] все торсионные точки на минимальной целочисленной модели имеют целые координаты. Три нетривиальные 2-торсионные точки — корни кубического: $x \in \{0, -1, -9\}$, т.е. $(0, 0), (-1, 0), (-9, 0)$.

Непосредственная подстановка показывает, что $(3, \pm 12)$ и $(-3, \pm 6)$ лежат на E_0, поскольку $12^2 = 3 \cdot 4 \cdot 12 = 144$ и $6^2 = (-3) \cdot (-2) \cdot 6 = 36$. Используя формулу удвоения (или стандартные вычисления вручную/ПО), получаем $2(3, 12) = (0, 0)$ и $2(-3, 6) = (-1, 0)$, откуда эти точки порядка 4. Других целых торсионных точек нет. По теореме Мазура торсионная подгруппа

$$\begin{aligned} E_0(\mathbb{Q})_{\text{tors}} = \{&O, (0, 0), (-1, 0), (-9, 0), \\ &(3, \pm 12), (-3, \pm 6)\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

□

Теорема 4 (Ранг через минимальную модель). Для

$$E_0 : \quad y^2 = x(x + 1)(x + 9)$$

имеем

$$E_0(\mathbb{Q}) \;\simeq\; \mathbb{Z}/2\mathbb{Z} \;\oplus\; \mathbb{Z}/4\mathbb{Z}, \qquad \operatorname{rank} E_0(\mathbb{Q}) = 0.$$

Доказательство. Сначала устраним квадратичный член в уравнении Вейерштрасса: заменой $x = X - \frac{10}{3}$ получаем

$$y^2 = X^3 - \frac{73}{3}X + \frac{1190}{27}.$$

Устраняя знаменатели подстановкой $X = \frac{x'}{9}$, $y = \frac{y'}{27}$, получаем краткую целую модель

$$y'^2 = x'^3 - 1971\, x' + 32130.$$

Эта кривая $\mathbb{Q}$-изоморфна минимальной модели

$$E : \; y^2 = x^3 + x^2 - 24x + 36,$$

имеющей проводимость $N = 48$ и принадлежащей изогении 48a. По таблицам Кремоны и LMFDB имеем

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \qquad \operatorname{rank} E(\mathbb{Q}) = 0.$$

Следовательно, то же верно для E_0. См. [19, 20]. □

Следствие 1 (Нет рациональных точек с квадратным x). Единственная рациональная точка на E_0 с x, являющимся рациональным квадратом, — это $(x, y) = (0, 0)$.

Доказательство. По предложению 1 и теореме 4 $E_0(\mathbb{Q})$ — в точности перечисленный торсионный набор. Просмотр x-координат $\{0, -1, -9, \pm 3\}$ показывает, что единственный квадрат среди них — это $x = 0$. $\square$

Теорема 5 (Безусловное закрытие остаточной ветви для нечётных простых). В остаточной конфигурации ($p \geq 5$, $p \mid \Delta$, $x = 2d > d \geq 1$) указанная система не имеет нетривиальных целых решений (т.е. решений с $n \neq 0$). Равносильно, подслучай $d < x$ невозможен.

Доказательство. Нетривиальное решение порождает рациональную точку на E_0 с $x = (n/\Delta_1)^2$ — ненулевым квадратом. По следствию 1 это невозможно. $\square$

Отсюда никакое нечётное простое p не может делить одновременно X и Δ.

Случай $p = 2$. Пишем $X = 2^x X_0$, $\Delta = 2^d \Delta_0$, $x, d \geq 1$, X_0, Δ_0 нечётны.

Рассмотрим три взаимоисключающие опции:

(B) $2x > 2d$.

Если $x \geq d + 2$ (т.е. $2x \geq 2d + 4$), то $\nu_2(X^2 - 8\Delta^2) = 2d + 3$, $\nu_2(X^2 - 9\Delta^2) = 2d$, следовательно, $\nu_2(\text{ЛЧ}) = 4d + 3$ (нечётно), тогда как $\nu_2(\text{ПЧ}) = 2 + \nu_2(a^2u^2) + 2x$ чётно. Противоречие.

Если $x = d + 1$ (т.е. $2x = 2d + 2$), то

$$X^2 - 8\Delta^2 = 2^{2d}\Big(4X_0^2 - 8\Delta_0^2\Big) = 2^{2d+2}\,(X_0^2 - 2\Delta_0^2),$$

где скобка нечётна; значит $\nu_2(X^2 - 8\Delta^2) = 2d + 2$. Кроме того,

$$X^2 - 9\Delta^2 = 2^{2d}\Big(4X_0^2 - 9\Delta_0^2\Big),$$

и $4X_0^2 - 9\Delta_0^2 \equiv 4 - 9 \equiv 3 \pmod 8$ нечётно, значит $\nu_2(X^2 - 9\Delta^2) = 2d$. Следовательно, $\nu_2(\text{ЛЧ}) = (2d + 2) + 2d = 4d + 2$.

Так как $\nu_2(\Delta) \geq 1$, числа a и u одной чётности; при $\gcd(a, u) = 1$ оба нечётны. Тогда $\nu_2(a^2u^2) = 0$ и

$$\nu_2(\text{ПЧ}) = \nu_2\Big(4a^2u^2X^2\Big) = 2 + 0 + 2x = 2 + 2(d + 1) = 2d + 4.$$

Сравнивая, при $d \geq 2$ имеем $4d + 2 \neq 2d + 4$ (противоречие), а при $d = 1$ оценки совпадают, и надо сравнить нечётные части. По модулю 8:

$$\frac{X^2 - 8\Delta^2}{2^4} \cdot \frac{X^2 - 9\Delta^2}{2^2} = (X_0^2 - 2\Delta_0^2)\,(4X_0^2 - 9\Delta_0^2) \equiv 7 \cdot 3 \equiv 5 \pmod 8,$$

тогда как нечётная часть правой стороны есть $X_0^2 \equiv 1 \pmod 8$. Противоречие. Значит, подслучай $x = d + 1$ невозможен.

(C) $2x = 2d$. Тогда $\nu_2(X^2 - 8\Delta^2) = 2d$ и $\nu_2(X^2 - 9\Delta^2) \geq 2d + 3$ (так как $X_0^2 \equiv 1 \pmod 8$). Следовательно, $\nu_2(\text{ЛЧ}) \geq 4d + 3$ (нечётно), в то время как $\nu_2(\text{ПЧ}) = 2 + \nu_2(a^2u^2) + 2x$ чётно. Противоречие.

(A) $p = 2$ и $x < d$.

Предположим $2 \mid \gcd(X, \Delta)$. Пишем $X = 2^x X_0$ и $\Delta = 2^d \Delta_0$ при $x \geq 1$, $d > x$, X_0, Δ_0 нечётны. Так как $2 \mid \Delta$ и $\gcd(a, u) = 1$, то a и u нечётны.

Шаг 1: Оценка по 2. Сравнение 2-адических оценок в $(\star)$ даёт

$$\nu_2(\text{ЛЧ}) = 4x, \qquad \nu_2(\text{ПЧ}) = 2x + 2.$$

Отсюда $4x = 2x + 2$ и, следовательно,

$$x = 1, \qquad d \geq 2. \tag{22}$$

Шаг 2: Нормализация и тождество произведения. Положим

$$M := 2^{2d-2}\Delta_0^2, \qquad A := X_0^2 - 8M, \qquad B := X_0^2 - 9M.$$

Деление $(\star)$ на 16 (с учётом (22)) даёт

$$A \cdot B = (auX_0)^2. \tag{23}$$

Так как X_0 нечётно,

$$\gcd(A, B) = \gcd(X_0^2 - 8M,\ X_0^2 - 9M) = \gcd(X_0^2, M) = \gcd(X_0^2, \Delta_0^2) =: g.$$

Пусть $h := \gcd(X_0, \Delta_0)$; тогда $g = h^2$ — нечётный полный квадрат.

Шаг 3: Определение знака по модулю 8. Поскольку $8M \equiv 0 \pmod 8$, имеем

$$A \equiv X_0^2 \equiv 1 \pmod 8.$$

Запишем, для некоторого $\varepsilon \in \{\pm 1\}$ и взаимно простых целых $m, n \geq 0$,

$$A = \varepsilon\, g\, m^2, \qquad B = \varepsilon\, g\, n^2, \tag{24}$$

(это следует из (23) и $\gcd(A/g, B/g) = 1$). Редуцируя первое равенство в (24) по модулю 8 и используя $g \equiv 1 \pmod 8$, получаем

$$1 \equiv A \equiv \varepsilon\, g\, m^2 \equiv \varepsilon \pmod 8.$$

Следовательно,

$$\varepsilon = +1, \qquad \text{т.е.} \quad A = g\, m^2. \tag{25}$$

Кроме того,

$$B \equiv X_0^2 - 9M \equiv \begin{cases} 1 - 4 \equiv 5 \pmod 8, & d = 2, \\ 1 - 0 \equiv 1 \pmod 8, & d \geq 3, \end{cases}$$

так как $M \equiv 4 \pmod 8$ при $d = 2$ и $M \equiv 0 \pmod 8$ при $d \geq 3$. Но из (24), (25) следует $B \equiv gn^2 \equiv 1 \pmod 8$. Значит, случай $d = 2$ невозможен, и остаётся

$$d \geq 3, \qquad A = g\,m^2, \quad B = g\,n^2. \tag{26}$$

В частности, m, n нечётны (так как $A \equiv B \equiv 1 \pmod 8$ и $g \equiv 1 \pmod 8$), и $\gcd(m, n) = 1$.

Шаг 4: Два диофантовых следствия. Из $A - B = M$ и (26) следует

$$g\,(m^2 - n^2) = M = 2^{2d-2}\Delta_0^2. \tag{27}$$

Пишем $\Delta_0 = h\,\Delta_1$ (напомним $g = h^2$). Тогда (27) принимает вид

$$m^2 - n^2 = 2^{2d-2}\,\Delta_1^2. \tag{28}$$

Используя $9A - 8B = X_0^2$, получаем также

$$g\,(9m^2 - 8n^2) = X_0^2 \quad \Longrightarrow \quad 9m^2 - 8n^2 = k^2 \tag{29}$$

для некоторого нечётного k.

Шаг 5: Финальное противоречие через бинарную форму $x^2 + 2y^2$. Из (29) следует

$$(3m)^2 = k^2 + 8n^2. \tag{30}$$

Пусть $D := \gcd(k, n)$. Из (30) видно, что D нечётно и $D \mid 3m$; значит $D = 3^j$ при $j \in \{0, 1\}$ (иначе $\gcd(m, n) \neq 1$).

Случай $j = 0$ (примитивный). Тогда существуют взаимно простые целые s, t такие, что

$$3m = s^2 + 2t^2, \qquad n = st, \qquad k = \pm(s^2 - 2t^2),$$

и s, t нечётны, поскольку n нечётно; см., напр., [9, гл. 5, §2]. Используя (28), получаем

$$m^2 - n^2 = \frac{(s^2 + 2t^2)^2}{9} - s^2t^2 = \frac{(s-t)(s+t)(s-2t)(s+2t)}{9} = 2^{2d-2}\Delta_1^2.$$

Отсюда

$$(s-t)(s+t)\cdot(s-2t)(s+2t) = 9 \cdot 2^{2d-2}\,\Delta_1^2. \tag{31}$$

Здесь $s \pm t$ чётны, тогда как $s \pm 2t$ нечётны; кроме того $\gcd(s - 2t, s + 2t) = \gcd(s - 2t, 4t) = 1$. Следовательно, нечётная часть (31) равна $\pm 9\Delta_1^2$ и, из взаимной простоты, с точностью до знаков

$$s - 2t = A^2, \qquad s + 2t = 9B^2 \quad \text{или} \quad s - 2t = -A^2, \qquad s + 2t = 9B^2,$$

для некоторых нечётных A, B. В первом подслучае

$$4t = (s+2t) - (s-2t) = 9B^2 - A^2 = (3B - A)(3B + A).$$

Оба множителя чётны, и ровно один кратен 4; значит $\nu_2(9B^2 - A^2) \geq 3$, что противоречит $\nu_2(4t) = 2$. Во втором подслучае

$$4t = 9B^2 + A^2 \equiv 1 + 1 \equiv 2 \pmod 4,$$

поэтому $\nu_2(4t) = 1$ — снова противоречие.

Случай $j = 1$ (непримитивный). Тогда существуют взаимно простые нечётные s, t такие, что

$$m = s^2 + 2t^2, \qquad n = 3st, \qquad k = \pm 3(s^2 - 2t^2),$$

и

$$m^2 - n^2 = (s-t)(s+t)(s-2t)(s+2t) = 2^{2d-2}\Delta_1^2.$$

Как и выше, из нечётной части получаем (с точностью до знаков)

$$s - 2t = A^2, \qquad s + 2t = B^2 \quad \text{или} \quad s - 2t = -A^2, \qquad s + 2t = B^2,$$

с нечётными A, B. Тогда

$$4t = B^2 - A^2 = (B - A)(B + A) \quad \text{или} \quad 4t = B^2 + A^2.$$

В первом случае $\nu_2(B^2 - A^2) \geq 3$, что противоречит $\nu_2(4t) = 2$; во втором $B^2 + A^2 \equiv 2 \pmod 4$, так что $\nu_2(4t) = 1$, опять противоречие.

Во всех подслучаях приходим к противоречию. Следовательно, подслучай $p = 2$ с $x < d$ невозможен.

Добавление: нечётное простое $p = 3$ при $d < x$. Для полноты разбора рассмотрим оставшийся подслучай $p = 3$ при предположении $p \mid X$ и $p \mid \Delta$. Пишем $X = 3^x X_0$, $\Delta = 3^d \Delta_0$ с $x > d \geq 1$ и $\gcd(X_0, 3) = \gcd(\Delta_0, 3) = 1$. Тогда

$$X^2 - 8\Delta^2 = 3^{2d}\Big(3^{2(x-d)}X_0^2 - 8\,\Delta_0^2\Big), \qquad X^2 - 9\Delta^2 = 3^{2d}\Big(3^{2(x-d)}X_0^2 - 9\,\Delta_0^2\Big).$$

Отсюда

$$\begin{aligned}
&\nu_3\Big(X^2 - 8\Delta^2\Big) = 2d,\\
&\nu_3\Big(X^2 - 9\Delta^2\Big) = \nu_3\Big((X - 3\Delta)(X + 3\Delta)\Big) = (d+1) + (d+1) = 2d + 2.
\end{aligned}$$

так как $x > d$ влечёт $\nu_3(X \pm 3\Delta) = d + 1$. Следовательно,

$$\nu_3\Big(\text{ЛЧ }(\star)\Big) = 4d + 2, \qquad \nu_3\Big(\text{ПЧ }(\star)\Big) = 2x,$$

поскольку $\gcd(a,u) = 1$ и $3 \mid \Delta = u^2 - a^2$ влекут $3 \nmid au$. Значит $4d + 2 = 2x$, то есть $x = 2d + 1$.

Делим ($\star$) на 3^{4d+2} и редуцируем по модулю 3:

$$\frac{X^2 - 8\Delta^2}{3^{2d}} \cdot \frac{X^2 - 9\Delta^2}{3^{2d+2}} = 4a^2u^2 \cdot \frac{X^2}{3^{4d+2}} \\ \implies (-8\Delta_0^2)(-\Delta_0^2) \equiv 4a^2u^2X_0^2 \pmod 3. \tag{32}$$

Так как a, u, X_0, Δ_0 взаимно просты с 3, их квадраты равны $1 \bmod 3$. Следовательно, $8 \cdot 1 \equiv 1 \cdot 1 \pmod 3$, то есть $2 \equiv 1 \pmod 3$, что невозможно. Следовательно, конфигурация $p = 3$ при $d < x$ также невозможна.

Во всех случаях получаем противоречие. Значит никакое простое p не делит одновременно X и Δ, т.е. $\gcd(X, \Delta) = 1$. □

Следствие 2. Если $2 \mid \Delta$, то $2 \nmid X$. Если $3 \mid \Delta$, то $3 \nmid X$.

4 Полный разбор по делимости au на 3 и по чётности

Положим $A_0 := a^2u^2$ (это не $A = 6\Delta$). Далее работаем только с уравнением ($\star$).

Ветка I: $3 \mid au$ — невозможно

При $\gcd(a,u) = 1$ ровно одно из a, u делится на 3, отсюда $\Delta = u^2 - a^2 \equiv \pm 1 \pmod 3$, т.е. $3 \nmid \Delta$.

Подслучай $3 \nmid X$. Тогда $X^2 \equiv 1 \pmod 3$, и $\Delta^2 \equiv 1 \pmod 3$, следовательно

$$X^2 - 8\Delta^2 \equiv 1 - 2 \equiv 2 \ (\mathrm{mod} 3), \qquad X^2 - 9\Delta^2 \equiv 1 - 0 \equiv 1 \ (\mathrm{mod} 3),$$

и $\nu_3(\text{ЛЧ}) = 0$. С другой стороны, $\nu_3(\text{ПЧ}) = \nu_3(4A_0) = 2\nu_3(au) \geq 2$. Противоречие.

Подслучай $3 \mid X$. Пусть $x := \nu_3(X) \geq 1$ и $k := \nu_3(au) \geq 1$ (так как $\gcd(a,u) = 1$ и $3 \mid au$, ровно одно из a, u делится на 3). Тогда

$$\Delta = u^2 - a^2 \equiv \pm 1 \pmod 3 \qquad \text{и} \qquad \nu_3(\Delta) = 0.$$

Вычислим 3-адические оценки двух множителей слева в ($\star$):

Первый множитель. Поскольку Δ — 3-адическая единица и $8 \equiv -1 \pmod 3$,

$$X^2 - 8\Delta^2 \equiv 0 - (-1) \equiv 1 \pmod 3,$$

поэтому
$$\nu_3\Big(X^2-8\Delta^2\Big)=0. \tag{33}$$
<u>Второй множитель.</u> Пишем
$$X^2-9\Delta^2=(X-3\Delta)(X+3\Delta).$$
Так как $\nu_3(X)=x\geq 1$ и $\nu_3(3\Delta)=1$, при $x\geq 2$ имеем
$$X\pm 3\Delta=3\Big(3^{x-1}X_0\pm\Delta\Big)\quad \text{с}\quad 3\nmid\Big(3^{x-1}X_0\pm\Delta\Big),$$
откуда
$$\text{если } x\geq 2: \qquad \nu_3(X\pm 3\Delta)=1 \ \text{ и } \ \nu_3\Big(X^2-9\Delta^2\Big)=2. \tag{34}$$
Если $x=1$, то
$$X\pm 3\Delta=3\Big(X_0\pm\Delta\Big),\qquad X_0,\Delta \text{ — 3-адические единицы.}$$
Не более одного из $X_0\pm\Delta$ кратно 3 (поскольку $(X_0+\Delta)-(X_0-\Delta)=2\Delta$ не кратно 3). Следовательно,
$$\text{если } x=1: \qquad \nu_3\Big(X^2-9\Delta^2\Big)=\nu_3(X-3\Delta)+\nu_3(X+3\Delta)=2+r, \tag{35}$$
для некоторого целого $r\geq 0$.
<u>Сравнение с правой частью.</u> Из ($\star$) и (33) имеем
$$\nu_3(\text{ЛЧ})=\nu_3\Big(X^2-9\Delta^2\Big).$$
Справа
$$\nu_3(\text{ПЧ})=\nu_3\Big(4a^2u^2X^2\Big)=2\,\nu_3(au)+2x=2k+2x.$$

Если $x\geq 2$, то по (34) $\nu_3(\text{ЛЧ})=2$, в то время как $\nu_3(\text{ПЧ})=2k+2x\geq 2\cdot 1+2\cdot 2=6$, что невозможно.

Если $x=1$, то из (35) и равенства оценок следует
$$2+r=\nu_3(\text{ЛЧ})=\nu_3(\text{ПЧ})=2k+2,$$
откуда
$$x=1 \qquad \text{и} \qquad r=2k. \tag{36}$$
Равносильно,
$$\nu_3\Big(X^2-9\Delta^2\Big)=2k+2 \quad\Longleftrightarrow\quad \nu_3\Big(X_0^2-\Delta^2\Big)=2k,$$
т.е. $X_0^2\equiv\Delta^2 \pmod{3^{2k}}$, но $X_0^2\not\equiv\Delta^2 \pmod{3^{2k+1}}$.

Лемма 3 (Граничный случай $x = 1$, $r = 2k$ невозможен). Пусть $\gcd(a, u) = 1$, $\Delta := u^2 - a^2 \neq 0$, и $A_0 = a^2u^2$. Если $\nu_3(au) = k \geq 1$, $\nu_3(X) = 1$ и $\nu_3\Big((X/3)^2 - \Delta^2\Big) = 2k$ (эквивалентно, $x = 1$ и $r = 2k$ в (36)), то ($\star$) не имеет целых решений.

Доказательство. По лемме 2 $\gcd(X, \Delta) = 1$. Редуцирование ($\star$) по модулю X даёт

$$(-8\Delta^2)(-9\Delta^2) \equiv 0 \pmod{X} \implies 72\,\Delta^4 \equiv 0 \pmod{X},$$

следовательно, Δ обратима по модулю X и $X \mid 72$. Так как $\nu_3(X) = 1$, обязательно $X \in \{\pm3, \pm6, \pm12, \pm24\}$.

(i) Оба a, u нечётны. Тогда $u \pm a$ чётны, причём одно из них кратно 4, поэтому $\nu_2(\Delta) = \nu_2(u-a) + \nu_2(u+a) \geq 3$, значит $\Delta^2 \equiv 0 \pmod{16}$. Из $\gcd(X, \Delta) = 1$ следует $2 \nmid X$, т.е. X нечётно. Следовательно, $\nu_2(X^2 - 8\Delta^2) = \nu_2(X^2 - 9\Delta^2) = 0$, и $\nu_2(\text{ЛЧ}) = 0$, тогда как $\nu_2(\text{ПЧ}) = \nu_2(4A_0X^2) = 2$ (так как A_0 и X нечётны) — противоречие.

(ii) a, u разной чётности. Тогда Δ нечётно и $v_2(A_0) \geq 2$. Для чётного X (т.е. $X \in \{\pm6, \pm12, \pm24\}$):

$$\nu_2(X^2 - 8\Delta^2) = \begin{cases} 2, & \nu_2(X) = 1, \\ 3, & \nu_2(X) \geq 2, \end{cases} \qquad \nu_2(X^2 - 9\Delta^2) = 0,$$

значит $\nu_2(\text{ЛЧ}) \in \{2, 3\}$, тогда как $\nu_2(\text{ПЧ}) = 2 + \nu_2(A_0) + 2\nu_2(X) \geq 2 + 2 + 2 = 6$ — опять противоречие. Следовательно, X должен быть нечётным, т.е. $X = \pm3$.

(iii) Оставшаяся возможность $X = \pm3$. Подставляя $X^2 = 9$ в ($\star$) и деля на 9,

$$(1 - \Delta^2)\,(9 - 8\Delta^2) = (2au)^2.$$

Кроме того,

$$\begin{aligned}\gcd(1 - \Delta^2,\, 9 - 8\Delta^2) &= \gcd\Big(1 - \Delta^2,\, (9 - 8\Delta^2) - 8(1 - \Delta^2)\Big) \\ &= \gcd(1 - \Delta^2,\, 1) = 1.\end{aligned}$$

Значит, произведение двух взаимно простых целых — квадрат, следовательно, каждый множитель — квадрат с точностью до знака. При $|\Delta| \geq 2$ оба множителя отрицательны, значит они должны быть отрицательными квадратами. Но $1 - \Delta^2 = -s^2$ влечёт $\Delta^2 - s^2 = 1$, то есть $(\Delta - s)(\Delta + s) = 1$, что имеет единственные целые решения $(\Delta, s) = (\pm1, 0)$. При $\Delta = \pm1$ левая часть равна 0, тогда как $(2au)^2 > 0$, противоречие. $\square$

Следовательно, единственная 3-адическая возможность при $3 \mid X$, а именно (36), невозможна. На этом ветка I ($3 \mid au$) завершена.

Итак, при $3 \mid au$ уравнение ($\star$) не имеет решений.

Ветка II: $3 \nmid au$ — невозможно

Здесь $a^2 \equiv u^2 \equiv 1 \pmod 3$, следовательно $\Delta \equiv 0 \pmod 3$ и, по следствию 2, $3 \nmid X$.

Подветка II.1: оба a, u нечётны. Тогда $u \pm a$ чётны, причём одна из сумм кратна 4; следовательно,

$$\nu_2(\Delta) = \nu_2(u-a) + \nu_2(u+a) \geq 3, \qquad \Delta^2 \equiv 0 \pmod{16}.$$

Из $\gcd(X, \Delta) = 1$ следует $2 \nmid X$, т.е. X нечётен. Сравним $(\star)$ по модулю 16:

$$X^2 - 8\Delta^2 \equiv X^2, \qquad X^2 - 9\Delta^2 \equiv X^2 \pmod{16}.$$

Левая часть $\equiv X^4 \equiv 1 \pmod{16}$, тогда как правая $4A_0X^2 \equiv 4 \pmod{16}$ [8]. Противоречие.

Подветка II.2: a, u разной чётности. Здесь Δ нечётно, а $\nu_2(A_0) \geq 2$.

Если X чётен и $\nu_2(X) = 1$, то $\nu_2(X^2 - 8\Delta^2) = 2$ и $\nu_2(X^2 - 9\Delta^2) = 0$, значит $\nu_2(\text{ЛЧ}) = 2$, в то время как $\nu_2(\text{ПЧ}) \geq 6$. Противоречие.

Если X чётен и $\nu_2(X) \geq 2$, то $\nu_2(X^2 - 8\Delta^2) = 3$ и $\nu_2(X^2 - 9\Delta^2) = 0$, значит $\nu_2(\text{ЛЧ}) = 3$, тогда как $\nu_2(\text{ПЧ}) \geq 8$. Противоречие.

Случай X нечётен. Здесь Δ нечётно и, поскольку мы в ветке II ($3 \nmid au$), имеем $3 \mid \Delta$, $3 \nmid X$, и $\gcd(X, \Delta) = 1$ по лемме 2. Предположим, к противному, что выполняется $(\star)$:

$$(X^2 - 8\Delta^2)(X^2 - 9\Delta^2) = 4\,A_0\,X^2, \qquad A_0 = a^2u^2.$$

Шаг 1: Сведение к $X = \pm 1$. Редуцируя $(\star)$ по модулю X, получаем

$$(-8\Delta^2)(-9\Delta^2) \equiv 0 \pmod{X} \quad \Longrightarrow \quad 72\,\Delta^4 \equiv 0 \pmod{X}.$$

Поскольку $\gcd(X, \Delta) = 1$, отсюда $X \mid 72$. Так как X нечётен и $3 \nmid X$, единственная возможность — $X = \pm 1$.

Шаг 2: Исключение случая $X = \pm 1$. При $X^2 = 1$ уравнение $(\star)$ становится

$$(1 - 8\Delta^2)(1 - 9\Delta^2) = 4A_0 = (2au)^2. \tag{37}$$

Правая часть — положительный полный квадрат. Обозначим $Z := 1 - 8\Delta^2$, $W := 1 - 9\Delta^2$. Заметим, что при $\Delta \neq 0$ оба множителя Z и W — отрицательные целые.

Подшаг 2a: Взаимная простота множителей. По алгоритму Евклида,

$$\begin{aligned}\gcd(Z, W) &= \gcd(1 - 8\Delta^2,\, 1 - 9\Delta^2) \\ &= \gcd(1 - 8\Delta^2,\, -\Delta^2) \\ &= \gcd(1 - 8\Delta^2,\, \Delta^2).\end{aligned}$$

Так как $(1-8\Delta^2)+8\Delta^2=1$, имеем $\gcd(1-8\Delta^2,\,\Delta^2)=\gcd(1,\,\Delta^2)=1$. Значит, Z и W взаимно просты.

Подшаг 2b: Следствие для произведения-квадрата. В $\mathbb{Z}$, если произведение двух взаимно простых чисел — полный квадрат, то каждый множитель — квадрат с точностью до единицы; см., например, [15]. Поскольку $ZW=(2au)^2>0$ и $Z,W<0$, их единицы должны быть обе равны -1; следовательно, существуют целые m,n такие, что

$$Z=-(m^2), \qquad W=-(n^2).$$

Из $W=1-9\Delta^2=-(n^2)$ получаем

$$(3\Delta)^2-n^2=1 \quad\Longleftrightarrow\quad (3\Delta-n)(3\Delta+n)=1.$$

Единственные факторизации 1 в $\mathbb{Z}$: $1\cdot 1$ и $(-1)\cdot(-1)$. Обе приводят к $3\Delta=\pm1$, что невозможно при целочисленном Δ. (Эквивалентно, единственные целые решения $x^2-y^2=1$ — $x=\pm1$, $y=0$.)

Следовательно, (37) не имеет решений, и случай нечётного X невозможен в подветке II.2. Совместив с чётными случаями для X, рассмотренными выше, подветка II.2 закрыта.

Тем самым ветка $3\nmid au$ невозможна.

5 Завершение доказательства

Мы показали, что уравнение $(\star)$ не имеет целых решений X как при $3\mid au$, так и при $3\nmid au$. По теореме 3 любая факторизация 4+4 порождает решение $(\star)$; поскольку $(\star)$ не имеет целых решений, факторизация 4+4 невозможна.

Теорема 6 (Основной результат). Для любых взаимно простых целых $a\neq u>0$ многочлен $P_{a,u}(t)$ не раскладывается в $\mathbb{Z}[t]$ в произведение двух унитарных многочленов степени 4.

6 Исключение факторизации 2+6: прямой критерий и аргумент по дискриминанту

Напомним обозначения

$$P_{a,u}(t)=t^8+At^6+Bt^4+Ct^2+D, \qquad A=6\Delta, \quad \Delta:=u^2-a^2\neq 0,$$

$$B=\Delta^2-2A_0, \quad C=-A_0A, \quad D=A_0^2, \qquad A_0:=a^2u^2.$$

Таким образом, $P_{a,u}$ — чётный, унитарный, примитивный в $\mathbb{Z}[t]$ и допускает представление

$$P_{a,u}(t) = Q(t^2), \qquad Q(x) := x^4 + Ax^3 + Bx^2 + Cx + D \in \mathbb{Z}[x]. \tag{38}$$

Покажем, что факторизация типа 2+6 невозможна.

Шаг 0: Структурное разбиение класса 2+6

Пусть

$$P_{a,u}(t) = Q_2(t) \cdot H_6(t), \qquad \deg Q_2 = 2,\ \deg H_6 = 6.$$

По чётности $P_{a,u}$ и инволюции $t \mapsto -t$ (лемма 1), имеем:

Если Q_2 не чётен, то обязательно $Q_2(-t) \mid H_6(t)$. Сгруппировав сопряжённые множители, получаем чётный квартник и ещё один квартник:

$$P_{a,u}(t) = \underbrace{Q_2(t)\,Q_2(-t)}_{\text{степень 4, чётный}} \cdot \underbrace{\frac{H_6(t)}{Q_2(-t)}}_{\text{степень 4}},$$

т.е. факторизация перегруппируется к случаю 4+4, который уже исключён.

Следовательно, единственный остаток для анализа — чётный квадратный многочлен

$$Q_2(t) = t^2 + q, \qquad q \in \mathbb{Z}.$$

Исключим эту последнюю возможность прямым необходимым и достаточным условием плюс вычислением дискриминанта.

Шаг 1: Критерий для чётного квадратного делителя

Лемма 4 (Критерий чётного квадратного делителя). Для $q \in \mathbb{Z}$ выполняется

$$\boxed{(t^2 + q) \;\mid\; P_{a,u}(t) \iff Q(-q) = 0},$$

где Q задан как в (38). Иными словами,

$$(t^2 + q) \mid P_{a,u}(t) \iff q^4 - Aq^3 + Bq^2 - Cq + D = 0.$$

Доказательство. Разделим $Q(x)$ на $x+q$ в $\mathbb{Z}[x]$: $Q(x) = (x+q)R(x)+S$ с $R \in \mathbb{Z}[x]$ и постоянным остатком $S = Q(-q)$. Подставляя $x = t^2$ и пользуясь (38), получаем

$$P_{a,u}(t) = Q(t^2) = (t^2 + q)\, R(t^2) + S.$$

Значит, $(t^2 + q) \mid P_{a,u}$ тогда и только тогда, когда $S = 0$, т.е. $Q(-q) = 0$. $\square$

Замечание 3. Случай $q = 0$ автоматически невозможен: если $t^2 \mid P_{a,u}(t)$, то свободный член должен обращаться в ноль, но $D = A_0^2 = a^4u^4 > 0$.

Шаг 2: Препятствие по дискриминанту

Перепишем равенство $Q(-q) = 0$ из леммы 4 как квадратное уравнение относительно неизвестного $A_0 = a^2u^2$, в то время как Δ и q рассматриваются как фиксированные целые. Используя $A = 6\Delta,\ B = \Delta^2 - 2A_0,\ C = -A_0A = -6\Delta A_0,\ D = A_0^2$, получаем

$$\begin{aligned} Q(-q) &= q^4 - Aq^3 + Bq^2 - Cq + D \\ &= q^4 - 6\Delta q^3 + (\Delta^2 - 2A_0)q^2 + 6\Delta A_0 q + A_0^2 \\ &= \underbrace{A_0^2}_{\text{квадратное по } A_0} + \underbrace{(6\Delta q - 2q^2)}_{=:b}\, A_0 + \underbrace{(\Delta^2 q^2 - 6\Delta q^3 + q^4)}_{=:c}. \end{aligned}$$

Итак, $Q(-q) = 0$ — квадратное уравнение по A_0:

$$A_0^2 + b\, A_0 + c = 0, \qquad b = 6\Delta q - 2q^2, \quad c = \Delta^2 q^2 - 6\Delta q^3 + q^4.$$

Его дискриминант по A_0 равен

$$\begin{aligned} \mathrm{Disc}_{A_0} &= b^2 - 4c = (6\Delta q - 2q^2)^2 - 4(\Delta^2 q^2 - 6\Delta q^3 + q^4) \\ &= \left(36\Delta^2 q^2 - 24\Delta q^3 + 4q^4\right) - \left(4\Delta^2 q^2 - 24\Delta q^3 + 4q^4\right) \\ &= \boxed{32\,\Delta^2\, q^2}. \end{aligned}$$

Предложение 2 (Несовершенный квадрат «кандидат-корней»). Если $\Delta \neq 0$ и $q \neq 0$, то $\mathrm{Disc}_{A_0} = 32\,\Delta^2\, q^2$ не является полным квадратом в $\mathbb{Z}$.

Доказательство. $\nu_2(\mathrm{Disc}_{A_0}) = \nu_2(32) + 2\nu_2(\Delta q) = 5 + 2\nu_2(\Delta q)$, что нечётно при любом $\Delta q \neq 0$. Полный квадрат в $\mathbb{Z}$ должен иметь чётную 2-адическую оценку. Значит, Disc_{A_0} не квадрат в $\mathbb{Z}$. $\square$

Замечание 4. Это препятствие вида «нечётная 2-адическая оценка дискриминанта исключает квадрат» — стандартный приём в элементарных диофантовых рассуждениях; см. также ориентированные на задачи изложение в [16].

Следствие 3 (Нет целого решения по A_0). При $\Delta \neq 0$ и $q \neq 0$ квадратное уравнение $A_0^2 + bA_0 + c = 0$ не имеет решений $A_0 \in \mathbb{Z}$.

Доказательство. Корни равны $\dfrac{-b \pm \sqrt{\mathrm{Disc}_{A_0}}}{2}$; по предложению 2 дискриминант не является целым квадратом, следовательно, корни иррациональны. □

Шаг 3: Вывод для 2+6

Теорема 7 (Факторизации 2+6 нет). Пусть $a, u \in \mathbb{Z}_{>0}$ взаимно просты и $a \neq u$ (значит, $\Delta \neq 0$). Тогда $P_{a,u}(t)$ не раскладывается в $\mathbb{Z}[t]$ в произведение квадратика и шестистепенного многочлена.

Доказательство. Как отмечено выше, всякая 2+6 с нечётным квадратным множителем перегруппируется в 4+4, что невозможно. Итак, остаётся исключить чётный квадратик t^2+q. По лемме 4, $(t^2+q) \mid P_{a,u}$ тогда и только тогда, когда $Q(-q) = 0$. Если $q = 0$, делимость на t^2 потребовала бы $D = 0$, что ложно. Если $q \neq 0$, то по следствию 3 равенство $Q(-q) = 0$ не имеет решений $A_0 = a^2u^2 \in \mathbb{Z}$. Следовательно, не существует $q \in \mathbb{Z}$, при котором $t^2 + q$ делит $P_{a,u}$. Значит, факторизации 2+6 нет. □

Замечание 5 (Что здесь используется из предыдущих разделов). Доказательство логически независимо от диофантового анализа 4+4, за исключением чисто структурного наблюдения, что нечётный квадратный множитель вынуждает перегруппировку в 4+4 (путём спаривания $Q_2(t)$ с его сопряжением $Q_2(-t)$). «Твёрдый» остаток (чётный квадратик $t^2 + q$) полностью закрывается леммой 4 и вычислением дискриминанта.

7 Исключение прочих факторизаций

После теоремы 7, исключившей все факторизации типа 2+6, оставшиеся шаблоны степени 8 исключаются тривиальной перегруппировкой.

Предложение 3. Пусть $P_{a,u}(t) \in \mathbb{Z}[t]$ как выше. Если существует любая из факторизаций, то $P_{a,u}$ допускает факторизацию типа 2+6:

(a) 2+2+4: $P_{a,u} = Q_1\, Q_2\, H_4$ при $\deg Q_i = 2$, $\deg H_4 = 4$;
(b) 2+2+2+2: $P_{a,u} = Q_1\, Q_2\, Q_3\, Q_4$ при $\deg Q_i = 2$;
(c) 3+3+2: $P_{a,u} = F_3\, G_3\, Q_2$ при $\deg F_3 = \deg G_3 = 3$, $\deg Q_2 = 2$.

Доказательство. (a) Группируем как $P_{a,u} = \underbrace{Q_1}_{\text{deg=2}} \cdot \underbrace{(Q_2H_4)}_{\text{deg=6}}$.

(b) Группируем как $P_{a,u} = \underbrace{Q_1}_{\text{deg=2}} \cdot \underbrace{(Q_2Q_3Q_4)}_{\text{deg=6}}$.

(c) Группируем как $P_{a,u} = \underbrace{Q_2}_{\text{deg=2}} \cdot \underbrace{(F_3G_3)}_{\text{deg=6}}$. □

Следствие 4. Ни один из шаблонов 2+2+4, 2+2+2+2 или 3+3+2 не реализуется для $P_{a,u}(t)$.

Доказательство. По предложению 3 каждый из них вёл бы к факторизации 2+6, что невозможно по теореме 7. □

8 Полная неприводимость

Теорема 8 (Неприводимость). Для любых взаимно простых целых $a \neq u > 0$ многочлен $P_{a,u}(t)$ неприводим в $\mathbb{Z}[t]$.

Доказательство. Все разбиения степени 8 исключаются следующим образом.

(i) Случай 4+4 невозможен по теореме 3 и анализу уравнения $(\star)$ (от леммы 1 до следствия 2 и последующего 2/3-адического разветвления).

(ii) Случай 2+6 исключён в разделе 6.

(iii) После (ii) любые оставшиеся шаблоны 2+2+4, 2+2+2+2, 3+3+2 перегруппируются в 2+6 по предложению 3, следовательно, невозможны по (ii).

Значит, нет нетривиальных факторизаций в $\mathbb{Z}[t]$. Так как $P_{a,u}(t)$ унитарен и примитивен, неприводимость над $\mathbb{Z}$ следует. □

Заключение

Мы показали, что для любых взаимно простых целых $a \neq u > 0$ чётный кубоидный многочлен $P_{a,u}(t)$ не допускает факторизации типа 4+4 в $\mathbb{Z}[t]$. Ключевой шаг — сведение потенциальной факторизации к диофантовому условию $(X^2 - 8\Delta^2)(X^2 - 9\Delta^2) = 4a^2u^2X^2$, из которого, с помощью 2- и 3-адических оценок и леммы $\gcd(X, \Delta) = 1$, следует отсутствие целых решений. Затем мы закрыли подлинный случай 2+6 точным критерием делимости в сочетании с препятствием по дискриминанту. Наконец, после исключения 2+6 любые остающиеся шаблоны (2+2+4, 2+2+2+2, 3+3+2) тривиально перегруппируются в 2+6 и потому невозможны. В совокупности, $P_{a,u}(t)$ не допускает нетривиальной факторизации в $\mathbb{Z}[t]$, что устанавливает полную неприводимость [1, 2, 3].

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] R. K. Guy, Unsolved Problems in Number Theory, 3rd ed., Springer, 2004.

[4] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 6th ed., Oxford University Press, 2008.

[5] D. S. Dummit, R. M. Foote, Abstract Algebra, 3rd ed., Wiley, 2004.

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

[7] J. Neukirch, Algebraic Number Theory, Springer, 1999.

[8] J. P. Serre, A Course in Arithmetic, Springer GTM 7, 1973.

[9] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer GTM 84, 1990.

[10] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd ed., Springer GTM 58, 1984.

[11] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd ed., Springer, 2004.

[12] D. A. Marcus, Number Fields, Springer, Graduate Texts in Mathematics, vol. 197, 1977.

[13] K. Conrad, Gauss's Lemma and Unique Factorization in $\mathbb{Z}$ and $F[T]$, Lecture notes, Univ. of Connecticut, c. 2010–2014.

[14] K. Conrad, Eisenstein's Criterion, Lecture notes, c. 2010–2014.

[15] I. Stewart, D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd ed., A K Peters, 2002.

[16] M. R. Murty, J. Esmonde, Problems in Algebraic Number Theory, 2nd ed., Springer GTM 190, 2005.

[17] J. H. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Springer GTM 106, 2009.

[18] J. W. S. Cassels, Lectures on Elliptic Curves, London Math. Soc. Student Texts 24, CUP, 1991.

[19] J. E. Cremona, Elliptic Curves over $\mathbb{Q}$: A Database, online tables for curves over $\mathbb{Q}$ (isogeny class 48a), updated editions.

[20] The LMFDB Collaboration, Elliptic curve 48a3 over $\mathbb{Q}$ (minimal model $y^2 = x^3 + x^2 - 24x + 36$, rank 0, torsion $\mathbb{Z}/2 \oplus \mathbb{Z}/4$), The L-functions and Modular Forms Database.