On the Irreducibility of the Cuboid Polynomial $P_{a,u}(t)$

Valery Asiryan

asiryanvalery@gmail.com

October 9, 2025

Abstract

In this paper we consider the even monic degree-8 cuboid polynomial $P_{a,u}(t)$ with coprime integers $a \neq u > 0$. We prove irreducibility over $\mathbb{Z}$ by excluding all degree-8 splittings. First, any putative 4+4 factorization is shown to force a specific Diophantine constraint which has no integer solutions by a short 2- and 3-adic analysis. Second, we exclude every 2+6 factorization via an exact divisor criterion and a discriminant obstruction. Finally, after ruling out 2+6, the patterns 2+2+4, 2+2+2+2, and 3+3+2 regroup trivially to 2+6 and are therefore impossible. Consequently, $P_{a,u}(t)$ admits no nontrivial factorization in $\mathbb{Z}[t]$.

Keywords Irreducibility over $\mathbb{Z}$; even monic polynomials; cuboid (Euler) polynomial $P_{a,u}(t)$; factorization types 4+4, 2+6, 2+2+4, 2+2+2+2, 3+3+2; Diophantine constraints; p-adic valuations (2-adic, 3-adic); discriminant obstruction; Gauss's lemma; parity/involution regrouping; elliptic curves.

MSC 2020 **Primary**: 12E05 (Polynomials: irreducibility). **Secondary**: 11D72 (Equations in many variables; Diophantine equations), 11S05 (Local and p-adic fields), 11Y05 (Factorization; primality).

1 Problem Statement and Notation

Let $a, u \in \mathbb{Z}_{>0}$ be coprime and $a \neq u$. We consider the even monic polynomial [1, 2, 3]

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

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

We work in $\mathbb{Z}[t]$. The polynomial $P_{a,u}$ is even, monic, and primitive: $\mathrm{cont}(P_{a,u}) = 1$ [5, 13, 6]. Standard irreducibility criteria such as Eisenstein's (including the shifted variant $t \mapsto t + c$) generally do not apply uniformly to $P_{a,u}$; cf. [14].

Theorem 1 (Goal)**.** *For any coprime $a, u \in \mathbb{Z}_{>0}$ with $a \neq u$, the polynomial $P_{a,u}(t)$ does* not *factor in $\mathbb{Z}[t]$ as a product of two monic polynomials of degree 4 (the case 4+4).*

2 Normal Form of a 4+4 Factorization and the Necessary Condition $(\star)$

Lemma 1 (Gauss + involution)**.** *If $P_{a,u} = FG$ with monic $F, G \in \mathbb{Z}[t]$ and $\deg F = \deg G = 4$, then, after swapping the factors if necessary, one of the following holds:*

(E) both factors are even: *$F = t^4+pt^2+q$, $G = t^4+rt^2+s$ ($p, q, r, s \in \mathbb{Z}$);*

(C) a conjugate pair: *$G(t) = F(-t)$, where $F = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$.*

Idea. Primitivity and Gauss's lemma yield primitivity and monicity of the factors [5, 13, 6]. The involution $\tau : t \mapsto -t$ fixes $P_{a,u}$; either both factors are invariant (even), or τ swaps the factors (a conjugate pair). □

Detailed derivation in case (E)

Let $F = t^4 + pt^2 + q$, $G = t^4 + rt^2 + s$. From $FG = P_{a,u}$ we obtain the system

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

From (1) we have $r = A - p$. Introduce

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

Then (2) and (4) rewrite as

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

Thus q, s are integer roots of the quadratic equation $X^2 - MX + D = 0$. Denote (the discriminant of this quadratic)

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

Then

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

Substitute (6) into (3). The left-hand side of (3) equals

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

Hence from (3) we get

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

Set

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

What follows is a direct computation.

Computing M.

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

Computing $2C - AM$. Since $C = -a^2u^2A = -6\Delta\, a^2u^2$, we have

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

Therefore,

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

Thus (7) becomes

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

Divide by -2 to obtain the fundamental relation

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

Computing T^2. By definition,

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

Deriving the starred equation. Square (8) and substitute the expression for T^2:

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

Since $X^2 \neq 8\Delta^2$ (see below), we can cancel $(X^2 - 8\Delta^2)$ and obtain

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

Moving everything to the left and grouping, we arrive at the Diophantine equation

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

(see the remark below on the legitimacy of cancellation).

Remark 1 (Legitimacy of cancellation and a consequence). If $X^2 = 8\Delta^2$, then comparing the 2-adic valuations yields $2\,\nu_2(X) = 3 + 2\,\nu_2(\Delta)$, which is impossible (the left-hand side is even, the right-hand side is odd). Hence for $\Delta \neq 0$ the equality $X^2 = 8\Delta^2$ has no integer solutions, and cancellation by the factor $X^2 - 8\Delta^2$ is valid [8, 10, 9]. Consequently, (1)–(4) *imply* $(\star)$. The converse, in general, is not claimed: in addition one needs that $T^2 = M^2 - 4D$ be a perfect square and $q = \frac{M \pm T}{2} \in \mathbb{Z}$.

Case (C): conjugate pair

Assume

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

so that $F(t)F(-t) = P_{a,u}(t)$. Equating coefficients gives the system

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

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

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

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

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

Step 1: the sign of δ is forced. From (12) we have $\delta = \pm A_0$. If $\delta = -A_0$, then (11) becomes

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

Using (9), $2\beta = \alpha^2 + 6\Delta$, we get $\gamma^2 = -A_0\alpha^2$. Hence $\gamma = \alpha = 0$. Then (9) yields $\beta = 3\Delta$, and (10) gives $9\Delta^2 + 2(-A_0) = \Delta^2 - 2A_0$, i.e. $8\Delta^2 = 0$, which contradicts $\Delta \neq 0$. Therefore necessarily

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

Step 2: a convenient reparametrization. Put $m := au$, so $A_0 = m^2$. With $\delta = A_0 = m^2$, (11) implies

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

hence $m \mid \gamma$. Write $\gamma = m\kappa$ with $\kappa \in \mathbb{Z}$. Using (9) (i.e. $2\beta = \alpha^2 + 6\Delta$) we obtain

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

Introduce

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

Then from (13)

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

In terms of s, t one readily checks that

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

Step 3: eliminating α, β, γ from (10). Substitute (14) and $\delta = m^2$ into (10):

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

Multiply by $576 = \operatorname{lcm}(64, 2, 144)$ and use ($\dagger$), i.e. $\Delta^2 = (st)^2/144$, to clear denominators:

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

Rearranging,

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

Set $U := s^2$, $V := t^2$ (nonnegative integers). Then (15) becomes

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

Completing the square gives an identity

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

Therefore both terms vanish:

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

The first equality $UV = 0$ means $s\,t = 0$, hence by ($\dagger$) we get $\Delta = 0$, which contradicts our standing assumption $\Delta \neq 0$.

Conclusion. Thus the system (9)–(12) has no integer solutions when $\Delta \neq 0$. Equivalently, the factorization $P_{a,u}(t) = F(t)F(-t)$ with a monic quartic $F \in \mathbb{Z}[t]$ is impossible.

Theorem 2 (Case (C) is impossible)**.** *For coprime integers $a \neq u > 0$ (so $\Delta = u^2 - a^2 \neq 0$), there are no integers $\alpha, \beta, \gamma, \delta$ with $\delta^2 = A_0^2$ such that*

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

In particular, no 4+4 factorization of type (C) *(conjugate pair) exists.*

Remark 2. This argument is independent of the analysis in the even–even case *(E)* and does not use any auxiliary factorization of the elimination polynomial. It relies only on (9)–(12), the sign determination $\delta = A_0$, the reparametrization (s, t) given by $\kappa^2 = \alpha^2 + 12\Delta$, and the elementary identity

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

which forces $st = 0$, hence $\Delta = 0$, a contradiction.

Theorem 3 (Necessary condition for 4+4)**.** *Let $\Delta = u^2 - a^2 \neq 0$. If $P_{a,u}(t)$ factors in $\mathbb{Z}[t]$ as a product of two monic quartics, then there exists $X \in \mathbb{Z}$ satisfying $(\star)$.*

Proof. By Lemma 1 any 4+4 factorization is of type (E) or (C). By Theorem 2 case (C) is excluded; hence we are in (E): $F = t^4 + pt^2 + q$, $G = t^4 + rt^2 + s$. As shown in the derivation of $(\star)$, setting $X := p - 3\Delta$ and eliminating q, s via (1)–(4) yields precisely $(\star)$. □

3 Key Lemma: $\gcd(X, \Delta) = 1$

Lemma 2. *If $X \in \mathbb{Z}$ satisfies $(\star)$, then* $\gcd(X, \Delta) = 1$.

Proof. Suppose, to the contrary, that a prime p divides both X and Δ [7, 9, 10, 11, 12]. Write

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

Case $p \geq 3$. As usual:

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

If $d > x$, both brackets are $\not\equiv 0 \pmod{p}$, and $\nu_p(\text{LHS}) = 4x$. The right-hand side has $\nu_p(\text{RHS}) = 2x + \nu_p(4a^2u^2) = 2x$ (since $\gcd(a, u) = 1 \Rightarrow p \nmid$

au). Contradiction. If $d = x$, the two brackets cannot both be divisible by p (otherwise $\Delta_0^2 \equiv 0$), hence $\nu_p(\text{LHS}) \geq 4x + 1 > 2x = \nu_p(\text{RHS})$. Contradiction [9, 11].

Addendum: odd prime p, the hypothetical subcase $d < x$. For completeness, suppose p is an odd prime with $p \mid \Delta$ and $x := \nu_p(X) > d := \nu_p(\Delta) \geq 1$. Then one necessarily has

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

so that

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

On the right-hand side of $(\star)$ we have $\nu_p(4a^2u^2X^2) = 2x$ because $p \mid (u^2 - a^2)$ implies $p \nmid a$ and $p \nmid u$. Hence $4d = 2x$ and therefore

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

Cancelling p^{4d} in $(\star)$ yields

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

and with (16) this becomes

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

Reducing modulo p (since $d \geq 1$) gives

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

i.e.

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

Thus 18 must be a quadratic residue modulo p. Since $\left(\frac{3^2}{p}\right) = 1$, this is equivalent to

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

and by the classical description of $(2/p)$ via quadratic reciprocity (see, e.g., [4]) we obtain

$$p \equiv 1 \text{ or } 7 \pmod{8}. \tag{18}$$

Write $X_0 = h\,\xi$ and $\Delta_0 = h\,\Delta_1$ with $h := \gcd(X_0, \Delta_0)$ and $\gcd(\xi, \Delta_1) = 1$. Set

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

From the computation of $\gcd(A, B)$ in the main text we have $\gcd(A', B') = 1$ and

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

Since $A'B' \in \mathbb{Z}$, it follows that $\frac{2au\,\xi}{h} \in \mathbb{Z}$. Hence there exist $\varepsilon \in \{\pm 1\}$ and coprime integers m, n such that

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

Claim (sign determination). $\varepsilon = +1$.
Proof. Reduce (19) modulo 3. Since $p \geq 5$, $p^{2d} \equiv 1 \pmod 3$, whence

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

If $\varepsilon = -1$, then $A' = -m^2$ and $B' = -n^2$, so $A', B' \in \{0, 2\}$ (mod3). From $B' \equiv \xi^2$ it follows that $\xi \equiv 0 \pmod 3$, and then $A' \equiv -2\Delta_1^2 \equiv \Delta_1^2 \pmod 3$ forces $\Delta_1 \equiv 0 \pmod 3$, which in turn implies $3 \mid m$ and $3 \mid n$ — a contradiction to $\gcd(m, n) = 1$. □

With $\varepsilon = +1$, reducing $B' = n^2$ modulo p gives $n^2 \equiv -9\Delta_1^2 \pmod p$, hence $(-1/p) = 1$ and therefore $p \equiv 1 \pmod 4$. Together with (18) (i.e. $(2/p) = 1$) this forces the sharper congruence

$$p \equiv 1 \pmod 8. \tag{20}$$

In particular, the branch $p \equiv 7 \pmod 8$ is excluded.

Residual subcase and current status. In the remaining configuration $p \equiv 1 \pmod 8$ one arrives at the system

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

with $\gcd(m, n) = 1$ and $\gcd(\xi, \Delta_1) = 1$. Using the standard factorizations $(m \mp n)$ and the corresponding parameterizations in the odd/even parity of Δ_1, one checks that both identities for $p^{2d}\xi^2$ reduce to the same expression; i.e., by the present (elementary) methods this residual case does not yield a contradiction.

Retain the residual odd-prime setting $p \geq 5$, $p \mid \Delta$, $d := \nu_p(\Delta) \geq 1$, $x := \nu_p(X) > d$, for which $x = 2d$. As explained earlier, after clearing common factors the system

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

yields the genus–1 curve

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

and the pencil of quadrics shows that $\mathrm{Jac}(\mathcal{C})$ is the elliptic curve

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

Moreover, the extra constraint coming from the residual system is precisely that the x–coordinate on E_0 be a rational square: writing $u := n/\Delta_1$, the two congruences "u^2+1 and u^2+9 are squares" translate to

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

Put differently, we need to decide whether $E_0(\mathbb{Q})$ contains a point with x a nonzero square. We now compute $E_0(\mathbb{Q})$ unconditionally.

Proposition 1 (Torsion subgroup)**.** *For the elliptic curve*

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

the torsion subgroup is

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

In particular, $2(3,12) = (0,0)$ *and* $2(-3,6) = (-1,0)$*, so* $(3,12)$ *and* $(-3,6)$ *are points of order* 4*.*

Proof. By the Nagell–Lutz theorem [17, 18], all torsion points on a minimal integral model have integer coordinates. The three nontrivial 2-torsion points are the roots of the cubic: $x \in \{0,-1,-9\}$, i.e. $(0,0),(-1,0),(-9,0)$.

A direct substitution shows that $(3,\pm 12)$ and $(-3,\pm 6)$ lie on E_0 because $12^2 = 3\cdot 4\cdot 12 = 144$ and $6^2 = (-3)\cdot(-2)\cdot 6 = 36$. Using the duplication formula (or standard software/hand computation) one verifies that $2(3,12) = (0,0)$ and $2(-3,6) = (-1,0)$, hence these points have order 4. No further integral torsion points exist, so by Mazur's theorem the torsion subgroup is exactly $\{O,(0,0),(-1,0),(-9,0),(3,\pm 12),(-3,\pm 6)\} \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$. □

Theorem 4 (Rank via a minimal model)**.** *For*

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

we have

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

Proof. First remove the quadratic term in the Weierstrass equation: with the change of variables $x = X - \frac{10}{3}$ we obtain

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

Clearing denominators via $X = \frac{x'}{9}$, $y = \frac{y'}{27}$ gives the short integral model

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

This curve is $\mathbb{Q}$-isomorphic to the minimal model

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

which has conductor $N = 48$ and belongs to the isogeny class 48a. From Cremona's tables and the LMFDB we have

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

Hence the same holds for E_0. See [19, 20]. □

Corollary 1 (No rational points with square x)**.** *The only rational point of E_0 with x a rational square is $(x, y) = (0, 0)$.*

Proof. By Proposition 1 and Theorem 4, $E_0(\mathbb{Q})$ is exactly the listed torsion set. Inspecting their x–coordinates $\{0, -1, -9, \pm 3\}$ shows that the only square among them is $x = 0$. □

Theorem 5 (Unconditional closure of the residual odd–prime branch)**.** *In the residual configuration ($p \geq 5$, $p \mid \Delta$, $x = 2d > d \geq 1$) the system above has no nontrivial integer solutions (i.e. no solutions with $n \neq 0$). Equivalently, the subcase $d < x$ cannot occur.*

Proof. A nontrivial solution forces a rational point on E_0 with $x = (n/\Delta_1)^2$ a nonzero square. By Corollary 1 this is impossible. □

Hence no odd prime p can divide both X and Δ.

Case $p = 2$. Write $X = 2^x X_0$, $\Delta = 2^d \Delta_0$, $x, d \geq 1$, X_0, Δ_0 odd.

Consider three mutually exclusive options:

(B) $2x > 2d$.

If $x \geq d+2$ (i.e. $2x \geq 2d+4$), then $\nu_2(X^2 - 8\Delta^2) = 2d+3$, $\nu_2(X^2 - 9\Delta^2) = 2d$, hence $\nu_2(\text{LHS}) = 4d + 3$ (odd), whereas $\nu_2(\text{RHS}) = 2 + \nu_2(a^2u^2) + 2x$ is even. Contradiction.

If $x = d + 1$ (i.e. $2x = 2d + 2$), then

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

where the bracket is odd; thus $\nu_2(X^2 - 8\Delta^2) = 2d + 2$. Moreover,

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

and $4X_0^2 - 9\Delta_0^2 \equiv 4 - 9 \equiv 3 \pmod 8$ is odd, hence $\nu_2(X^2 - 9\Delta^2) = 2d$. Therefore $\nu_2(\text{LHS}) = (2d + 2) + 2d = 4d + 2$.

Since $\nu_2(\Delta) \geq 1$, the numbers a and u have the same parity; with $\gcd(a, u) = 1$ this forces both to be odd. Then $\nu_2(a^2u^2) = 0$ and

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

Comparing, for $d \geq 2$ we have $4d + 2 \neq 2d + 4$ (contradiction), while for $d = 1$ the valuations coincide and we must compare odd parts. Modulo 8:

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

whereas the odd part of the right-hand side is $X_0^2 \equiv 1 \pmod 8$. Contradiction. Hence the subcase $x = d + 1$ is impossible.

(C) $2x = 2d$. Then $\nu_2(X^2 - 8\Delta^2) = 2d$ and $\nu_2(X^2 - 9\Delta^2) \geq 2d + 3$ (since $X_0^2 \equiv 1 \pmod 8$). Thus $\nu_2(\text{LHS}) \geq 4d + 3$ (odd), whereas $\nu_2(\text{RHS}) = 2 + \nu_2(a^2u^2) + 2x$ is even. Contradiction.

(A) $p = 2$ *and* $x < d$.

Assume $2 \mid \gcd(X, \Delta)$. Write $X = 2^x X_0$ and $\Delta = 2^d \Delta_0$ with $x \geq 1$, $d > x$, and X_0, Δ_0 odd. Since $2 \mid \Delta$ and $\gcd(a, u) = 1$, both a and u are odd.

Step 1: Valuation at 2. Comparing 2-adic valuations in $(\star)$ gives

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

Hence $4x = 2x + 2$ and therefore

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

Step 2: Normalization and the product identity. Set

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

Dividing $(\star)$ by 16 (using (22)) yields

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

As X_0 is odd,

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

Let $h := \gcd(X_0, \Delta_0)$; then $g = h^2$ is an odd perfect square.

Step 3: Sign determination by residue modulo 8. Since $8M \equiv 0 \pmod 8$, we have

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

Write, for some $\varepsilon \in \{\pm 1\}$ and coprime integers $m, n \geq 0$,

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

(this follows from (23) and $\gcd(A/g, B/g) = 1$). Reducing the first identity in (24) modulo 8 and using $g \equiv 1 \pmod 8$ gives

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

Hence

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

Moreover,

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

since $M \equiv 4 \pmod 8$ for $d = 2$ and $M \equiv 0 \pmod 8$ for $d \geq 3$. But by (24), (25) we must have $B \equiv gn^2 \equiv 1 \pmod 8$. Therefore the case $d = 2$ is impossible, and we are left with

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

In particular, m, n are odd (because $A \equiv B \equiv 1 \pmod 8$ and $g \equiv 1 \pmod 8$), and $\gcd(m, n) = 1$.

Step 4: Two Diophantine consequences. From $A - B = M$ and (26) we obtain

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

Write $\Delta_0 = h\,\Delta_1$ (recall $g = h^2$). Then (27) becomes

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

Using $9A - 8B = X_0^2$ we also get

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

for some odd integer k.

Step 5: Final contradiction via the binary form $x^2 + 2y^2$. From (29) we have

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

Let $D := \gcd(k, n)$. From (30) one checks that D is odd and $D \mid 3m$; hence $D = 3^j$ with $j \in \{0, 1\}$ (otherwise $\gcd(m, n) \neq 1$).

Case $j = 0$ (primitive). Then there exist coprime integers s, t with

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

and s, t are odd because n is odd; see, e.g., [9, Ch. 5, §2]. Using (28) we compute

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

Thus

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

Here $s \pm t$ are even, while $s \pm 2t$ are odd; also $\gcd(s - 2t, s + 2t) = \gcd(s - 2t, 4t) = 1$. Hence the odd part of (31) equals $\pm 9\Delta_1^2$ and, by coprimeness, up to signs

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

for some odd A, B. In the first subcase,

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

Both factors are even, and exactly one of them is divisible by 4; thus $\nu_2(9B^2 - A^2) \geq 3$, which contradicts $\nu_2(4t) = 2$. In the second subcase,

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

so $\nu_2(4t) = 1$, again a contradiction.

Case $j = 1$ (non-primitive). Then there exist coprime odd s, t such that

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

and

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

As above, from the odd part we get (up to signs)

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

with odd A, B. Hence

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

In the first case $\nu_2(B^2 - A^2) \geq 3$, contradicting $\nu_2(4t) = 2$; in the second case $B^2 + A^2 \equiv 2 \pmod 4$, so $\nu_2(4t) = 1$, again a contradiction.

In all subcases we reach a contradiction. Therefore the subcase $p = 2$ with $x < d$ is impossible.

Addendum: the odd prime $p = 3$ with $d < x$. For completeness we treat the remaining subcase $p = 3$ under the standing assumption that $p \mid X$ and $p \mid \Delta$. Write $X = 3^x X_0$, $\Delta = 3^d \Delta_0$ with $x > d \geq 1$ and $\gcd(X_0, 3) = \gcd(\Delta_0, 3) = 1$. Then

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

Hence

$$\nu_3\Big(X^2 - 8\Delta^2\Big) = 2d,$$
$$\nu_3\Big(X^2 - 9\Delta^2\Big) = \nu_3\Big((X - 3\Delta)(X + 3\Delta)\Big) = (d + 1) + (d + 1) = 2d + 2.$$

since $x > d$ implies $\nu_3(X \pm 3\Delta) = d + 1$. Therefore

$$\nu_3\Big(\text{LHS of } (\star)\Big) = 4d + 2, \qquad \nu_3\Big(\text{RHS of } (\star)\Big) = 2x,$$

because $\gcd(a, u) = 1$ and $3 \mid \Delta = u^2 - a^2$ force $3 \nmid au$. Thus $4d + 2 = 2x$, i.e. $x = 2d + 1$.

Divide $(\star)$ by 3^{4d+2} and reduce modulo 3:

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

As a, u, X_0, Δ_0 are all coprime to 3, their squares are 1 mod 3. Hence $8 \cdot 1 \equiv 1 \cdot 1 \pmod 3$, i.e. $2 \equiv 1 \pmod 3$, a contradiction. Therefore the configuration $p = 3$ with $d < x$ is impossible as well.

In all cases we reach a contradiction. Hence no prime p can divide both X and Δ, i.e. $\gcd(X, \Delta) = 1$. □

Corollary 2. *If* $2 \mid \Delta$, *then* $2 \nmid X$. *If* $3 \mid \Delta$, *then* $3 \nmid X$.

4 Complete Case Split by Divisibility of au by 3 and by Parity

Set $A_0 := a^2u^2$ (this is *not* $A = 6\Delta$). We now work solely with equation $(\star)$.

Branch I: $3 \mid au$ — impossible

With $\gcd(a,u)=1$, exactly one of a,u is divisible by 3, hence $\Delta = u^2 - a^2 \equiv \pm 1 \pmod 3$, i.e. $3 \nmid \Delta$.

Subcase $3 \nmid X$. Then $X^2 \equiv 1 \pmod 3$, and $\Delta^2 \equiv 1 \pmod 3$, therefore

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

and $\nu_3(\mathrm{LHS}) = 0$. On the other hand, $\nu_3(\mathrm{RHS}) = \nu_3(4A_0) = 2\nu_3(au) \geq 2$. Contradiction.

Subcase $3 \mid X$. Let $x := \nu_3(X) \geq 1$ and set $k := \nu_3(au) \geq 1$ (since $\gcd(a,u)=1$ and $3 \mid au$, exactly one of a,u is divisible by 3). Then

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

We compute the 3-adic valuations of the two factors on the left of $(\star)$:
First factor. Because Δ is a 3-adic unit and $8 \equiv -1 \pmod 3$,

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

so

$$\nu_3\Big(X^2 - 8\Delta^2\Big) = 0. \tag{33}$$

Second factor. Write

$$X^2 - 9\Delta^2 = (X - 3\Delta)(X + 3\Delta).$$

Since $\nu_3(X) = x \geq 1$ and $\nu_3(3\Delta) = 1$, for $x \geq 2$ we have

$$X \pm 3\Delta = 3\Big(3^{x-1}X_0 \pm \Delta\Big) \quad \text{with} \quad 3 \nmid \Big(3^{x-1}X_0 \pm \Delta\Big),$$

hence

$$\text{if } x \geq 2: \qquad \nu_3(X \pm 3\Delta) = 1 \ \text{ and } \ \nu_3\Big(X^2 - 9\Delta^2\Big) = 2. \tag{34}$$

If $x = 1$, then

$$X \pm 3\Delta = 3\Big(X_0 \pm \Delta\Big), \qquad X_0, \Delta \text{ are 3-adic units.}$$

At most one of $X_0 \pm \Delta$ is divisible by 3 (since $(X_0 + \Delta) - (X_0 - \Delta) = 2\Delta$ is not divisible by 3). Therefore

$$\text{if } x = 1: \qquad \nu_3\Big(X^2 - 9\Delta^2\Big) = \nu_3(X - 3\Delta) + \nu_3(X + 3\Delta) = 2 + r, \tag{35}$$

for some integer $r \geq 0$.

Comparison with the right-hand side. From $(\star)$ and (33) we get

$$\nu_3(\text{LHS}) = \nu_3\Big(X^2 - 9\Delta^2\Big).$$

On the right,

$$\nu_3(\text{RHS}) = \nu_3\Big(4a^2u^2X^2\Big) = 2\,\nu_3(au) + 2x = 2k + 2x.$$

If $x \geq 2$, then by (34) we have $\nu_3(\text{LHS}) = 2$, whereas $\nu_3(\text{RHS}) = 2k + 2x \geq 2 \cdot 1 + 2 \cdot 2 = 6$, which is impossible.

If $x = 1$, then by (35) and equality of valuations we must have

$$2 + r = \nu_3(\text{LHS}) = \nu_3(\text{RHS}) = 2k + 2,$$

hence

$$x = 1 \qquad \text{and} \qquad r = 2k. \tag{36}$$

Equivalently,

$$\nu_3\Big(X^2 - 9\Delta^2\Big) = 2k + 2 \quad \Longleftrightarrow \quad \nu_3\Big(X_0^2 - \Delta^2\Big) = 2k,$$

i.e. $X_0^2 \equiv \Delta^2 \pmod{3^{\,2k}}$ but $X_0^2 \not\equiv \Delta^2 \pmod{3^{\,2k+1}}$.

Lemma 3 (The edge case $x = 1$, $r = 2k$ is impossible)**.** *Assume* $\gcd(a, u) = 1$, $\Delta := u^2 - a^2 \neq 0$, *and* $A_0 = a^2u^2$. *If* $\nu_3(au) = k \geq 1$, $\nu_3(X) = 1$, *and* $\nu_3\Big((X/3)^2 - \Delta^2\Big) = 2k$ *(equivalently,* $x = 1$ *and* $r = 2k$ *in* (36)*), then* $(\star)$ *has no integer solutions.*

Proof. By Lemma 2 we have $\gcd(X, \Delta) = 1$. Reducing $(\star)$ modulo X gives

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

hence Δ is invertible modulo X and $X \mid 72$. Since $\nu_3(X) = 1$, necessarily $X \in \{\pm 3, \pm 6, \pm 12, \pm 24\}$.

(i) Both a, u odd. Then $u \pm a$ are even with one of them divisible by 4, so $\nu_2(\Delta) = \nu_2(u - a) + \nu_2(u + a) \geq 3$, hence $\Delta^2 \equiv 0 \pmod{16}$. From $\gcd(X, \Delta) = 1$ we get $2 \nmid X$, i.e. X is odd. Therefore $\nu_2(X^2 - 8\Delta^2) = \nu_2(X^2 - 9\Delta^2) = 0$, so $\nu_2(\text{LHS}) = 0$, whereas $\nu_2(\text{RHS}) = \nu_2(4A_0X^2) = 2$ (since A_0 and X are odd) — a contradiction.

(ii) a, u of opposite parity. Then Δ is odd and $v_2(A_0) \geq 2$. For even X (i.e. $X \in \{\pm 6, \pm 12, \pm 24\}$):

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

thus $\nu_2(\text{LHS}) \in \{2,3\}$, while $\nu_2(\text{RHS}) = 2+\nu_2(A_0)+2\nu_2(X) \geq 2+2+2 = 6$ — again a contradiction. Hence X must be odd, i.e. $X = \pm 3$.

(iii) The remaining possibility $X = \pm 3$. Substituting $X^2 = 9$ into $(\star)$ and dividing by 9,

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

Moreover,

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

Thus two coprime integers multiply to a square, so each factor is a square up to sign. For $|\Delta| \geq 2$ both factors are negative, hence they must be negative squares. But $1-\Delta^2 = -s^2$ implies $\Delta^2 - s^2 = 1$, i.e. $(\Delta - s)(\Delta + s) = 1$, whose only integer solutions are $(\Delta, s) = (\pm 1, 0)$. For $\Delta = \pm 1$ the left-hand side above is 0, whereas $(2au)^2 > 0$, a contradiction. □

Consequently, the only 3-adic possibility under $3 \mid X$, namely (36), cannot occur. This completes Branch I ($3 \mid au$).

Therefore, when $3 \mid au$, equation $(\star)$ has no solutions.

Branch II: $3 \nmid au$ — impossible

Here $a^2 \equiv u^2 \equiv 1 \pmod 3$, hence $\Delta \equiv 0 \pmod 3$ and, by Corollary 2, $3 \nmid X$.

Sub-branch II.1: both a, u odd. Then $u \pm a$ are even, with one of the sums divisible by 4; hence

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

From $\gcd(X, \Delta) = 1$ it follows that $2 \nmid X$, i.e. X is odd. Compare $(\star)$ modulo 16:

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

The left-hand side $\equiv X^4 \equiv 1$ (mod 16), while the right-hand side $4A_0X^2 \equiv 4 \pmod{16}$ [8]. Contradiction.

Sub-branch II.2: a, u of opposite parity. Here Δ is odd, while $\nu_2(A_0) \geq 2$.

If X is even with $\nu_2(X) = 1$, then $\nu_2(X^2 - 8\Delta^2) = 2$ and $\nu_2(X^2 - 9\Delta^2) = 0$, so $\nu_2(\text{LHS}) = 2$, whereas $\nu_2(\text{RHS}) \geq 6$. Contradiction.

If X is even with $\nu_2(X) \geq 2$, then $\nu_2(X^2 - 8\Delta^2) = 3$ and $\nu_2(X^2 - 9\Delta^2) = 0$, so $\nu_2(\text{LHS}) = 3$, whereas $\nu_2(\text{RHS}) \geq 8$. Contradiction.

Case X odd. Here Δ is odd and, since we are in Branch II ($3 \nmid au$), we have $3 \mid \Delta$, $3 \nmid X$, and $\gcd(X, \Delta) = 1$ by Lemma 2. Assume, for a contradiction, that ($\star$) holds:

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

Step 1: Reduction to $X = \pm 1$. Reducing ($\star$) modulo X gives

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

Since $\gcd(X, \Delta) = 1$, this implies $X \mid 72$. As X is odd and $3 \nmid X$, the only possibility is $X = \pm 1$.

Step 2: Excluding the case $X = \pm 1$. With $X^2 = 1$, the equation ($\star$) becomes

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

The right-hand side is a positive perfect square. Let $Z := 1 - 8\Delta^2$ and $W := 1 - 9\Delta^2$. Note that for $\Delta \neq 0$ both factors Z and W are negative integers.

Substep 2a: Coprimality of the factors. Using the Euclidean algorithm,

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

Since $(1 - 8\Delta^2) + 8\Delta^2 = 1$, we have $\gcd(1 - 8\Delta^2,\, \Delta^2) = \gcd(1,\, \Delta^2) = 1$. Thus Z and W are coprime.

Substep 2b: Consequence for a square product. In $\mathbb{Z}$, if a product of two coprime integers is a perfect square, then each factor is a square up to a unit; see, e.g., [15]. Since $ZW = (2au)^2 > 0$ and $Z, W < 0$, their units must both be -1; hence there exist integers m, n such that

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

From $W = 1 - 9\Delta^2 = -(n^2)$ we get

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

The only factorizations of 1 in $\mathbb{Z}$ are $1 \cdot 1$ and $(-1) \cdot (-1)$. Both cases give $3\Delta = \pm 1$, which is impossible for integer Δ. (Equivalently, the only integer solutions of $x^2 - y^2 = 1$ are $x = \pm 1$, $y = 0$.)

Therefore (37) has no solutions, and the case X odd is impossible in Sub-branch II.2. Combining with the even cases for X treated above, Sub-branch II.2 is closed.

Thus Branch $3 \nmid au$ is impossible.

5 Completion of the Proof

We have shown that equation $(\star)$ has no integer solutions X either when $3 \mid au$ or when $3 \nmid au$. By Theorem 3, any 4+4 factorization yields a solution of $(\star)$; since $(\star)$ has no integer solutions, a 4+4 factorization is impossible.

Theorem 6 (Main result)**.** *For any coprime integers $a \neq u > 0$, the polynomial $P_{a,u}(t)$ does not factor in $\mathbb{Z}[t]$ as a product of two monic polynomials of degree 4.*

6 Excluding a 2+6 Factorization: a Direct Criterion and a Discriminant Argument

Recall the notation

$$P_{a,u}(t) = t^8 + At^6 + Bt^4 + Ct^2 + D, \qquad A = 6\Delta, \quad \Delta := u^2 - a^2 \neq 0,$$
$$B = \Delta^2 - 2A_0, \quad C = -A_0 A, \quad D = A_0^2, \qquad A_0 := a^2u^2.$$

Thus $P_{a,u}$ is even, monic, primitive in $\mathbb{Z}[t]$ and admits the representation

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

We show that a factorization of type 2+6 is impossible.

Step 0: Structural split of the class 2+6

Suppose

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

By evenness of $P_{a,u}$ and the involution $t \mapsto -t$ (Lemma 1), we have:

If Q_2 is *not* even, then necessarily $Q_2(-t) \mid H_6(t)$. Grouping the conjugate factors, we obtain an even quartic and another quartic:

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

i.e. the factorization regroups to the case 4+4, which has already been excluded.

Hence the only residue to analyze is the *even* quadratic

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

We now rule out this last possibility by a direct necessary and sufficient condition plus a discriminant computation.

Step 1: Criterion for an even quadratic divisor

Lemma 4 (Even quadratic divisor criterion)**.** *For $q \in \mathbb{Z}$ we have*

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

where Q is as in (38)*. In other words,*

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

Proof. Divide $Q(x)$ by $x+q$ in $\mathbb{Z}[x]$: $Q(x) = (x+q)R(x) + S$ with $R \in \mathbb{Z}[x]$ and a constant remainder $S = Q(-q)$. Substituting $x = t^2$ and using (38) gives

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

Thus $(t^2+q) \mid P_{a,u}$ if and only if $S = 0$, i.e. $Q(-q) = 0$. □

Remark 3. The case $q = 0$ is automatically impossible: if $t^2 \mid P_{a,u}(t)$, then the constant term must vanish, but $D = A_0^2 = a^4u^4 > 0$.

Step 2: A discriminant obstruction

We rewrite the equality $Q(-q) = 0$ from Lemma 4 as a quadratic equation in the unknown $A_0 = a^2u^2$ while Δ and q are regarded as fixed integers. Using $A = 6\Delta,\ B = \Delta^2 - 2A_0,\ C = -A_0A = -6\Delta A_0,\ D = A_0^2$, we compute

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

Thus $Q(-q) = 0$ is the quadratic equation in A_0:

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

Its discriminant with respect to A_0 equals

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

Proposition 2 (Irrationality of the would-be roots)**.** *If $\Delta \neq 0$ and $q \neq 0$, then $\mathrm{Disc}_{A_0} = 32\,\Delta^2\,q^2$ is* not *a perfect square in $\mathbb{Z}$.*

Proof. We have $\nu_2(\mathrm{Disc}_{A_0}) = \nu_2(32) + 2\nu_2(\Delta q) = 5 + 2\nu_2(\Delta q)$, which is odd for all $\Delta q \neq 0$. A perfect square in $\mathbb{Z}$ must have even 2-adic valuation. Hence Disc_{A_0} is not a square in $\mathbb{Z}$. □

Remark 4. This "odd 2-adic valuation of the discriminant forces non-squareness" obstruction is a standard device in elementary Diophantine arguments; compare also the problem-oriented expositions in [16].

Corollary 3 (No integer solution for A_0)**.** *For $\Delta \neq 0$ and $q \neq 0$ the quadratic equation $A_0^2 + bA_0 + c = 0$ has no solutions $A_0 \in \mathbb{Z}$.*

Proof. The roots are $\dfrac{-b \pm \sqrt{\mathrm{Disc}_{A_0}}}{2}$; by Proposition 2 the discriminant is not an integer square, hence the roots are irrational. □

Step 3: Conclusion for 2+6

Theorem 7 (No 2+6 factorization)**.** *Let $a, u \in \mathbb{Z}_{>0}$ be coprime and $a \neq u$ (so $\Delta \neq 0$). Then $P_{a,u}(t)$ does not factor in $\mathbb{Z}[t]$ as a product of a quadratic and a sextic polynomial.*

Proof. As noted above, any 2+6 with a non-even quadratic regroups to a 4+4, which is impossible. Thus it remains to exclude an even quadratic $t^2 + q$. By Lemma 4, $(t^2 + q) \mid P_{a,u}$ iff $Q(-q) = 0$. If $q = 0$, divisibility by t^2 would force $D = 0$, which is false. If $q \neq 0$, then by Corollary 3 the equality $Q(-q) = 0$ has no solutions $A_0 = a^2u^2 \in \mathbb{Z}$. Hence there is no $q \in \mathbb{Z}$ for which $t^2 + q$ divides $P_{a,u}$. Therefore no 2+6 factorization exists. □

Remark 5 (What this uses from previous sections). The proof is logically independent of the 4+4 Diophantine analysis, except for the purely structural observation that a non-even quadratic factor forces regrouping into 4+4 (via pairing $Q_2(t)$ with its conjugate $Q_2(-t)$). The "hard" residue (even quadratic $t^2 + q$) is completely settled by Lemma 4 and the discriminant computation.

7 Excluding other factorizations

After Theorem 7 has ruled out all factorizations of type 2+6, the remaining degree–8 patterns are excluded by trivial regrouping.

Proposition 3. *Let $P_{a,u}(t) \in \mathbb{Z}[t]$ be as above. If any of the following factorizations exists, then $P_{a,u}$ admits a factorization of type 2+6:*

(a) 2+2+4: $P_{a,u} = Q_1\, Q_2\, H_4$ with $\deg Q_i = 2$, $\deg H_4 = 4$;

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

Proof. (a) Group as $P_{a,u} = \underbrace{Q_1}_{\deg=2} \cdot \underbrace{(Q_2 H_4)}_{\deg=6}$.

(b) Group as $P_{a,u} = \underbrace{Q_1}_{\deg=2} \cdot \underbrace{(Q_2 Q_3 Q_4)}_{\deg=6}$.

(c) Group as $P_{a,u} = \underbrace{Q_2}_{\deg=2} \cdot \underbrace{(F_3 G_3)}_{\deg=6}$. □

Corollary 4. *None of the patterns* 2+2+4*,* 2+2+2+2*, or* 3+3+2 *can occur for* $P_{a,u}(t)$*.*

Proof. By Proposition 3 each would imply a 2+6 factorization, which is impossible by Theorem 7. □

8 Irreducibility in Full

Theorem 8 (Irreducibility)**.** *For any coprime integers* $a \neq u > 0$*, the polynomial* $P_{a,u}(t)$ *is irreducible in* $\mathbb{Z}[t]$*.*

Proof. All degree-8 splittings are excluded as follows.

(i) The case 4+4 is impossible by Theorem 3 and the analysis of equation $(\star)$ (from Lemma 1 to Corollary 2 and the subsequent 2-/3-adic split).

(ii) The case 2+6 is excluded in Section 6.

(iii) After (ii), any of the remaining patterns 2+2+4, 2+2+2+2, 3+3+2 would regroup to 2+6 by Proposition 3, hence are impossible by (ii).

Therefore no nontrivial factorization in $\mathbb{Z}[t]$ exists. Since $P_{a,u}(t)$ is monic and primitive, irreducibility over $\mathbb{Z}$ follows. □

Conclusions

We have shown that for any coprime integers $a \neq u > 0$ the even cuboid polynomial $P_{a,u}(t)$ admits no factorization of type 4+4 in $\mathbb{Z}[t]$. The key step is the reduction of a potential factorization to the Diophantine condition $(X^2 - 8\Delta^2)(X^2 - 9\Delta^2) = 4a^2u^2X^2$, from which, using 2- and 3-adic estimates and the lemma $\gcd(X, \Delta) = 1$, the absence of integer solutions follows. We then closed the genuine 2+6 case via an exact divisor criterion combined with a discriminant obstruction. Finally, after excluding 2+6, any remaining patterns (2+2+4, 2+2+2+2, 3+3+2) regroup trivially to 2+6 and are therefore impossible. Altogether, $P_{a,u}(t)$ admits no nontrivial factorization in $\mathbb{Z}[t]$, establishing irreducibility in full [1, 2, 3].

References

[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.