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

Valery Asiryan

asiryanvalery@gmail.com

September 29, 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, every 2+6 factorization either regroups to the forbidden 4+4 case (by evenness and the involution $t \mapsto -t$) or must contain an even quadratic factor; for the latter we use an exact divisor criterion and a discriminant obstruction, which rules it out arithmetically. By the same parity/involution argument, the types 2+2+4, 2+2+2+2, and 3+3+2 also reduce to 4+4 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.

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].

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

$$\sigma\, T\,(A - 2p) = \sigma\, T\,(6\Delta - 2X - 6\Delta) = -2\sigma X T = 2C - AM = -6\Delta X^2 + 48\Delta^3.$$

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:

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

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

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

(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 — the same outcome

Here $F = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$, $G(t) = F(-t)$. From $F(t)F(-t) = P_{a,u}(t)$ we get

$$2\beta - \alpha^2 = A, \tag{9}$$
$$\beta^2 + 2\delta - 2\alpha\gamma = B, \tag{10}$$
$$2\beta\delta - \gamma^2 - \alpha^2\delta = C, \tag{11}$$
$$\delta^2 = D. \tag{12}$$

Setting $X := \alpha - 3\Delta$ and eliminating γ from the second and third relations leads to an analogue of (8) and the same formula for T^2; in the end we again obtain $(\star)$.

Theorem 2 (Necessary condition for 4+4)**.** *If $P_{a,u}(t)$ factors in $\mathbb{Z}[t]$ as a product of two monic polynomials of degree 4, then there exists $X \in \mathbb{Z}$ satisfying $(\star)$ [1, 2].*

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 $\nu_p(\mathrm{LHS}) = 4x$. The right-hand side has $\nu_p(\mathrm{RHS}) = 2x + \nu_p(4a^2u^2) = 2x$ (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 $\nu_p(\mathrm{LHS}) \geq 4x + 1 > 2x = \nu_p(\mathrm{RHS})$. Contradiction [9, 11].

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 $\nu_2(\mathrm{LHS}) = 4d + 3$ (odd), whereas $\nu_2(\mathrm{RHS}) = 2 + \nu_2(a^2u^2) + 2x$ 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 $\nu_2(\mathrm{LHS}) = (2d + 2) + 2d = 4d + 2$.

  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

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

  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 $\nu_2(\mathrm{LHS}) \geq 4d + 3$ (odd), whereas $\nu_2(\mathrm{RHS}) = 2 + \nu_2(a^2u^2) + 2x$ is even. Contradiction.

(A) $2x < 2d$. Divide $(\star)$ by 2^{4x}:

$$\left(X_0^2 - 8 \cdot 2^{2(d-x)}\Delta_0^2\right) \cdot \left(X_0^2 - 9 \cdot 2^{2(d-x)}\Delta_0^2\right) = 4a^2u^2.$$

Since $2(d - x) \geq 2$, both brackets on the left are odd, so their product is odd, whereas the right-hand side is divisible by 4. Contradiction.

In all cases we get the impossibility $2 \mid \gcd(X, \Delta)$ [8, 10]. The lemma is proved. $\square$

Corollary 1. *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 $(\star)$ [4, 9].

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 $x := \nu_3(X) \geq 1$. Then $\nu_3(X^2 - 8\Delta^2) = 0$ (since $8\Delta^2 \equiv 2 \ (\mathrm{mod} 3)$), while

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

where $\nu_3(X \pm 3\Delta) \geq 1$. Hence $\nu_3(X^2 - 9\Delta^2) \leq 3$. Thus $\nu_3(\mathrm{LHS}) \leq 3$, while $\nu_3(\mathrm{RHS}) = \nu_3(4A_0) + 2x \geq 2 + 2 = 4$. Contradiction.

Therefore, when $3 \mid au$, equation $(\star)$ has no solutions [4].

Branch II: $3 \nmid au$ — impossible

Here $a^2 \equiv u^2 \equiv 1 \ (\mathrm{mod} 3)$, hence $\Delta \equiv 0 \ (\mathrm{mod} 3)$ and, by Corollary 1, $3 \nmid X$.

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 $\equiv X^4 \equiv 1 \pmod{16}$, 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.

If X is odd, then $X^2 - 8\Delta^2$ is odd, while $X^2 - 9\Delta^2 = (X - 3\Delta)(X + 3\Delta)$ is a product of two even numbers (one divisible by 2, the other by 4), hence $\nu_2(\text{LHS})$ is odd ≥ 3, whereas $\nu_2(\text{RHS}) = 2 + \nu_2(A_0)$ is even ≥ 4. Contradiction [7, 9].

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 2, any 4+4 factorization yields a solution of $(\star)$; since $(\star)$ has no integer solutions, a 4+4 factorization is impossible.

Theorem 3 (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+2+4 Factorization

In this section we show that any factorization of degree 8 of the form

$$P_{a,u}(t) = Q_1(t)\, Q_2(t)\, H(t), \qquad \deg Q_1 = \deg Q_2 = 2, \ \deg H = 4,$$

necessarily regroups into a factorization of type 4+4, which has already been excluded above. The key facts are: (i) primitivity and monicity of factors (Gauss's lemma), (ii) evenness of $P_{a,u}$ and the involution $t \mapsto -t$ (Lemma 1).

Lemma 3 (Making groups monic)**.** *Let $P \in \mathbb{Z}[t]$ be monic and primitive of degree 8, and $P = \prod_{i=1}^{k} F_i$ a factorization into primitive polynomials with leading coefficients ± 1. Then for any partition of the factors into two groups, the products over the groups can be made monic by multiplying* exactly two *factors (one in each group) by* (-1).

Proof. The product of the leading coefficients of all F_i equals $+1$. Hence the products of the leading coefficients over the groups are either $(+1, +1)$ or $(-1, -1)$. In the latter case multiply one factor in each group by (-1) to get leading coefficient $+1$ in both groups [5, 6]. □

Lemma 4 (Parity of pairs)**.** *If $Q(t) \in \mathbb{Z}[t]$ is quadratic and not even, then in any factorization of the even $P_{a,u}(t)$ the factor $Q(t)$ is accompanied by the conjugate $Q(-t)$, and their product is even:*

$$Q(t)Q(-t) \in \mathbb{Z}[t] \quad \textit{even}, \qquad \deg(Q(t)Q(-t)) = 4.$$

If Q_1, Q_2 are even quadratics, then $Q_1(t)Q_2(t)$ is also even.

Proof. From $P_{a,u}(t) = P_{a,u}(-t)$ and a factorization $P_{a,u} = \prod F_i$ we have $\prod F_i(t) = \prod F_i(-t)$. Comparing the multisets of irreducible factors in $\mathbb{Z}[t]$ (up to units ± 1), each factor not invariant under the involution must be accompanied by its conjugate; their product is invariant, i.e., even. If both quadratics are even, their product is clearly even [5, 13]. □

Proposition 1. *Suppose $P_{a,u}(t) = Q_1(t)\, Q_2(t)\, H(t)$, where $\deg Q_1 = \deg Q_2 = 2$ and $\deg H = 4$. Then there is a factorization*

$$P_{a,u}(t) = G(t)\, H(t), \qquad G(t) := Q_1(t)Q_2(t),$$

in which G and H can be made monic even *polynomials of degree* 4.

Proof. By Lemma 4, the product $G := Q_1 Q_2$ is an even polynomial of degree 4 (either "both even" or "a pair Q, $Q(-t)$"). Since $P_{a,u}$ is even, H is also even (otherwise the product would not be even). Applying Lemma 3 to the groups $\{Q_1, Q_2\}$ and $\{H\}$, by multiplying (-1) to one factor in each group if necessary, we make G and H monic. Thus we get a factorization of type 4+4 [5, 6, 13]. □

Corollary 2. *A* 2+2+4 *factorization of $P_{a,u}(t)$ is impossible.*

Proof. By Proposition 1, any 2+2+4 factorization yields a 4+4 factorization, whose impossibility was proved above (see $(\star)$ and the conclusion of the section excluding 4+4). □

7 Excluding a 2+2+2+2 Factorization

We now exclude a complete quadratic factorization.

Proposition 2. *If* $P_{a,u}(t) = Q_1(t)\,Q_2(t)\,Q_3(t)\,Q_4(t)$ *with* $\deg Q_i = 2$, *then there exist pairs*

$$G_1(t) := Q_1(t)Q_2(t), \qquad G_2(t) := Q_3(t)Q_4(t),$$

for which we have a factorization

$$P_{a,u}(t) = G_1(t)\,G_2(t),$$

where G_1 *and* G_2 *can be made* monic even *polynomials of degree* 4.

Proof. Group the factors in pairs. By Lemma 4, each pair either consists of two even quadratics, or contains a conjugate pair $Q(t), Q(-t)$; thus G_1 and G_2 are even of degree four. Applying Lemma 3 to the pairs $\{Q_1, Q_2\}$ and $\{Q_3, Q_4\}$, multiplying by (-1) if necessary, we make G_1, G_2 monic. Hence we obtain a 4+4 factorization. □

Corollary 3. *A* 2+2+2+2 *factorization of* $P_{a,u}(t)$ *is impossible.*

Proof. Proposition 2 reduces it to a 4+4 factorization, already ruled out above (see ($\star$) and the final conclusion about the impossibility of 4+4). □

8 Reducing 2+6 to 4+4 Under Structural Conditions

Consider a factorization

$$P_{a,u}(t) = Q(t)\,H(t), \qquad \deg Q = 2,\ \deg H = 6.$$

Proposition 3 (Sufficient conditions for the reduction 2+6 → 4+4)**.** *If in the factorization* $P_{a,u} = Q \cdot H$ *at least one of the conditions holds:*

(i) the quadratic factor Q *is* not *even;*

(ii) the sextic H *has a quadratic (or a pair of linear) factor(s) in* $\mathbb{Z}[t]$, *then the* 2+6 *factorization regroups to a* 4+4 *factorization.*

Proof. (i) If Q is not even, then by Lemma 4 in any factorization of the even $P_{a,u}$, the factor $Q(t)$ is accompanied by the conjugate factor $Q(-t)$. Since there are no other factors outside H, we have $Q(-t) \mid H(t)$. Then

$$P_{a,u}(t) = \underbrace{Q(t)Q(-t)}_{\text{deg=4 even}} \cdot \underbrace{\frac{H(t)}{Q(-t)}}_{\text{deg=4}},$$

i.e., the case 4+4. Monicity of the groups is achieved by normalization via Lemma 3.

(ii) If $H = R \cdot J$ with $\deg R = 2$, then $P_{a,u} = Q \cdot R \cdot J$ is a 2+2+4 factorization, which by Prop. 1 reduces to 4+4 [14]. $\square$

Corollary 4 (Excluding a portion of 2+6 factorizations)**.** *Since a* 4+4 *factorization is impossible for* $P_{a,u}$*, all* 2+6 *factorizations covered by Proposition 3 are also impossible.*

Remark 2 (What is *not* covered by the reduction). The only "hard" residue of the class 2+6 not reducible to 4+4 purely structurally is: Q is even (necessarily of the form $t^2 + q$), while the even sextic H *has no* linear/quadratic factors in $\mathbb{Z}[t]$. This remaining case is settled in Section 10.

9 Reducing 2+3+3 to 4+4 Under Structural Conditions

Let

$$P_{a,u}(t) = F(t)\,F(-t)\,Q(t), \qquad \deg F = 3,\ \deg Q = 2.$$

Then $H(t) := F(t)F(-t)$ is an even monic polynomial of degree 6, and we are in a special case of the 2+6 scheme: $P_{a,u} = H \cdot Q$.

Proposition 4 (Sufficient conditions for the reduction 3+3+2 $\to$ 4+4)**.** *If at least one of the following holds:*

(i) the quadratic factor Q *is* not *even;*

(ii) the sextic $H = F \cdot F(-t)$ *has a quadratic (or a pair of linear) factor(s) in* $\mathbb{Z}[t]$*,*

then the 3+3+2 *factorization regroups to* 4+4*.*

Proof. This is a direct application of Prop. 3 to the factorization $P_{a,u} = H \cdot Q$. In case (i), by Lemma 4 the factor $Q(-t)$ divides the even sextic H, and $Q(t)Q(-t)$ yields a quartic; in case (ii) the presence of a quadratic in H gives 2+2+4 $\Rightarrow$ 4+4. $\square$

Corollary 5 (Excluding a portion of 3+3+2 factorizations)**.** *Since* 4+4 *is excluded, all* 3+3+2 *factorizations covered by Prop. 4 are impossible.*

Remark 3 (The remaining case). If Q is even, and $H = F \cdot F(-t)$ has no linear/quadratic factors in $\mathbb{Z}[t]$ (i.e., is either irreducible as an even sextic, or is a product of two irreducible cubics), then there is no structural reduction to 4+4; this case needs a separate analysis.

10 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

$$P_{a,u}(t) = Q(t^2), \qquad Q(x) := x^4 + Ax^3 + Bx^2 + Cx + D \in \mathbb{Z}[x]. \quad (13)$$

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 $t \mapsto -t$, we have (cf. Lemma 4 and Prop. 3 in the previous sections):

- If Q_2 is *not* even, then necessarily $Q_2(-t) \mid H_6(t)$ and $P_{a,u}(t) = \underbrace{Q_2(t)Q_2(-t)}_{\text{deg=4, even}} \cdot \underbrace{\frac{H_6(t)}{Q_2(-t)}}_{\text{deg=4}}$, 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 5 (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 (13)*. 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 (13) 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. $Q(-q) = 0$. $\square$

Remark 4. 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 5 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

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

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

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

Its discriminant with respect to A_0 equals

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

Proposition 5 (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 $\mathbb{Z}$. $\square$

Corollary 6 (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 5 the discriminant is not an integer square, hence the roots are irrational. $\square$

Step 3: Conclusion for 2+6

Theorem 4 (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 5, $(t^2 + q) \mid P_{a,u}$ 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 6 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. $\square$

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 5 and the discriminant computation.

11 Excluding a 2+3+3 Factorization

In this section we show that a factorization of type 3+3+2 is impossible.

Proposition 6 (Structural reduction of 3+3+2)**.** *Assume*

$$P_{a,u}(t) = F(t)\,F(-t)\,Q(t), \qquad \deg F = 3,\ \deg Q = 2.$$

Then exactly one of the following occurs:

(a) Q is not *even, in which case $Q(-t) \mid F(t)F(-t)$ and the factorization regroups as*

$$P_{a,u}(t) = \underbrace{Q(t)Q(-t)}_{\text{deg=4, } \textit{even}} \cdot \underbrace{\frac{F(t)F(-t)}{Q(-t)}}_{\text{deg=4}},$$

i.e., into the already excluded case 4+4;

(b) Q is even, hence $Q(t) = t^2 + q$ for some $q \in \mathbb{Z}$.

Proof. This is the standard involution argument (cf. Lemma 4): since $P_{a,u}(t) = P_{a,u}(-t)$, any factor not fixed by $t \mapsto -t$ must be accompanied by its conjugate; with only one quadratic factor present, either it is even, or the conjugate $Q(-t)$ divides $F(t)F(-t)$, yielding (a) and hence 4+4. If Q is even and monic, it must be of the form $t^2 + q$. $\square$

Thus, to exclude 3+3+2, it suffices to rule out case (b).

Lemma 6 (Even quadratic divisor criterion revisited). *Let* $Q(x) = x^4 + Ax^3 + Bx^2 + Cx + D \in \mathbb{Z}[x]$ *be as in* (13) *with* $P_{a,u}(t) = Q(t^2)$. *Then, for* $q \in \mathbb{Z}$,

$$(t^2 + q) \mid P_{a,u}(t) \quad \Longleftrightarrow \quad Q(-q) = 0.$$

In particular, with $A = 6\Delta$, $B = \Delta^2 - 2A_0$, $C = -6\Delta A_0$, $D = A_0^2$ *(where* $A_0 = a^2u^2$, $\Delta = u^2 - a^2 \neq 0$*), the equality* $Q(-q) = 0$ *is the quadratic equation*

$$A_0^2 + (6\Delta q - 2q^2)A_0 + (\Delta^2 q^2 - 6\Delta q^3 + q^4) = 0$$

in the unknown A_0.

Proof. Identical to Lemma 5: divide $Q(x)$ by $x + q$ in $\mathbb{Z}[x]$ and substitute $x = t^2$. □

Proposition 7 (No even quadratic divisor). *If* $\Delta \neq 0$, *then there is no* $q \in \mathbb{Z}$ *with* $(t^2 + q) \mid P_{a,u}(t)$.

Proof. If $q = 0$, divisibility by t^2 would force $D = 0$, but $D = a^4u^4 > 0$. If $q \neq 0$, the discriminant of the quadratic in A_0 from Lemma 6 equals $\mathrm{Disc}_{A_0} = 32\,\Delta^2 q^2$, which is *not* a perfect square in $\mathbb{Z}$ (its 2-adic valuation is $5 + 2\nu_2(\Delta q)$, hence odd). Therefore the equation has no solution $A_0 \in \mathbb{Z}$, i.e., no such q exists. □

Theorem 5 (No 3+3+2). *For 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* $F(t)F(-t)Q(t)$ *with* $\deg F = 3$, $\deg Q = 2$.

Proof. By Proposition 6, either Q is not even, which regroups to 4+4 (already excluded), or $Q(t) = t^2 + q$, which is impossible by Proposition 7. □

Remark 6. This argument is logically independent of the Diophantine condition for 4+4 except for the purely structural regrouping in the non-even quadratic case. The genuinely remaining case $Q(t) = t^2 + q$ is killed by the discriminant computation from §10, hence the whole class 3+3+2 is excluded.

12 Irreducibility in Full

Theorem 6 (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 2 and the analysis of equation ($\star$) (from Lemma 1 to Corollary 1 and the subsequent 2-/3-adic split).

(ii) The types 2+2+4 and 2+2+2+2 regroup to 4+4 by Lemma 4 and Lemma 3, hence are impossible (Propositions 1 and 2 with Corollaries 2 and 3).

(iii) Any factorization with odd-degree factors must come in conjugate pairs $F(t)F(-t)$ by evenness; thus patterns with linear/cubic factors reduce to either 3+3+2 or 1+1+6, both of which regroup to 4+4 by Lemma 4 (see Proposition 4 and Corollary 5).

(iv) The remaining 2+6 case is ruled out in Section 10: a non-even quadratic forces a 4+4, while an even quadratic $t^2 + q$ cannot divide $P_{a,u}(t)$ by the exact divisor criterion $Q(-q) = 0$ and the discriminant obstruction $\mathrm{Disc}_{A_0} = 32\Delta^2 q^2$ (Theorem 4).

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. From the 4+4 prohibition we immediately obtain the impossibility of factorizations 2+2+4 and 2+2+2+2 (by regrouping even factors and conjugate pairs). Moreover, any factorization of types 2+6 and 3+3+2 that structurally reduces to 4+4 (a non-even quadratic or the presence of a quadratic/linear divisor in the sextic) is also excluded. Thus, a strict 4+4 ban is proved and a wide class of its immediate consequences for degree-8 factorizations is obtained [1, 2, 3].

Finally, we close the remaining 2+6 case that does *not* structurally reduce to 4+4: if an even quadratic $t^2 + q$ divides $P_{a,u}(t)$, then (with $P_{a,u}(t) = Q(t^2)$, $Q(x) = x^4 + Ax^3 + Bx^2 + Cx + D$) one must have the exact divisor condition $Q(-q) = 0$. Viewing this as a quadratic equation in $A_0 = a^2u^2$ (with fixed $\Delta = u^2 - a^2 \neq 0$ and $q \neq 0$) yields the discriminant $\mathrm{Disc}_{A_0} = 32\,\Delta^2 q^2$, which is never a perfect square in $\mathbb{Z}$; hence such a 2+6 factorization is impossible.

Together with the previous sections this excludes not only 4+4 but also all possible regroupings (2+2+4, 2+2+2+2, and 3+3+2) as well as the genuine 2+6 case. Altogether, $P_{a,u}(t)$ admits no nontrivial factorization in $\mathbb{Z}[t]$, establishing irreducibility in full.

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 GTM 1977 (reprints).

[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.