Irreducibility of the Cuboid Polynomial $P_{a,u}(t)$ via a Rank–Zero Elliptic Curve

Valery Asiryan

asiryanvalery@gmail.com

October 13, 2025

Abstract

For coprime integers $a \neq u > 0$ put $\Delta := u^2 - a^2 \neq 0$ and $A_0 := a^2u^2$. Consider

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

We prove $P_{a,u}(t)$ is irreducible over $\mathbb{Z}$. The argument is: (1) over $K = \mathbb{Q}(\sqrt{2})$, $P_{a,u}$ splits as H_-H_+ with coprime conjugate quartics $H_\pm$; (2) any hypothetical K–factorization of $H_\pm$ forces a rational point on a fixed genus–one quartic $\mathcal{C} : v^2 = 16y^4 + 136y^2 + 1$ with the structural constraint $\tau = y^2 = (au/\Delta)^2$; (3) the Jacobian of $\mathcal{C}$ admits a Weierstrass model $E/\mathbb{Q}$ on which a Magma computation certifies $\operatorname{rank} E(\mathbb{Q}) = 0$ and $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; (4) the only rational τ arising from $\mathcal{C}(\mathbb{Q})$ are $\tau \in \{0, 1/4\}$, incompatible with coprime integers $a \neq u > 0$. Therefore $H_\pm$ are irreducible in $K[t]$, whence $P_{a,u}$ is irreducible in $\mathbb{Q}[t]$ and in $\mathbb{Z}[t]$ by Gauss.

Keywords Irreducibility; perfect cuboid; quadratic extensions; genus–one quartics; Jacobians; elliptic curves; rank zero; torsion.

MSC 2020 **Primary**: 12E05. **Secondary**: 11D09, 11G05, 11R09.

1 Split over $K = \mathbb{Q}(\sqrt{2})$ and coprimeness

Let $a, u \in \mathbb{Z}_{>0}$ be coprime with $a \neq u$ [1, 2], and put

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

Write (cf. [3])

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

Let $K := \mathbb{Q}(\sqrt{2})$.

Lemma 1 (Explicit K–split)**.** *In* $K[t]$*,*

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

Proof. With $s = t^2$,

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

□

Lemma 2 (Coprimeness)**.** $\gcd(H_-, H_+) = 1$ *in* $K[t]$*.*

Proof. A common root t_0 gives $s_0 = t_0^2$ solving both $s^2 + (3 \mp 2\sqrt{2})\Delta s - A_0 = 0$; subtracting yields $4\sqrt{2}\,\Delta\, s_0 = 0 \Rightarrow s_0 = 0 \Rightarrow A_0 = 0$, impossible. □

2 Reduction to a fixed genus–one quartic

Put $S := t^2$ and

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

If h_- splits in $K[S]$, then $\Delta_S = (r + s\sqrt{2})^2$ with $r, s \in \mathbb{Q}$. Comparing parts,

$$2rs = -12\Delta^2, \qquad r^2 + 2s^2 = 17\Delta^2 + 4A_0. \tag{2}$$

Eliminating r and setting $T := s^2$ gives

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

so the discriminant

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

must be a rational square.

Introduce

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

Dividing (4) by X^2 yields the conic

$$v^2 = 16\tau^2 + 136\tau + 1. \tag{5}$$

The structural constraint $\tau = (au/\Delta)^2$ forces τ to be a rational square, say $\tau = y^2$, and we arrive at the fixed genus–one quartic

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

3 The Jacobian of $\mathcal{C}$ and a convenient elliptic model

Let $F(Y) = 16Y^4 + 136Y^2 + 1$ with coefficients $(a, b, c, d, e) = (16, 0, 136, 0, 1)$. The classical invariants (see, e.g., Cassels or Lang [4, 5]) are

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

A Weierstrass model of $\mathrm{Jac}(\mathcal{C})$ is

$$E_0:\ Y^2 = X^3 - 27\,I\,X - 27\,J = Y^2 = X^3 - 504\,576\,X + 131\,604\,480. \tag{7}$$

Its j–invariant equals $j(E_0) = \frac{1\,556\,068}{81}$.

For arithmetic convenience we work on an equivalent model

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

which has the same j and three rational 2–torsion points $(0,0), (8,0), (9,0)$. Since $\mathcal{C}$ has a rational point $(y, v) = (0, 1)$, the standard construction based at it identifies $\mathcal{C}$ birationally with its Jacobian (see Cassels, Ch. 1–2 [4]); we henceforth view E as a convenient Weierstrass model of $\mathrm{Jac}(\mathcal{C})$ for computations.

Remark 1 (Explicit isomorphism $E_0 \simeq E$). On $E_0:\ y^2 = x^3 - 504576\,x + 131604480$ set

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

(equivalently, $x = 12^2X - 816,\ y = 12^3Y$). A direct substitution yields $Y^2 = X^3 - 17X^2 + 72X$. Moreover $\Delta(E_0) = 12^{12}\Delta(E)$ and $j(E_0) = j(E)$.

Remark 2 (Torsion on E). For E in (8), the three points $(0,0), (8,0), (9,0)$ are rational 2–torsion. Moreover, the points $(6, \pm 6)$ and $(12, \pm 12)$ have order 4 (indeed $2(6,6) = (9,0)$ and $2(12,12) = (9,0)$). Together with O, this yields

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

4 Rank and torsion of E (via computation)

Proposition 1 (Rank 0 and torsion)**.** *For the curve $E/\mathbb{Q}$ given by* (8)*, one has*

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

Computational proof. A Magma session (Appendix) [6] on the model $E : Y^2 = X(X-8)(X-9)$ returns

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

It also enumerates the integral points $(0,0), (8,0), (9,0), (6, \pm 6), (12, \pm 12)$ (the negatives of the nonzero Y–coordinates are symmetric), which generate the torsion subgroup. This proves the proposition. □

5 Rational points on $\mathcal{C}$

Let $\overline{\mathcal{C}}$ be the smooth projective model of $\mathcal{C}$. For an even quartic with leading and trailing coefficients perfect squares (16 and 1), $\overline{\mathcal{C}}$ has two rational points at infinity (two branches of $v = \pm 4y^2$ as $y \to \infty$). The affine chart contains $(0, \pm 1)$, and the curve is of genus 1.

Proposition 2. *There is a birational equivalence $\phi : \overline{\mathcal{C}} \dashrightarrow E$ over $\mathbb{Q}$, sending one point at infinity to $O \in E(\mathbb{Q})$. Since both curves are smooth projective curves of genus 1 over $\mathbb{Q}$, any birational map over $\mathbb{Q}$ is an isomorphism; consequently $\overline{\mathcal{C}}(\mathbb{Q})$ and $E(\mathbb{Q})$ are in natural bijection. In particular*

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

Among the eight points, two are the points at infinity on $\overline{\mathcal{C}}$, and the six affine points are exactly

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

Proof. Since $\operatorname{rank} E(\mathbb{Q}) = 0$ by Proposition 1, we have $|E(\mathbb{Q})| = |E(\mathbb{Q})_{\mathrm{tors}}| = 8$ (see Remark 2). The isomorphism above then gives $|\overline{\mathcal{C}}(\mathbb{Q})| = 8$. We exhibit eight rational points on $\overline{\mathcal{C}}$: the two points at infinity and the six affine ones listed (direct substitution into $v^2 = 16y^4 + 136y^2 + 1$ shows they lie on $\mathcal{C}$). Hence these are all rational points. □

Corollary 1. *The only rational values of $\tau = y^2$ arising from $\mathcal{C}(\mathbb{Q})$ are*

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

6 Excluding the structural values of τ

Recall $\tau = (au/\Delta)^2$ with $\Delta = u^2 - a^2 \neq 0$.

Lemma 3. *For coprime integers $a \neq u > 0$ one has $\tau \notin \{0, 1/4\}$.*

Proof. $\tau = 0$ would imply $au = 0$, impossible. If $\tau = 1/4$, then

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

If $u^2 - a^2 = 2au$, then $(u - a)^2 = 2a^2$, i.e. $u/a = 1 \pm \sqrt{2}$ (irrational), impossible. If $a^2 - u^2 = 2au$, then $(a - u)^2 = 2u^2$, i.e. $a/u = 1 \pm \sqrt{2}$ (irrational), impossible. This excludes both cases. □

Remark 3 (Even-factor criterion over totally real K). Since $K = \mathbb{Q}(\sqrt{2})$ is totally real and $A_0 > 0$, any factorization of $t^4 + \alpha t^2 - A_0$ in $K[t]$ must be even in t. Indeed, writing $(t^2 + pt + q)(t^2 - pt + r)$ and comparing the t–term shows $(r - q)p = 0$; the case $r = q$ forces $q^2 = -A_0$, impossible in a totally real field. Hence $p = 0$ and the problem reduces to the quadratic $S^2 + \alpha S - A_0$ in $S = t^2$ (i.e. to (1)).

Corollary 2 (No K–split of $h_\pm$)**.** *Under the standing hypotheses, the discriminant* (1) *is never a square in* $K = \mathbb{Q}(\sqrt{2})$*. Hence* $h_-(S)$ *and* $h_+(S)$ *do not split in* $K[S]$*, and each* $H_\pm(t)$ *is irreducible in* $K[t]$*.*

Proof. Assume for contradiction that Δ_S is a square in K (equivalently, that $h_-(S)$ splits in $K[S]$). Then, by the algebra of Section 2, there exist $v, \tau \in \mathbb{Q}$ with $v^2 = 16\tau^2 + 136\tau + 1$ and $\tau = (au/\Delta)^2 = y^2$, i.e. $\mathcal{C}$ has a rational point with $y^2 = \tau$. By Corollary 1 and Lemma 3 this is impossible. The same argument applies to $h_+(S)$.

Finally, by Remark 3, any factorization of $H_\pm(t)$ in $K[t]$ would be even in t and would force a splitting of $h_\pm(S)$ in $K[S]$, which we have just excluded. Therefore each $H_\pm$ is irreducible in $K[t]$. □

7 Irreducibility of $P_{a,u}(t)$ over $\mathbb{Z}$

Theorem 1. *For any coprime integers* $a \neq u > 0$*, the polynomial* $P_{a,u}(t) \in \mathbb{Z}[t]$ *is irreducible.*

Proof. By Lemmas 1 and 2, $P_{a,u} = H_-H_+$ in $K[t]$ with $\gcd(H_-, H_+) = 1$. By Corollary 2, both $H_\pm$ are irreducible in $K[t]$. Any factorization in $\mathbb{Q}[t]$ would, in $K[t]$, be a product of a subcollection of $\{H_-, H_+\}$; since neither $H_\pm$ lies in $\mathbb{Q}[t]$, only the trivial factorization remains. Thus $P_{a,u}$ is irreducible in $\mathbb{Q}[t]$, and by Gauss's lemma (primitivity) [5, Ch. VIII] in $\mathbb{Z}[t]$. □

Appendix: Magma verification for Sections 4 and 5

Code.

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

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

Transcript.

```
Elliptic Curve defined by y^2 = x^3 + x^2 - 24*x + 36 over Rational
↪  Field
48a3
```

```
48
Abelian Group isomorphic to Z/2 + Z/4
Defined on 2 generators
Relations:
    2*T.1 = 0
    4*T.2 = 0
[ 2, 4 ]
0 true
[ (0 : 0 : 1), (6 : -6 : 1), (8 : 0 : 1), (9 : 0 : 1), (12 : 12 : 1) ]
[ <(0 : 0 : 1), 1>, <(6 : -6 : 1), 1>, <(8 : 0 : 1), 1>, <(9 : 0 : 1),
↪  1>, <(12
: 12 : 1), 1> ]
true
{@ (1 : -4 : 0), (1 : 4 : 0), (0 : -1 : 1), (0 : 1 : 1), (-1 : -24 :
↪  2), (-1 :
24 : 2), (1 : -24 : 2), (1 : 24 : 2) @}
```

The last set lists the eight rational points on $\overline{\mathcal{C}}$ in *weighted* projective coordinates $(X : Y : Z)$ of $\mathbb{P}(1, 2, 1)$ (weights $1, 2, 1$). On the affine chart $Z \neq 0$ we have the identification

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

Thus $(1 : \pm 24 : 2)$ corresponds to $(y, v) = (\frac{1}{2}, \pm 6)$, and the eight rational points are the two points at infinity $(1 : \pm 4 : 0)$ together with the six affine points $(0, \pm 1)$ and $(\pm\frac{1}{2}, \pm 6)$ used in Proposition 2.

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

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

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

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