Six exclusions at rational torsion order 256

11 November 2026.

Theorem. Let $A/\mathbb{Q}$ be a principally polarized abelian surface that is split over $\mathbb{Q}$. If

$$\#A(\mathbb{Q})_{\mathrm{tors}} = 256,$$

then $A[2] \subseteq A(\mathbb{Q})$. Consequently its rational torsion group is one of

$$C_2^3 \times C_{32}, \qquad C_2^2 \times C_4 \times C_{16}, \qquad C_2^2 \times C_8^2.$$

No existence assertion is made for these three groups. In particular, the six groups

$$[4,64], \quad [8,32], \quad [16,16], \quad [2,2,64], \quad [2,4,32], \quad [2,8,16]$$

are impossible for genus-2 Jacobians split over $\mathbb{Q}$, at every splitting degree.

1. The full elliptic 2-adic image

Let $E/\mathbb{Q}$ have rational torsion $C_8 \times C_2$. Choose a basis of its Tate module in which

$$T = E(\mathbb{Q})_{\mathrm{tors}} = \left\langle \frac{e_1}{8}, \frac{e_2}{2} \right\rangle \subseteq (\mathbb{Q}_2/\mathbb{Z}_2)^2, \qquad D = \mathrm{diag}(8,2).$$

The pointwise stabilizer of T is

$$H_0 = \{I + MD : M \in M_2(\mathbb{Z}_2)\}.$$

All these matrices are invertible. The group has index 96 in $\mathrm{GL}_2(\mathbb{Z}_2)$: its reduction modulo 8 has order 16, while $\#\,\mathrm{GL}_2(\mathbb{Z}/8) = 1536$.

The curve E is non-CM, since Olson's classification of rational torsion on CM elliptic curves excludes a point of order 8. By Rouse–Zureick-Brown, Corollary 1.3, the index of its 2-adic image divides 64 or 96. Since that image is contained in H_0, its index is a multiple of 96. Hence its image is exactly H_0.

2. A matrix lemma for maximal gluing

Lemma. Let $E, F/\mathbb{Q}$ have exact rational torsion $C_8 \times C_2$. Let $q \geq 2$ be a power of 2 and let $\psi : E[q] \to F[q]$ be a Galois-equivariant isomorphism. Put

$$B = (E \times F)/\,\mathrm{graph}(\psi).$$

If $\#B(\mathbb{Q})_{\mathrm{tors}} = 256$, then $B[2]$ is rational.

Proof. Choose a basis of T_2E adapted to T as above. Choose a basis of T_2F lifting its image under ψ. Thus the gluing is the identity modulo q. This second basis need not be adapted to the rational torsion of F. Choose $P \in \mathrm{GL}_2(\mathbb{Z}_2)$ so that multiplication by P converts its coordinates to an adapted basis. The rational torsion of F, in the gluing coordinates, is therefore $P^{-1}T$.

For a Galois element, write g, h for its matrices in the gluing coordinates. We have

$$h \equiv g \pmod{q}, \qquad g \equiv h \equiv I \pmod{2}, \qquad \det h = \det g.$$

The first image is exactly H_0. We write

$$M = (g - I)D^{-1}, \qquad V = (h - g)/q.$$

Both are integral, and M ranges over every element of $M_2(\mathbb{Z}_2)$.

The two elliptic quotient maps from B are surjective on rational torsion: each kernel on rational torsion has order 16 and the proposed total order is 256. Consider

$$\tau : B \longrightarrow E \times F, \qquad [X, Y] \longmapsto (qX, qY).$$

Its image on rational torsion projects onto both elliptic torsion groups. The kernel of either projection is the corresponding subgroup qT. After using adapted coordinates on both factors, this image modulo $qT \times qT$ is therefore the graph of an isomorphism

$$\varphi : T/qT \longrightarrow T/qT.$$

Choose rational lifts under the first elliptic quotient of the generators $e_1/8$ and $e_2/2$. By adding graph elements to representatives, we may write them as

$$\left(\frac{e_1}{8q}, \frac{Ne_1}{8q}\right), \qquad \left(\frac{e_2}{2q}, \frac{Ne_2}{2q}\right).$$

Here

$$N = P^{-1}L, \qquad L = \begin{pmatrix} a & c/4 \\ 4b & d \end{pmatrix}, \qquad a, b, c, d \in \mathbb{Z}_2.$$

Indeed, the second elliptic images are linear combinations of the two adapted generators with coefficient columns (a, b) and (c, d). Changing a representative by a point of $F[q]$ changes these coefficients by even integers, so their reductions modulo 2 represent the induced automorphism of $T/2T$. Consequently $ad - bc$ is odd. In particular,

$$DN^{-1} = \frac{1}{ad - bc} \begin{pmatrix} 8d & -2c \\ -8b & 2a \end{pmatrix} P \in 2M_2(\mathbb{Z}_2). \tag{1}$$

This holds even if L has a nonintegral upper-right entry.

Rationality of the two chosen lifts says that, for every Galois element, there is an integral matrix W such that

$$(h - I)N - (g - I) = qWD. \tag{2}$$

Put

$$K = \frac{D}{q}(I - N^{-1}) \in M_2(\mathbb{Q}_2).$$

Rearranging (2) gives

$$V = WDN^{-1} - MK. \tag{3}$$

Choose a Galois element for which $M = I$, which exists by the full-image result. Then (1) and (3), together with the integrality of V, show that K is integral.

For every Galois element, $\det(g + qV) = \det g$. Since q is even and $g \equiv I \pmod 2$, expansion of the determinant gives

$$\operatorname{tr}(V) \equiv 0 \pmod 2.$$

Reducing (3) modulo 2 and using (1), we obtain

$$\operatorname{tr}(MK) \equiv 0 \pmod 2 \qquad \text{for all } M \in M_2(\mathbb{F}_2).$$

The trace pairing on $M_2(\mathbb{F}_2)$ is nondegenerate, so $K \equiv 0 \pmod 2$. Equation (3) now shows that $V \equiv 0 \pmod 2$ for every Galois element. Thus

$$h \equiv g \pmod{2q}.$$

Explicitly, identify the 2-primary torsion of B with two copies of $(\mathbb{Q}_2/\mathbb{Z}_2)^2$ through

$$\theta(x, z) = \left[\frac{\tilde{x}}{q}, \frac{\tilde{x}}{q} + \tilde{z}\right],$$

where tildes denote lifts. Changing a lift of x changes the representative by a graph element, so this is well defined. Its inverse is induced by $(X, Y) \mapsto (qX, Y - X)$. The Galois action in these coordinates is

$$(x, z) \longmapsto (gx, Vx + hz).$$

Equivalently, on T_2B it has block matrix

$$\begin{pmatrix} g & 0 \\ (h-g)/q & h \end{pmatrix}.$$

Its reduction modulo 2 is the identity. Hence all of $B[2]$ is rational. □

3. Proof of the theorem

Choose complementary elliptic subvarieties E, F of A. Their torsion groups embed in $A(\mathbb{Q})_{\text{tors}}$, and the elliptic quotient sequences give

$$256 \mid \#E(\mathbb{Q})_{\text{tors}} \, \#F(\mathbb{Q})_{\text{tors}}.$$

Mazur's theorem bounds each factor by 16. Thus both groups are $C_8 \times C_2$.

The complementary elliptic decomposition writes A as a quotient by the graph of an anti-isometry $E[n] \to F[n]$. Put $q = 2^{v_2(n)}$. Passing to the graph of its restriction to $E[q]$ preserves rational 2-primary torsion, since the discarded isogeny degree is odd. If $q = 1$, the rational torsion is the direct product of the two elliptic groups, with full rational 2-torsion. If $q \geq 2$, the intermediate quotient has rational 2-primary torsion of order 256; the same elliptic quotient bound shows that its entire rational torsion group has order 256. Thus the lemma applies. In either case $A[2]$ is rational.

Write its rational torsion as $C_{d_1} \times C_{d_2} \times C_{d_3} \times C_{d_4}$, with $d_1 \mid d_2 \mid d_3 \mid d_4$. Full rational 2-torsion gives $2 \mid d_i$, while the Weil pairing over $\mathbb{Q}$ forces $d_1, d_2 \mid 2$. Thus $d_1 = d_2 = 2$ and $d_3 d_4 = 64$, giving precisely the three groups in the statement. □

References and verification

1. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47 (1977), Theorem (8). Primary paper.

2. L. D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. 14 (1974), 195–205. Published paper. Rational CM torsion excludes order 8.
3. J. Rouse and D. Zureick-Brown, *Elliptic curves over Q and 2-adic images of Galois*, Research in Number Theory 1 (2015), article 12, Corollary 1.3. Primary paper, page 2. The source uses row vectors; transposing to column conventions leaves its index result unchanged.
4. N. Bruin and K. Doerksen, *The arithmetic of genus two curves with (4,4)-split Jacobians*, Canad. J. Math. 63 (2011), Section 2, especially Proposition 2.8 and Lemma 2.6. Primary paper.

The proof applies to every splitting degree and does not depend on a bounded search or a finite-level gluing classification.

The supplementary exact matrix checks, with completed log, verify the stabilizer index, the non-degenerate trace pairing, 2,560 determinant calculations, and 9,216 rational-matrix identities, including 7,680 cases with a fractional upper-right entry. These are ancillary checks of the displayed identities; they are not a finite search for all gluing degrees.