Rational 7-torsion and the 2-primary torsion of geometrically split Jacobians

11 November 2026

Theorem and scope

Theorem. Let $A/\mathbb{Q}$ be a principally polarized abelian surface that is simple over $\mathbb{Q}$ and geometrically split. If $A(\mathbb{Q})$ has a point of order 7, then

$$\#A(\mathbb{Q})[2^\infty] \leq 4.$$

Corollary. No genus-2 Jacobian in this class has rational torsion containing $C_2 \times C_{28}$. In particular, the exact group $[2, 28]$ is impossible in the census column **geometrically split, simple over** $\mathbb{Q}$. More generally, every group with 7-torsion and 2-primary subgroup of order at least eight is excluded in this class, including [56] and $[2, 2, 14]$.

Here geometrically split means that $A_{\overline{\mathbb{Q}}}$ is isogenous to a product of elliptic curves. There is no restriction on the splitting degree or the integral endomorphism ring. The principal polarization is used in the cyclic cubic case. The theorem does not exclude $[2, 28]$ for Jacobians split over $\mathbb{Q}$, or for geometrically simple Jacobians. The combined geometrically split existence and infinitude question for $[2, 28]$ therefore remains open. The bound also leaves [28] and $[2, 14]$ unexcluded.

The complete proof is available as PDF and LaTeX. The exact Magma certificate and its completed log accompany the proof.

1. Conventions and the existing reduction

For a number field k, put $G_k = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$. Write T_ℓ for the Tate module, $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$, and χ_ℓ for the cyclotomic character. We use residual semisimplification to compare different stable lattices in one rational Tate representation; rational torsion is not moved along arbitrary isogenies.

The published rational-7-torsion and 2-rank proof, especially Proposition 2, the cyclic-field reduction, and its remarks on $[2, 28]$, gives the following inputs.

- If the geometric elliptic factors are nonisogenous, or form a non-CM square with quadratic endomorphism field, rational 7-torsion forces the entire rational 2-primary torsion to have order at most four. This uses Kenku–Momose's quadratic elliptic torsion theorem.
- For a CM elliptic square, a point count at 3 gives the same bound.
- The only remaining endomorphism fields are cyclic of degree 3 or 6.

In these last two cases put

$$D = \mathrm{End}^0(A_{\overline{\mathbb{Q}}}) \simeq M_2(\mathbb{Q}), \qquad F = \mathrm{End}^0_{\mathbb{Q}}(A) = \mathbb{Q}(\sqrt{-3}),$$

and let L be the smallest field over which all geometric endomorphisms are defined. The normalization and cubic untwisting below are those proved in the order-63 proof, Sections 5–7 and 10.2, and the order-26/39 proof, Section 8. We show that, in either remaining case, rational 7-torsion is incompatible with rational 2-torsion.

2. Cyclic cubic endomorphism field: polarization at 3

Suppose $\mathrm{Gal}(L/\mathbb{Q}) = C_3$. Cubic untwisting expresses the rational Tate representation as

$$V_\ell(A) \simeq V_\ell(E_0) \otimes_{\mathbb{Q}_\ell} W_\ell,$$

where $E_0/\mathbb{Q}$ is non-CM and W is the two-dimensional rational representation given by a faithful character

$$\psi : G_{\mathbb{Q}} \longrightarrow \mu_3 \subset F^\times, \qquad \ker \psi = G_L.$$

This is the construction in Section 10.2 of the order-63 proof before its specialization to an elliptic isogeny class. Replacing ψ by its inverse does not affect the argument.

2.1. Principal polarization forces a rational 3-isogeny on E_0

Suppose that $E_0[3]$ is irreducible over $\mathbb{F}_3$. Let

$$\mathcal{O} = \mathbb{Z}_3[\zeta_3], \qquad \pi = \zeta_3 - 1, \qquad T_0 = T_3(E_0) \otimes_{\mathbb{Z}_3} \mathcal{O}.$$

The lattice T_0 is $G_{\mathbb{Q}}$-stable, with $G_{\mathbb{Q}}$ acting on its second factor by ψ. Since π^2 is a unit times 3, the module $T_0/3T_0$ is an extension of $W_0 = E_0[3]$ by itself, with natural submodule $\pi T_0/3T_0$.

This extension is nonsplit. Modulo π^2, write

$$\psi(g) = 1 + c(g)\pi,$$

where $c : G_{\mathbb{Q}} \to \mathbb{F}_3$ is a nonzero additive character. A $G_{\mathbb{Q}}$-linear splitting would give an $\mathbb{F}_3$-linear endomorphism S of W_0 satisfying, up to an irrelevant overall sign,

$$\rho(g)^{-1} S \rho(g) - S = c(g) I.$$

Taking traces gives $2c(g) = 0$ in $\mathbb{F}_3$, a contradiction. As W_0 is irreducible, a nonsplit length-two self-extension has a unique proper nonzero submodule.

It follows that every $G_{\mathbb{Q}}$-stable $\mathbb{Z}_3$-lattice in this rational representation is $\pi^j T_0$ for some integer j. Indeed, scale such a lattice T by a power of 3 so that $T \subseteq T_0$ but $T \not\subseteq 3T_0$. If its image modulo $3T_0$ is the whole module, Nakayama gives $T = T_0$. Otherwise its image is the unique proper nonzero submodule, so $T \subseteq \pi T_0$. Then $\pi^{-1}T \subseteq T_0$ but $\pi^{-1}T \not\subseteq \pi T_0$. Its reduction cannot be that proper submodule, and Nakayama gives $\pi^{-1}T = T_0$.

The space of $G_{\mathbb{Q}}$-equivariant alternating forms on $V_3(A)$ with cyclotomic similitude is one-dimensional over $\mathbb{Q}_3$. To see this, restrict first to G_L. By Faltings's theorem and $\mathrm{End}_L(E_0) = \mathbb{Z}$,

equivariant bilinear forms on $V_3(E_0)$ with cyclotomic multiplier form the line spanned by the elliptic Weil pairing e. Thus the alternating forms on $V_3(A)$ have the form $e \otimes b$, with b symmetric on the multiplicity space. Invariance under μ_3 forces b to be a scalar multiple of

$$b_0(a,b) = \mathrm{Tr}_{\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3}(a\bar{b}).$$

For this trace pairing, the dual of $\mathcal{O}$ is the inverse different $\pi^{-1}\mathcal{O}$. Since $T_3(E_0)$ is self-dual for e, the dual of $\pi^j T_0$ under $q(e \otimes b_0)$, for $q \in \mathbb{Q}_3^\times$, is

$$\pi^{-j-1-2v_3(q)} T_0.$$

Self-duality would require

$$2j = -1 - 2v_3(q),$$

which is impossible by parity. A principal polarization supplies exactly such a perfect alternating form on $T_3(A)$. Hence $E_0[3]$ is reducible, and E_0 has a rational cyclic 3-isogeny. The argument in fact excludes every polarization of degree prime to 3 in the isogeny class under the irreducibility hypothesis.

2.2. Rational 7-torsion and $X_0(21)$

Since 7 splits in F, the two characters of W over $\mathbb{F}_7$ are ψ and ψ^{-1}. A trivial constituent coming from $A(\mathbb{Q})[7] \neq 0$ forces $E_0[7]$ to have one of these character constituents. Thus $E_0[7]$ is reducible and E_0 has a rational cyclic 7-isogeny. The coprime kernels of the 3- and 7-isogenies give a rational cyclic 21-isogeny.

The exact certificate enumerates all rational points of $X_0(21)$, using algebraic rank zero and its torsion group $C_2 \times C_4$. Its four noncuspidal j-invariants are

$$-\frac{189613868625}{128}, \qquad \frac{3375}{2}, \qquad -\frac{1159088625}{2097152}, \qquad -\frac{140625}{8}.$$

For each, the elliptic 2-division polynomial is irreducible with nonsquare discriminant, so its splitting field has Galois group S_3. These properties are unchanged by quadratic twists; none of the four values is 0 or 1728.

An S_3 extension has no cyclic cubic subextension, so it is linearly disjoint from L. Therefore $E_0[2]$ remains irreducible on G_L. The representation W becomes trivial there, so the residual semisimplification of $A[2]$ restricted to G_L has two copies of this nontrivial irreducible constituent and has no trivial constituent. In particular $A(\mathbb{Q})[2] = 0$. This completes the cubic case.

3. Cyclic sextic field: a level-21 point with square discriminant

Suppose $\mathrm{Gal}(L/\mathbb{Q}) = C_6$, and let K be its quadratic subfield. The construction in Section 8 of the order-26/39 proof gives the following facts without a torsion assumption.

1. Both L and K are totally real.
2. After an isogeny normalizing the action of $\mathbb{Z}[\zeta_3]$ and a cubic twist, one obtains $B/\mathbb{Q}$ whose geometric endomorphisms are all defined over K.
3. There is $\theta \in \mathrm{End}_{\mathbb{Q}}(B)$ with $\theta^2 = -3$. For each elliptic $E_0 \subset B_K$, the restriction of θ gives a cyclic K-isogeny of degree 3 to its distinct conjugate E_0^τ.
4. On G_K, the original representation differs from that of B by a faithful cubic multiplicity character ψ, with kernel G_L.

3.1. The level-7 structure and its conjugation

Rational 7-torsion supplies a one-dimensional constituent in one of the two 7-adic F-blocks. The lattice argument in Proposition 9.1 of the order-26/39 proof applies with 7 in place of 13. Here are the steps needed for this application.

- In a chosen F-block of the normalized surface, cubic twisting preserves reducibility modulo 7. Choose a $G_{\mathbb{Q}}$-stable line in that residual block of B.
- Inclusion of E_0 followed by projection to the chosen block is a G_K-equivariant isomorphism on rational Tate modules. Faltings's theorem gives irreducibility of $V_7(E_0)$, and the projection cannot vanish: otherwise $V_7(E_0)$ would be stable under θ, contradicting $\theta E_0 \neq E_0$.
- Realize the block lattice by a K-isogeny $h : E_0 \to E$ of degree 7^b and pull the residual line back to a G_K-stable subgroup $C_7 \subset E[7]$.
- Galois action outside G_K gives a G_K-equivariant isomorphism $T_7(E^\tau) \to T_7(E)$. By Faltings's theorem it is a $\mathbb{Z}_7$-unit times a primitive generator of $\mathrm{Hom}_K(E^\tau, E)$, whose degree is prime to 7.
- Transporting the degree-three isogeny through h gives an isogeny of degree $3 \cdot 7^{2b}$. Its primitive generator must consequently have degree 3. The Galois-stable residual line is respected by this generator.

Reversing the direction if necessary, we obtain a cyclic isogeny $\nu : E \to E^\tau$ of degree 3 with $\nu(C_7) = \tau C_7$. Its kernel and C_7 define

$$x = (E, \ker \nu + C_7) \in Y_0(21)(K), \qquad \tau(x) = w_3(x).$$

The last equality is the moduli definition of w_3: quotient by $\ker \nu$ sends $E[3]/\ker \nu$ to the kernel of the conjugate degree-three isogeny, and sends C_7 to τC_7. This is the same compatibility argument used at level 39. The point x cannot be rational, since a w_3-fixed point would give a degree-three endomorphism of a non-CM elliptic curve.

3.2. The elliptic 2-division field

Suppose $A(\mathbb{Q})[2] \neq 0$. After extension of scalars to $\mathbb{F}_4$, the multiplicity characters on G_K are ψ and ψ^{-1}. A trivial residual constituent forces $E[2] \otimes \mathbb{F}_4$ to have one of these nontrivial cubic characters as a constituent. Its determinant over $\mathbb{F}_2$ is 1, so its two characters are ψ and ψ^{-1}. The only subgroup of $\mathrm{GL}_2(\mathbb{F}_4) = S_3$ with these constituents is C_3; the natural S_3 module remains irreducible over $\mathbb{F}_4$. The intervening 7-power isogeny leaves $E[2]$ unchanged. Thus the 2-division field of E is exactly L/K, and its discriminant is a square in K.

For $j(E) \notin \{0, 1728\}$ the identity

$$j(E) - 1728 = \frac{c_6(E)^2}{\Delta(E)}$$

shows that $j(E) - 1728$ is a square in K. Hence x lifts to a K-point of the double cover of $X_0(21)$ obtained by adjoining $\sqrt{j - 1728}$. The next section determines the relevant points of this genus-three cover.

4. The discriminant cover and its rank-zero quotients

Use the standard model

$$X_0(21) : y^2 + xy = x^3 - 4x - 1, \qquad t = \frac{y - x - 3}{x + 1}.$$

The certificate checks that the j-map has degree 32, that its four cusp pole orders are $21, 7, 3, 1$, and that the designated w_3 satisfies $\Phi_3(j, j \circ w_3) = 0$, whereas w_7 and w_{21} do not. It also checks the point counts against the Hecke traces at primes through 43 away from 3 and 7.

In the function field one has

$$x^2 - (t^2 + 3t + 3)x - t^2 - 6t - 10 = 0, \qquad j - 1728 = H \cdot (\text{a rational function})^2, \qquad H = t(x + 2).$$

Write the cover as $z^2 = H$. The involution w_3 fixes t. Put $q = t/(x + 2)$. Then

$$\frac{w_3(H)}{H} = q^2, \qquad q\, w_3(q) = 1.$$

The two involutions lifting w_3 have the elliptic quotients

$$\begin{aligned} C_+ &: \quad U^2 = t(t^2 + 5t + 7), \quad U = z(1 + q), \\ C_- &: \quad U^2 = t(t^2 + t + 7), \quad U = z(1 - q). \end{aligned}$$

The identities defining these quotients are checked exactly. Both elliptic curves have rank zero by algebraic higher 2-isogeny descent. Their full rational torsion groups and the corresponding finite t-values are

Curve	Rational torsion	Finite t-values
C_+	C_2	0
C_-	C_6	$0, 1, 7$

Each also has the point at infinity. The fibers $t = 0, \infty$ on $X_0(21)$ are exactly its four cusps. At the remaining values the two x-coordinates are

t	x
1	$(7 \pm 3\sqrt{13})/2$
7	$(73 \pm 21\sqrt{13})/2.$

Since $\tau(x) = w_3(x)$, conjugation of any lift to the cover agrees with one of the two lifts of w_3. Its image on the corresponding elliptic quotient is rational. The complete rational point sets above therefore force

$$K = \mathbb{Q}(\sqrt{13}), \qquad t \in \{1, 7\}.$$

The corresponding j-invariants are

$$\begin{aligned} t = 1 &: \quad 6565897584689283072 \pm 1821052339310297088\sqrt{13}, \\ t = 7 &: \quad 75497472 \pm 20938752\sqrt{13}. \end{aligned}$$

They are neither 0 nor 1728. Thus every elliptic curve over K with one of these values is a quadratic twist of the model $E_j = \text{EllipticCurveFromjInvariant}(j)$.

5. Frobenius at 29

The prime 29 splits in $\mathbb{Q}(\sqrt{13})$. For both displayed j-invariants and both primes above 29, the certificate checks that E_j has good reduction, its 2-division polynomial splits completely, and its Frobenius trace has absolute value 6.

The actual E is a quadratic twist of E_j, with unchanged 2-division field. Therefore ψ is unramified and trivial on Frobenius at these primes: it is the faithful cubic 2-division character. If the quadratic twist were ramified, inertia would act on the original mod-7 representation as $-I$, since E_j and ψ are both unramified. This contradicts the trivial constituent supplied by rational 7-torsion. Hence the quadratic twist is unramified and its trace is $a \in \{6, -6\}$.

A rational Frobenius at 29 belongs to G_K, where the cubic multiplicity twist is now trivial. The Frobenius polynomial of A is consequently

$$P_{29}(T) = (T^2 - aT + 29)^2.$$

The same representation is unramified, so A has good reduction at 29. Prime-to-29 rational torsion injects into its reduction, and its order must divide

$$P_{29}(1) = (30 - a)^2 \in \{576, 1296\}.$$

Neither integer is divisible by 7. This contradiction completes the sextic case.

6. Conclusion

In both the cubic and sextic cases, rational 7-torsion precludes rational 2-torsion. The entire rational 2-primary group is then trivial, because every nontrivial finite 2-group has an element of order two. In all other geometric cases the existing argument bounds its order by four. This proves the theorem.

The exclusion of $[2, 28]$ concerns only the Q-simple geometrically split column. Its geometrically simple example is retained, its split-over-$\mathbb{Q}$ case is not settled here, and the combined geometrically split infinitude grade remains open. The same general bound excludes groups outside the census, such as cyclic [56], in the Q-simple geometrically split class.

7. Verification

The standalone certificate qsimple_228_checks.m checks every new numerical input with an assertion: the modular model and j-map, cusps and Hecke traces, identification of w_3, the genus of the discriminant cover, the exact quotient identities, algebraic rank-zero upper bounds, complete elliptic torsion sets, the four rational j-classes and their S_3 2-division groups, and both embeddings above 29 for each remaining quadratic fiber. Its log ends with `VERIFIED_228_MODULAR_CERTIFICATE_DONE`.

The proof has been independently reviewed, and the final certificate was independently rerun. The finite-field calculations at 29 were also recomputed separately. The completeness statements use algebraic descent and complete torsion enumeration, with no analytic-rank or BSD assumption. No bounded search is used as a nonexistence proof.

References

1. Rational 7-torsion and the 2-rank of geometrically split abelian surfaces, census proof of 10 November 2026: Proposition 2, the cyclic-field reduction, and the remarks on [2, 28].
2. No rational 63-torsion on a geometrically split abelian surface simple over $\mathbb{Q}$, census proof of 21 October 2026: Sections 5–7 and 10.2, including the general cubic untwisting construction.
3. No rational points of order 26 or 39 on geometrically split abelian surfaces, census proof of 21 October 2026: Section 8 and the lattice and level-structure steps of Proposition 9.1. The present proof repeats the transfer at 7 and supplies the new modular-cover calculation.
4. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366. Published paper. We use the isogeny and Tate-module endomorphism theorems; in Section 2.1 the required consequence is $\mathrm{End}_{G_L}(V_3(E_0)) = \mathbb{Q}_3$ for non-CM E_0.
5. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517. Primary paper: the good-reduction criterion and prime-to-residue-characteristic torsion injection.
6. Magma's small modular curve and j-map tools. The model and involution conventions are checked in the accompanying script. Its `TwoPowerIsogenyDescentRankBound` computations are algebraic upper bounds.