A GENUS-THREE HYPERELLIPTIC CURVE WITH RATIONAL JACOBIAN THREE-TORSION OF RANK THREE

ROY VAN RIJN

Abstract. We exhibit a hyperelliptic curve of genus three over the rationals whose Jacobian has rational three-torsion isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$. This supplies the genus-three example asked for by Levin, Yan and Wiljanen. The curve is a double cover of a rational conic with two commuting sign involutions. Three explicit maps of degree eight to elliptic curves with rational points of order three produce independent torsion classes; the Weil pairing gives the matching upper bound. Pullback and pushforward give dual isogenies of degree 2^9. Consequently, for every quadratic twist and every $n \geq 1$, its 3^n-Selmer group and 3^n-torsion in the Tate–Shafarevich group identify with those of the product of the three elliptic twists, without a finiteness assumption. We also determine all eight rational points and the full Mordell–Weil group, which is finite with invariant factors $[3, 6, 12]$.

hexagon:2611.01278v1

1. The existence question and the example

For a smooth projective curve $C/\mathbb{Q}$ of genus g, the Weil pairing bounds the dimension of $\mathrm{Jac}(C)(\mathbb{Q})[3]$ over $\mathbb{F}_3$ by g. Levin, Yan and Wiljanen [2, Theorem 9 and the following discussion] give hyperelliptic examples attaining this bound in genera one, two and four. Their rank-three example has genus four, and they ask whether a hyperelliptic curve with genus three and rational Jacobian three-torsion of rank three exists. We give such a curve.

Theorem 1. *Let $C/\mathbb{Q}$ be the smooth projective model of $R^2 = F(t)$, where*

$$\begin{aligned} F(t) = t^8 - 6t^7 - t^6 + 18t^5 + 93t^4 \\ - 36t^3 - 4t^2 + 48t + 16. \end{aligned} \tag{1}$$

Then C is hyperelliptic of genus three and

$$\mathrm{Jac}(C)(\mathbb{Q})[3] \simeq (\mathbb{Z}/3\mathbb{Z})^3.$$

For $(h_1, h_2, h_3) = (3/2, -3/4, -7/6)$, set

$$E_i : \quad Y^2 = X^3 + (h_i X + h_i + 1)^2. \tag{2}$$

There are explicit morphisms $\pi_i : C \to E_i$ of degree eight. Writing $A = E_1 \times E_2 \times E_3$ and $J = \mathrm{Jac}(C)$, the maps

$$\Phi = \sum_i \pi_i^* : A \longrightarrow J, \qquad \Psi = (\pi_{1*}, \pi_{2*}, \pi_{3*}) : J \longrightarrow A$$

are dual isogenies satisfying

$$\Psi\Phi = [8]_A, \qquad \Phi\Psi = [8]_J, \qquad \deg \Phi = \deg \Psi = 2^9. \tag{3}$$

The construction belongs to the classical method of splitting a Jacobian into elliptic factors. In particular, Howe, Leprévost and Poonen [1, Proposition 14] construct hyperelliptic genus-three Jacobians by gluing three elliptic curves when their twisting factor vanishes. Our proof gives the conic, the three quotients and all maps directly; it does not require an application of that proposition with implicit gluing data.

2020 *Mathematics Subject Classification.* 11G30, 11G10, 14H40.

Key words and phrases. hyperelliptic curve, rational torsion, split Jacobian, Selmer group.

The reason three independent classes survive is simple. Each elliptic curve in (2) has a rational point of order three. Pulling it back along a degree-eight map cannot kill it, because pullback followed by pushforward is multiplication by eight on the elliptic curve. Independence is a different issue: three maps alone would not suffice. Here the two sign involutions place the three pullbacks in different characters of a group of order four. Since four is invertible modulo three, these characters separate the classes. The same separation makes the off-diagonal push–pull maps vanish, and gives (3).

The assertion concerns $J(\mathbb{Q})[3]$, the subgroup killed by three. Theorem 3 below determines the full rational torsion. The Jacobian is geometrically nonsimple because of its elliptic factors. Müller and Reitsma [3, Theorem 1.1 and Remark 1.2] distinguish the occurrence of an exact full torsion group from that of a subgroup, and study geometrically simple examples. Theorem 1 addresses the existence question above. The full torsion in our example has invariant factors $[3, 6, 12]$, so it does not realize their possible exception $[3, 3, 3]$, even without the geometric simplicity condition.

The isogeny has a further consequence. For an abelian variety $B/\mathbb{Q}$ and a squareclass $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, let B^d denote the quadratic twist by the automorphism $[-1]$. We use $\mathrm{Sel}_m(B/\mathbb{Q})$ for the Selmer group for multiplication by m, and $\mathrm{Sha}(B/\mathbb{Q})$ for the Tate–Shafarevich group.

Theorem 2. *For the varieties in Theorem 1, every rational squareclass d and every integer $n \geq 1$, the twisted maps induce isomorphisms*

$$\mathrm{Sel}_{3^n}(J^d/\mathbb{Q}) \simeq \bigoplus_{i=1}^{3} \mathrm{Sel}_{3^n}(E_i^d/\mathbb{Q}),$$
$$\mathrm{Sha}(J^d/\mathbb{Q})[3^n] \simeq \bigoplus_{i=1}^{3} \mathrm{Sha}(E_i^d/\mathbb{Q})[3^n].$$

They also identify the full three-primary Tate–Shafarevich groups. No finiteness assumption on these groups is required.

Theorem 3. *For the curve of Theorem 1,*

$$C(\mathbb{Q}) = \{(-1, \pm 9), (0, \pm 4), (2, \pm 36), \infty_+, \infty_-\}, \qquad J(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}.$$

Here R/t^4 has value ± 1 at $\infty_\pm$. In particular J has rank zero and 216 rational points. Its conductor is 243000.

2. The conic and its three elliptic quotients

Put $d_0 = 3(t^2 + 2)$ and define functions on C by

$$x = \frac{t^2 - 4t - 2}{d_0}, \qquad y = \frac{-2t^2 - 4t + 4}{d_0}, \qquad w = \frac{12R}{d_0^2}. \tag{4}$$

They satisfy

$$6x^2 + 3y^2 = 2, \qquad w^2 = -\frac{9}{2}x^4 - \frac{117}{16}y^4 + \frac{59}{18}. \tag{5}$$

Conversely, generically $t = (y - 2/3)/(x - 1/3)$. Thus (5) is a birational model of C; it comes from parametrizing the conic by lines through $(1/3, 2/3)$.

Modulo seven the polynomial F and its derivative are coprime. As F is monic of degree eight, it is squarefree over $\mathbb{Q}$. The double cover of $\mathbf{P}^1$ therefore has eight simple branch points, and Riemann–Hurwitz gives genus three. In particular all nonconstant rational maps below extend uniquely to morphisms of smooth projective curves. Apparent poles in their formulas create no additional restrictions on the theorem.

The conic model has commuting involutions

$$\sigma_x(x, y, w) = (-x, y, w), \qquad \sigma_y(x, y, w) = (x, -y, w).$$

Together they generate a group $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$. The quotients by $\sigma_x, \sigma_y, \sigma_x\sigma_y$, respectively, have coordinates and equations

i	z_i	v_i	a_i	b_i	c_i
1	y	w	$-135/16$	$3/2$	$25/9$
2	x	$w/2$	$-135/16$	$39/8$	$1/144$
3	x/y	$-w/(3y^2)$	$25/9$	$59/18$	$1/144$

$$v_i^2 = a_i z_i^4 + b_i z_i^2 + c_i. \tag{6}$$

For the first two rows, eliminate x^2 or y^2 in (5). For the third, use $y^2 = 2/(3(2z_3^2+1))$. These substitutions give the displayed equations. They also show that each fixed field is generated by the stated z_i, v_i: adjoining x, y, or y, respectively, recovers $\mathbb{Q}(C)$ in degree two.

Each quartic on the right in (6) is squarefree: $a_i c_i \neq 0$ and $b_i^2 - 4a_i c_i \neq 0$. Its smooth projective double cover has genus one, with a rational point $(0, \sqrt{c_i})$. We next give the degree-four map from each such curve to the desired elliptic target.

Lemma 4. *Let $a, b, c \in \mathbb{Q}$ with $ac(b^2 - 4ac) \neq 0$. On the genus-one curve $v^2 = az^4 + bz^2 + c$, set*

$$U = \frac{v^2}{4z^2}, \qquad V = \frac{v}{8z}\left(az^2 - \frac{c}{z^2}\right). \tag{7}$$

These functions define a morphism of degree four to

$$V^2 = U\left(U^2 - \frac{b}{2}U + \frac{b^2 - 4ac}{16}\right). \tag{8}$$

The involution $(z, v) \mapsto (-z, v)$ sends (U, V) to $(U, -V)$.

Proof. Directly,

$$\frac{V^2}{U} = \frac{1}{16}(az^2 - c/z^2)^2 = U^2 - \frac{b}{2}U + \frac{b^2 - 4ac}{16}.$$

The cubic in (8) is squarefree by the hypotheses: its quadratic factor has nonzero constant term and discriminant ac. Hence the target is elliptic. As a function of z,

$$U = \frac{az^4 + bz^2 + c}{4z^2}$$

has degree four. The map z from the quartic curve to $\mathbf{P}^1$ has degree two, while U on the target elliptic curve has degree two. The tower of function fields therefore gives degree $(2 \cdot 4)/2 = 4$ for the displayed map. The final assertion follows directly from the formulas. □

Apply Lemma 4 to each row, and put $X_i = U_i - 1$, $Y_i = V_i$. In all three cases substitution into (8) gives (2). More explicitly the coefficient identities are

$$h_i^2 = 3 - b_i/2, \quad 2h_i(h_i+1) = 3 - b_i + (b_i^2 - 4a_i c_i)/16, \quad (h_i+1)^2 = 1 - b_i/2 + (b_i^2 - 4a_i c_i)/16.$$

Composing the quotient map of degree two with this map of degree four gives π_i of degree eight. The equations of the targets are nonsingular, since their discriminants are $16(h_i+1)^3(4h_i^3 - 27(h_i+1)) \neq 0$.

The action on the maps is

	σ_x	σ_y
π_1	$+$	$-$
π_2	$-$	$+$
π_3	$-$	$-$

(9)

where a minus sign means composition with $[-1]$ on the elliptic curve. For π_3, either sign change sends z_3 to $-z_3$ and fixes v_3; for the other two maps this is immediate from (6). The lemma proves all the signs.

3. The three rational torsion classes

On E_i, let O_i be the point at infinity and put

$$P_i = (0, -h_i - 1), \qquad f_i = Y + h_i X + h_i + 1.$$

The line $f_i = 0$ meets the cubic only at P_i, with intersection multiplicity three, because substitution leaves $X^3 = 0$. Also f_i has a pole of order three at O_i. Consequently

$$\operatorname{div}(f_i) = 3(P_i) - 3(O_i). \tag{10}$$

Since $h_i + 1 \neq 0$, the point $P_i \neq O_i$ has order exactly three.

Define $D_i = \pi_i^*([P_i - O_i]) \in J(\mathbb{Q})[3]$. Push–pull for finite morphisms of curves gives

$$\pi_{i*}\pi_i^* = [\deg \pi_i] = [8] \quad \text{on } E_i = \operatorname{Jac}(E_i).$$

It follows that $D_i \neq 0$. By (9), the action of G on D_i is the corresponding nontrivial character $\chi_i : G \to \{\pm 1\}$. For clarity, if $\sum_i e_i D_i = 0$ with $e_i \in \mathbb{F}_3$, apply

$$\frac{1}{4} \sum_{g \in G} \chi_j(g) g^*$$

on $J[3]$. Character orthogonality yields $e_j D_j = 0$. Thus each $e_j = 0$, and the three classes are independent.

Finally the canonical principal polarization gives a nondegenerate Galois-equivariant alternating pairing

$$e_3 : J[3] \times J[3] \longrightarrow \mu_3.$$

On rational points its value lies in $\mu_3(\mathbb{Q}) = \{1\}$. Hence $J(\mathbb{Q})[3]$ is an isotropic subspace of the six-dimensional symplectic $\mathbb{F}_3$-space $J[3](\overline{\mathbb{Q}})$, so its dimension is at most three. This proves the torsion assertion of Theorem 1.

The pulled-back functions $f_i \circ \pi_i$ make the classes explicit as cube-divisor functions by (10). The proof uses their divisors on the curve and requires no specialization to quadratic number fields.

4. Dual isogenies and descent on every quadratic twist

We first finish the isogeny assertion in Theorem 1. If $i \neq j$, choose $g \in G$ with $\chi_i(g) = -\chi_j(g)$. Its action g^* on J is an involution. Equations (9) give

$$g^*\pi_j^* = \chi_j(g)\pi_j^*, \qquad \pi_{i*}g^* = \chi_i(g)\pi_{i*}.$$

Therefore $\pi_{i*}\pi_j^* = -\pi_{i*}\pi_j^*$. The group of homomorphisms of abelian varieties has no integer torsion: the image of a homomorphism killed by a nonzero integer is connected and contained in a finite group scheme, and in characteristic zero must be zero. Thus all cross terms vanish. The diagonal terms are [8], proving $\Psi\Phi = [8]_A$.

It follows that $\ker \Phi \subset A[8]$ is finite. Since A and J both have dimension three, Φ is an isogeny. Now $(\Phi\Psi - [8]_J)\Phi = 0$, and surjectivity of Φ gives $\Phi\Psi = [8]_J$. Pullback and pushforward are dual under the canonical principal polarizations of curve Jacobians. Hence $\deg \Phi = \deg \Psi$, and

$$(\deg \Phi)^2 = \deg[8]_A = 8^6$$

gives $\deg \Phi = 8^3 = 2^9$, as claimed.

Proof of Theorem 2. The homomorphisms Φ and Ψ are defined over $\mathbb{Q}$ and commute with $[-1]$. They therefore descend on every quadratic twist to maps $\Phi^d : A^d \to J^d$ and $\Psi^d : J^d \to A^d$ with the same composites [8]. Here $A^d = E_1^d \times E_2^d \times E_3^d$.

Fix $m = 3^n$, and choose $a \in \mathbb{Z}$ with $8a \equiv 1 \pmod{m}$. On m-torsion, Φ^d and $a\Psi^d$ are inverse Galois-module maps. They induce inverse maps on global and local first cohomology of these torsion modules. For each completion $k = \mathbb{Q}_v$, they also give inverse maps

$$A^d(k)/mA^d(k) \longleftrightarrow J^d(k)/mJ^d(k).$$

Indeed the composites are multiplication by $8a$, which is the identity modulo m. Naturality in the Kummer exact sequence

$$0 \longrightarrow B[m] \longrightarrow B \xrightarrow{[m]} B \longrightarrow 0$$

identifies the images of these quotients in $H^1(k, B[m])$. This argument applies at every place, including three and the real place. Defining the Selmer group as the global cohomology classes lying in all these local Kummer images proves the first isomorphism. Cohomology and the Kummer conditions for a finite product are the direct sums of those for its factors.

For the second assertion use

$$\mathrm{Sha}(B/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, B) \longrightarrow \prod_v H^1(\mathbb{Q}_v, B)\right).$$

Functoriality gives maps on these kernels, with composites [8]. On the subgroups killed by 3^n, multiplication by a again gives inverse maps. On the union of these subgroups, multiplication by eight is an automorphism: on every element of finite three-power order its inverse is the unique inverse modulo that order. Thus the full three-primary groups are also isomorphic. The argument uses no finiteness assumption. □

5. Rational points and full rational torsion

Proof of Theorem 3. Exact elliptic two-descent gives rank bounds $(0, 0)$ for each of the three curves (2). The respective Cremona labels are $90a1, 90b1, 30a2$, with conductors $90, 90, 30$. Thus the isogeny gives rank zero and conductor $90 \cdot 90 \cdot 30 = 243000$ for J.

First determine the rational points. In the coordinates of (2), the six points of $E_1(\mathbb{Q})$ are

$$O, \quad (-1, 0), \quad (0, \pm 5/2), \quad (5, \pm 15).$$

There is no rational point at infinity on the conic $6x^2 + 3y^2 = 2$, and $y = 0$ would require $x^2 = 1/3$. Consequently $U = w^2/(4y^2) = X + 1$ is finite and belongs to $\{0, 1, 6\}$. Its fibre satisfies

$$-\frac{135}{16}y^4 + \left(\frac{3}{2} - 4U\right)y^2 + \frac{25}{9} = 0.$$

For $U = 0, 6$, the discriminants of these quadratics in y^2 are 96 and 600 respectively, both nonsquares in $\mathbb{Q}$. For $U = 1$ the polynomial factors as

$$-\frac{135}{16}(y - 2/3)(y + 2/3)(y^2 + 20/27).$$

It follows that $y = \pm 2/3$, then $x = \pm 1/3$ and $w = \pm 4/3$. The parametrization (4) gives $t = -1, 0, 2, \infty$. Substitution into (1) gives exactly the eight stated points, including both branches at infinity.

To determine torsion, good reduction and the elliptic decomposition give

p	7	11	13	17	19
$\#J(\mathbb{F}_p)$	432	1296	3888	3456	13824.

The gcd is $432 = 16 \cdot 27$. Thus Theorem 1 already determines the full three-primary subgroup, and it remains to determine the two-primary subgroup H.

Define the rational divisor classes

$$I = [\infty_- - \infty_+] \in J(\mathbb{Q}), \qquad P = [(0,4) - \infty_+] \in J(\mathbb{Q}).$$

Write $\bar{I}, \bar{P}$ for their reductions at seven and $\bar{\infty}_+$ for the reduction of ∞_+. Let $Q = [D - 2\bar{\infty}_+] \in J(\mathbb{F}_7)$, where D is the closed point of degree two defined by $t^2 + 1 = R - t + 2 = 0$.

Divisor-class arithmetic over $\mathbb{F}_7$ shows that $27\bar{I}, 27\bar{P}, 27Q$ are killed by four and generate subgroups of orders 4, 8, 16 successively. Precisely four of the resulting sixteen classes are killed by two. Since the two-part of $\#J(\mathbb{F}_7)$ is 16, we obtain

$$J(\mathbb{F}_7)[2^\infty] \simeq (\mathbb{Z}/4\mathbb{Z})^2, \qquad H \hookrightarrow (\mathbb{Z}/4\mathbb{Z})^2.$$

The same computation shows that $3\bar{I}$ has order four.

We next exhibit a rational point of order two that is not a double. Let $T = 3P$, and set

$$g = t^6 - 3t^5 - 3t^4 - 12t^3 + 6t^2 - 12t - 8.$$

The identity $g^2 - F(t)(t^2+2)^2 = -200t^6$ gives

$$\operatorname{div}\big(g + (t^2+2)R\big) = 6(0,4) - 6\infty_+,$$

so $2T = 0$. To show that T is not a double, work on the good reduction at 17. For $L = \mathbb{F}_{17}[\theta]/(F(\theta))$, the even-degree descent homomorphism

$$J(\mathbb{F}_{17})/2J(\mathbb{F}_{17}) \longrightarrow L^\times/(L^{\times 2}\mathbb{F}_{17}^\times)$$

sends $[(a,b) - \infty_+]$ to $a - \theta$. The rational infinity has trivial image; see Poonen–Schaefer [4, Section 5, Proposition 5.1 and (8)]. The rational point identifies degree-zero rational divisor classes with the Jacobian points, as required here. We use only that doubles have trivial image, not injectivity of the fake descent map. The image of the reduction of T is represented by $(-\theta)^3$, which has the same class as $-\theta$. The polynomial t^2+5 is an irreducible factor of F mod 17. In the corresponding factor $\mathbb{F}_{17^2}$, the norm of $-\theta$ is 5. This is a nonsquare in $\mathbb{F}_{17}$, and multiplying by a scalar $c \neq 0$ changes the norm to $5c^2$. Hence the image is nontrivial, even modulo scalars. Thus $T \neq 0$ and $T \notin 2J(\mathbb{Q})$.

Finally an explicit Pell identity supplies rational four-torsion. Put

$$\begin{aligned} A = {} & -t^8 + 8t^7 - 4t^6 - 52t^5 - 115t^4 \\ & + 296t^3 + 746t^2 + 764t - 139. \end{aligned}$$

Let B be the polynomial part of $A\sqrt{F}$ at infinity, with $\sqrt{F} = t^4 - 3t^3 - 5t^2 + \cdots$. Exact multiplication gives $B^2 - FA^2 = 19440000$. The leading terms give

$$\operatorname{div}(B + AR) = 12\infty_- - 12\infty_+.$$

Thus $3I$ is killed by four. Since $3\bar{I}$ has order four, so does $3I$. Its nonzero double cannot equal T, since T is not divisible by two. Consequently $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq H$. A larger subgroup of $(\mathbb{Z}/4\mathbb{Z})^2$ would be that whole group, in which every element of order two is a double, contradicting the property of T. Therefore $H \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Combining the two primary parts proves the asserted invariant factors. □

AI assistance and review. ChatGPT (OpenAI) assisted with mathematical arguments, literature checks, exposition, proof review and verification code.

References

[1] E. W. Howe, F. Leprévost and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), 315–364. arXiv:math/9809210.

[2] A. Levin, S. Yan and L. Wiljanen, *Quadratic fields with a class group of large 3-rank*, arXiv:1910.12276v1 (2019).

[3] J. S. Müller and B. Reitsma, *Computing torsion subgroups of Jacobians of hyperelliptic curves of genus 3*, arXiv:2211.03372v4 (2023).

[4] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188. Author's version.