# ELLIPTIC CURVES WITH TORSION $\mathbb{Z}/5\mathbb{Z}$: EXACT RANK FOUR OVER $\mathbb{Q}(k)$ AND RANK AT LEAST FIVE INFINITELY OFTEN

ANDREJ DUJELLA AND JUAN CARLOS PERAL

Abstract. We give two elliptic curves over $\mathbb{Q}(k)$ with torsion group $\mathbb{Z}/5\mathbb{Z}$ and rank exactly 4, with four explicit independent points. The upper bounds come from reducing the relevant elliptic surfaces modulo suitable primes and are unconditional. They match the known lower bound for the generic rank with this torsion, due to Eroshkin, and are not isomorphic to Eroshkin's curve or to each other: their parametrising maps to $X_1(5)$ have degree 8 instead of 12, the constructions are dihedral rather than biquadratic, and their branch loci differ. In each case two of the points come from a "doubling" step in the spirit of Jaswal. Adding one further condition to the second curve, coming from a quadratic twist over an intermediate conic, gives a fifth independent point over a genus-one curve of rank two. Hence there are infinitely many elliptic curves over $\mathbb{Q}$ with torsion $\mathbb{Z}/5\mathbb{Z}$ and rank at least 5, improving the known bound $C(\mathbb{Z}/5\mathbb{Z}) \geq 4$ to $C(\mathbb{Z}/5\mathbb{Z}) \geq 5$.

## 1. Results

Every elliptic curve over $\mathbb{Q}$ with a point of order 5 is a fibre of the universal curve

$$E_t:\ y^2 + (1-t)\,xy - t\,y = x^3 - t\,x^2,$$

with the 5-torsion point $P = (0,0)$; its nonzero multiples have $x$-coordinates 0 and $t$. As an elliptic surface over the $t$-line it is rational, with fibres $I_5$ at $t = 0, \infty$ and $I_1$ at the roots of $t^2 - 11t - 1$, so $E(\mathbb{Q}(t))$ has rank 0. The previously known lower bounds in Dujella's table [1] were $G(\mathbb{Z}/5\mathbb{Z}) \geq 4$ for curves over $\mathbb{Q}(t)$ (Eroshkin, 2020) and $C(\mathbb{Z}/5\mathbb{Z}) \geq 4$ for infinitely many curves over $\mathbb{Q}$ (Eroshkin, 2009).

For a point with $x$-coordinate $x$ on $E_t$, the $y$-coordinate is rational exactly when the discriminant

$$\mathscr{D}_t(x) = \big((1-t)x - t\big)^2 + 4\big(x^3 - tx^2\big)$$

is a square.

**Theorem 1** (First family)**.** *Let*

$$u = -\frac{20\,(k^2+1)^2}{(2k^2+5k-2)(5k^2-8k-5)}, \qquad t = \frac{u^2-4}{3(u^2-1)}.$$

*Then $E_t$ over $\mathbb{Q}(k)$ has torsion group $\mathbb{Z}/5\mathbb{Z}$ and rank exactly 4; points whose $x$-coordinates are*

$$x_1 = -\frac{t}{3t-1}, \qquad x_2 = -\frac{5153632t^3 - 3843928t^2 + 1025729t - 1024}{1025^2\,(3t-1)},$$

$$x_3 = \frac{u^2-4}{9(u-1)^2}, \quad x_4 = \frac{u^2-4}{9(u+1)^2}$$

*generate a subgroup of finite index in $E_t(\mathbb{Q}(k))$.*

**Theorem 2** (Second family)**.** *Let*

$$u = \frac{3k^4 + 16k^3 - 18k^2 - 16k + 3}{3(k^2+1)^2}, \qquad t = \frac{5 - 9u^2}{90(u^2-1)}.$$

*Then $E_t$ over $\mathbb{Q}(k)$ has torsion group $\mathbb{Z}/5\mathbb{Z}$ and rank exactly 4; points whose $x$-coordinates are*

$$x_1 = -\frac{8t+1}{20(10t+1)}, \qquad x_2 = \frac{t(27t+4)}{4(8t+1)},$$

$$x_3 = \frac{P(u)}{21600\,(u-1)(3u-5)^2(3u+5)(3u^2+4u+5)^2}, \quad x_4 = x_3\big|_{u\mapsto -u}$$

*generate a subgroup of finite index in $E_t(\mathbb{Q}(k))$, where*

$$P(u) = 19683u^9 - 715149u^8 - 323676u^7 + 4481892u^6 + 6257250u^5 \\ - 9618750u^4 - 7357500u^3 + 9562500u^2 - 10078125u + 6171875.$$

**Theorem 3** (Rank five over an elliptic curve)**.** *Let $C'$ be the curve*

$$C' : \ w^2 = -5\,(3k^4 + 116k^3 - 218k^2 - 116k + 3),$$

*which has genus one and the rational point $(k, w) = (-23, 1850)$; its Jacobian is $y^2 = x^3 + x^2 - 73x + 183$, of conductor 20800 and rank 2. Over the function field $\mathbb{Q}(C') = \mathbb{Q}(k, w)$, the curve $E_t$ with $t = t(k)$ as in Theorem 2 has torsion group $\mathbb{Z}/5\mathbb{Z}$ and rank at least 5: besides the four points of Theorem 2 it has the point with*

$$x_5 = -\frac{(s^2-3s-9)\,P_7(s)}{3(s-6)^2(s+3)^2(s+6)(2s+3)^2(s^2+2s-39)}, \qquad s = \frac{6(k^2+k-1)}{k^2-4k-1},$$

*where $P_7(s) = 2s^7 + 21s^6 - 54s^5 - 1161s^4 - 1701s^3 + 15552s^2 + 45198s + 30618$.*

**Corollary 4.** *There are infinitely many elliptic curves over $\mathbb{Q}$, with infinitely many distinct $j$-invariants, whose torsion group is $\mathbb{Z}/5\mathbb{Z}$ and whose rank is at least 5. Thus $C(\mathbb{Z}/5\mathbb{Z}) \geq 5$.*

In Theorems 1 and 2, $t$ is a rational function of $k$ of degree 8. For instance, in Theorem 2,

$$t = -\frac{k^8 + 24k^7 + 32k^6 - 168k^5 - 50k^4 + 168k^3 + 32k^2 - 24k + 1}{40k\,(6k^6 + 7k^5 - 42k^4 - 14k^3 + 42k^2 + 7k - 6)}.$$

## 2. Lower bounds

The lower bounds use the following observation.

**Lemma 5.** *Let $L$ be a field, $K = L(r, s)$ a biquadratic extension with $r^2, s^2 \in L$, and $E/L$ an elliptic curve. If $Q_1, \ldots, Q_4 \in E(K)$ have infinite order and lie in the eigenspaces of $E(K) \otimes \mathbb{Q}$ for $\mathrm{Gal}(K/L)$ belonging to four distinct characters, then they are independent.*

*Proof.* Eigenspaces for distinct characters intersect trivially and are linearly independent, and each $Q_i \otimes 1$ is a nonzero vector in its eigenspace. □

A point whose $y$-coordinate involves a square root $\sqrt{c}$ only through $2y + a_1x + a_3 = \sqrt{c} \cdot w$ with $w \in L$ is sent to its negative by the automorphisms changing the sign of $\sqrt{c}$; so it lies in the eigenspace of the character attached to $c$.

*Proof of rank $\geq 4$ in Theorem 1.* Put $L = \mathbb{Q}(u)$, $h = u(41u-80)$, $\tilde{h} = u(41u+80)$, and $K = L(r, s)$ with $r^2 = h$, $s^2 = \tilde{h}$. The classes of $h$ and $\tilde{h}$ in $L^\times/L^{\times 2}$ are independent, so $K/L$ is biquadratic. With $D = (2k^2 + 5k - 2)(5k^2 - 8k - 5)$ and $u$ as in the theorem,

$$r = \frac{20(k^2+1)(9k^2+2k-9)}{D}, \qquad s = \frac{20(k^2+1)(k^2-18k-1)}{D},$$

so $K \subseteq \mathbb{Q}(k)$, and $K = \mathbb{Q}(k)$ since both have degree 4 over $L$. Let $\delta = (3t-1)(3t-4)$ and $q = -(1573t+36)(3t-1)$. Direct calculation gives

$$\mathscr{D}_t(x_1) = \delta\Big(\frac{2t^2}{(3t-1)^2}\Big)^2, \qquad \mathscr{D}_t(x_2) = q\Big(\frac{2F(t)}{1025^3(3t-1)^2}\Big)^2,$$
$$\mathscr{D}_t(x_3) = h\Big(\frac{(u-2)^2(u+2)}{27(u-1)^3(u+1)}\Big)^2, \quad \mathscr{D}_t(x_4) = \tilde{h}\Big(\frac{(u-2)(u+2)^2}{27(u-1)(u+1)^3}\Big)^2,$$

with $F(t) = 271502704t^4 - 169959988t^3 + 15426651t^2 - 342512t - 87296$, and

$$\delta = \Big(\frac{3u}{u^2-1}\Big)^2, \qquad q = \Big(\frac{rs}{u(u^2-1)}\Big)^2.$$

Hence the four points lie in $E_t(K)$, in the eigenspaces of the trivial character, the product character, the character of $r$ and the character of $s$ respectively.

At $k = 1/2$ we have $u = 125/31$ and $t_0 = 1309/4888$. The fibre has good reduction at 59 and 71, with $\#E_{t_0}(\mathbb{F}_{59}) = 70$ and $\#E_{t_0}(\mathbb{F}_{71}) = 75$, so its torsion subgroup is exactly $\mathbb{Z}/5\mathbb{Z}$. The specialised points have $x$-coordinates $1309/961$, $566247748463/1206156099122$, $1309/8836$ and $1309/24336$, none of which is 0 or $t_0$; so they have infinite order, hence so do the four points over $\mathbb{Q}(k)$. Lemma 5 gives independence. Finally, $E_t(\mathbb{Q}(k))_{\mathrm{tors}}$ injects into $E_{t_0}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z}$ and contains $P$. □

*Proof of rank $\geq 4$ in Theorem 2.* Put $L = \mathbb{Q}(u)$, $h = 2(3u+5)$, $\tilde{h} = 2(5-3u)$, $K = L(r,s)$ with $r^2 = h$, $s^2 = \tilde{h}$; again $K/L$ is biquadratic. For $u$ as in the theorem,

$$r = -\frac{4(k^2+k-1)}{k^2+1}, \qquad s = \frac{2(k^2-4k-1)}{k^2+1},$$

so $K = \mathbb{Q}(k)$. Let $\delta = 5(10t+1)(18t+1)$ and $p = (8t+1)(18t+1)$. Direct calculation shows that $\mathscr{D}_t(x_1)$, $\mathscr{D}_t(x_2)$, $\mathscr{D}_t(x_3)$ and $\mathscr{D}_t(x_4)$ are respectively $\delta$, $p$, $h$ and $\tilde{h}$ times squares in $\mathbb{Q}(t)$ or $L$, and that

$$\delta = \Big(\frac{4u}{3(u^2-1)}\Big)^2, \qquad p = h\tilde{h}\Big(\frac{u}{15(u^2-1)}\Big)^2.$$

So the four points lie in $E_t(K)$, in the eigenspaces of the trivial character, the product character, the character of $r$ and the character of $s$.

At $k = 3/2$ we have $t_0 = -31919/604800$. The fibre has good reduction at 11 and 13, with $\#E_{t_0}(\mathbb{F}_{11}) = 15$ and $\#E_{t_0}(\mathbb{F}_{13}) = 20$, so its torsion subgroup is exactly $\mathbb{Z}/5\mathbb{Z}$, and none of the four specialised $x$-coordinates is 0 or $t_0$. The proof concludes as before. □

## 3. Upper bounds

**Decomposition of the rank.** In both theorems $\mathbb{Q}(u) = \mathbb{Q}(t)(\sqrt{\delta})$ and $\mathbb{Q}(k) = \mathbb{Q}(u)(\sqrt{h}, \sqrt{\tilde{h}})$ is biquadratic over $\mathbb{Q}(u)$, where $\tilde{h} = h(-u)$. Write $E^d$ for the quadratic twist $d\,w^2 = \mathscr{F}_t(x)$ of the universal curve, where $\mathscr{F}_t(x) = 4x^3 + (t^2-6t+1)x^2 + 2(t^2-t)x + t^2$, and $E_\varphi$ for the pullback of $E$ to the $u$-line. Let

$$r_d = \operatorname{rank} E^d(\mathbb{Q}(t)), \qquad r_h = \operatorname{rank} E^h_\varphi(\mathbb{Q}(u)).$$

The universal curve is an extremal rational elliptic surface (trivial lattice of rank $2+4+4 = 10$), so $\operatorname{rank} E(\mathbb{Q}(t)) = 0$ by the Shioda–Tate formula. Decomposing under $\mathrm{Gal}(\mathbb{Q}(k)/\mathbb{Q}(u))$ and then under $\mathrm{Gal}(\mathbb{Q}(u)/\mathbb{Q}(t))$, and using that $h\tilde{h}$ is the pullback of the class $q$ (Theorem 1) or $p$ (Theorem 2), and that $u \mapsto -u$ fixes $t$ and interchanges $h$ and $\tilde{h}$, we get

$$\operatorname{rank} E_t(\mathbb{Q}(k)) = r_\delta + r_c + r_{c\delta} + 2r_h,$$

where $c = q$ for Theorem 1 and $c = 5(8t+1)(10t+1)$ for Theorem 2 (so that $c\delta \equiv p$ there). By Section 2, $r_\delta, r_{c\delta}$ (Theorem 2) or $r_\delta, r_c$ (Theorem 1), and $r_h$ are at least 1.

**Reduction of the surfaces.** For each twist, let $X$ be the corresponding elliptic surface over $\mathbb{P}^1$ (a K3 surface for the twists over the $t$-line, with fibres $2I_5+2I_1+2I_0^*$; a surface with $\chi=3$ for the $h$-twists, with fibres $4I_5+4I_1+2I_0^*$). If $\ell$ is a prime not dividing $2\cdot 3\cdot 5$ at which the branch points of the twist stay distinct from each other and from the singular fibres, then $X$ has good reduction at $\ell$ with the same fibre configuration. Let

$$L_\ell(T)=\det\bigl(1-T\,\mathrm{Frob}_\ell \mid H^1(\mathbb{P}^1_{\overline{\mathbb{F}}_\ell}, j_*R^1f_*\mathbb{Q}_{\ell'})\bigr),$$

of degree 4 for the twists over the $t$-line and 8 for the $h$-twists. Specialisation of Néron–Severi groups is injective [6], and so is the cycle class map on $\mathrm{NS}\otimes\mathbb{Q}_{\ell'}$. By the Shioda–Tate decomposition [7], the Mordell–Weil group tensored with $\mathbb{Q}_{\ell'}$ is the orthogonal complement of the trivial lattice (spanned by the zero section, a fibre and the fibre components), and in $H^2(X_{\overline{\mathbb{F}}_\ell},\mathbb{Q}_{\ell'}(1))$ this complement lies in the parabolic cohomology above, Tate-twisted. The trivial lattice is stable under Frobenius, so the orthogonal projection onto its complement commutes with Frobenius. A section defined over the constant field $\mathbb{Q}$ has a Galois-invariant class, whose specialisation is fixed by $\mathrm{Frob}_\ell$ on $H^2(1)$; so the Mordell–Weil group over $\mathbb{Q}$ embeds, after $\otimes\mathbb{Q}_{\ell'}$, into the parabolic cohomology as classes on which Frobenius acts by $\ell$ (compare [8]). Hence

$$r\le \mathrm{ord}_{T=1/\ell}\,L_\ell(T),$$

unconditionally. By the Grothendieck–Lefschetz formula, $L_\ell(T)=\exp\bigl(\sum_{n\ge1}S_nT^n/n\bigr)$, where $S_n$ is the sum of the local traces over $\mathbb{P}^1(\mathbb{F}_{\ell^n})$ ($\ell^n+1-\#$ points for good fibres, $\pm1$ for split or non-split multiplicative fibres, 0 at $I_0^*$). For the twist by $d$, the local trace at a fibre $t$ is $\chi(d(t))\,a_t$, where $\chi$ is the quadratic character of $\mathbb{F}_{\ell^n}$ and $a_t$ is the local trace of $E_t$ (both fibres $t=0,\infty$ of $E$ are split of type $I_5$); so one point count of $E_t$ over each field serves all twists. The polynomials are fixed by $S_1,\dots,S_4$ and the functional equation $c_{d-i}=\varepsilon\,\ell^{d-2i}c_i$ ($d=\deg L_\ell$), up to the sign $\varepsilon$; when both signs are possible, the sign giving multiplicity 0 for an $h$-twist is excluded by the known section.

**Data.** For Theorem 1 all bounds come from $\ell=29$, for Theorem 2 from $\ell=29,31,47$. In each case the leading coefficient and discriminant of the twisting polynomial, its resultant with $t(t^2-11t-1)$ (respectively with the polynomial $W(u)$ cutting out the singular fibres of $E_\varphi$), and $125=\mathrm{disc}(t^2-11t-1)$ are units at $\ell$, and the branch points of $u\mapsto t$ lie over smooth fibres modulo $\ell$.

| | component | $\ell$ | $S_1,S_2,S_3,S_4$ | $L_\ell(T)$; $\mathrm{ord}_{1/\ell}$ |
|---|---|---|---|---|
| Thm 1 | $\delta$ | 29 | $-43,-1849,28982,-27889$ | $(1-841T^2)(1-43T+841T^2)$; 1 |
| | $q$ | 29 | $-43,-1849,28982,-27889$ | $(1-841T^2)(1-43T+841T^2)$; 1 |
| | $q\delta$ | 29 | $0,-2204,0,400316$ | $1-1102T^2+707281T^4$; 0 |
| | $h$ | 29 | $-13,27,-53098,-930053$ | $(1-841T^2)R_6(T)$; 1 |
| Thm 2 | $\delta$ | 29 | $-13,-169,30602,-2289169$ | $(1-841T^2)(1-13T+841T^2)$; 1 |
| | $c$ | 47 | $20,-5476,292820$ | $(1+47T)^2(1-74T+2209T^2)$; 0 |
| | $c\delta\equiv p$ | 31 | $38,-1444,-54682$ | $(1-961T^2)(1+38T+961T^2)$; 1 |
| | $h$ | 31 | $-80,-1954,-34280,113342$ | $(1-961T^2)R_6'(T)$; 1 |

Here

$$R_6(T)=1-13T+939T^2-29174T^3+789699T^4-9194653T^5+594823321T^6,$$
$$R_6'(T)=1-80T+3184T^2-95480T^3+3059824T^4-73881680T^5+887503681T^6,$$

with $R_6(1/29)=1800/841$ and $R_6'(1/31)=250/961$. For the $h$-twist of Theorem 1 at 29 the coefficients $c_0,\dots,c_4$ are $1,-13,98,-18241,0$: the sign $\varepsilon=+1$ gives multiplicity 0 (excluded) and $\varepsilon=-1$ gives the displayed polynomial. For Theorem 2 at 31 they are $1,-80,2223,-18600,0$, and again only the sign with multiplicity 1 is compatible with the known section. For the twists over the $t$-line, $S_3$ fixes the sign. The rows for $\delta$ and $q$ in Theorem 1 coincide; this is not a misprint.

*Proof of rank $\leq 4$ in Theorems 1 and 2.* The table gives $r_\delta + r_c + r_{c\delta} + 2r_h \leq 1+1+0+2 = 4$ for Theorem 1 and $\leq 1+0+1+2 = 4$ for Theorem 2. Together with Section 2 this proves rank exactly 4, and that the four points generate a subgroup of finite index. □

*Remark* 6. The choice of primes matters. At $\ell = 29$ the twists $c$ and $c\delta$ of Theorem 2 have multiplicities 1 and 2, and its $h$-twist has multiplicity 2, so $\ell = 29$ gives weaker upper bounds for these components. (The extra eigenvalues may come from sections defined over a quadratic extension of the constant field, but we have not identified such sections.) The primes $\ell = 47$ and $\ell = 31$ separate these contributions and give sharp bounds.

*Remark* 7 (Specialisations). If $k$ is 71-integral with $k \equiv 1/2 \pmod{71}$, the curve of Theorem 1 reduces to the curve with $t = 23$ over $\mathbb{F}_{71}$, of order 75; if $k$ is 11-integral with $k \equiv 3/2 \pmod{11}$, the curve of Theorem 2 reduces to the curve with $t = 4$ over $\mathbb{F}_{11}$, of order 15. These orders are odd, so such fibres have no rational 2-torsion, and by Mazur's theorem their torsion is exactly $\mathbb{Z}/5\mathbb{Z}$. By Silverman's specialisation theorem [9] all but finitely many of them have rank at least 4, and their $j$-invariants take infinitely many values. Several fibres of the second family have rank 5, for example $k = 4, 5, 1/4, 5/2$ (PARI's `ellrank` bounds; for curves without rational 2-torsion the upper bound may rely on GRH).

## 4. Rank five: proof of Theorem 3

**The fifth point.** In the setting of Theorem 2, $h\tilde{h} = 4(25 - 9u^2)$, and the conic $25 - 9u^2 = \square$ is parametrised by $u = 5(s^2-9)/(3(s^2+9))$; on it $h \equiv 5(s^2+9)$ modulo squares. Over the $s$-line the curve $E_t$ has rank 2 (the points $x_1, x_2$), and its twist by $h$ has rank 2 (the points $x_3, x_4$). The new input is the twist by

$$D(s) = -15(s^2 + 2s - 39),$$

a class on the conic that is not pulled back from the $u$-line; it carries the point $x_5$: $\mathscr{D}_t(x_5)$ is $D(s)$ times a square in $\mathbb{Q}(s)$. With $s = 6(k^2+k-1)/(k^2-4k-1)$, which lies in $\mathbb{Q}(k)$ because $\sqrt{h\tilde{h}} \in \mathbb{Q}(k)$, one has $u(s) = u(k)$ and

$$D(s) = \frac{9\,(-5)(3k^4 + 116k^3 - 218k^2 - 116k + 3)}{(k^2 - 4k - 1)^2},$$

so $\sqrt{D} = 3w/(k^2 - 4k - 1) \in \mathbb{Q}(C')$.

*Proof of Theorem 3.* All identities above are exact (checked in PARI/GP). Since $C'$ has genus one, $w \notin \mathbb{Q}(k)$ and $\mathbb{Q}(C') = \mathbb{Q}(k)(w)$ is quadratic over $\mathbb{Q}(k)$. Hence $E_t(\mathbb{Q}(C')) \otimes \mathbb{Q}$ splits into the $(+1)$- and $(-1)$-eigenspaces of $w \mapsto -w$, which are $E_t(\mathbb{Q}(k)) \otimes \mathbb{Q}$ and the part coming from the twist by $w^2$. The points $x_1, \ldots, x_4$ lie in the first and are independent by Theorem 2; $x_5$ lies in the second, since $w \mapsto -w$ changes the sign of $\sqrt{D}$ and so sends the point to its negative. The torsion of $E_t(\mathbb{Q}(C'))$ injects into that of a fibre: at $k = -23$, $s = 303/62$ and $t_0 = 239761/76507200$, with good reduction at 29 and 31 and $\#E_{t_0}(\mathbb{F}_{29}) = 35$, $\#E_{t_0}(\mathbb{F}_{31}) = 30$, so the torsion is $\mathbb{Z}/5\mathbb{Z}$, generated by $(0,0)$ and fixed by $w \mapsto -w$. If $x_5$ were torsion it would equal its own negative, hence be the identity, which it is not. So $x_5$ has infinite order, and the rank is at least 5. □

*Proof of Corollary 4.* $C'$ has a rational point and its Jacobian has rank 2, so $C'(\mathbb{Q})$ is infinite. By Silverman's specialisation theorem [9], all but finitely many of its points give curves of rank at least 5. The quartic defining $C'$ has unit leading coefficient and discriminant at 29, and $29 \nmid 20800$, so $C'$ has good reduction at 29. Take $P_0 = (-23, 1850)$ as the origin of $C'$. Reduction modulo 29 is then a homomorphism $C'(\mathbb{Q}) \to C'(\mathbb{F}_{29})$, whose kernel has finite index and is therefore infinite. Every point in the kernel reduces to $\overline{P_0} = (6, 23)$, so it has $k$ integral at 29 and $k \equiv -23 \pmod{29}$. For these points $t(k) \equiv 2 \pmod{29}$, and the fibre reduces to $E_2/\mathbb{F}_{29}$, which has 35 points; so it has

no rational 2-torsion, and by Mazur's theorem its torsion is exactly $\mathbb{Z}/5\mathbb{Z}$. Since $t$ is non-constant on $C'$, infinitely many $j$-invariants occur. □

**Fibres.** At several small points of $C'$ the five points are visibly independent, and some fibres have rank 6 (PARI's `ellrank` bounds; possibly GRH-dependent):

| $k$ | $s$ | det of the $5\times 5$ height matrix | rank bounds |
|---|---|---|---|
| $-23$ | $303/62$ | $9.81\times 10^7$ | $6,6$ |
| $19/17$ | $-237/122$ | $1.35\times 10^8$ | $6,6$ |
| $-19/8$ | $174/181$ | $2.09\times 10^8$ | $5,5$ |

**The exact rank.** Since $\mathbb{Q}(C') = \mathbb{Q}(k)(w)$,

$$\operatorname{rank} E_t(\mathbb{Q}(C')) = 4 + r_D + r_{Dh},$$

where $r_D$ and $r_{Dh}$ are the ranks over $\mathbb{Q}(s)$ of the twists by $D$ and $Dh$ of $E_t$ over the $s$-line; the 4 is exact by Theorem 2, $r_D \geq 1$ and $r_{Dh} \geq 0$. The corresponding elliptic surfaces have parabolic cohomology of dimension 16 and 20, so the method of Section 3 needs point counts over $\mathbb{F}_{\ell^8}$ and $\mathbb{F}_{\ell^{10}}$. The primes 7 and 11 are of bad reduction for these twists, and already $\ell = 13$ is beyond our computation, so we have not determined the exact rank. Nagao-type averages give 0.93 for $D$ and $-0.19$ for $Dh$, and the fibre at $k = -19/8$ has rank 5 by `ellrank` (possibly GRH-dependent); if the rank over $\mathbb{Q}(C')$ were at least 6, this fibre would be one of the finitely many exceptional fibres of Silverman's theorem. We therefore expect the rank to be exactly 5.

*Remark* 8 (Heuristics). If the number of curves with torsion $\mathbb{Z}/5\mathbb{Z}$ and height at most $H$ is of order $H^{1/6}$ [4], the heuristic of Park, Poonen, Voight and Wood [5] suggests the rank bound $1+24/6 = 5$ for this torsion. Rank 5 is then the borderline case, in which the model allows $H^{o(1)}$ curves; the family of Corollary 4, parametrised by the rational points of an elliptic curve, is very sparse ($O(\log H)$ curves of height at most $H$), so the result is consistent with the heuristic.

## 5. How the curves arise

In both cases a positive conic $\delta(t) = \square$ is parametrised by $u$, with deck involution $\iota(u) = -u$; let $E_\varphi = E_{t(u)}$. A twist $h$ of $E_\varphi$ with one point gives a second point on the twist by $\tilde{h} = h \circ \iota$, as in Jaswal's doubling lemma [3]. In his setting $h$ and $\tilde{h}$ have four distinct roots and the base has genus one. Here $h$ has a root at a fixed point of $\iota$ ($u = 0$, respectively $u = \infty$), so the curve $h = \square$, $\tilde{h} = \square$ is branched at only three points and is rational. The four points come from:

| point | Theorem 1 | Theorem 2 |
|---|---|---|
| $x_1$ | twist of $E$ by $\delta = (3t-1)(3t-4)$ | twist of $E$ by $\delta = 5(10t+1)(18t+1)$ |
| $x_2$ | twist of $E$ by $q = -(1573t+36)(3t-1)$ | twist of $E$ by $p = (8t+1)(18t+1)$ |
| $x_3$ | twist of $E_\varphi$ by $h = u(41u-80)$ | twist of $E_\varphi$ by $h = 2(3u+5)$ |
| $x_4$ | twist of $E_\varphi$ by $\tilde{h} = u(41u+80)$ | twist of $E_\varphi$ by $\tilde{h} = 2(5-3u)$ |

In both cases the class of $x_2$ equals $h\tilde{h}$ on the $u$-line, and it shares a root with $\delta$ on the $t$-line. The positive twists were located by Nagao-type averages of fibre traces (106 primes between 300 and 1000) over all 77 positive conics $\delta$ with rational roots found in a twist search; up to the automorphism $t \mapsto -1/t$ of the universal curve, these averages single out these two configurations as the only ones of total rank 4. The sections were reconstructed by interpolating $x$-coordinates from rank-1 specialisations and then verified symbolically.

## 6. Comparison

Eroshkin's curve over $\mathbb{Q}(T)$ [2] is $E_{-s(T)}$ in the notation above, with

$$s(T) = \frac{(T^3+2T^2-4)(T^3-2T^2+4)(T^3-2T-2)(T^3-2T+2)}{12\,T^2(T^2-4)(T^2-1)(T^2+2T+2)(T^2-2T+2)}.$$

We checked that his four points lie on the curve and are independent at $T = 7/3$ (determinant $5922.44\ldots$). His map $T \mapsto s(T)$ has degree 12 and is invariant under $T \mapsto -T$ and $T \mapsto 2/T$, a biquadratic (Klein four) structure. The maps $k \mapsto t$ of Theorems 1 and 2 have degree 8, and their Galois closures over the $t$-line are dihedral. The degree of the map to $X_1(5)$ is unchanged by reparametrisation and by $t \mapsto -1/t$, and $12/8$ is not an integer, so neither of our curves is isomorphic to a base change of Eroshkin's or conversely. An isomorphism between two curves of the form $E_t$ maps the rational point $P$ of order 5 to one of $\pm P, \pm 2P$; on the parameter, $\pm P$ give the same value of $t$ and $\pm 2P$ give $-1/t$. So after a reparametrisation of $k$ the two maps $k \mapsto t$ would have to agree up to $t \mapsto -1/t$. The two new curves are not isomorphic to each other: the branch values of the maps $k \mapsto t$ are $\{1/3, 4/3, -36/1573\}$ and $\{-1/10, -1/18, -1/8\}$, and these sets are not related by the identity or by $t \mapsto -1/t$.

## 7. Searches

The fifth point of Theorem 3 was found by searching for quadratic twists of the rank-2 curves over the three conics $h = \square$, $\tilde{h} = \square$ and $h\tilde{h} = \square$ that lie under the rational bases of Theorems 1 and 2; only the conic $h\tilde{h} = \square$ of Theorem 2 produced a class not pulled back from the $u$-line. The following searches detected nothing beyond rank 4 over $\mathbb{Q}(k)$ (Nagao averages, so heuristic):

- quadratic twists of the curve of Theorem 1 in its base parameter (coefficients up to 80, and $a \le 3$, $|b| \le 300$, $|c| \le 1500$), linear twists (coefficients up to 250) and products of linear factors (coefficients up to 40); a positive one with a soluble conic would give rank 5 over $\mathbb{Q}(w)$;
- the same searches on the rank-2 curves over the conics $h = \square$ and $h\tilde{h} = \square$ of Theorem 1 and $h = \square$ of Theorem 2, apart from classes pulled back from the $u$-line;
- twists $k(u-r)\,g(u)$ of $E_\varphi$ for which the base of Theorem 1 or 2 acquires a genus-one double cover ($r$ of height up to 300);
- the same searches on Eroshkin's curve, where by its symmetry a positive twist $h$ would come with $h \circ g$ and give rank 6 over a genus-one curve;
- a configuration as in Section 5 with a piece of rank 2: none occurred among the 77 conics.

## 8. Computations and use of AI

The searches, sections and specialisations were computed with PARI/GP 2.15.4 and Python/NumPy; all identities used in the proofs, including those for Theorem 3, were checked exactly in PARI/GP. The trace sums $S_n$ in Section 3 were computed by point counting over $\mathbb{P}^1(\mathbb{F}_{\ell^n})$ in PARI/GP; for Theorem 1 they were obtained independently in two separate implementations and agree. Scripts reproducing all identities, all trace sums $S_n$ and the resulting $L$-polynomials, and the numerical data of Sections 2–4, are available as ancillary files. The exact-rank argument by reduction of the surfaces follows the second author's note on Theorem 1. The construction was found in an investigation carried out with Claude (Anthropic), an AI system, following ideas of Jaswal [3]. The eigenspace proof of Theorem 1, which needs no rank upper bounds, follows a suggestion received on an earlier version of this note. The authors directed the work and take full responsibility for this note.

## Acknowledgments

A.D. acknowledges support from the Croatian Science Foundation under the project no. IP-2022-10-5008 (TEBAG), the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", Grant No. PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and the European Union: NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, Institutional grant of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math).

## References

[1] A. Dujella, *Infinite families of elliptic curves with high rank and prescribed torsion*, https://web.math.pmf.unizg.hr/~duje/tors/generic.html.
[2] Yu. Eroshkin, personal communication to A. Dujella (family of rank 4 over $\mathbb{Q}(t)$ with torsion $\mathbb{Z}/5\mathbb{Z}$, 2020).
[3] M. Jaswal, *Elliptic curves with torsion group $\mathbb{Z}/6\mathbb{Z}$ and generic rank four*, preprint, Zenodo, 2026, https://zenodo.org/records/23735797.
[4] R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170.
[5] J. Park, B. Poonen, J. Voight and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. **21** (2019), 2859–2903.
[6] D. Maulik and B. Poonen, *Néron–Severi groups under specialization*, Duke Math. J. **161** (2012), 2167–2206.
[7] M. Schütt and T. Shioda, *Mordell–Weil Lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **70**, Springer, 2019.
[8] R. van Luijk, *K3 surfaces with Picard number one and infinitely many rational points*, Algebra Number Theory **1** (2007), 1–15.
[9] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
*Email address*, A. Dujella: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
*Email address*, J. C. Peral: juancarlos.peral@ehu.es