ELLIPTIC CURVES WITH TORSION GROUP $\mathbb{Z}/6\mathbb{Z}$ AND GENERIC RANK FOUR

MANVIR JASWAL

Abstract. We give an elliptic curve over $\mathbb{Q}(t)$ with non-constant j-invariant, torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and Mordell–Weil rank exactly 4. The largest rank previously known for such a curve was 3, due to Lecacheux and reached by several later families. The curve is the pullback of the universal elliptic curve with a point of order 6 along an explicit rational function of degree 16 that is invariant under $t \mapsto -t$ and $t \mapsto 1/t$. The upper bound for the rank comes from the specialization criterion of Gusić and Tadić and a 2-descent of a single fiber. The rank splits along the characters of the symmetry group: the curve descends to $\mathbb{Q}\big((t+1/t)^2\big)$, where it and three of its quadratic twists have rank exactly 1. All but finitely many rational fibers have torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 4. We also give an explicit family over an elliptic curve of rank two which shows that infinitely many elliptic curves over $\mathbb{Q}$ have torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 5, a bound that Dujella's tables credit to Eroshkin (2009, personal communication). One member of this family has rank exactly 6. Over $\mathbb{Q}(\sqrt{2})$ the same kind of construction gives infinitely many curves with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 6; whether the same holds over $\mathbb{Q}$ is open. All results are unconditional.

Contents

1. Introduction 1
2. The curve with a point of order six 5
3. Generic rank four: proof of Theorem 1.1 10
4. Rank five over an elliptic curve of rank two: proof of Theorem 1.2 19
5. Rank six over $\mathbb{Q}(\sqrt{2})$: proof of Theorem 1.3 24
Appendix A. Computations 28
Appendix B. The rank in Remark 4.7 28
Declarations 29
References 30

1. Introduction

By Mazur's theorem [28], the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is one of fifteen groups. For each such group T, Dujella's tables [5] record lower bounds for

$$G(T) = \sup\{\operatorname{rank} E(\mathbb{Q}(t)) : E(\mathbb{Q}(t))_{\mathrm{tors}} \cong T\},$$
$$C(T) = \limsup\{\operatorname{rank} E(\mathbb{Q}) : E(\mathbb{Q})_{\mathrm{tors}} \cong T\},$$

Date: October 28, 2026.
2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 14J27, 11G35.
Key words and phrases. Elliptic curves, Mordell–Weil rank, torsion subgroup, specialization, elliptic surfaces, height pairing.

where $C(T) \geq r$ means that infinitely many curves over $\mathbb{Q}$ with torsion T have rank at least r, and in $G(T)$ the curve E runs over the elliptic curves over $\mathbb{Q}(t)$ with non-constant j-invariant. For $T = \mathbb{Z}/6\mathbb{Z}$ the tables, as read on October 24, 2026, list $G(T) \geq 3$ and $C(T) \geq 5$ [5], and the same values appear in Dujella's survey [7, §8]. Our main result, Theorem 1.1, raises the first of these bounds to $G(\mathbb{Z}/6\mathbb{Z}) \geq 4$. The largest rank known for a curve over $\mathbb{Q}$ with torsion $\mathbb{Z}/6\mathbb{Z}$ is 9 [3]; Elkies and Klagsbrun found such a curve [13, §13].

Several families reach the bound 3. The tables credit it to Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008), Dujella–Peral (2012, 2020), MacLeod (2014, 2015) and Voznyy (2021); the entries for Eroshkin and for Voznyy are personal communications, and Woo's family is in his thesis [43]. Lecacheux's family, from the Journées Arithmétiques (Lille, 2001), is published in [24, §3.2.1, Théorème 6] (2003), Kihara's in [22] and MacLeod's in [27, §7.2], and the families of Eroshkin and of Dujella and Peral (2012) are published in [11, §§5–6]. For six of these families Dujella, Peral and Tadić [11, §§3–7] showed, with the criterion of Gusić and Tadić [15], that the rank over $\mathbb{Q}(t)$ is exactly 3: Lecacheux's (§3), Kihara's (§4), two members of Eroshkin's two-parameter family (§5), Dujella and Peral's (§6) and MacLeod's (§7). Kihara [22] also gave infinitely many curves with a point of order 6 and rank at least 4, parametrized by the rational points of an elliptic curve of positive rank.

Problem 2.6(b) in Dujella's list of open problems [6] asks:

> "Are there infinitely many elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/6\mathbb{Z}$ and rank ≥ 6?"

For $T = \mathbb{Z}/6\mathbb{Z}$ the model of Park, Poonen, Voight and Wood predicts that only finitely many curves have rank greater than 5 [31, §8.3], the value of $C(T)$ in the tables, and Dujella notes that this lower bound is then best possible [7, §8]. Park, Poonen, Voight and Wood also predict that only $H^{o(1)}$ curves of height at most H meet such a bound, and remark that the known infinite families meeting it lie over elliptic curves of positive rank ([31, §8.3, p. 22], in the authors' version of May 15, 2019). The family of Theorem 1.2 is of this kind. A family over $\mathbb{Q}(t)$ gives more. By Silverman's theorem (Theorem 2.4), Hilbert's irreducibility theorem and Lemma 2.2(a), an elliptic curve over $\mathbb{Q}(t)$ with non-constant j-invariant, torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank r has specializations over $\mathbb{Q}$, with distinct j-invariants, that have torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least r, and their number up to height H is at least a positive power of H. So the same count would suggest $G(\mathbb{Z}/6\mathbb{Z}) \leq 4$. The authors note, following Elkies, that one cannot call their heuristic for boundedness convincing until the model is refined to predict the rank distribution in parametric families [31, Remark 1.1.3]. Indeed, under the parity conjecture, a family of rank 4 whose root number is -1 on a positive proportion of its specializations gives a positive power of H curves of height at most H with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 5, against the $H^{o(1)}$ prediction; compare [8] and [7, §8] for $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. For the family of Theorem 1.1 both root numbers occur, for instance $+1$ at $t = 2$ and -1 at $t = 3$; we do not know whether -1 occurs on a positive proportion of its specializations.

Throughout, for c in a field of characteristic 0 we write

$$E_c\colon\ y^2 = x^3 + (1 + 6c - 3c^2)\,x^2 - 16c^3x, \qquad T_c = \big(-4c,\, 4c(1+c)\big), \tag{1.1}$$

the model of [11, §2]. For $c \notin \{0, -1, -1/9\}$ it is an elliptic curve and T_c is a point of order 6 (Section 2); over $\mathbb{Q}(c)$ it is the universal elliptic curve with a point of order 6.

Theorem 1.1. *Let*

$$c(t) = \frac{8t^2(t^2-1)^2(t^4-8t^2-1)(t^4+8t^2-1)}{(t^8+62t^4+1)(t^8+24t^6+14t^4+24t^2+1)} \in \mathbb{Q}(t), \tag{1.2}$$

and let E be the elliptic curve $E_{c(t)}$ over $\mathbb{Q}(t)$.

(a) *The j-invariant of E is non-constant, and $E(\mathbb{Q}(t))_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$, generated by $T_{c(t)}$.*

(b) $\operatorname{rank} E(\mathbb{Q}(t)) = 4$. *The points $P(t)$, $P(-t)$, $P(1/t)$, $P(-1/t)$ of Lemma 3.1 and $T_{c(t)}$ generate a subgroup of index 8 of $E(\mathbb{Q}(t))$, and $E(\mathbb{Q}(t))$ is generated by $T_{c(t)}$, $P(t)$ and the three points M_g ($g(t) = -t$, $1/t$, $-1/t$) of Proposition 3.7, which satisfy $2M_g = P(t) + P(gt)$.*

(c) *For all but finitely many $t_0 \in \mathbb{Q}$ the curve $E_{c(t_0)}$ is an elliptic curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 4. For $t_0 = 13/6$ its rank is exactly 4.*

Since $j(E)$ is non-constant, part (c) gives infinitely many pairwise non-isomorphic curves over $\mathbb{Q}$ with torsion $\mathbb{Z}/6\mathbb{Z}$ and rank at least 4. The map (1.2) is invariant under the group $V_4 = \{t, -t, 1/t, -1/t\}$, and $c(t) = \widehat{c}(\nu)$ with $\nu = (t + 1/t)^2$, for a map $\widehat{c}$ of degree 4 (3.1). Since $(t - 1/t)^2 = \nu - 4$, the field $\mathbb{Q}(t)$ is $\mathbb{Q}(\nu)(\sqrt{\nu}, \sqrt{\nu - 4})$. Accordingly $E(\mathbb{Q}(t)) \otimes \mathbb{Q}$ is the sum of the eigenspaces of V_4 for its four characters, which correspond to the curve $E_{\widehat{c}(\nu)}$ over $\mathbb{Q}(\nu)$ and to its quadratic twists by ν, $\nu - 4$ and $\nu(\nu - 4)$. Each eigenspace contains one of four combinations of $P(t)$, $P(-t)$, $P(1/t)$, $P(-1/t)$, which are independent by (b), and the dimensions add up to $\operatorname{rank} E(\mathbb{Q}(t)) = 4$; so each eigenspace is a line, and all four curves have rank exactly 1 (Proposition 3.6). Proposition 3.5 gives the height matrix of the four points, and with it the heights of the combinations of them that span the four lines.

Theorem 1.2. *Let $\mathcal{C}$ be the curve in the affine space with coordinates (u, z_1, z_2) defined by*

$$z_1^2 = 4u^2 - 60u + 113, \qquad z_2^2 = 64u^2 - 7, \tag{1.3}$$

and let $c(u) = -3(2u + 1)/(2(4u^2 - 6u + 5))$. Then $\mathcal{C}$ is a smooth curve of genus one with infinitely many rational points, and for all but finitely many $(u, z_1, z_2) \in \mathcal{C}(\mathbb{Q})$ the elliptic curve $E_{c(u)}$ over $\mathbb{Q}$ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 5. These curves have infinitely many distinct j-invariants. At the point $(u, z_1, z_2) = (-1199/222, 2612/111, 4787/111)$ of $\mathcal{C}$, where $c(u) = 181152/1898473$, the curve $E_{c(u)}$ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank exactly 6.

Theorem 1.2 gives an explicit construction for the bound $C(\mathbb{Z}/6\mathbb{Z}) \geq 5$, which Dujella's tables credit to Eroshkin (2009, personal communication) [5] and which Dujella's list of open problems states as known [6, Problem 2.6].

Theorem 1.3. *Let $K = \mathbb{Q}(\sqrt{2})$. There are a smooth projective curve $\mathcal{C}'$ of genus one over K with infinitely many K-points and a morphism $\varphi_K \colon \mathcal{C}' \to \mathbb{P}^1$ of degree 8, given explicitly in Section 5, such that for all but finitely many $\xi \in \mathcal{C}'(K)$ the curve $E_{\varphi_K(\xi)}$ over K has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank at least 6 over K. These curves have infinitely many distinct j-invariants.*

Over quadratic fields, Dujella's table of curves of high rank with prescribed torsion lists, for torsion $\mathbb{Z}/6\mathbb{Z}$, a curve of rank at least 15 over $\mathbb{Q}(\sqrt{330374})$, credited there to Elkies and Klagsbrun and to Voznyy [4]. Aguirre, Dujella, Jukić Bokun and Peral gave one of rank at least 11 over $\mathbb{Q}(\sqrt{3521})$ [1, §4.3]. These are single curves, each over its own field. Over $\mathbb{Q}$, Problem 2.6(b) remains open.

The constructions. All three constructions rest on one mechanism, stated in Lemma 2.10. Start from a map φ of degree 2 from a line to the c-line, with its involution ι, and a quadratic polynomial h such that the quadratic twist of E_φ (the curve (1.1) with $c = \varphi$) by h has independent points over the function field of the line. Let $\mathcal{C}$ be the genus-one curve $z_1^2 = h$,

$z_2^2 = \tilde{h}$, over which h and its transform $\tilde{h}$ by ι are both squares; it is a Galois cover of the c-line of degree 8 with dihedral group. Over $\mathcal{C}$ each point of the twist gives a point of E_φ, its image; the lift $\tilde{\iota}$ of ι to $\mathcal{C}$ transforms the images into as many further points. The images change sign under $z_1 \mapsto -z_1$ and are fixed by $z_2 \mapsto -z_2$, and their transforms do the reverse; so the two kinds of points lie in different eigenspaces of these automorphisms of $\mathcal{C}$, and m independent points of the twist give $2m$ independent points of E_φ over the function field of $\mathcal{C}$.

For Theorem 1.1, φ and h depend on a parameter t, and the twist has two independent points; (1.2) is φ evaluated at a point of $\mathcal{C}$ over $\mathbb{Q}(t)$, and the four points of Lemma 3.1, one V_4-orbit, are the images of the two twist points and their transforms, evaluated at that point (Section 3.2). The rank is computed as in [11]. By the criterion of Gusić and Tadić [15, Theorem 1.3], whose condition at t_0 can be checked by hand from Table 1, the specialization at $t_0 = 13/6$ is injective, so the rank over $\mathbb{Q}(t)$ is at most that of the fiber at t_0. That fiber has rank 4: a 2-descent gives the upper bound, and the four specialized points are independent.

In Theorem 1.2, $c(u)$ has degree 2, it is invariant under $\iota(u) = (4-u)/(2u+1)$, and $\mathcal{C}$ is the curve over which both $4u^2 - 60u + 113$ and its transform by ι (up to a square, $64u^2 - 7$) become squares. The bound 5 comes from five independent points $P_1, \dots, P_5$ over the function field of $\mathcal{C}$ (4.2). The map $u \mapsto c(u)$ and the point P_1 come from a family of Eroshkin over $\mathbb{Q}(U, V)$, published by Dujella, Peral and Tadić [11, §5.1]: the map of its member $V = -2/3$ to the c-line is $c(u)$ composed with the quotient by an involution τ of the U-line (Lemma 4.6). The other four points are two points of the quadratic twist of $E_{c(u)}$ by $4u^2 - 60u + 113$, which become points of $E_{c(u)}$ over the function field of $\mathcal{C}$, and their transforms by the lift $\tilde{\iota}$ of ι to $\mathcal{C}$. The fiber of rank 6 lies over the value of u of smallest height at which the five points specialize to independent points (Remark 4.5); there `mwrank` finds six independent points, and a 2-descent gives the upper bound 6 (Proposition 4.4). Theorem 1.3 has the same shape over $K = \mathbb{Q}(\sqrt{2})$, except that no point comes from Eroshkin's family. Its six points are the images of three independent points R_a, R_b, R' of the quadratic twist of $E_{c_K(u)}$ over $K(u)$, where c_K is a map of degree 2 as above, by a quadratic polynomial $h_K \in K[u]$, and their transforms by the lift $\tilde{\iota}_K$ of the involution ι_K of $u \mapsto c_K(u)$ (Lemma 2.10, Section 5). The field K enters through the third point R': a twist point whose factorization in Lemma 2.10(e)(i) contains the pair $\omega \pm \alpha$ over just one root of the twisting polynomial, each factor with multiplicity 1, needs that root in the base field, and the roots of h_K lie in K (end of Section 5). The bounds 5 and 6 of Theorems 1.2 and 1.3 are lower bounds for the ranks over the function fields of the genus-one curves, which we do not compute.

Families over an elliptic curve of positive rank go back to Néron: his curves of rank at least 11 are the fibers of such a family (see [12, Lecture I]). With prescribed torsion they were used by Yamagishi for a point of order 3 [44, Theorem 4.5], by Kihara for a point of order 6 [22], by Lecacheux [25, Théorème 7], [26] and by Rabarison [32] (see [9, §5.4]), by Elkies [12, Lectures II and III], by Dujella and Peral [9, §§5.4, 6.6], [10, §4], and by Dujella, Kazalicki and Peral [8, §9]. Theorems 1.2 and 1.3 use the mechanism of the author's papers on the torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [17] and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ [16]: over the function field of a curve of genus one and positive rank on which the twisting polynomial becomes a square, the points of a quadratic twist of positive rank become points of the untwisted curve, and Silverman's theorem gives the specialization.

Plan. Section 2 collects the facts on E_c that the proofs use and states the construction behind all three theorems (Section 2.5), and Sections 3, 4 and 5 prove Theorems 1.1, 1.2 and 1.3. Appendix A describes the computations, and Appendix B proves the upper bound of Remark 4.7.

2. The curve with a point of order six

The three proofs use the following facts about the curve (1.1): its model and the parameter c on $X_1(6)$, its torsion over $\mathbb{Q}$ and over quadratic fields, criteria for the injectivity of specialization and for the independence of points, and, in Propositions 3.5, 3.6 and 3.7 only, Shioda's height pairing.

2.1. **The model.** Let k be a field of characteristic 0. For $c \in k$ put $a = 1 + 6c - 3c^2$ and $b = -16c^3$, so that (1.1) reads $y^2 = x(x^2 + ax + b)$. One has

$$a^2 - 4b = (c+1)^3(9c+1), \qquad \Delta(E_c) = 16b^2(a^2-4b) = 4096\,c^6(c+1)^3(9c+1), \tag{2.1}$$

so E_c is an elliptic curve for $c \notin \{0, -1, -1/9\}$. The multiples of $T_c = (-4c, 4c(1+c))$ are

$$2T_c = (4c^2, -4c^2(c+1)), \quad 3T_c = (0,0), \quad 4T_c = (4c^2, 4c^2(c+1)), \quad 5T_c = (-4c, -4c(1+c)),$$

so T_c has order 6. The model comes from Tate's normal form $y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2$ [11, §2], and every elliptic curve over k with a k-rational point of order 6 is isomorphic to some E_c with $c \in k \smallsetminus \{0, -1, -1/9\}$ [23, Table 3]. Its j-invariant $j(E_c) = 256(a^2-3b)^3/(b^2(a^2-4b))$ is a rational function of c of degree 12, the index of $\pm\Gamma_1(6)$ in $\mathrm{PSL}_2(\mathbb{Z})$; so $c \mapsto (E_c, \pm T_c)$ identifies the c-line with the modular curve $X_1(6)$, with cusps $c = 0, -1, -1/9, \infty$.

If $c = n/d$ with n, d in a polynomial ring and $d \neq 0$, then $(x, y) \mapsto (d^2x, d^3y)$ is an isomorphism from E_c to

$$Y^2 = X^3 + AX^2 + BX, \qquad A = d^2 + 6nd - 3n^2, \quad B = -16n^3d, \tag{2.2}$$

and $A^2 - 4B = (n+d)^3(9n+d)$. We use this model whenever c is a quotient of polynomials.

2.2. **Torsion.**

Lemma 2.1. *Let k be a number field and $c \in k \smallsetminus \{0, -1, -1/9\}$.*

(a) *E_c has four k-rational points of order dividing 2 if and only if $(c+1)(9c+1) \in k^{*2}$.*
(b) *If $T_c \in 2E_c(k)$, then $-c \in k^{*2}$.*
(c) *If $E_c(k)$ contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then k contains a primitive cube root of unity.*

Proof. (a) The points of order 2 other than $(0,0)$ are $(x, 0)$ with $x^2 + ax + b = 0$, whose discriminant is $(c+1)^3(9c+1)$ by (2.1). (b) The map $E_c(k) \to k^*/k^{*2}$ sending (x, y) to x for $x \neq 0$, $(0,0)$ to b and O to 1 is a homomorphism whose kernel contains $2E_c(k)$ [39, Proposition X.4.9]. So $x(T_c) = -4c$ is a square. (c) This follows from the Weil pairing [39, Corollary III.8.1.1]. □

Lemma 2.2. *Let E be an elliptic curve over a number field k with a k-rational point of order 6.*

(a) *If $k = \mathbb{Q}$, then $E(\mathbb{Q})_{\mathrm{tors}}$ is $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*
(b) *If $[k : \mathbb{Q}] = 2$, then $E(k)_{\mathrm{tors}}$ is $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Proof. These are the groups containing an element of order 6 in Mazur's list [28] and in the list of Kenku and Momose [21] and Kamienny [19] for quadratic fields, as stated in [20, Theorem 1]. □

Corollary 2.3. *Let $c \in \mathbb{Q} \smallsetminus \{0, -1, -1/9\}$. If neither $-c$ nor $(c+1)(9c+1)$ is a square in $\mathbb{Q}$, then $E_c(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$.*

Proof. By Lemma 2.2, $E_c(\mathbb{Q})_{\mathrm{tors}}$ is $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The last needs four points of order dividing 2, excluded by Lemma 2.1(a). In $\mathbb{Z}/12\mathbb{Z}$ the subgroup of order 6 is $2(\mathbb{Z}/12\mathbb{Z})$, so $T_c \in 2E_c(\mathbb{Q})$, excluded by Lemma 2.1(b). □

2.3. **Specialization.** Let k be a number field, C a smooth projective geometrically irreducible curve over k, and $\mathcal{E}$ an elliptic curve over $k(C)$ given by a Weierstrass equation. For $\xi \in C(k)$ outside the finite set where a coefficient has a pole or the discriminant vanishes, the reduction of the equation at ξ is an elliptic curve $\mathcal{E}_\xi$ over k, and reduction of points gives a homomorphism $\sigma_\xi \colon \mathcal{E}(k(C)) \to \mathcal{E}_\xi(k)$, the specialization map.

Theorem 2.4 (Silverman [37, Theorem C] and Northcott)**.** *If the j-invariant of $\mathcal{E}$ is not constant, then σ_ξ is injective for all but finitely many $\xi \in C(k)$.*

Silverman's theorem says that the points ξ at which σ_ξ is not injective have bounded height, and by Northcott's theorem only finitely many points of $C(k)$ have bounded height. Silverman's theorem is stated for families of abelian varieties without constant part, that is, whose $k(C)/k$-trace is zero; an elliptic curve with non-constant j-invariant is not isogenous to a constant curve, so it has no constant part.

Lemma 2.5. *In this setting, σ_ξ is injective on $\mathcal{E}(k(C))_{\mathrm{tors}}$ for every ξ at which it is defined.*

Proof. Let v be the place of $k(C)$ at ξ and $\widehat{k(C)}_v \cong k((\pi))$ its completion, whose residue field k has characteristic 0. The kernel of reduction on $\mathcal{E}(k((\pi)))$ is the group of points of the formal group of the model at v, which has no torsion in residue characteristic 0 [39, Proposition IV.3.2]. □

Theorem 2.6 (Gusić–Tadić [15, Theorem 1.3]; see also [11, §1])**.** *Let $\mathcal{E} \colon y^2 = x^3 + Ax^2 + Bx$ with $A, B \in \mathbb{Z}[t]$ be an elliptic curve over $\mathbb{Q}(t)$ that is not isomorphic over $\mathbb{Q}(t)$ to a curve defined over $\mathbb{Q}$, and assume that $\mathcal{E}$ has exactly one non-trivial $\mathbb{Q}(t)$-rational point of order 2. Let $t_0 \in \mathbb{Q}$ be such that, for every non-constant square-free divisor h of B or of $A^2 - 4B$ in $\mathbb{Z}[t]$, the rational number $h(t_0)$ is not a square in $\mathbb{Q}$. Then the specialized curve $\mathcal{E}_{t_0}$ is elliptic and the specialization map $\mathcal{E}(\mathbb{Q}(t)) \to \mathcal{E}_{t_0}(\mathbb{Q})$ is injective.*

Lemma 2.7. *Let E be an elliptic curve over a number field k, let ℓ be a prime not dividing the order of $E(k)_{\mathrm{tors}}$, and let $P_1, \dots, P_r \in E(k)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be primes of good reduction of E, with residue fields $\mathbb{F}_{\mathfrak{p}_i}$, and suppose that the images of $P_1, \dots, P_r$ in $\bigoplus_i E(\mathbb{F}_{\mathfrak{p}_i})/\ell E(\mathbb{F}_{\mathfrak{p}_i})$ are linearly independent over $\mathbb{F}_\ell$. Then $P_1, \dots, P_r$ are linearly independent in $E(k) \otimes \mathbb{Q}$.*

Proof. Suppose $\sum n_i P_i$ is a torsion point R with integers n_i not all 0; dividing by a common factor of the n_i (a point with a torsion multiple is torsion) we may assume that ℓ does not divide all n_i. As ℓ does not divide the order of R, $R \in \ell E(k)$, so the image of $\sum n_i P_i$ in each $E(\mathbb{F}_{\mathfrak{p}_i})/\ell E(\mathbb{F}_{\mathfrak{p}_i})$ is 0, a non-trivial relation over $\mathbb{F}_\ell$. □

2.4. **Heights.** Let $\mathcal{E}$ be an elliptic curve over $\overline{\mathbb{Q}}(t)$ with non-constant j-invariant, $S \to \mathbb{P}^1$ its Kodaira–Néron model and χ the Euler characteristic of $\mathcal{O}_S$. Shioda's height pairing [36], in the form of [35, §§11.6–11.8 and Table 4], is a symmetric bilinear form on $\mathcal{E}(\overline{\mathbb{Q}}(t))$ that

vanishes on torsion and induces a positive definite form on $\mathcal{E}(\overline{\mathbb{Q}}(t))/\mathcal{E}(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$; its value on the diagonal is

$$\langle P,P\rangle = 2\chi + 2(P\cdot O) - \sum_v \mathrm{contr}_v(P), \tag{2.3}$$

where $(P\cdot O)$ is the intersection number of the sections P and O, and $\mathrm{contr}_v(P)$ is $i(n-i)/n$ if the fiber at v has type I_n and P meets its component Θ_i (numbered cyclically, Θ_0 meeting O), and 0 if P meets Θ_0. Only fibers of type I_n occur where we use this formula; for the other types see [35, §11.8, Table 4]. The off-diagonal values follow by polarization.

The following is [38, Lemma 5.1] at the places of $\overline{\mathbb{Q}}(t)$. We include the short proof.

Lemma 2.8. *Let $\mathcal{E}\colon Y^2 = X^3 + AX^2 + BX$ with A, B polynomials, minimal at a place v where it has multiplicative reduction of type I_n with $v(A) = 0$, and let $P = (X, Y)$ be a section. Then P meets a non-identity component Θ_i of the fiber at v if and only if $v(X) \geq 0$, $v(Y) > 0$ and $v(f'(X)) > 0$, where $f(X) = X^3 + AX^2 + BX$; in that case $\min(i, n-i) = \min(v(Y), n/2)$.*

Proof. A section meets a non-identity component if and only if its reduction at v is the singular point of the fiber, that is, the conditions stated: the points of the identity component with $v(Y) > 0$ reduce to a smooth point of order 2, where f' is a unit. Over the completion at a geometric point above v the curve is a Tate curve with $v(q) = n$. Two minimal models of the form $Y^2 =$ cubic differ by $X \mapsto \alpha^2 X + r$, $Y \mapsto \alpha^3 Y$ with α a unit, so $v(Y)$ does not depend on the model. On the Tate model $y^2 + xy = x^3 + a_4(q)x + a_6(q)$, written as $y'^2 =$ cubic with $y' = y + x/2$, the point with parameter w, $0 < v(w) = i < n$, has $y' = (w - q/w)/2 + 2w^2 - 2(q/w)^2 + \dots$, where every term after the first has valuation $> \min(i, n-i)$, so $v(y') = \min(i, n-i)$ for $i \neq n/2$ and $v(y') \geq n/2$ for $i = n/2$. Since $i(n-i)/n$ depends only on $\min(i, n-i)$, this determines the contribution. □

2.5. **Twist data and transforms.** In Sections 3.2, 4 and 5, m independent points of a quadratic twist over a line give $2m$ independent points of a pullback of the curve (1.1) over a genus-one cover of the line, by one construction, which we now set up. Let k be a field of characteristic 0.

Definition 2.9. We call a quadruple $\mathcal{D} = (e, f, h_1, h_0)$ of elements of k with $e \neq 0$ and $e \neq 2f$ a *twist datum* over k. To $\mathcal{D}$ we attach

$$n = -12(2u+1), \qquad d = (4u-7)(eu+f)+12(2u+1), \qquad \varphi = n/d, \qquad h = u^2+h_1u+h_0,$$

the constants $\kappa = (7e-18f)/(8e)$ and $\lambda = \kappa + \frac{1}{4} = 9(e-2f)/(8e)$, the Möbius transformation $\iota(u) = (-u/2 + \kappa)/(u + \frac{1}{2})$, the polynomial $\tilde{h}(u) = (u + \frac{1}{2})^2 h(\iota(u))$, the polynomials $A = d^2 + 6nd - 3n^2$ and $B = -16n^3 d$ of (2.2), the quadratic twist

$$E^{(h)}\colon\ Y^2 = X^3 + hAX^2 + h^2BX$$

of (2.2) over $k(u)$, and the curve $\mathcal{C}_{\mathcal{D}}\colon z_1^2 = h(u)$, $z_2^2 = \tilde{h}(u)$ over k; when it is irreducible (for instance under the hypotheses of Lemma 2.10) its function field is $k(\mathcal{C}_{\mathcal{D}}) = k(u, z_1, z_2)$.

So $\varphi = 0$ exactly at $u = -\frac{1}{2}$ and $u = \infty$, and $\varphi = -1$ exactly at the roots $\frac{7}{4}$ and $-f/e$ of $n + d = (4u-7)(eu+f)$. The conditions $e \neq 0$, $e \neq 2f$ say that $\deg d = 2$ and $d(-\frac{1}{2}) = \frac{9}{2}(e-2f) \neq 0$, so that φ has degree 2. Conversely, a map of degree 2 from $\mathbb{P}^1$ to the c-line that is unramified over $c = 0$, whose two points over $c = 0$ and one point over $c = -1$ are rational over k, takes this form after the change of coordinate on $\mathbb{P}^1$ that moves these three points to $-\frac{1}{2}$, ∞ and $\frac{7}{4}$, and a common rescaling of numerator and denominator. Indeed, after the change of coordinate the numerator is a constant multiple of $2u+1$ and

the sum of numerator and denominator vanishes at $\frac{7}{4}$, and the rescaling makes them n and $(4u-7)(eu+f)$ for some $e, f \in k$. So a twist datum is such a map with three marked points, together with a monic quadratic h. With $\omega^2 = 4u+2$ the marked points $-\frac{1}{2}$, ∞ and $\frac{7}{4}$ lie at $\omega = 0$, ∞ and ± 3: $2u+1 = \omega^2/2$ and $4u-7 = (\omega-3)(\omega+3)$. The map of Theorem 1.2 is φ for $\mathcal{D} = (8, -4, -15, \frac{113}{4})$ (Section 4), and that of Remark 4.7 for $\mathcal{D} = (4, 1, 0, 2)$ with $u = w$ (Appendix B).

Lemma 2.10. *Let $\mathcal{D}$ be a twist datum over k such that $h(-\frac{1}{2}) \neq 0$ and $h\tilde{h}$ has four distinct roots in $\bar{k}$.*

(a) (The involution.) *ι is the involution of the u-line that exchanges $-\frac{1}{2}$ with ∞ and $\frac{7}{4}$ with $-f/e$, and*

$$\iota(u) + \tfrac{1}{2} = \frac{\lambda}{u+\frac{1}{2}}, \qquad n(\iota(u)) = \frac{\lambda\, n(u)}{(u+\frac{1}{2})^2}, \qquad d(\iota(u)) = \frac{\lambda\, d(u)}{(u+\frac{1}{2})^2}.$$

So $\varphi \circ \iota = \varphi$, and ι generates the group of automorphisms of $k(u)$ over $k(\varphi)$. Moreover $\tilde{h}(u) = h(-\frac{1}{2})(u+\frac{1}{2})^2 + (h_1 - 1)\lambda(u+\frac{1}{2}) + \lambda^2$ and $(u+\frac{1}{2})^2 \tilde{h}(\iota(u)) = \lambda^2 h(u)$.

(b) (The cover.) *The smooth projective model of $\mathcal{C}_\mathcal{D}$ is a geometrically irreducible curve of genus one, and*

$$\beta_1(u, z_1, z_2) = (u, -z_1, z_2), \qquad \beta_2(u, z_1, z_2) = (u, z_1, -z_2),$$
$$\tilde{\iota}(u, z_1, z_2) = \Big(\iota(u),\ \frac{z_2}{u+\frac{1}{2}},\ \frac{\lambda z_1}{u+\frac{1}{2}}\Big)$$

are automorphisms of it that preserve φ. They satisfy $\tilde{\iota}^2 = 1$ and $\tilde{\iota}\beta_1\tilde{\iota} = \beta_2$ and generate a dihedral group of order 8; $k(\mathcal{C}_\mathcal{D})$ is a Galois extension of $k(\varphi)$ with this group, so $\varphi\colon \mathcal{C}_\mathcal{D} \to \mathbb{P}^1$ has degree 8.

(c) (Twist points and transforms.) *For $(X, Y) \in E^{(h)}(k(u))$,*

$$P = \Big(\frac{X}{h\, d^2},\ \frac{Y}{h\, z_1\, d^3}\Big)$$

is a point over $k(\mathcal{C}_\mathcal{D})$ of E_φ, the curve (1.1) with $c = \varphi$, and $(X, Y) \mapsto P$ is an injective homomorphism $E^{(h)}(k(u)) \to E_\varphi(k(\mathcal{C}_\mathcal{D}))$; we call P the image *of (X, Y). For $P \in E_\varphi(k(\mathcal{C}_\mathcal{D}))$, the* transform *$\tilde{\iota}^* P$ of P is the point obtained by replacing (u, z_1, z_2) by $\tilde{\iota}(u, z_1, z_2)$ in the coordinates of P; $P \mapsto \tilde{\iota}^* P$ is an automorphism of the group $E_\varphi(k(\mathcal{C}_\mathcal{D}))$. If P is the image of (X, Y), then*

$$\tilde{\iota}^* P = \Big(\frac{\tilde{X}}{\tilde{h}\, d^2},\ \frac{\tilde{Y}}{\tilde{h}\, z_2\, d^3}\Big), \qquad \tilde{X} = \frac{(u+\frac{1}{2})^6 X(\iota(u))}{\lambda^2}, \quad \tilde{Y} = \frac{(u+\frac{1}{2})^9\, Y(\iota(u))}{\lambda^3},$$

and $(\tilde{X}, \tilde{Y})$ is a point over $k(u)$ of the twist $Y^2 = X^3 + \tilde{h}AX^2 + \tilde{h}^2 BX$. The automorphisms β_1 and β_2 act on images by -1 and $+1$, and on their transforms by $+1$ and -1.

(d) (Independence.) *If $Q_1, \dots, Q_m \in E^{(h)}(k(u))$ are linearly independent, then their images $P_1, \dots, P_m$ and the transforms $\tilde{\iota}^* P_1, \dots, \tilde{\iota}^* P_m$ are $2m$ linearly independent points of $E_\varphi(k(\mathcal{C}_\mathcal{D}))$.*

(e) (Two shapes of twist points.) *Let $\omega^2 = 4u+2$, so that $k(u)(\omega) = k(\omega)$, and let $q, r, W \in k(u)$ with $q \neq 0$, $W \neq 0$. Then $A^2 - 4B = (4u-7)^3(eu+f)^3(9n+d)$, and:*

(i) $(2(2u+1)q^2,\ 2(2u+1)(4u-7)\, q\, r)$ lies on $E^{(h)}$ if and only if $\mathcal{F}(\omega)\mathcal{F}(-\omega) = h^2(A^2 - 4B)$, where $\mathcal{F}(\omega) = 4(2u+1)q^2 + hA + 2(4u-7)r\,\omega \in k(\omega)$;

(ii) $(3(2u+1)dW^2,\ 3(2u+1)(4u-7)dWr)$ *lies on* $E^{(h)}$ *if and only if* $\mathcal{F}_+\mathcal{F}_- = (A^2-4B)W^4$, *where* $\mathcal{F}_\pm = AW^2 + 18432(2u+1)^2h \pm 192(2u+1)(4u-7)r \in k(u)$.

Proof. (a) Since $(u+\frac12)(\iota(u)+\frac12) = -\frac{u}{2}+\kappa+\frac{u}{2}+\frac14 = \lambda$ and $\lambda \neq 0$, ι is an involution that exchanges $-\frac12$ and ∞, and $\iota(\frac74)+\frac12 = \lambda/\frac94 = \frac12 - \frac{f}{e}$. Hence $n(\iota(u)) = -24(\iota(u)+\frac12) = \lambda n(u)/(u+\frac12)^2$. Next, $4\iota(u)-7 = 4(\iota(u)+\frac12)-9 = -9(u+\frac{f}{e})/(u+\frac12)$ and $e\iota(u)+f = e(\iota(u)+\frac12) - \frac{e-2f}{2} = -(e-2f)(4u-7)/(8(u+\frac12))$, so $(4\iota(u)-7)(e\iota(u)+f) = \lambda(4u-7)(eu+f)/(u+\frac12)^2$; subtracting the formula for n gives the one for d, and $\varphi\circ\iota = \varphi$. As $d(-\frac12) \neq 0$ and $\deg d = 2 > \deg n$, the polynomials n and d are coprime and φ has degree 2; so $k(u)/k(\varphi)$ is Galois of degree 2, and $\iota \neq 1$ generates its group. Writing $h(u) = (u+\frac12)^2 + (h_1-1)(u+\frac12) + h(-\frac12)$ and substituting $\iota(u)+\frac12 = \lambda/(u+\frac12)$ gives the formula for $\tilde h$; substituting it once more gives $(u+\frac12)^2\tilde h(\iota(u)) = \lambda^2 h(u)$.

(b) By (a), $\tilde h$ has degree 2 with leading coefficient $h(-\frac12)$. As $h\tilde h$ has four simple roots, none of h, $\tilde h$, $h\tilde h$ is a square in $\bar k(u)$, and $\mathcal{C}_\mathcal{D} \to \mathbb{P}^1_u$ is a $(\mathbb{Z}/2\mathbb{Z})^2$-cover branched exactly over the four roots of $h\tilde h$, each with two points of index 2 above it, and unramified over $u=\infty$. By the Riemann–Hurwitz formula $2g-2 = 4\cdot(-2)+4\cdot 2$, so $g=1$. On $\mathcal{C}_\mathcal{D}$ one has $(z_2/(u+\frac12))^2 = \tilde h(u)/(u+\frac12)^2 = h(\iota(u))$ by the definition of $\tilde h$, and $(\lambda z_1/(u+\frac12))^2 = \lambda^2 h(u)/(u+\frac12)^2 = \tilde h(\iota(u))$ by (a); so $\tilde\iota$ maps $\mathcal{C}_\mathcal{D}$ to itself, and $\varphi\circ\tilde\iota = \varphi\circ\iota = \varphi$. Using $(u+\frac12)(\iota(u)+\frac12) = \lambda$ one finds $\tilde\iota^2 = 1$, and directly $\tilde\iota\beta_1 = \beta_2\tilde\iota$. So β_1, β_2, $\tilde\iota$ generate a group of order 8 in which $\beta_1\tilde\iota$ has order 4 (its square is $\beta_1\beta_2$), a dihedral group. It fixes $k(\varphi)$, and $[k(\mathcal{C}_\mathcal{D}) : k(\varphi)] = [k(\mathcal{C}_\mathcal{D}) : k(u)]\,[k(u) : k(\varphi)] = 4\cdot 2$, so $k(\mathcal{C}_\mathcal{D})/k(\varphi)$ is Galois with this group.

(c) Over $k(u)(z_1)$, where $h = z_1^2$, the map $(X,Y) \mapsto (X/h,\ Y/(hz_1))$ is an isomorphism from $E^{(h)}$ to (2.2), and $(X,Y) \mapsto (X/d^2, Y/d^3)$ is the inverse of the isomorphism of (2.2) from E_φ. Their composite, restricted to points over $k(u)$, is an injective homomorphism into $E_\varphi(k(u,z_1)) \subset E_\varphi(k(\mathcal{C}_\mathcal{D}))$. Since E_φ is defined over $k(\varphi)$, which $\tilde\iota$ fixes, $\tilde\iota$ acts on $E_\varphi(k(\mathcal{C}_\mathcal{D}))$ through its action on coordinates, by a group automorphism. The formula for $\tilde\iota^* P$ follows from $h(\iota(u)) = \tilde h(u)/(u+\frac12)^2$, $d(\iota(u)) = \lambda d(u)/(u+\frac12)^2$ and $\tilde\iota^* z_1 = z_2/(u+\frac12)$. By (a), $A(\iota(u)) = \lambda^2 A(u)/(u+\frac12)^4$ and $B(\iota(u)) = \lambda^4 B(u)/(u+\frac12)^8$, and substituting these and $h(\iota(u)) = \tilde h(u)/(u+\frac12)^2$ into the equation of $E^{(h)}$ at $\iota(u)$, multiplied by $(u+\frac12)^{18}/\lambda^6$, shows that $(\tilde X, \tilde Y)$ lies on the twist by $\tilde h$. The coordinates of an image involve z_1 only through the factor $1/z_1$ of its y-coordinate and do not involve z_2; those of a transform involve z_2 only through $1/z_2$ and do not involve z_1. This gives the signs.

(d) The commuting involutions β_1^*, β_2^* split $E_\varphi(k(\mathcal{C}_\mathcal{D}))\otimes\mathbb{Q}$ into the direct sum of their four joint eigenspaces. By (c) the images $P_1,\dots,P_m$ are linearly independent and lie in the eigenspace where $\beta_1^* = -1$ and $\beta_2^* = 1$, and their transforms are linearly independent ($\tilde\iota^*$ is an automorphism) and lie in the eigenspace where $\beta_1^* = 1$ and $\beta_2^* = -1$. As the sum of two different eigenspaces is direct, the $2m$ points are linearly independent.

(e) By (2.2), $A^2-4B = (n+d)^3(9n+d)$, and $n+d = (4u-7)(eu+f)$. Both parts are identities in $k(u)$: in (i),

$$Y^2 - X(X^2+hAX+h^2B) = -\tfrac{X}{4}(\mathcal{F}(\omega)\mathcal{F}(-\omega) - h^2(A^2-4B)),$$

from $\mathcal{F}(\omega)\mathcal{F}(-\omega) = (4(2u+1)q^2+hA)^2 - 8(2u+1)(4u-7)^2r^2$ and $X(X^2+hAX+h^2B) = \frac{X}{4}((2X+hA)^2 - h^2(A^2-4B))$; in (ii), using $B = 27648(2u+1)^3 d$,

$$Y^2 - X(X^2+hAX+h^2B) = -\frac{d^2W^2}{4096}(\mathcal{F}_+\mathcal{F}_- - (A^2-4B)W^4).$$

As $X \neq 0$ in both cases, the assertions follow. □

Write elements of $k(\omega)$ as $\mathcal{F} = \mathcal{F}_0 + \mathcal{F}_1\omega$ with $\mathcal{F}_0, \mathcal{F}_1 \in k(u)$. By Lemma 2.10(e)(i), twist points of the first shape, up to sign, correspond to the elements $\mathcal{F}$ of norm $\mathcal{F}(\omega)\mathcal{F}(-\omega) = h^2(A^2 - 4B)$ such that $(\mathcal{F}_0 - hA)/(4(2u+1))$ is a non-zero square q^2, taken up to $\mathcal{F}(\omega) \leftrightarrow \mathcal{F}(-\omega)$; then $r = \mathcal{F}_1/(2(4u-7))$. Over $\bar{k}$, $h^2(A^2 - 4B)$ is a product of linear factors in ω, so such points with q, r polynomials are found by sharing these factors between $\mathcal{F}(\omega)$ and $\mathcal{F}(-\omega)$ and testing the square condition. For example, for the point $Q_b = (X_b, Y_b)$ of Section 4, where $\mathcal{D} = (8, -4, -15, \frac{113}{4})$, $(X_b/4, Y_b/8)$ has the first shape with $q = 8(2u^2 - 3u - 11)$, and

$$\mathcal{F}(\omega) = \tfrac{1}{4}(\omega - 6)(\omega - 1)(\omega - 3)^2(\omega + 3)(\omega + 2)^3(\omega^2 + 4\omega - 24)^2,$$

while $h^2(A^2 - 4B) = \frac{1}{16}(\omega^2 - 36)(\omega^2 - 1)(\omega^2 - 9)^3(\omega^2 - 4)^3(\omega^2 - 4\omega - 24)^2(\omega^2 + 4\omega - 24)^2$. In (e)(ii), $X \cdot h^2B$ is a square, so the sum of the point and the point $(0, 0)$ of order 2 has the square X-coordinate $h^2B/X = (96(2u+1)h/W)^2$, and the factorization takes place in $k(u)$; the constants of $\mathcal{F}_\pm$ are $18432 = 2 \cdot 96^2$ and $192 = 2 \cdot 96$.

3. Generic rank four: proof of Theorem 1.1

3.1. **The family and its points.** Let $c(t) = N(t)/D(t)$ be the map (1.2), with $N(t) = 8t^2(t^2-1)^2(t^4 - 8t^2 - 1)(t^4 + 8t^2 - 1)$ of degree 14 and $D(t) = (t^8 + 62t^4 + 1)(t^8 + 24t^6 + 14t^4 + 24t^2 + 1)$ of degree 16. The group $V_4 = \{t, -t, 1/t, -1/t\}$ of Möbius transformations fixes $\nu = (t + 1/t)^2$, and $\mathbb{Q}(t)/\mathbb{Q}(\nu)$ is a Galois extension with group V_4. One checks that

$$c(t) = \widehat{c}((t + 1/t)^2), \qquad \widehat{c}(\nu) = \frac{8(\nu - 4)(\nu^2 - 4\nu - 64)}{(\nu^2 - 4\nu + 64)(\nu^2 + 20\nu - 32)}. \tag{3.1}$$

The map (1.2) was found with Lemma 2.10: it is φ_t evaluated at a point over $\mathbb{Q}(t)$ of the genus-one curve $\mathcal{C}_t$ attached to a twist datum over $\mathbb{Q}(t)$ for which the twist has two independent points (Section 3.2). A similar device was used by Lecacheux [24, §3.2.1, Théorème 6]: two of her families of rank 2 over $\mathbb{Q}(a, b)$, in her two parameters a and b, have common members along a curve that is an elliptic curve over $\mathbb{Q}(a)$, and a $\mathbb{Q}(a)$-rational point of it gives a curve over $\mathbb{Q}(a)$ with three independent points. Yamagishi [44, §4] used a base surface with an elliptic fibration in the same way for points of order 3.

Let $E = E_{c(t)}$ over $\mathbb{Q}(t)$ and $\widehat{E} = E_{\widehat{c}(\nu)}$ over $\mathbb{Q}(\nu)$, so that E is the base change of $\widehat{E}$ to $\mathbb{Q}(t)$. The singular fibers of E come from the factorizations

$$N + D = (t^2 + 1)^2(t^6 - t^4 + 31t^2 + 1)(t^6 + 31t^4 - t^2 + 1),$$
$$9N + D = (t^8 - 34t^4 + 96t^2 + 1)(t^8 + 96t^6 - 34t^4 + 1),$$

together with those of N and D and the double zero of c at $t = \infty$. Since the curve (1.1) over the c-line has fibers of types I_6, I_3, I_2, I_1 over $c = 0, -1, \infty, -1/9$, the model (2.2) of E, $Y^2 = X^3 + AX^2 + BX$ with $A = D^2 + 6ND - 3N^2$ and $B = -16N^3D$, has fibers of type I_{12} at $t = 0, \pm 1, \infty$, I_6 at the eight roots of $(t^4 - 8t^2 - 1)(t^4 + 8t^2 - 1)$ and at $t = \pm\sqrt{-1}$, I_3 at the twelve roots of the two sextics, I_2 at the sixteen roots of D, and I_1 at the sixteen roots of $9N + D$. Their Euler numbers add up to $4 \cdot 12 + 10 \cdot 6 + 12 \cdot 3 + 16 \cdot 2 + 16 = 192$, so $\chi = 16$. The polynomial A is monic of degree $32 = 2\chi$ and B has degree $58 \le 4\chi$, so the model is integral at $t = \infty$ in the coordinates X/t^{32}, Y/t^{48}. Its invariant $c_4 = 16(A^2 - 3B)$ equals $16A^2$ where $B = 0$ and $4A^2$ where $A^2 = 4B$, and A does not vanish at any of these places, so c_4 does not vanish at any singular fiber: the model is minimal and all singular fibers are multiplicative.

Lemma 3.1. *Let*

$$x_P(t) = -\frac{8t^2(t+1)^6(t^4-8t^2-1)(t^4+8t^2-1)(t^8+32t^5-66t^4+96t^3+1)^2}{(t^8+62t^4+1)(t^8+24t^6+14t^4+24t^2+1)(3t^8+12t^6+62t^4-12t^2-1)^2}$$

and

$$y_P(t) = x_P(t)\,\frac{(t^2+1)(t^6-t^4+31t^2+1)\,\Phi(t)}{D(t)(t^8+32t^5-66t^4+96t^3+1)(3t^8+12t^6+62t^4-12t^2-1)},$$

where

$$\begin{aligned}\Phi(t) = {} & t^{24}-24t^{23}+24t^{22}-304t^{21}-886t^{20}+936t^{19}\\ & -6984t^{18}-16448t^{17}+50895t^{16}-263856t^{15}+361776t^{14}-637984t^{13}\\ & +212044t^{12}-113904t^{11}-358608t^{10}-576t^9+207t^8-16440t^7\\ & +3768t^6-48t^5-118t^4+72t^3+24t^2+1.\end{aligned}$$

Then $y_P^2 = x_P^3 + (1+6c-3c^2)x_P^2 - 16c^3x_P$, so $P(t) = (x_P, y_P) \in E(\mathbb{Q}(t))$. Since c is V_4-invariant, $P(-t)$, $P(1/t)$ and $P(-1/t)$ also lie in $E(\mathbb{Q}(t))$, and V_4, acting on $E(\mathbb{Q}(t))$ through its action on $\mathbb{Q}(t)$, permutes these four points, which are distinct, simply transitively.

Proof. The first assertion is a polynomial identity, checked in [18]. The rest is immediate from $c(gt) = c(t)$ for $g \in V_4$. The four points are distinct, since their x-coordinates are. □

3.2. **How the map was found.** The proofs of Theorems 1.1, 1.2 and 1.3 do not use this subsection; Remark 3.9 does. The map (1.2) and the points of Lemma 3.1 come from Lemma 2.10 applied to the twist datum $\mathcal{D}_t$ over $\mathbb{Q}(t)$ given by

$$e_t = \frac{32(3t^2+1)}{3(t^2-1)^2}, \qquad f_t = -\frac{8(9t^4+21t^2-2)}{3(t^2-1)^2},$$

$$h_t = u^2 - \frac{9t^6+81t^4+123t^2+11}{16(3t^2+1)}\,u + \frac{135t^8+720t^6+936t^4-204t^2-19}{32(3t^2+1)^2}.$$

Here $\lambda_t = 81t^2(t^2+3)/(16(3t^2+1))$, $h_t(-\frac{1}{2})$ is the square of $9t^2(t^2+3)/(4(3t^2+1))$, and $h_t\tilde{h}_t$ has four distinct roots, so Lemma 2.10 applies; we write d_t, φ_t, ι_t and $\tilde{h}_t$ for the objects of Definition 2.9 for $\mathcal{D}_t$, and $\mathcal{C}_t$ for the genus-one curve $\mathcal{C}_{\mathcal{D}_t}$ over $\mathbb{Q}(t)$. On the twist of (2.2) by h_t lies the point

$$\begin{aligned}Q_t &= \big(3(2u+1)d_t\,W^2,\ 3(2u+1)(4u-7)d_t\,W\,r\big),\\ W &= \frac{(t+1)^2(4(3t^2+1)u-9t^3+6t^2-27t+2)}{2(t-1)(3t^2+1)},\\ r &= \frac{l_1(4u-7)(e_tu+f_t)^3(u-r_2)-l_2(u-r_1)W^4}{384(2u+1)},\end{aligned}$$

where $r_1 = (9t^2-2)/4$, $r_2 = (3t^2+25)/(4(3t^2+1))$, $l_1 = 3(t+1)^6/(8(3t^2+1))$ and $l_2 = 1024(3t^2+1)^2/(9(t-1)^2(t+1)^8)$; r is a polynomial of degree 3 in u. To see that Q_t lies on the twist, note that $9n+d_t = 4e_t(u-r_1)(u-r_2)$, $l_1l_2 = 4e_t$, and one checks that $2(AW^2+18432(2u+1)^2h_t) = l_1(4u-7)^2(e_tu+f_t)^3(u-r_2)+l_2(4u-7)(u-r_1)W^4$; so in Lemma 2.10(e)(ii) $\mathcal{F}_+ = l_1(4u-7)^2(e_tu+f_t)^3(u-r_2)$ and $\mathcal{F}_- = l_2(4u-7)(u-r_1)W^4$, whose

product is $(A^2-4B)W^4$. Since $\mathcal{D}_{-t}=\mathcal{D}_t$, Q_{-t} lies on the same twist. Let $\xi\in\mathcal{C}_t(\mathbb{Q}(t))$ be the point

$$u=-\frac{9t^8-402t^4+64t^2+9}{128t^2(3t^2+1)},\qquad z_1=-\frac{9(3t^8+12t^6+62t^4-12t^2-1)}{128t^2(3t^2+1)},$$
$$z_2=\frac{81(t^2+3)(t^8+12t^6-62t^4-12t^2-3)}{512(3t^2+1)^2}.$$

It was found without a search: the four points of $\mathcal{C}_t$ over $u=\infty$ are defined over $\mathbb{Q}(t)$, and, taking one of them as origin, ξ is the negative of another. Then $\varphi_t(\xi)$ is (1.2), and reduction at ξ (Remark 3.2(2) below) maps the images of Q_t and Q_{-t} and their transforms to $P(t)$, $P(-t)$, $P(1/t)$ and $P(-1/t)$. As these are independent (Proposition 3.4), so are the four points of E_{φ_t} over $\mathbb{Q}(t)(\mathcal{C}_t)$, and so are Q_t and Q_{-t}.

Remark 3.2 (Re-marking; families and sections). (1) One may mark the other point $-f/e$ over $c=-1$ instead of $\frac74$. Let $\lambda^*=81/(16\lambda)$ and $u'=-\frac12+\lambda^*(u+\frac12)$, so that $u'=-\frac12$ at $u=-\frac12$ and $u'=\frac74$ at $u=-f/e$. Suppose that $h(-\frac12)$ is a non-zero square in k, with a square root $\sqrt{h(-\frac12)}$. Put

$$e'=\tfrac29(e-2f),\qquad f'=\tfrac19(e-2f)-\tfrac94 e,\qquad h'(u')=\frac{\lambda^{*2}}{h(-\frac12)}\,\tilde h(u),$$

which defines a monic quadratic $h'=u^2+h_1'u+h_0'$. Then $\mathcal{D}'=(e',f',h_1',h_0')$ is a twist datum, $n(u')=\lambda^*n(u)$ and $d'(u')=\lambda^*d(u)$, so that $\varphi'(u')=\varphi(u)$ and $\iota'(u')=-\frac12+\lambda^*(\iota(u)+\frac12)$; moreover $\tilde h'(u')=(81\lambda^*/16)^2h(u)/h(-\frac12)$, and

$$\psi(u,z_1,z_2)=\Big(u',\ \frac{\lambda^*z_2}{\sqrt{h(-\frac12)}},\ \frac{81\lambda^*z_1}{16\sqrt{h(-\frac12)}}\Big)$$

is an isomorphism $\mathcal{C}_{\mathcal{D}}\to\mathcal{C}_{\mathcal{D}'}$ with $\varphi'\circ\psi=\varphi$, $\psi\tilde\iota=\tilde\iota'\psi$ and $\psi\beta_1=\beta_2'\psi$. So ψ exchanges the roles of h and $\tilde h$: ψ^* carries images (for $\mathcal{D}'$) to points on which β_1, β_2 act as on transforms (for $\mathcal{D}$). Re-marking $\mathcal{D}'$ gives back $\mathcal{D}$. All of this is checked as in Lemma 2.10(a).

(2) Let $\mathcal{D}=\mathcal{D}_t$ be a twist datum over $k=k_0(t)$ that satisfies the hypotheses of Lemma 2.10, and $\xi\in\mathcal{C}_{\mathcal{D}}(k_0(t))$ with $c(t)=\varphi(\xi)\notin\{0,-1,-\frac19,\infty\}$. Then E_φ has good reduction at ξ. Reduction at ξ (the map σ_ξ of Section 2.3, with $k_0(t)$ in place of k) is a homomorphism $E_\varphi(k(\mathcal{C}_{\mathcal{D}}))\to E_{c(t)}(k_0(t))$, computed on images and transforms by evaluating their coordinates at ξ where these are defined. If g is a Möbius transformation of the t-line and $\psi_g\colon\mathcal{C}_{\mathcal{D}_t}\to\mathcal{C}_{\mathcal{D}_{g(t)}}$ an isomorphism with $\varphi_{g(t)}\circ\psi_g=\varphi_t$ that maps $\xi(t)$ to $\xi(g(t))$, then $c(g(t))=c(t)$.

The symmetry of (1.2) under V_4 was found, not imposed, and the construction explains it. The twist datum $\mathcal{D}_t$ of this subsection and ξ are even in t. And $\mathcal{D}_{1/t}$ is the re-marking of $\mathcal{D}_t$ as in Remark 3.2(1), with the square root $9t^2(t^2+3)/(4(3t^2+1))$ of $h_t(-\frac12)$. Here $\lambda_t^*=(3t^2+1)/(t^2(t^2+3))$, $u'=-\frac12+\lambda_t^*(u+\frac12)$, and the isomorphism $\psi_t(u,z_1,z_2)=(u',\frac49\lambda_t^{*2}z_2,\frac94\lambda_t^{*2}z_1)$ from $\mathcal{C}_t$ to $\mathcal{C}_{1/t}$ maps $\xi(t)$ to $\xi(1/t)$ and pulls the image of $Q_{1/t}$ back to the transform of the image of Q_t. So $c(gt)=c(t)$ for $g\in V_4$ (Remark 3.2(2)), and the four points of Lemma 3.1 form one V_4-orbit because the images of the two twist points and their transforms do. The same construction applied to the family of Section 5 gives the map of Remark 3.9. Rank 5 by this method would need a twist datum $\mathcal{D}$ over $\mathbb{Q}(t)$, like $\mathcal{D}_t$, for which E_φ has five independent points over $\mathbb{Q}(t)(\mathcal{C}_{\mathcal{D}})$ (three independent twist points would

give six, by Lemma 2.10(d)), and a point of $\mathcal{C}_{\mathcal{D}}$ over $\mathbb{Q}(t)$ as in Remark 3.2(2) at which their reductions stay independent.

3.3. **Torsion, rank and independence.**

Proposition 3.3. $E(\mathbb{Q}(t))_{\mathrm{tors}} = \langle T_{c(t)} \rangle \cong \mathbb{Z}/6\mathbb{Z}$.

Proof. At $t_0 = 13/6$ one has

$$c_0 = c(13/6) = -\frac{1399560636185947872}{17725485300475372897},$$

which is not 0, -1 or $-1/9$, and neither $-c_0$ nor $(c_0+1)(9c_0+1)$ is a square in $\mathbb{Q}$. So $E_{c_0}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ by Corollary 2.3, and $E(\mathbb{Q}(t))_{\mathrm{tors}}$ injects into it by Lemma 2.5. It contains $T_{c(t)}$, of order 6. □

TABLE 1. The non-constant irreducible factors f of B and of A^2-4B in $\mathbb{Z}[t]$, for the model $Y^2 = X^3 + AX^2 + BX$ of E in Section 3; the value $f(13/6)$; and a prime that divides $f(13/6)$ to an odd power and divides no other value in the table.

f	divides	$f(13/6)$	prime
$t-1$	B	$2^{-1}\cdot 3^{-1}\cdot 7$	7
t	B	$2^{-1}\cdot 3^{-1}\cdot 13$	13
$t+1$	B	$2^{-1}\cdot 3^{-1}\cdot 19$	19
t^4-8t^2-1	B	$-2^{-4}\cdot 3^{-4}\cdot 21407$	21407
t^4+8t^2-1	B	$2^{-4}\cdot 3^{-4}\cdot 75937$	75937
t^8+62t^4+1	B	$2^{-8}\cdot 3^{-8}\cdot 229\cdot 2389\cdot 5689$	229
$t^8+24t^6+14t^4+24t^2+1$	B	$2^{-8}\cdot 3^{-8}\cdot 5695220833$	5695220833
t^2+1	A^2-4B	$2^{-2}\cdot 3^{-2}\cdot 5\cdot 41$	5
$t^6-t^4+31t^2+1$	A^2-4B	$2^{-6}\cdot 3^{-6}\cdot 17\cdot 625589$	17
$t^6+31t^4-t^2+1$	A^2-4B	$2^{-6}\cdot 3^{-6}\cdot 36528517$	36528517
$t^8-34t^4+96t^2+1$	A^2-4B	$2^{-8}\cdot 3^{-8}\cdot 73\cdot 4326649$	73
$t^8+96t^6-34t^4+1$	A^2-4B	$2^{-8}\cdot 3^{-8}\cdot 1093\cdot 1873\cdot 7933$	1093

Proposition 3.4. *The points $P(t)$, $P(-t)$, $P(1/t)$, $P(-1/t)$ are linearly independent in $E(\mathbb{Q}(t))\otimes\mathbb{Q}$, and $\operatorname{rank} E(\mathbb{Q}(t)) = 4$. The curve $E_{c(13/6)}$ over $\mathbb{Q}$ has rank exactly 4.*

Proof. We follow [11, §3.2]. We use the model $Y^2 = X^3 + AX^2 + BX$ of E above, with $A = D^2+6ND-3N^2$ and $B = -16N^3D$ in $\mathbb{Z}[t]$. The polynomial $A^2-4B = (N+D)^3(9N+D)$ is not a square in $\mathbb{Q}[t]$, so this curve has exactly one non-trivial point of order 2 over $\mathbb{Q}(t)$, and its j-invariant, $j(E_c)\circ c$ of degree $12\cdot 16 = 192$, is non-constant. The polynomial B is -2^{13} times a product of powers of the seven primitive irreducible polynomials in the upper part of Table 1, and A^2-4B is a product of powers of the five in the lower part. So a non-constant square-free divisor h of B or of A^2-4B in $\mathbb{Z}[t]$ is $\pm m\prod_{f\in S} f$ with $m \mid 2$ and S a non-empty set of factors from one part of the table. For $f\in S$ the prime listed for f in Table 1 divides $h(13/6)$ to an odd power, since it divides no other value in the table and is prime to 6. So $h(13/6)$ is not a square, and by Theorem 2.6 the specialization map $E(\mathbb{Q}(t)) \to E_{c_0}(\mathbb{Q})$ at $t_0 = 13/6$ is injective. We found $t_0 = 13/6$ by testing the values $t_0 = 2a/(3b)$ with integers $|a| \le 16$ and $1 \le b \le 7$ for this condition and for the bound 4 from a 2-descent.

A 2-descent through the rational 2-isogeny of E_{c_0} with Cremona's `mwrank` [2] gives the unconditional upper bound 4 for its rank: the Selmer groups of the isogeny and of its dual have ranks 4 and 2, and the 2-Selmer group, which contains the image of the rational point of order 2, has rank 5. PARI's `ellrank` [30] gives the same bound. At the primes $p = 29$, 47, 71 and 79, all of good reduction, where $E_{c_0}(\mathbb{F}_p)$ has a non-trivial cyclic 5-Sylow subgroup, identify $E_{c_0}(\mathbb{F}_p)/5E_{c_0}(\mathbb{F}_p)$ with $\mathbb{Z}/5\mathbb{Z}$ so that the image of the specialization of $P(t)$ is 1. At $p = 29$, 47, 71 and 79 respectively, the images of the specializations of $P(t)$, $P(-t)$, $P(1/t)$, $P(-1/t)$ are then $(1,2,4,2)$, $(1,3,2,4)$, $(1,1,4,0)$ and $(1,2,4,0)$; these rows form a matrix of determinant 4 over $\mathbb{F}_5$, so the images of the four points in $\bigoplus_p E_{c_0}(\mathbb{F}_p)/5E_{c_0}(\mathbb{F}_p)$ are linearly independent over $\mathbb{F}_5$. So the four specialized points are independent by Lemma 2.7, as $E_{c_0}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$. Hence $\operatorname{rank} E_{c_0}(\mathbb{Q}) = 4$. The four points are independent, since their specializations are, and $\operatorname{rank} E(\mathbb{Q}(t)) \le \operatorname{rank} E_{c_0}(\mathbb{Q})$, since specialization is injective; so $\operatorname{rank} E(\mathbb{Q}(t)) = 4$. As $E(\mathbb{Q}(t))$ injects into $E_{c_0}(\mathbb{Q})$, it is finitely generated, so the four points generate a subgroup of finite index. With $T_{c(t)}$ they generate a subgroup of index 8 (Proposition 3.7). □

3.4. The height matrix and the characters of V_4.

Proposition 3.5. *The height pairing of Section 2.4 on the four points $P(t)$, $P(-t)$, $P(1/t)$, $P(-1/t)$ has the matrix*

$$G = \begin{pmatrix} 23 & -12 & 2 & -1 \\ -12 & 23 & -1 & 2 \\ 2 & -1 & 23 & -12 \\ -1 & 2 & -12 & 23 \end{pmatrix}, \qquad \det G = 145920 = 2^9 \cdot 3 \cdot 5 \cdot 19.$$

Proof. We use the minimal model $Y^2 = X^3 + AX^2 + BX$ of Section 3 with $\chi = 16$ (at $t = \infty$ in the coordinates X/t^{32}, Y/t^{48}), on which $P(t)$ is (D^2x_P, D^3y_P). Its X-coordinate has a double pole at each of the eight roots of $3t^8 + 12t^6 + 62t^4 - 12t^2 - 1$ (over $\overline{\mathbb{Q}}$) and no pole elsewhere, $t = \infty$ included; so $P(t)$ meets O once over each root, and $(P \cdot O) = 8$. By Lemma 2.8, $P(t)$ meets a non-identity component exactly at the places of Table 2, with total contribution $5/3 + 3 + 10 \cdot \frac{5}{6} + 6 \cdot \frac{2}{3} + 16 \cdot \frac{1}{2} = 25$, so $\langle P, P\rangle = 32 + 16 - 25 = 23$ by (2.3). The other entries come in the same way from the points $P(t) + P(gt)$, $g \in V_4$, by polarization: for $g(t) = -t$, $1/t$, $-1/t$ these have heights 22, 50 and 44 (Table 3), so $\langle P(t), P(gt)\rangle = -12$, 2, -1; by symmetry under V_4 the matrix depends only on the element of V_4 relating two points. □

The matrix G is invariant under the regular representation of V_4, with eigenvalues 12, 38, 32, 10 on the four characters. In the next proposition, images are taken under the identification, made in its proof, of the eigenspaces of V_4 on $E(\mathbb{Q}(t)) \otimes \mathbb{Q}$ with the Mordell–Weil groups, tensored with $\mathbb{Q}$, of the four curves.

Proposition 3.6. *The curve $\widehat{E}$ over $\mathbb{Q}(\nu)$ and its quadratic twists by ν, $\nu - 4$ and $\nu(\nu - 4)$ each have rank exactly* 1. *Modulo torsion and up to finite index they are generated by the images of*

$$P(t) + P(-t) + P(1/t) + P(-1/t), \quad P(t) - P(-t) + P(1/t) - P(-1/t),$$
$$P(t) - P(-t) - P(1/t) + P(-1/t), \quad P(t) + P(-t) - P(1/t) - P(-1/t),$$

whose heights over the t-line are 48, 152, 128 *and* 40.

TABLE 2. The places where $P(t)$ meets a non-identity component of the fiber (Lemma 2.8): the place, its degree, the type of the fiber, $\min(i, n-i)$, and the contribution $i(n-i)/n$ at each of its geometric points.

place	degree	type	$\min(i,n-i)$	contribution
$t=0$	1	I_{12}	2	5/3
$t+1=0$	1	I_{12}	6	3
$t^4-8t^2-1=0$	4	I_6	1	5/6
$t^4+8t^2-1=0$	4	I_6	1	5/6
$t^2+1=0$	2	I_6	1	5/6
$t^6-t^4+31t^2+1=0$	6	I_3	1	2/3
$t^8+62t^4+1=0$	8	I_2	1	1/2
$t^8+24t^6+14t^4+24t^2+1=0$	8	I_2	1	1/2

TABLE 3. The places where $P(t)+P(gt)$ ($=2M_g$, Proposition 3.7) meets a non-identity component of the fiber (Lemma 2.8), for $g(t)=-t$, $1/t$, $-1/t$: $\min(i,n-i)$ (a dash for Θ_0; the contribution is $\min(i,n-i)(n-\min(i,n-i))/n$ at each geometric point), the total contribution, $((P(t)+P(gt))\cdot O)$ and the height $\langle P(t)+P(gt), P(t)+P(gt)\rangle$.

place	degree	type	$-t$	$1/t$	$-1/t$
$t-1=0$	1	I_{12}	6	–	6
$t=0$	1	I_{12}	4	2	2
$t+1=0$	1	I_{12}	6	–	6
$t^4-8t^2-1=0$	4	I_6	2	–	–
$t^4+8t^2-1=0$	4	I_6	2	–	–
$t^2+1=0$	2	I_6	2	2	2
$t^6-t^4+31t^2+1=0$	6	I_3	1	1	1
$t^6+31t^4-t^2+1=0$	6	I_3	–	1	1
$t=\infty$	1	I_{12}	–	2	2
total contribution			26	14	20
$(\cdot O)$			8	16	16
height			22	50	44

Proof. For a character $\varepsilon \neq 1$ of V_4 with kernel H, the fixed field $\mathbb{Q}(t)^H$ is $\mathbb{Q}(\nu)(\sqrt{\delta_\varepsilon})$ with $\delta_\varepsilon = \nu$, $\nu-4$ or $\nu(\nu-4)$, since $\sqrt{\nu} = t+1/t$ is fixed by $t \mapsto 1/t$, $\sqrt{\nu-4} = t-1/t$ by $t \mapsto -1/t$, and $\sqrt{\nu(\nu-4)} = t^2 - 1/t^2$ by $t \mapsto -t$. The ε-eigenspace of V_4 on $E(\mathbb{Q}(t)) \otimes \mathbb{Q}$ is therefore isomorphic to $\widehat{E}^{(\delta_\varepsilon)}(\mathbb{Q}(\nu)) \otimes \mathbb{Q}$, the twist by δ_ε, since $(E(\mathbb{Q}(t)) \otimes \mathbb{Q})^H = \widehat{E}(\mathbb{Q}(t)^H) \otimes \mathbb{Q}$, E being the base change of $\widehat{E}$, and the part of $\widehat{E}(\mathbb{Q}(\nu)(\sqrt{\delta_\varepsilon})) \otimes \mathbb{Q}$ on which $\sqrt{\delta_\varepsilon} \mapsto -\sqrt{\delta_\varepsilon}$ acts by -1 is the image of $\widehat{E}^{(\delta_\varepsilon)}(\mathbb{Q}(\nu)) \otimes \mathbb{Q}$. Likewise the invariant subspace is isomorphic to $\widehat{E}(\mathbb{Q}(\nu)) \otimes \mathbb{Q}$. The four displayed points lie in the four eigenspaces (in the order $1, \nu, \nu-4, \nu(\nu-4)$) and are independent by Proposition 3.4, so each eigenspace has dimension at least 1; the dimensions add up to $\operatorname{rank} E(\mathbb{Q}(t)) = 4$ (Proposition 3.4). The heights are $\varepsilon G \varepsilon^{\mathsf{T}}$. □

Proposition 3.7. *Let $D_1 = t^8+62t^4+1$ and $D_2 = t^8+24t^6+14t^4+24t^2+1$. For $g(t) = -t$, $1/t$, $-1/t$ there is a point M_g of $E(\mathbb{Q}(t))$ with $2M_g = P(t) + P(gt)$ and*

$$x(M_{-t}) = -\frac{1024t^4(t^2-1)^3(t^8-66t^4+1)}{D_1^2 D_2},$$

$$x(M_{1/t}) = \frac{8t(t+1)^6(t^8-4t^7+32t^6-60t^5+126t^4-60t^3+32t^2-4t+1)^2}{D_1 D_2^2},$$

$$x(M_{-1/t}) = \frac{8t(t^2-1)^3(t^8-66t^4+1)^3}{D_1 D_2(t^8+4t^7+8t^6-12t^5+46t^4+12t^3+8t^2-4t+1)^2}.$$

Then $E(\mathbb{Q}(t)) = \langle T_{c(t)}\rangle \oplus \mathbb{Z}P(t) \oplus \mathbb{Z}M_{-t} \oplus \mathbb{Z}M_{1/t} \oplus \mathbb{Z}M_{-1/t}$, and $T_{c(t)}$ and $P(\pm t^{\pm 1})$ generate a subgroup of index 8.

Proof. We argue over $\mathbb{Q}(t)$ rather than from generators of a special fiber: the height pairing on $E(\mathbb{Q}(t))$ takes values in $\frac{1}{24}\mathbb{Z}$ and the group G_1 below has height determinant $2280 = 2^3\cdot 3\cdot 5\cdot 19$, so only the primes 2 and 3 can divide the index of G_1 in $E(\mathbb{Q}(t))$, and saturation at these two primes is checked exactly below. The computations in this proof are deposited in [18]. At each $x(M_g)$ the cubic $x^3+(1+6c-3c^2)x^2-16c^3x$ is a square in $\mathbb{Q}(t)$, and of the two points with that x-coordinate one doubles to $P(t)+P(gt)$. Let G_1 be the group generated by $T = T_{c(t)}$, $P(t)$ and the three points M_g; it contains $P(gt) = 2M_g - P(t)$. By Proposition 3.5 and $2M_g = P(t)+P(gt)$, the height matrix of $P(t)$, M_{-t}, $M_{1/t}$, $M_{-1/t}$ has rows $(23, \frac{11}{2}, \frac{25}{2}, 11)$, $(\frac{11}{2}, \frac{11}{2}, 3, 3)$, $(\frac{25}{2}, 3, \frac{25}{2}, 3)$, $(11, 3, 3, 11)$ and determinant $2280 = 145920/8^2$, so T and $P(\pm t^{\pm 1})$ generate a subgroup of index 8 of G_1. The singular fibers of E have types I_{12}, I_6, I_3, I_2 and I_1 (Section 3.1), so by (2.3) and polarization the height pairing takes values in $\frac{1}{24}\mathbb{Z}$. Since $E(\mathbb{Q}(t))$ has rank 4 (Proposition 3.4) and $E(\mathbb{Q}(t))_{\mathrm{tors}} = \langle T\rangle$ (Proposition 3.3), the Gram matrix of a basis of $E(\mathbb{Q}(t))/\langle T\rangle$ has entries in $\frac{1}{24}\mathbb{Z}$, so $[E(\mathbb{Q}(t)) : G_1]^2$ divides $2280\cdot 24^4 = 2^{15}\cdot 3^5\cdot 5\cdot 19$, and it suffices to show that $G_1 \cap \ell E(\mathbb{Q}(t)) = \ell G_1$ for $\ell = 2$ and $\ell = 3$. For $\ell = 2$ it suffices to show that no non-zero $Q = \sum_i n_i Q_i$ with $n_i \in \{0,1\}$ and $(Q_1,\dots,Q_5) = (P(t), M_{-t}, M_{1/t}, M_{-1/t}, T)$ lies in $2E(\mathbb{Q}(t))$. If $Q = 2R$, then $x(R)$ is a root in $\mathbb{Q}(t)$ of $(X^2+16c^3)^2 - 4x(Q)X\big(X^2+(1+6c-3c^2)X-16c^3\big)$. For each of the 31 choices of the n_i this quartic, cleared of denominators and specialized at $t = 2$, has no root modulo some prime $p \in \{7, 11, 13, 29\}$ not dividing its leading coefficient, namely, for $(n_1,\dots,n_5)$,

$$p = 7 \text{ if } n_3 = 1; \qquad p = 13 \text{ for } (1,1,0,0,0),\ (0,0,0,1,1);$$
$$p = 29 \text{ for } (1,1,0,1,1); \qquad p = 11 \text{ for the other 12.}$$

A root β/α with coprime $\alpha, \beta \in \mathbb{Z}[t]$ would give, by Gauss's lemma, a factor $\alpha X - \beta$ in $\mathbb{Z}[t][X]$, hence the root $\beta(2)/\alpha(2)$ modulo such a prime. For $\ell = 3$, specialize at $t = 2$, where $c(2) = -230112/2639137 \notin \{0, -1, -1/9\}$, and reduce modulo $p = 7$, 11, 13, 19, 29: there $E_{c(2)}$ has good reduction, the specialized generators are p-integral, and $E_{c(2)}(\mathbb{F}_p)$ has a cyclic 3-Sylow subgroup, so $Q \mapsto (\#E_{c(2)}(\mathbb{F}_p)/3)\,\bar{Q}$, with values in $\langle 2\bar{T}\rangle$, is a homomorphism vanishing on $3E(\mathbb{Q}(t))$. We identify each $\langle 2\bar{T}\rangle$ with $\mathbb{Z}/3\mathbb{Z}$ by $2\bar{T} \mapsto 1$. The values of the five homomorphisms (rows, $p = 7$, 11, 13, 19, 29) on $P(t)$, M_{-t}, $M_{1/t}$, $M_{-1/t}$, T (columns) are

$$\begin{pmatrix} 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 \\ 2 & 0 & 2 & 2 & 0 \end{pmatrix},$$

a matrix of determinant 1 over $\mathbb{F}_3$, so these five homomorphisms are linearly independent on $G_1/3G_1$; as they vanish on $3E(\mathbb{Q}(t))$, $G_1 \cap 3E(\mathbb{Q}(t)) = 3G_1$. □

3.5. **Proof of Theorem 1.1.** (a) The j-invariant of E is $j(E_c) \circ c$, a rational function of t of degree $12 \cdot 16 = 192$; the torsion is Proposition 3.3. (b) is Propositions 3.4 and 3.7. (c) By Theorem 2.4, applied over $\mathbb{P}^1$, the specialization map is injective for all but finitely many $t_0 \in \mathbb{Q}$, so these fibers have rank at least 4. Outside the finitely many t_0 with $c(t_0) \in \{0, -1, -1/9\}$, Corollary 2.3 shows that the torsion of $E_{c(t_0)}(\mathbb{Q})$ is $\mathbb{Z}/6\mathbb{Z}$ unless $-c(t_0)$ or $(c(t_0)+1)(9c(t_0)+1)$ is a square, that is, unless t_0 is the t-coordinate of a rational point of $y^2 = -N(t)D(t)$ or of $y^2 = (N(t)+D(t))(9N(t)+D(t))$. The square-free parts of these polynomials have degrees 24 and 28, with distinct roots, and their total degrees 30 and 32 are even, so these are hyperelliptic curves of genus 11 and 13; by Faltings' theorem [14, Satz 7] they have finitely many rational points. The rank at $t_0 = 13/6$ is Proposition 3.4. □

Remark 3.8. The curve E is not a pullback of any of the families of [11], which have a rational point of order 6 and rank exactly 3, nor of the families 2-isogenous to them, even along maps defined over $\overline{\mathbb{Q}}$.

(a) For maps defined over $\mathbb{Q}$ we use the fields between $\mathbb{Q}(c)$ and $\mathbb{Q}(t)$, which are exactly $\mathbb{Q}(c)$, $\mathbb{Q}(\nu)$, $\mathbb{Q}(t^2)$, $\mathbb{Q}(t+1/t)$, $\mathbb{Q}(t-1/t)$ and $\mathbb{Q}(t)$. Indeed $N(T)D(t) - N(t)D(T)$ is a constant times $(T-t)(T+t)(tT-1)(tT+1)R(T,t)$, where R has degree 12 in T and is irreducible over $\mathbb{Q}(t)$, since $R(T,2)$ is irreducible over $\mathbb{Q}$ of degree 12. A field strictly between $\mathbb{Q}(c)$ and $\mathbb{Q}(t)$ corresponds to a block of the action of the Galois group on the roots of $N(T) - cD(T)$ that contains t, and such a block is a union of orbits of the stabilizer of t. These orbits are $\{t\}$, $\{-t\}$, $\{1/t\}$, $\{-1/t\}$ and the twelve roots of R, and the size of the block divides 16, so the block is $\{t,-t\}$, $\{t,1/t\}$, $\{t,-1/t\}$ or $\{\pm t, \pm 1/t\}$. So a curve over a subfield of $\mathbb{Q}(t)$ containing $\mathbb{Q}(c)$ that becomes isomorphic over $\mathbb{Q}(t)$ to E has rank 0, 1, 2 or 4. It is one of the following: E_c, of rank 0 over $\mathbb{Q}(c)$ by the Shioda–Tate formula, as its fibers are I_6, I_3, I_2, I_1; $\widehat{E}$ or one of its quadratic twists by ν, $\nu-4$, $\nu(\nu-4)$, of rank 1; for σ one of $t \mapsto -t$, $1/t$, $-1/t$, the curve E over $\mathbb{Q}(t)^\sigma = \mathbb{Q}(t^2)$, $\mathbb{Q}(t+1/t)$, $\mathbb{Q}(t-1/t)$ or its quadratic twist by $\mathbb{Q}(t)/\mathbb{Q}(t)^\sigma$, of rank 2 by Proposition 3.6; or E itself. In particular E is not the pullback, along a map defined over $\mathbb{Q}$, of any of the families of [11] or of their 2-isogenous families, since such a pullback is defined over a field containing $\mathbb{Q}(c)$ (see (b)).

(b) For maps defined over $\overline{\mathbb{Q}}$ we use critical values. We call g a left factor of c if $c = g \circ \rho$ for a rational function ρ; a left factor has all its critical values among those of c. Each family of [11] is $E_{c_{\text{pub}}}$ scaled by a square as in (2.2), where c_{pub} is its map to the c-line. Its 2-isogenous family also has a point of order 6 and, being isogenous to it, rank 3. The 2-isogenous family is $E_{w_2 \circ c_{\text{pub}}}$ scaled by a square, where $w_2(c) = -(c+1)/(9c+1)$. Indeed, with $a(c) = 1+6c-3c^2$ and $b(c) = -16c^3$, the 2-isogenous curve $y^2 = x^3 - 2a(c)x^2 + (a(c)^2 - 4b(c))x$ is $E_{w_2(c)}$ scaled by the square $\mu = ((9c+1)/2)^2$: $-2a(c) = \mu\, a(w_2(c))$ and $a(c)^2 - 4b(c) = (c+1)^3(9c+1) = \mu^2\, b(w_2(c))$. The six maps c_{pub} have degrees 10, 4, 4, 4, 4 and 8. The first is Lecacheux's, and its degree does not divide 16. The others are, in the parameter t of [11] and in the order

Kihara, Eroshkin at $V = 1/3$ and at $V = -1/3$, Dujella–Peral, MacLeod,

$$\frac{-8t^4+50t^3+69t^2-175t-98}{8t^4-338t^3-789t^2+1183t+98}, \qquad \frac{-12t(t-2)(t+1)}{(t^2+2)^2}, \qquad \frac{-12t(2t-1)(t+1)}{16t^4-11t^2+4},$$

$$\frac{-t^4-24t^3-262t^2-1704t-4345}{t^4-2t^2+1248t+8737}, \qquad \frac{N_{\mathrm{M}}}{D_{\mathrm{M}}},$$

$$\begin{aligned} N_{\mathrm{M}} &= 17t^8-4408t^7-148516t^6+10431416t^5-139383418t^4 \\ &\quad +257277560t^3+3768607772t^2-10095985528t-21319623439, \\ D_{\mathrm{M}} &= 445t^8-26680t^7+298540t^6+7487800t^5-100559026t^4 \\ &\quad -816359048t^3+14922867436t^2-55316709112t+68821828189, \end{aligned}$$

and their critical values are, in the same order, $-1/17$, $-9/25$, $-25/169$; 3, $-3/2$, ∞; -3, $3/5$ and the roots of $9c^2-8c+16$; the roots of $13c^2+5c+1$ and of $27c^2+70c-21$; -3, $3/5$, $11/189$. The critical values of $w_2 \circ c_{\mathrm{pub}}$ are their images under w_2. The critical values of $c(t)$ are 0, -1 and the roots of $40095c^6+25272c^5+11286c^4+2708c^3+6119c^2-244c-68$, which is irreducible over $\mathbb{Q}$; since $c(1/t) = c(t)$, the critical point $t = \infty$ (of ramification index 2) has the value $c(0) = 0$. So no critical value of the ten maps c_{pub} and $w_2 \circ c_{\mathrm{pub}}$ of degree 4 or 8 is a critical value of $c(t)$: they are rational, quadratic over $\mathbb{Q}$ or ∞, and none is 0 or -1.

The points of order 6 of $E_c(\overline{\mathbb{Q}}(t))$ are $\pm T_c$. The 2-torsion polynomial $x^2+(1+6c-3c^2)x-16c^3$ has discriminant $(c+1)^3(9c+1)$. The polynomial $9N+D$ is square-free of degree 16 and prime to $N+D$, so $(N+D)(9N+D)$ is not a square in $\overline{\mathbb{Q}}[t]$, and $(0,0)$ is the only point of order 2. Next, the 3-division polynomial of E_c is $\psi_3 = (x-4c^2)(3x^3+(24c+4)x^2+16c^2x+64c^4)$. Its cubic factor is irreducible over $\mathbb{Q}$ as a polynomial in x and c, and the curve it defines has the smooth point $(x,c) = (-4/3, 0)$, so it is absolutely irreducible. Hence the cubic factor has no root in $\overline{\mathbb{Q}}(t)$ when $c = c(t)$, as $3 \nmid 16$, and the 3-torsion over $\overline{\mathbb{Q}}(t)$ is $\langle 2T_c \rangle$. A pullback of a published family along ρ is isomorphic to $\rho^* E_g = E_{g\circ\rho}$ with $g = c_{\mathrm{pub}}$, by (2.2), and a pullback of its 2-isogenous family is isomorphic to $E_{g\circ\rho}$ with $g = w_2 \circ c_{\mathrm{pub}}$, by the scaling above. An isomorphism $E_c \cong E_{g\circ\rho}$ over $\overline{\mathbb{Q}}(t)$ therefore maps T_c to $\pm T_{g\circ\rho}$, so $c = g \circ \rho$ (c is the Tate-normal-form parameter on $X_1(6)$), which the degrees and critical values above exclude.

Remark 3.9 (A second curve of rank four). There is a second elliptic curve over $\mathbb{Q}(s)$ with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank exactly 4, which is not related to E by base change and is not a base change of any of the families of [11], even over $\overline{\mathbb{Q}}$. The construction of Section 3.2 applies also to the family of twist data of Section 5, read as one twist datum over $\mathbb{Q}(s)$. With h, $\tilde{h}$ and φ_s the objects of Definition 2.9 for this twist datum, let

$$u_s = \frac{N_u(s)}{8(s-4)^2(s+2)^4(s^2-4s+6)^2(s^4-4s^3+60s^2-112s+136)} \cdot \frac{1}{s^6-6s^5+34s^4-96s^3+156s^2-136s+128},$$

$$\begin{aligned}N_u(s) = 5s^{20} - 108s^{19} + 452s^{18} + 4144s^{17} - 115992s^{16} + 1262912s^{15}\\ - 9934784s^{14} + 60351936s^{13} - 289077232s^{12} + 1102350528s^{11}\\ - 3390499392s^{10} + 8497369600s^{9} - 17469156352s^{8} + 29523179520s^{7}\\ - 41049909248s^{6} + 46893897728s^{5} - 43590451200s^{4} + 32079142912s^{3}\\ - 17818566656s^{2} + 6906347520s - 1230962688.\end{aligned}$$

Then $h(u_s)$ and $\tilde{h}(u_s)$ are squares in $\mathbb{Q}(s)$, so the genus-one curve of this twist datum has points ξ_s over $\mathbb{Q}(s)$ with $u(\xi_s) = u_s$; changing the signs of $z_1(\xi_s)$ and $z_2(\xi_s)$ changes only the signs of the points below. The map $c_2(s) = \varphi_s(\xi_s)$ has degree 40; its numerator and denominator have degrees 38 and 40. Reduction at ξ_s (Remark 3.2(2)) sends the images of the family's two twist points and their transforms to four points of $E_{c_2(s)}$ over $\mathbb{Q}(s)$. One checks, as in Section 3, with the data in [18], that these points are independent and that $E_{c_2(s)}$ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ and rank exactly 4 over $\mathbb{Q}(s)$: the hypothesis of Theorem 2.6 holds at $s = -16$, and a 2-descent of that fiber gives the upper bound 4, which its four specialized points attain. This curve is not related to E by base change, in either direction and even over $\overline{\mathbb{Q}}$ (compare the degrees 192 and 480 of their j-invariants). Moreover $c_2(s) = \tilde{c}((s-1)^2)$, where $\tilde{c}$ has degree 20, a simple zero at ∞ and 38 simple critical points with distinct critical values, $\tilde{c}(0) = 0$, and neither 0 nor ∞ is a critical point of $\tilde{c}$. So the ramification indices of c_2 are at most 2, with at most four ramified points over each value and more than two only over $c = 0$. If $c_2 = g \circ \rho$ with $\deg g \geq 2$ and $\deg \rho = m \geq 2$, then c_2 has at least m ramified points above each critical value of g. Indeed, above a ramification point of g all m points of the fiber of ρ are ramified for c_2, and the indices are at most 2. So $m \leq 4$. As m divides 40, m is 2 or 4, and $m = 4$ would put all critical values of g at $c = 0$. This is impossible, since a rational function of degree at least 2 has at least two critical values. Hence $m = 2$: the left factors of c_2 have degrees 1, 20 and 40. Neither 20 nor 40 divides 16, so c_2 and (1.2) have no common left factor of degree at least 2. As the maps c_{pub} have degrees 10, 4 and 8, E_{c_2} is not a base change of any of the families of [11], even over $\overline{\mathbb{Q}}$. Here, as in Remark 3.8, the points of order 6 of $E_{c_2}(\overline{\mathbb{Q}}(s))$ are $\pm T_{c_2}$, since $(c_2+1)(9c_2+1)$ has a simple zero and $3 \nmid 40$.

4. Rank five over an elliptic curve of rank two: proof of Theorem 1.2

Throughout this section $H_1 = 4u^2 - 60u + 113$ and $H_2 = 64u^2 - 7$, so that $\mathcal{C}$ is $z_1^2 = H_1$, $z_2^2 = H_2$, and

$$c(u) = \frac{n}{d}, \qquad n = -24u - 12, \quad d = 32u^2 - 48u + 40,$$

with $A = d^2 + 6nd - 3n^2$ and $B = -16n^3 d$ as in (2.2).

4.1. The curve.

Lemma 4.1. *The curve $\mathcal{C}$ is smooth of genus one, its smooth projective model has the rational points $(u, z_1, z_2) = (1/3, 29/3, 1/3)$ and $(1 : \pm 2 : \pm 8 : 0)$, and $\mathcal{C}(\mathbb{Q})$ is infinite. Its Jacobian is*

$$y^2 + xy = x^3 - 66791x + 6638025,$$

of conductor $331170 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 83$, with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$ and rank 2; the points $(-242, 3061)$ and $(598, 13141)$ are independent.

Proof. The quadratics H_1 and H_2 have discriminant 1792 each and resultant 51094800, so they are square-free and coprime, and $\mathcal{C} \to \mathbb{A}^1_u$ is a $(\mathbb{Z}/2\mathbb{Z})^2$-cover branched exactly over the four roots $(15 \pm 4\sqrt{7})/2$ and $\pm\sqrt{7}/8$, with two points of index 2 above each and no branching at $u = \infty$. By the Riemann–Hurwitz formula $2g - 2 = 4 \cdot (-2) + 8$, so $g = 1$; the closure in $\mathbb{P}^3$ is a smooth intersection of two quadrics, whose points at infinity are $(1 : \pm 2 : \pm 8 : 0)$. With $r = 2u - 15 + z_1$ one has $u = (r + 112/r + 30)/4$ and $z_1 = (r - 112/r)/2$, and $w = rz_2$ satisfies $w^2 = 4r^4 + 240r^3 + 4489r^2 + 26880r + 50176$; the classical invariants of this quartic [2, §3.6] give the displayed Jacobian. Its torsion subgroup is $\mathbb{Z}/4\mathbb{Z}$: the point $(178, 541)$ has order 4, and the torsion subgroup injects into the groups of points over $\mathbb{F}_{11}$ and $\mathbb{F}_{41}$ [39, §VII.3], which have orders 16 and 44. Its rank is at least 2. Indeed, at $p = 17$ and $p = 23$ its group of points over $\mathbb{F}_p$ has order 24, and the images of $(-242, 3061)$ and $(598, 13141)$ in that group modulo 3, identified with $\mathbb{Z}/3\mathbb{Z}$ so that the image of the first point is 1, are $(1, 0)$ at $p = 17$ and $(1, 2)$ at $p = 23$, which are independent over $\mathbb{F}_3$. As there is no 3-torsion, the two points are independent by Lemma 2.7. The rank is at most 2 by 2-descent (`mwrank`, which finds 2-Selmer rank 3, and `ellrank`). As $\mathcal{C}$ has a rational point, it is isomorphic to its Jacobian, so $\mathcal{C}(\mathbb{Q})$ is infinite. □

4.2. **The map and the involution.** The involution $\iota(u) = (4-u)/(2u+1)$ satisfies $c \circ \iota = c$; it is the non-trivial automorphism of $u \mapsto c(u)$, whose branch points are $c = -3/2$ and $c = 3/22$, since the discriminant of $cd - n$ in u is $-64(2c + 3)(22c - 3)$. One checks

$$H_1(\iota(u)) = \frac{9H_2(u)}{(2u+1)^2}, \qquad H_2(\iota(u)) = \frac{9H_1(u)}{(2u+1)^2}, \qquad d(\iota(u)) = \frac{9d(u)}{(2u+1)^2}, \tag{4.1}$$

so $\tilde{\iota}(u, z_1, z_2) = \big(\iota(u), 3z_2/(2u+1), 3z_1/(2u+1)\big)$ is an automorphism of $\mathcal{C}$, and the map $\varphi = c(u) \colon \mathcal{C} \to \mathbb{P}^1$ of degree 8 satisfies $\varphi \circ \tilde{\iota} = \varphi$. These are the objects of Lemma 2.10 for the twist datum $\mathcal{D} = (8, -4, -15, \frac{113}{4})$: there $\kappa = 2$, $\lambda = \frac{9}{4}$, $h = H_1/4$ and $\tilde{h} = \frac{9}{16}H_2$, and $\tilde{\iota}$ is the lemma's lift in the coordinates $z_1/2$, $3z_2/4$. Over the cusps $c \in \{0, -1, -1/9, \infty\}$ the values of u are $u = -1/2, \infty$ over 0; the roots of $n + d = 4(4u - 7)(2u - 1)$ over -1; those of $9n + d = 4(2u - 17)(4u + 1)$ over $-1/9$; and those of d over ∞. Over each cusp the two values of u are distinct, and H_1H_2 does not vanish there. So φ is unramified over the cusps, and above each cusp lie 8 points of the smooth projective model of $\mathcal{C}$; the proof of Proposition 4.3 uses this.

4.3. **Five points.** On $Y^2 = X^3 + AX^2 + BX$ and on its quadratic twist $Y^2 = X^3 + H_1AX^2 + H_1^2BX$ we have the points

$$\begin{aligned}
F\colon\ & X = 128(2u+1)^3, \quad Y = 512(2u-3)(2u+1)^3(4u-7),\\
Q_a\colon\ & X = 3456(2u-5)^2(2u+1)(4u^2-6u+5),\\
& Y = 13824(2u-5)(2u-3)(2u+1)(4u-7)(4u^2-6u+5)(4u^2+12u-31),\\
Q_b\colon\ & X = 512(2u+1)(2u^2-3u-11)^2,\\
& Y = 2048(2u+1)(4u-7)(2u^2-3u-11)(8u^4-84u^3+86u^2-123u+122),
\end{aligned}$$

F on the first curve and Q_a, Q_b on the twist, as one checks directly. Here $H_1/4$ is the quadratic h of the twist datum $\mathcal{D}$ above (the line $V = -2/3$ singled out by the scan described in Section 4.6), and we found Q_a by interpolation from integral values of u. With $F = (X_F, Y_F)$, $Q_a = (X_a, Y_a)$ and $Q_b = (X_b, Y_b)$, they give five points of $E_{c(u)}$ over the

function field $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(u, z_1, z_2)$:

$$P_1 = \Big(\frac{X_F}{d^2}, \frac{Y_F}{d^3}\Big), \qquad P_2 = \Big(\frac{X_a}{H_1 d^2}, \frac{Y_a}{H_1 z_1 d^3}\Big), \qquad P_3 = \Big(\frac{X_b}{H_1 d^2}, \frac{Y_b}{H_1 z_1 d^3}\Big), \tag{4.2}$$
$$P_4 = \tilde{\iota}^* P_2, \qquad P_5 = \tilde{\iota}^* P_3,$$

where $\tilde{\iota}^*$ replaces (u, z_1, z_2) by $\tilde{\iota}(u, z_1, z_2)$; by (4.1), P_4 and P_5 again lie on $E_{c(u)}$, since $c \circ \iota = c$. As $H_1 = 4h$, the map $(X, Y) \mapsto (X/4, Y/8)$ takes the twist by H_1 to the twist by h; so P_2, P_3 are the images of $(X_a/4, Y_a/8)$ and $(X_b/4, Y_b/8)$, points of the twist by h of the shapes (ii) and (i) of Lemma 2.10(e) (with $W = 6(2u-5)$ and $q = 8(2u^2 - 3u - 11)$), and P_4, P_5 are their transforms.

Proposition 4.2. *The points $P_1, \dots, P_5$ are linearly independent in $E_{c(u)}(\mathbb{Q}(\mathcal{C})) \otimes \mathbb{Q}$.*

Proof. At the rational point $(u_0, z_1, z_2) = (-1199/222, 2612/111, 4787/111)$ of $\mathcal{C}$ one has $c(u_0) = 181152/1898473 \notin \{0, -1, -1/9\}$, and none of d, H_1, $2u+1$ and their transforms by ι vanishes, so specialization at this point (the map σ_ξ of Section 2.3) is a homomorphism $E_{c(u)}(\mathbb{Q}(\mathcal{C})) \to E_{c(u_0)}(\mathbb{Q})$, defined on the five points. Neither $-c(u_0)$ nor $(c(u_0)+1)(9c(u_0)+1)$ is a square, so $E_{c(u_0)}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ by Corollary 2.3. At the primes $p = 47$, 59, 107, 163 and 179, all of good reduction, where $E_{c(u_0)}(\mathbb{F}_p)$ has a non-trivial cyclic 5-Sylow subgroup, identify $E_{c(u_0)}(\mathbb{F}_p)/5E_{c(u_0)}(\mathbb{F}_p)$ with $\mathbb{Z}/5\mathbb{Z}$ so that the first non-zero image of a specialized point is 1. The images of the specializations of $P_1, \dots, P_5$, in this order, are then $(1, 4, 4, 0, 1)$ at $p = 47$, $(1, 3, 4, 2, 0)$ at $p = 59$, $(1, 1, 2, 3, 2)$ at $p = 107$, $(1, 3, 1, 4, 4)$ at $p = 163$ and $(0, 1, 2, 2, 2)$ at $p = 179$, and the matrix of these five vectors has determinant 4 over $\mathbb{F}_5$. So the specialized points, and hence $P_1, \dots, P_5$, are independent by Lemma 2.7. □

4.4. **Torsion.**

Proposition 4.3. *For all but finitely many $\xi \in \mathcal{C}(\mathbb{Q})$ the curve $E_{\varphi(\xi)}$ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$.*

Proof. Only finitely many points lie over the cusps. At any other ξ, by Corollary 2.3 the torsion is $\mathbb{Z}/6\mathbb{Z}$ unless $-\varphi(\xi)$ or $(\varphi(\xi)+1)(9\varphi(\xi)+1)$ is a square in $\mathbb{Q}$, in which case ξ lifts to a rational point of one of the double covers $w^2 = -\varphi$ and $w^2 = (\varphi+1)(9\varphi+1)$ of the smooth projective model of $\mathcal{C}$. Since φ is unramified over the cusps, $-\varphi$ has simple zeros at the 8 points over 0 and simple poles at the 8 points over ∞, and $(\varphi+1)(9\varphi+1) = (n+d)(9n+d)/d^2$ has simple zeros at the 16 points over -1 and $-1/9$ and poles of even order. So each double cover is geometrically irreducible and branched at exactly 16 points, and by the Riemann–Hurwitz formula it has genus 9. By Faltings' theorem [14, Satz 7] each has finitely many rational points. □

4.5. **Proof of Theorem 1.2.** By Lemma 4.1, $\mathcal{C}$ is a smooth curve of genus one with infinitely many rational points. The j-invariant of $E_{c(u)}$ over $\mathbb{Q}(\mathcal{C})$ is $j(E_c) \circ \varphi$, which is non-constant, so by Theorem 2.4 and Proposition 4.2 the rank of $E_{\varphi(\xi)}(\mathbb{Q})$ is at least 5 for all but finitely many $\xi \in \mathcal{C}(\mathbb{Q})$, and the torsion is $\mathbb{Z}/6\mathbb{Z}$ outside a finite set by Proposition 4.3. A non-constant map $\mathcal{C} \to \mathbb{P}^1$ has finite fibers, so infinitely many j-invariants occur. The last assertion is Proposition 4.4. □

Proposition 4.4. *The curve $E_{c(u_0)}$, where $u_0 = -1199/222$ and $c(u_0) = 181152/1898473$, has the minimal model*

$$y^2 + xy = x^3 - 65745799435837346242891 0\, x + 20516433167380447195636 2048386260100,$$

of conductor $2\cdot3\cdot5\cdot17\cdot37\cdot127\cdot131\cdot619\cdot1543\cdot2287\cdot3067$*; its torsion subgroup is* $\mathbb{Z}/6\mathbb{Z}$ *and its rank is exactly* 6.

Proof. The torsion was found in the proof of Proposition 4.2. The six points of Table 4, which `mwrank` finds, lie on the minimal model. At the primes $p = 47$, 59, 107, 163, 167 and 179, all of good reduction, where its group of points over $\mathbb{F}_p$ has a non-trivial cyclic 5-Sylow subgroup, identify that group modulo 5 with $\mathbb{Z}/5\mathbb{Z}$ so that the first non-zero image of one of the six points is 1. The images of the six points, in the order of Table 4, are then $(0,0,1,3,2,4)$ at $p=47$, $(1,0,4,0,1,1)$ at $p=59$, $(1,3,0,2,4,3)$ at $p=107$, $(1,4,0,3,2,4)$ at $p=163$, $(0,1,1,4,1,1)$ at $p=167$ and $(1,1,0,3,4,2)$ at $p=179$, and these six vectors are linearly independent over $\mathbb{F}_5$, so the six points are independent by Lemma 2.7. A 2-descent through the rational 2-isogeny (`mwrank`: the Selmer groups of the 2-isogeny and of its dual have ranks 5 and 3, and the 2-Selmer rank is $7 = 6+1$) and PARI's `ellrank` both give the upper bound 6. □

TABLE 4. Six independent points on the minimal model of $E_{c(u_0)}$, where $u_0 = -1199/222$ and $c(u_0) = 181152/1898473$.

(x, y)
$(1888649992223/4,\ 944213759652673/8)$
$(-835121738180,\ -414468213180786110)$
$(-64451165999140/361,\ -3860909012148798241450/6859)$
$(606333911420,\ 171575761543188290)$
$(23717141180359939580/564001,\ -1154817593956164512348005590 10/423564751)$
$(1185881717587472380/998001,\ -1046474088097179874413417490/997002999)$

Remark 4.5. We tested every rational number $u = a/b$ in lowest terms with $|a| \le 1200$ and $1 \le b \le 1200$: $H_1(u)$ and $H_2(u)$ are both squares exactly for $u = -1/2$ (over the cusp $c = 0$), 1/3, 4/3, 11/5, 8/11 and $-1199/222$. The fibers over $u = 1/3$ and $u = 11/5 = \iota(1/3)$ (where $c = -45/62$) have rank at most 2, and those over $u = 4/3$ and $u = 8/11$ (where $c = -99/74$) rank at most 3, by a 2-descent through the rational 2-isogeny (`mwrank`; `ellrank` gives the same bounds). So the specialization of the five points is not injective there. Propositions 4.2 and 4.4 use the remaining value, $u_0 = -1199/222$.

4.6. **Relation with Eroshkin's family.** Dujella, Peral and Tadić [11, §5.1] published a two-parameter family due to Eroshkin (2008, personal communication): the curve $y^2 = x^3 + A_{\mathrm{Er}}(U,V)x^2 + B_{\mathrm{Er}}(U,V)x$ over $\mathbb{Q}(U,V)$ (we write U, V for their u, v), where A_{Er} is their polynomial $A(u,v)$, of degree 12, and $B_{\mathrm{Er}} = -16(U+V)^3(V-1)^3(V+1)^3(U-1)^3(U+1)^3D_{\mathrm{Er}}$, where

$$D_{\mathrm{Er}} = U^2+UV+V^2-2VU^2-2V^2U+U^3V+V^3U-2U^3V^2-2U^2V^3+U^4V^2+V^4U^2+U^3V^3,$$

together with two points, with x-coordinates $4(V-1)^2(V+1)^3(U-1)^2(U+1)^3$ and $-4(U-1)(U+1)(V-1)^3(V+1)^2(U+V)^3$. They proved in [11, §5.2] that the lines $V = 1/3$ and $V = -1/3$ give families of rank exactly 3 over $\mathbb{Q}(t)$, $U = (1-t)/(1+t)$.

Lemma 4.6. (a) *With* $N_{\mathrm{Er}} = (U+V)(V^2-1)(U^2-1)$ *one has* $A_{\mathrm{Er}} = D_{\mathrm{Er}}^2 + 6N_{\mathrm{Er}}D_{\mathrm{Er}} - 3N_{\mathrm{Er}}^2$ *and* $B_{\mathrm{Er}} = -16N_{\mathrm{Er}}^3D_{\mathrm{Er}}$*; so Eroshkin's family is* $E_{c_{\mathrm{Er}}}$ *with* $c_{\mathrm{Er}} = N_{\mathrm{Er}}/D_{\mathrm{Er}}$*, scaled as in* (2.2).

(b) *At* $V=-2/3$ *the map* $U\mapsto c_{\mathrm{Er}}(U,-2/3)$ *has degree* 4 *and is invariant under* $\tau(U)=(2U-3)/(3U-2)$, *and*

$$c_{\mathrm{Er}}(U,-2/3)=c\Big(-\frac{1}{2}+\frac{3}{5}\big(U+\tau(U)\big)\Big),$$

with $c(u)$ *the map of Theorem 1.2.*

(c) *Put* $q_{\mathrm{Er}}=(3U^2-10U+12)(12U^2-10U+3)$. *Then* $c_{\mathrm{Er}}(U,-2/3)=-15(3U-2)(U^2-1)/q_{\mathrm{Er}}$ *and* $D_{\mathrm{Er}}(U,-2/3)=q_{\mathrm{Er}}/81$, *and we write* γ *for* $c_{\mathrm{Er}}(U,-2/3)$. *Under the substitution of (b) the point* P_1 *of (4.2) pulls back to the point* (x_1,y_1) *of* E_γ *with* $x_1=720(U^2-1)^3(3U-2)/q_{\mathrm{Er}}^2$, $y_1=x_1(4U^2-15U+6)(9U^2-30U+11)/q_{\mathrm{Er}}$. *Eroshkin's second* x*-coordinate at* $V=-2/3$, *divided by* D_{Er}^2 *as in (2.2), gives the point* $P_{\mathrm{Er}}=(x_2,y_2)$ *of* E_γ *with* $x_2=500(U^2-1)(3U-2)^3/q_{\mathrm{Er}}^2$, $y_2=x_2(8U^2-15U+2)(9U^2-15U+1)/q_{\mathrm{Er}}$. *These two points and* $4T_\gamma=(4\gamma^2,4\gamma^2(\gamma+1))$ *lie on the line*

$$y=\frac{36U^4-255U^3+323U^2-45U-34}{q_{\mathrm{Er}}}\,x+\frac{18000(U^2-1)^3(3U-2)^3}{q_{\mathrm{Er}}^3},$$

and their x*-coordinates are distinct; so the pullback of* P_1 *is* $-P_{\mathrm{Er}}-4T_\gamma=-P_{\mathrm{Er}}+2T_\gamma$, *where* T_γ *is the point* T_c *of (1.1) on* E_γ *(*$2T_\gamma$ *has order* 3*).*

(d) *At* $V=-1/3$ *and* $U=(1-t)/(1+t)$, $c_{\mathrm{Er}}=\gamma_1(t)$ *with* $\gamma_1(t)=-12t(2t-1)(t+1)/(16t^4-11t^2+4)$.

Proof. Parts (a), (b) and (d) are identities between rational functions, and part (c) is a relation between two points of E_γ over $\mathbb{Q}(U)$, checked with the group law. All four were checked against the formulas printed in [11, §5.1], in (a) against their $A(u,v)$ and $B(u,v)$ [18]. □

So the map $u\mapsto c(u)$ of Theorem 1.2 and the point P_1 come from Eroshkin's family as published in [11, §5.1], for whose member $V=-2/3$ the map to the c-line is $c(u)$ composed with the quotient by the involution τ; the curve $\mathcal{C}$ and the points $P_2,\dots,P_5$ are constructed here. We found this member by a scan along a one-parameter family of twist data through the twist datum $(4,1,0,2)$ of the line $V=-1/3$ (Lemma 4.6(d), Section 2.5), which estimated, for each datum, the rank over the function field of its genus-one curve from averages over primes p of the fiber sums $-\frac{1}{p}\sum a_p$ modulo p, in the manner of Nagao's formula [29, 33]; besides that line, the scan singled out only the line $V=-2/3$ and one degenerate member. No proof uses the scan.

Remark 4.7. A further construction also gives infinitely many curves over $\mathbb{Q}$ with a point of order 6 and rank at least 5 (by Theorem 2.4, as in the proof of Theorem 1.2). Over the genus-one curve $z^2=64t^4+48t^3-47t^2-24t+16$, which has infinitely many rational points, the curve $E_{\gamma_1(t)}$ with $\gamma_1(t)=-12t(2t-1)(t+1)/(16t^4-11t^2+4)$, the line $V=-1/3$ of Eroshkin's family, has rank exactly 5 over the function field. The points $S_1(t)$, $S_2(t)$, $S_3(t)$ of [11, §5.1] and $S_2(t')$, $S_3(t')$ are independent points, where $t'=\big(-(8t^2-5t-4)+3z\big)/\big(2(16t^2+8t-8)\big)$ is a root of the quadratic factor of $\gamma_1(X)-\gamma_1(t)$. The curve $z^2=64t^4+48t^3-47t^2-24t+16$ has infinitely many rational points because, with the point at infinity where $z/t^2\to 8$ as origin, its point $(t,z)=(1/2,3/2)$ has infinite order: its reductions modulo 5 and 7, primes of good reduction (the quartic has discriminant $2^{20}3^4\cdot 11\cdot 19$), have orders 2 and 3, and a point of finite order keeps its order in the reduction at a prime $p\ge 3$ of good reduction [39, §VII.3]. On the model (2.2) with $n=-12t(2t-1)(t+1)$ and $d=16t^4-11t^2+4$, which is the curve printed in [11, §5.1], the points S_1, S_2, S_3 have X-coordinates $1728t^2(t+1)^3$,

$864t^3(2t-1)^3$ and $864t^3(t+1)^2(2t-1)$. For the lower bound, at $(t,z)=(-32/21,4804/441)$, where $t'=17/55$ and $c=1884960/3146929$, the curve E_c over $\mathbb{Q}$ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$. At the primes $p=47$, 53, 101, 103 and 109, of good reduction for E_c, the images of the specializations of $S_1(t)$, $S_2(t)$, $S_3(t)$, $S_2(t')$, $S_3(t')$ in $E_c(\mathbb{F}_p)/5E_c(\mathbb{F}_p)\cong\mathbb{Z}/5\mathbb{Z}$, normalized as in Proposition 4.2 (with the Y-coordinates of S_1, S_2, S_3 chosen as the polynomials in t with leading coefficients -82944, 110592 and -27648), are

$$(1,3,4,1,1),\quad (1,0,4,2,2),\quad (1,3,3,4,1),\quad (1,1,0,2,4),\quad (1,2,0,4,0),$$

at $p=47$, 53, 101, 103 and 109 respectively, which are linearly independent over $\mathbb{F}_5$; so the specialized points, and hence these five points, are independent by Lemma 2.7. The upper bound is proved in Appendix B.

5. Rank six over $\mathbb{Q}(\sqrt{2})$: proof of Theorem 1.3

Let $K=\mathbb{Q}(\sqrt{2})$. The proof of Theorem 1.3 follows that of Theorem 1.2, with the twist datum

$$e=\tfrac{64}{7}-\tfrac{64}{21}\sqrt{2},\quad f=-\tfrac{40}{7}+\tfrac{40}{21}\sqrt{2},\quad h_1=-\tfrac{227}{16}-\tfrac{81}{8}\sqrt{2},\quad h_0=\tfrac{571}{16}+\tfrac{405}{16}\sqrt{2}$$

over K (Definition 2.9) in place of the twist datum $(8,-4,-15,\frac{113}{4})$ of Section 4. How this twist datum was found is told at the end of this section. We mark the objects of Definition 2.9 attached to this twist datum with a subscript K: with $n=-12(2u+1)$ as before,

$$d_K=(\tfrac{256}{7}-\tfrac{256}{21}\sqrt{2})u^2+(-\tfrac{440}{7}+\tfrac{608}{21}\sqrt{2})u+(52-\tfrac{40}{3}\sqrt{2}),$$
$$h_K=u^2+(-\tfrac{227}{16}-\tfrac{81}{8}\sqrt{2})u+(\tfrac{571}{16}+\tfrac{405}{16}\sqrt{2}),$$

and $c_K(u)=n/d_K$. Here $\kappa=\frac{73}{32}$ and $\lambda=\frac{81}{32}$, so the involution of c_K is $\iota_K(u)=(-u/2+73/32)/(u+1/2)$, and

$$\tilde{h}_K(u)=(u+\tfrac{1}{2})^2h_K(\iota_K(u))=(\tfrac{1377}{32}+\tfrac{243}{8}\sqrt{2})u^2+(\tfrac{2349}{512}+\tfrac{1215}{256}\sqrt{2})u+(-\tfrac{1053}{512}-\tfrac{2673}{512}\sqrt{2}).$$

Let $\mathcal{C}'$ be the smooth projective model of the curve $z_1^2=h_K(u)$, $z_2^2=\tilde{h}_K(u)$ over K (the curve $\mathcal{C}_{\mathcal{D}}$ of Definition 2.9 for this twist datum), and $\varphi_K=c_K(u)\colon\mathcal{C}'\to\mathbb{P}^1$. With $A=d_K^2+6nd_K-3n^2$ and $B=-16n^3d_K$ as in (2.2), consider on the twist $Y^2=X^3+h_KAX^2+h_K^2BX$ over $K(u)$ the points

$$R_a=\big(3(2u+1)d_K\,W^2,\ 3(2u+1)(4u-7)d_K\,W\,r_a\big),$$
$$R_b=\big(2(2u+1)q_b^2,\ 2(2u+1)(4u-7)q_b\,r_b\big),$$
$$R'=\big(2(2u+1)q'^2,\ 2(2u+1)(4u-7)q'r'\big),$$

of the shapes (ii), (i) and (i) of Lemma 2.10(e), where

$$\begin{aligned}
W &= (4+6\sqrt{2})u - (\tfrac{41}{2}+15\sqrt{2}),\\
r_a &= \tfrac{128}{3}\sqrt{2}\,u^3 + (120+64\sqrt{2})u^2 - (717+508\sqrt{2})u + (\tfrac{1653}{2}+\tfrac{3515}{6}\sqrt{2}),\\
q_b &= (\tfrac{128}{7}-\tfrac{192}{7}\sqrt{2})u^2 + (-10+42\sqrt{2})u + (83+51\sqrt{2}),\\
r_b &= (\tfrac{16384}{49}-\tfrac{45056}{147}\sqrt{2})u^4 + (\tfrac{34688}{49}+\tfrac{106880}{147}\sqrt{2})u^3 - (\tfrac{9840}{7}+\tfrac{8032}{7}\sqrt{2})u^2\\
&\quad + (1940+\tfrac{4430}{3}\sqrt{2})u - (1646+\tfrac{3557}{3}\sqrt{2}),\\
q' &= (32+32\sqrt{2})u^2 + (-94-58\sqrt{2})u + (-55-37\sqrt{2}),\\
r' &= (\tfrac{2048}{21}+\tfrac{4096}{21}\sqrt{2})u^4 + (\tfrac{49024}{21}+\tfrac{33536}{21}\sqrt{2})u^3 + (-\tfrac{57296}{7}-\tfrac{41008}{7}\sqrt{2})u^2\\
&\quad + (\tfrac{748}{3}+\tfrac{578}{3}\sqrt{2})u + (\tfrac{7370}{3}+\tfrac{5245}{3}\sqrt{2}).
\end{aligned}$$

Theorem 5.1. (a) *$\mathcal{C}'$ is a curve of genus one over K with the K-point $(u, z_1, z_2) = (7/4, -\frac{27}{8}-\frac{9}{8}\sqrt{2}, -\frac{243}{32}-\frac{405}{64}\sqrt{2})$; its Jacobian is isomorphic over K to the base change of*

$$J\colon\ y^2 = x^3 + x^2 - 1133697x + 464225247,$$

of conductor 30912, and $J(K)$ has rank 2. So $\mathcal{C}'(K)$ is infinite.

(b) *φ_K has degree 8 and is unramified over the cusps $0, -1, -1/9, \infty$.*

(c) *R_a, R_b, R' lie on $Y^2 = X^3 + h_K AX^2 + h_K^2 BX$ and generate a subgroup of rank 3 of its group of $K(u)$-points.*

(d) *$E_{c_K(u)}$ has rank at least 6 over $K(\mathcal{C}')$.*

(e) *For all but finitely many $\xi \in \mathcal{C}'(K)$, $E_{\varphi_K(\xi)}(K)_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ and $\operatorname{rank} E_{\varphi_K(\xi)}(K) \geq 6$; these curves have infinitely many j-invariants.*

Theorem 1.3 is part (e), with (a) and (b).

Proof. (a) The quadratics h_K and $\tilde{h}_K$ are square-free and coprime, and $h_K(-\frac{1}{2}) \neq 0$ (it is the leading coefficient of $\tilde{h}_K$), so Lemma 2.10 applies, and by Lemma 2.10(b) the curve has genus one; the point is checked directly ($c_K(7/4) = -1$, a cusp, which does not matter for its use as a base point). A quartic model of $\mathcal{C}'$, built from its K-points over $u = \infty$ and passing through the point over $u = 7/4$, is

$$\begin{aligned}
z^2 &= (\tfrac{1377}{32}+\tfrac{243}{8}\sqrt{2})r^4 + (-\tfrac{2349}{256}-\tfrac{1215}{128}\sqrt{2})r^3 + (-\tfrac{51742719}{8192}-\tfrac{9177381}{2048}\sqrt{2})r^2\\
&\quad + (\tfrac{1099413}{4096}+\tfrac{784161}{4096}\sqrt{2})r + (\tfrac{3725399547}{16384}+\tfrac{10537018245}{65536}\sqrt{2}),
\end{aligned}$$

with $z_1 = u + r$ and $z = (2r - h_1)z_2$. Its classical invariants [2, §3.6] give a Jacobian isomorphic over K to J. Over K, $J(K)\otimes\mathbb{Q} \cong (J(\mathbb{Q})\oplus J^{(2)}(\mathbb{Q}))\otimes\mathbb{Q}$, where $J^{(2)}\colon y^2+xy+y = x^3+x^2-17714x+900047$ is the twist of J by 2, of conductor 966. Each of $J(\mathbb{Q})$ and $J^{(2)}(\mathbb{Q})$ has rank exactly 1: $(267, 13440)$ and $(-135, 991)$ have infinite order, and 2-descents through the rational 2-isogenies (`mwrank`: 2-Selmer rank 2, so rank at most 1, for each) and `ellrank` give the upper bound 1. As $\mathcal{C}'$ has a K-point, it is isomorphic to its Jacobian, so $\mathcal{C}'(K)$ is infinite.

(b) c_K has degree 2 in u and $\mathcal{C}' \to \mathbb{P}^1_u$ has degree 4. The preimages under c_K of the cusps $c = 0$, -1, $-1/9$ and ∞ are, respectively, $u = -1/2$ and $u = \infty$; the roots $7/4$ and $5/8$ of $n + d_K = 4e(u - \frac{7}{4})(u - \frac{5}{8})$; the roots $\frac{25}{4}+\frac{9}{2}\sqrt{2}$ and $\frac{23}{8}-\frac{9}{4}\sqrt{2}$ of $9n + d_K$; and the two roots of d_K, which is irreducible over K with discriminant of norm $2^{12}3^8\cdot 17/7^2$. So the two values of u over each cusp are distinct. The polynomials h_K and $\tilde{h}_K$ have degree 2, so $\mathcal{C}' \to \mathbb{P}^1_u$ is

unramified over $u=\infty$, and $h_K\tilde{h}_K$ does not vanish at the other seven values of u: its values at $-1/2$, $7/4$ and $5/8$ have norms $3^{24}/2^{30}$, $3^{24}7^4/2^{34}$ and $3^{24}7^4/2^{38}$, and its resultants with $9n+d_K$ and with d_K have norms $3^{48}17^2/2^8$ and $3^{48}7^4/2^{16}$. So φ_K is unramified over the cusps.

(c) The points are checked directly. To see that they are independent, let E' be the twist $Y^2=X^3+h_KAX^2+h_K^2BX$. It has no point of order 11 over $K(u)$, since such a point would give a non-constant map from $\mathbb{P}^1$ to $X_1(11)$, which has genus 1 ($j(E')=j(E_{c_K(u)})$ is not constant). Let $\mathfrak{p}=(103,\sqrt{2}-38)$, a prime of K of degree one. For $u_1=34$, 44 and 86 the fiber E'_{u_1} has good reduction at $\mathfrak{p}$, with $88=8\cdot 11$ points over $\mathbb{F}_{103}$, so specialization at u_1, reduction modulo $\mathfrak{p}$ and the quotient by 11 times the group of points over $\mathbb{F}_{103}$ give a homomorphism $\theta_{u_1}\colon E'(K(u))\to\mathbb{Z}/11\mathbb{Z}$ (the coordinates of R_a, R_b, R' are polynomials in u). We identify the quotients with $\mathbb{Z}/11\mathbb{Z}$ so that $\theta_{34}(R_a)=\theta_{44}(R_a)=\theta_{86}(R_b)=1$. Then the vectors $(\theta_{u_1}(R_a),\theta_{u_1}(R_b),\theta_{u_1}(R'))$ are $(1,6,1)$, $(1,5,3)$ and $(0,1,5)$ [18], and have rank 3 over $\mathbb{F}_{11}$. As in the proof of Lemma 2.7, if $m_aR_a+m_bR_b+m'R'$ were torsion with integers m_a, m_b, m' not all divisible by 11 (to which any relation reduces), it would have order prime to 11, hence lie in $11E'(K(u))$ and in the kernel of each θ_{u_1}, and (m_a,m_b,m') would be a non-zero solution modulo 11 of three independent linear equations. So R_a, R_b, R' are independent.

(d) The twist datum of this section satisfies the hypotheses of Lemma 2.10 by (a) and (b) ($h_K(-\frac{1}{2})\neq 0$), with $\lambda=\frac{81}{32}$, so $\tilde{\iota}_K$ is the lift $\tilde{\iota}$ of the lemma. By Lemma 2.10(c) and (d) with $m=3$, the images of R_a, R_b, R' in $E_{c_K(u)}(K(\mathcal{C}'))$ and their transforms by $\tilde{\iota}_K$ are six independent points, as R_a, R_b, R' are independent by (c).

(e) The j-invariant $j(E_c)\circ\varphi_K$ is non-constant, so by Theorem 2.4 over K the specialization is injective at all but finitely many $\xi\in\mathcal{C}'(K)$, which gives rank at least 6 there. For torsion, let ξ not lie over a cusp. By Lemma 2.2(b), $E_{\varphi_K(\xi)}$ has torsion $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. The last needs a primitive cube root of unity in the real field K (Lemma 2.1(c)). The groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ need $(\varphi_K(\xi)+1)(9\varphi_K(\xi)+1)\in K^{*2}$, and $\mathbb{Z}/12\mathbb{Z}$ needs $-\varphi_K(\xi)\in K^{*2}$ (Lemma 2.1); as in Proposition 4.3 the two double covers of $\mathcal{C}'$ that these conditions define have genus 9, so by Faltings' theorem only finitely many ξ qualify. Finally, $E_{\varphi_K(\xi)}(K)_{\mathrm{tors}}\cong\mathbb{Z}/18\mathbb{Z}$ does not occur: by [20, Theorem 8], $\mathbb{Q}(\sqrt{33})$ is the quadratic field of smallest absolute discriminant over which $\mathbb{Z}/18\mathbb{Z}$ appears as a torsion group, and the discriminant of K is $8<33$. Since $j(E_c)\circ\varphi_K$ has finite fibers, infinitely many j-invariants occur. □

Over $\mathbb{Q}$, Problem 2.6(b) of [6] remains open. We do not know whether $G(\mathbb{Z}/6\mathbb{Z})\geq 5$, nor the ranks of the curves $E_{c(u)}$ and $E_{c_K(u)}$ of Sections 4 and 5 over the function fields of $\mathcal{C}$ and $\mathcal{C}'$, for which Proposition 4.2 and Theorem 5.1(d) give the lower bounds 5 and 6.

How the twist datum was found. The proofs of Theorems 1.1, 1.2 and 1.3 do not use this account; Remark 3.9 does. The twist datum of this section is the member at $s_0=4-3\sqrt{2}$

of the family of twist data over $\mathbb{Q}(s)$ given by

$$e(s) = \frac{2(s+2)^2(s^2-4s+6)^2}{9(s-1)^2(s^2-2s+4)},$$
$$f(s) = -\frac{7s^6-64s^5+180s^4-352s^3+700s^2-192s+288}{18(s-1)^2(s^2-2s+4)},$$
$$h_1(s) = -\frac{(7s^4-84s^3+210s^2-196s+252)(7s^4-42s^3+192s^2-448s+480)}{14(s+2)^4(s^2-4s+6)^2},$$
$$h_0(s) = \frac{N_0(s)}{16(s+2)^6(s^2-4s+6)^2},$$
$$N_0(s) = 49s^{10}-1568s^9+18076s^8-106976s^7+389380s^6-958400s^5$$
$$+1728064s^4-2407808s^3+2428672s^2-1809408s+1041408,$$

whose member at $s=0$ is the twist datum $(8,-4,-15,\frac{113}{4})$ of Section 4. We found the family without a search, by deforming the twist datum of Section 4 in the one direction, found to first order, in which both points Q_a and Q_b persist, solving to high order in power series, and parametrizing the resulting curve of twist data, a rational plane sextic in (e,f). Along the family the twist by $h=u^2+h_1(s)u+h_0(s)$ has two points over $\mathbb{Q}(s)(u)$, of the shapes (ii) and (i) of Lemma 2.10(e), namely $(3(2u+1)d\,W(s)^2,\cdot)$ and $(2(2u+1)q(s)^2,\cdot)$ with

$$W(s) = \frac{3(s^2-2s+4)}{2(s-1)(s+2)}\Big(4u - \frac{7s^4-72s^3+174s^2-160s+240}{(s+2)^2(s^2-4s+6)}\Big),$$
$$q(s) = \frac{2(s-1)}{3(s^2-2s+4)}\Big(16(s^2-4s+6)u^2$$
$$-\frac{8(7s^6-73s^5+279s^4-577s^3+790s^2-1020s+432)}{(s+2)^2(s^2-4s+6)}\,u$$
$$+\frac{49s^7-728s^6+3712s^5-9124s^4+17252s^3-26320s^2+21792s-25344}{(s+2)^3(s^2-4s+6)}\Big),$$

whose Y-coordinates the equation of the twist determines up to sign; at $s=0$ they are $(X_a/4, Y_a/8)$ and $(X_b/4, Y_b/8)$ of Section 4, and at s_0 they are R_a and R_b.

The third point R' is where $\sqrt{2}$ enters. With $\omega^2 = 4u+2$ as in Lemma 2.10(e), one has $16h_K = (\omega^2-\alpha_1^2)(\omega^2-\alpha_2^2)$ with $\alpha_1 = 6+3\sqrt{2}$ and $\alpha_2 = \frac{3}{2}(1+\sqrt{2})$. In the factorizations $\mathcal{F}(\omega)\mathcal{F}(-\omega) = h_K^2(A^2-4B)$ of Lemma 2.10(e)(i), the factors of h_K enter $\mathcal{F}$ as $(\omega-\alpha_1)^2(\omega+\alpha_2)^2$ for R_b, where $(\omega-\alpha_1)(\omega+\alpha_2)$ is the value at s_0 of a factor of $16h$ with coefficients in $\mathbb{Q}(s)$, and as $(\omega+\alpha_1)^2(\omega^2-\alpha_2^2)$ for R', in which the pair $\pm\alpha_2$ over the root $\frac{19}{16}+\frac{9}{8}\sqrt{2}$ of h_K occurs with multiplicities 1, 1. For a twist datum over a field k that satisfies the hypotheses of Lemma 2.10, with $h \in k[u]$ prime to A^2-4B, a factorization in which the factors of h enter $\mathcal{F} \in k[\omega]$ in this way needs a root of h in k: the automorphisms of $\bar{k}$ over k permute the factors of h and preserve their multiplicities in $\mathcal{F}$, so they map the pair of multiplicity 1 to itself and fix the root of h over which it lies. Along the family h is prime to A^2-4B, and the discriminant of h in u is $13s^4-52s^3+96s^2-88s+112$ times a square in $\mathbb{Q}(s)$, so h has no root in $\mathbb{Q}(s)$. With $\eta = 3(s^2+2)/(2(s^2-4s+6))$ and $\zeta = 3(4-s)/(2(s+2))$, the family lies on a two-parameter family of twist data with parameters η and ζ, and s_0 is where it meets the line $\zeta = \frac{3}{2}(1+\sqrt{2})$, along which h splits and the twist has a point of the shape of R' [18]; at s_0 that point is R'.

Appendix A. Computations

The computations were done with PARI/GP 2.17.3 [30] and SageMath 10.9 [34], which includes Cremona's `mwrank` [2], in exact arithmetic, and no proof uses floating-point arithmetic. The programs, their outputs and the data are deposited in [18]. Together they take under an hour on one core of an AMD EPYC 4484PX processor, most of them a few seconds each; the deposit gives the time of each program. The primes in the proofs of Lemma 4.1 and Propositions 3.4, 4.2 and 4.4 are the first primes $p \geq 11$, in increasing order, at which the curve has good reduction, the points are integral and the group of points over $\mathbb{F}_p$ has a non-trivial cyclic ℓ-Sylow subgroup, with $\ell = 3$ for Lemma 4.1 and $\ell = 5$ for the others. Primes that do not raise the rank of the vectors are left out.

Section 3. We verify, in the coordinate t, the identities of Section 3.1, Tables 1, 2 and 3, the torsion and the reductions modulo 5 at $t_0 = 13/6$, the genera in the proof of Theorem 1.1(c), the height matrix of Proposition 3.5 and the data of Section 3.2. For Proposition 3.7 we verify the points M_g and their height matrix, find the primes for the 31 quartics at $t = 2$ and compute the reductions at $t = 2$ modulo 7, 11, 13, 19 and 29. For Remarks 3.8 and 3.9 we factor $N(T)D(t) - N(t)D(T)$ and $R(T, 2)$, compute the critical values of the maps by resultants and the torsion over $\overline{\mathbb{Q}}(t)$ and $\overline{\mathbb{Q}}(s)$, check the four points of Remark 3.9 and compute its rank bounds at $s = -16$.

Section 4. We verify Lemma 4.1, (4.1), the points (4.2), the specialization at $u_0 = -1199/222$ with the reductions of Propositions 4.2 and 4.4, the statements on the cusps and the search of Remark 4.5, and we check the identities of Lemma 4.6 against the formulas of [11, §5.1]. For Remark 4.7 we verify t', the five points and their reductions at $(t, z) = (-32/21, 4804/441)$; its upper bound (Appendix B) uses the L-polynomials of two of the twists over $\mathbb{F}_7$ and of the other two over $\mathbb{F}_{23}$.

Section 5. We verify the family at the end of Section 5: its two points over $\mathbb{Q}(s)(u)$, its members at $s = 0$ and s_0, the discriminant of h, and the line through s_0 along which the twist has a point of the shape of R'. We also verify the data displayed in Section 5 and the computations in the proof of Theorem 5.1: the norms in (b), the reductions modulo 11 in (c), the Jacobian of $\mathcal{C}'$ and the ranks of J and $J^{(2)}$ in (a).

Independent checks. Every computation that a proof uses was done twice, by separately written programs (often one in PARI/GP and one in SageMath) that start from the formulas printed here or in [11, §5.1] or from the deposited data files, and every rank bound from a 2-descent was computed both with `mwrank` and with PARI's `ellrank`; the deposit pairs each statement with its programs, and the exceptions it lists are computations that no proof uses.

Appendix B. The rank in Remark 4.7

We prove that the curve $E_{\gamma_1(t)}$ of Remark 4.7 has rank at most 5 over the function field of the genus-one curve of that remark, where $\gamma_1(t) = -12t(2t-1)(t+1)/(16t^4 - 11t^2 + 4)$. Write $c = \gamma_1(t)$. Then $c = -12(2w+1)/(16w^2+5)$ with $w = t - 1/(2t)$, $\mathbb{Q}(t) = \mathbb{Q}(w)(\sqrt{w^2+2})$ and $\mathbb{Q}(w) = \mathbb{Q}(c)(\sqrt{\delta_1})$ with $\delta_1 = 9 - 12c - 5c^2$. The function field of the curve $z^2 = 64t^4+48t^3-47t^2-24t+16$ is the Galois closure of $\mathbb{Q}(t)/\mathbb{Q}(c)$; its group is D_4, and its quadratic subfields over $\mathbb{Q}(c)$ are $\mathbb{Q}(c)(\sqrt{\delta})$ for $\delta = \delta_1$, δ_2, $\delta_1\delta_2$, where $\delta_2 = 9c^2-8c+16$: the other root of $-12(2X+1)/(16X^2+5) = c$ is $w' = (5-8w)/(16w+8)$, and $(w^2+2)(w'^2+2) = \delta_2\,(9/(16c))^2$, $w'^2 + 2 = (64t^4 + 48t^3 - 47t^2 - 24t + 16)\,(3/(8t(2w+1)))^2$. Since $E_c(\mathbb{Q}(c))$ is finite, the

decomposition of the Mordell–Weil group, tensored with $\mathbb{Q}$, into representations of D_4 shows that the rank is $r_1+r_2+r_{12}+2r_3$, where r_1, r_2, r_{12} are the ranks over $\mathbb{Q}(c)$ of the quadratic twists of E_c by δ_1, δ_2, $\delta_1\delta_2$, and r_3 is the rank over $\mathbb{Q}(w)$ of the quadratic twist by w^2+2 of E_c, $c=-12(2w+1)/(16w^2+5)$. Indeed, r_1, r_2, r_{12} are the multiplicities of the non-trivial characters of D_4, and its irreducible representation of dimension 2 is induced from the character of the subgroup fixing $\mathbb{Q}(w)$ whose kernel is the subgroup fixing $\mathbb{Q}(t)$; so, by Frobenius reciprocity, its multiplicity is the rank of the part of $E_c(\mathbb{Q}(t))\otimes\mathbb{Q}$ on which the non-trivial automorphism of $\mathbb{Q}(t)$ over $\mathbb{Q}(w)$ acts by -1, that is, r_3. The singular fibers of the first three surfaces are those of E_c, of types I_6, I_3, I_1, I_2 over $c=0$, -1, $-1/9$, ∞, and fibers of type I_0^* over the roots of δ_1, δ_2 and $\delta_1\delta_2$ respectively; those of the fourth are two fibers of each of these four types, over the points of the w-line above these values of c, where $w\mapsto c$ is unramified, and two of type I_0^*, at $w=\pm\sqrt{-2}$. So their conductors have degrees 8, 8, 12 and 12, and their L-polynomials at primes of good reduction degrees 4, 4, 8 and 8 [41, Lecture 1, Theorem 9.3]. These four elliptic surfaces have good reduction at $p=7$, 7, 23, 23 respectively, and their L-polynomials there are $(1-7T)(1+7T)(1+4T+49T^2)$, $1-14T^2+7^4T^4$, $(1+23T)^2(1-22T+211T^2-6348T^3+111619T^4-6156502T^5+23^6T^6)$ and $(1-23T)^2(1+34T+1019T^2+25300T^3+539051T^4+9514594T^5+23^6T^6)$, in which $T=1/p$ is a root of multiplicity 1, 0, 0 and 2. Each L-polynomial $L(T)$ was computed [18] from the numbers of points over $\mathbb{F}_{p^k}$ of all the fibers, singular ones included, for $k\le\frac12\deg L+1$ (for the second, $k\le\frac12\deg L+2$), and the functional equation $L(T)=\pm(pT)^{\deg L}L(1/(p^2T))$, whose sign these counts determine. By a theorem of Tate [40], stated in [41, Lecture 1, Theorem 12.1(1)], the rank over $\mathbb{F}_p(c)$, resp. $\mathbb{F}_p(w)$, is at most this multiplicity. Reduction modulo p maps the Mordell–Weil group over $\mathbb{Q}(c)$, resp. $\mathbb{Q}(w)$, into that over $\mathbb{F}_p(c)$, resp. $\mathbb{F}_p(w)$, injectively after tensoring with $\mathbb{Q}$. Indeed, the singular fibers keep their types modulo p and stay distinct, so the surface has a smooth projective model over $\mathbb{Z}_{(p)}$ and the trivial lattices of the surfaces over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_p$ have the same rank. Specialization of Néron–Severi groups is injective after tensoring with $\mathbb{Q}$ [42, Proposition 6.2]; van Luijk states this with $\mathbb{Q}_\ell$-coefficients, and as $\mathbb{Q}_\ell$ is a field extension of $\mathbb{Q}$, a map of $\mathbb{Q}$-vector spaces is injective if it is after tensoring with $\mathbb{Q}_\ell$. Specialization also maps the trivial lattice into the trivial lattice, so it induces an injection of the quotients by the trivial lattices, tensored with $\mathbb{Q}$. By the Shioda–Tate theorem [35, Theorem 6.3] these quotients are the Mordell–Weil groups, a section corresponding to its class, so that the induced map is reduction of points. So the rank is at most $1+0+0+2\cdot2=5$.

Declarations

Use of AI. This paper and its results were produced by an AI research system that the author designed, built and directs, running on Anthropic's Claude Opus 5.5 in Claude Code and OpenAI's GPT-6 Astra in Codex. The author chooses the problems and prioritizes the work. Separate AI agents checked each result, and a second program confirmed the computations the proofs use, with any exceptions listed in the public deposit. The system also searched the literature and checked the citations against reliable sources. The author read the paper, reran the computations from the deposit and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [18].

References

1. Julián Aguirre, Andrej Dujella, Mirela Jukić Bokun, and Juan Carlos Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields*, Period. Math. Hungar. **68** (2014), 222–230, doi:10.1007/s10998-014-0032-5; arXiv:1204.5343v2.
2. John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
3. Andrej Dujella, *High rank elliptic curves with prescribed torsion*, https://web.math.pmf.unizg.hr/~duje/tors/tors.html (accessed October 28, 2026).
4. ———, *High rank elliptic curves with prescribed torsion over quadratic fields*, https://web.math.pmf.unizg.hr/~duje/tors/torsquad.html (accessed October 25, 2026).
5. ———, *Infinite families of elliptic curves with high rank and prescribed torsion*, https://web.math.pmf.unizg.hr/~duje/tors/generic.html (accessed October 24, 2026).
6. ———, *Open problems on Diophantine m-tuples and elliptic curves*, https://web.math.pmf.unizg.hr/~duje/pdf/open2.pdf, version of October 24, 2026.
7. ———, *High-rank elliptic curves with given torsion group and some applications*, Banach Center Publ. **126** (2023), 9–26, doi:10.4064/bc126-1; author's copy https://web.math.pmf.unizg.hr/~duje/pdf/dujella-NuTMiC2a.pdf (accessed October 28, 2026), whose section numbering is used here.
8. Andrej Dujella, Matija Kazalicki, and Juan Carlos Peral, *Elliptic curves with torsion groups* $\mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **115** (2021), no. 4, Paper No. 169, doi:10.1007/s13398-021-01112-5; arXiv:2105.06215v2.
9. Andrej Dujella and Juan Carlos Peral, *Elliptic curves with torsion group* $\mathbb{Z}/8\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, Trends in Number Theory, Contemp. Math., vol. 649, Amer. Math. Soc., Providence, RI, 2015, pp. 47–62, doi:10.1090/conm/649/13019; arXiv:1306.0027v1, whose numbering differs: §§5.4 and 6.6 cited here are §§4.4 and 5.5 there.
10. ———, *Construction of high rank elliptic curves*, J. Geom. Anal. **31** (2021), no. 7, 6698–6724, doi:10.1007/s12220-020-00373-7; authors' copy https://web.math.pmf.unizg.hr/~duje/pdf/DujellaPeralConstruction.pdf (accessed October 28, 2026), whose section numbering is used here.
11. Andrej Dujella, Juan Carlos Peral, and Petra Tadić, *Elliptic curves with torsion group* $\mathbb{Z}/6\mathbb{Z}$, Glas. Mat. Ser. III **51(71)** (2016), no. 2, 321–333, doi:10.3336/gm.51.2.03; arXiv:1503.03667v1.
12. Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007, Preprint, arXiv:0709.2908v1.
13. Noam D. Elkies and Zev Klagsbrun, *New rank records for elliptic curves having rational torsion*, ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 4, Math. Sci. Publ., Berkeley, CA, 2020, pp. 233–250, doi:10.2140/obs.2020.4.233; arXiv:2003.00077v1.
14. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, doi:10.1007/BF01388432.
15. Ivica Gusić and Petra Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137–152, doi:10.1016/j.jnt.2014.09.023; arXiv:1409.7189v2.
16. Manvir Jaswal, *Infinitely many elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *and rank at least six*, 2026, Zenodo, doi:10.5281/zenodo.23437117.
17. ———, *Infinitely many elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *and rank at least four*, 2026, Zenodo, doi:10.5281/zenodo.23364156.
18. ———, *Programs and data for "Elliptic curves with torsion group* $\mathbb{Z}/6\mathbb{Z}$ *and generic rank four"*, 2026, Zenodo, doi:10.5281/zenodo.23735657.
19. Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, doi:10.1007/BF01232025.
20. Sheldon Kamienny and Filip Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), no. 3, 291–305, doi:10.4064/aa152-3-5; arXiv:1103.5906v5, whose theorem numbering is used here.
21. Monsur A. Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, doi:10.1017/S0027763000002816.
22. Shoichi Kihara, *On the rank of the elliptic curves with a rational point of order 6*, Proc. Japan Acad. Ser. A Math. Sci. **82** (2006), no. 7, 81–82, doi:10.3792/pjaa.82.81.
23. Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237, doi:10.1112/plms/s3-33.2.193.

24. Odile Lecacheux, *Rang de courbes elliptiques avec groupe de torsion non trivial*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 231–247, doi:10.5802/jtnb.400.
25. ———, *Rang de familles de courbes elliptiques*, Acta Arith. **109** (2003), no. 2, 131–142, doi:10.4064/aa109-2-2.
26. ———, *Rang de courbes elliptiques dont le groupe de torsion est non trivial*, Ann. Sci. Math. Québec **28** (2004), no. 1–2, 145–151.
27. Allan J. MacLeod, *A simple method for high-rank families of elliptic curves with specified torsion*, 2014, Preprint, arXiv:1410.1662v1.
28. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186, doi:10.1007/BF02684339.
29. Koh-ichi Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscripta Math. **92** (1997), no. 1, 13–32, doi:10.1007/BF02678178.
30. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr/.
31. Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903, doi:10.4171/JEMS/893; arXiv:1602.01431v3; authors' version of May 15, 2019, https://jvoight.github.io/articles/bounded-ranks.pdf.
32. F. Patrick Rabarison, *Torsion et rang des courbes elliptiques définies sur les corps de nombres algébriques*, Ph.D. thesis, Université de Caen, 2008.
33. Michael Rosen and Joseph H. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), no. 1, 43–67, doi:10.1007/s002220050238.
34. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026, https://www.sagemath.org.
35. Matthias Schütt and Tetsuji Shioda, *Elliptic surfaces*, Algebraic geometry in East Asia—Seoul 2008, Adv. Stud. Pure Math., vol. 60, Math. Soc. Japan, Tokyo, 2010, pp. 51–160, doi:10.2969/aspm/06010051; arXiv:0907.0298v3, whose numbering is used here.
36. Tetsuji Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240.
37. Joseph H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211, doi:10.1515/crll.1983.342.197.
38. ———, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), no. 183, 339–358, doi:10.1090/S0025-5718-1988-0942161-4.
39. ———, *The arithmetic of elliptic curves*, second ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009, doi:10.1007/978-0-387-09494-6.
40. John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, Exp. No. 306, pp. 415–440, https://www.numdam.org/item/SB_1964-1966___9___415_0/; Exposé of February 1966.
41. Douglas Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280, doi:10.1090/pcms/018/09; arXiv:1101.1939v1, whose numbering is used here.
42. Ronald van Luijk, *An elliptic K3 surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119, doi:10.1016/j.jnt.2006.06.006; arXiv:math/0411606v1, whose theorem numbering is used here.
43. Jeechul Woo, *Arithmetic of elliptic curves and surfaces: Descents and quadratic sections*, Ph.D. thesis, Harvard University, Cambridge, MA, 2010.
44. Hizuru Yamagishi, *On elliptic curves of rank four with three-division rational point*, Pacific J. Math. **206** (2002), no. 1, 231–244, doi:10.2140/pjm.2002.206.231.

Toronto, Canada
Email address: manvirjaswal@icloud.com
URL: https://manvirjaswal.github.io