INFINITELY MANY ELLIPTIC CURVES WITH TORSION $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ AND RANK AT LEAST SIX

MANVIR JASWAL

Abstract. We show that there are infinitely many elliptic curves over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank at least 6, answering the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ of Problem 2.6 in Dujella's list of open problems. The largest rank previously known to occur infinitely often with this torsion was 5, due to Eroshkin. The curves are fibers of a one-parameter family of Dujella and Peral, which has rank 6 over the function field of an elliptic curve of rank one. The heuristic of Park, Poonen, Voight and Wood predicts that only finitely many curves with this torsion have rank greater than 5.

hexagon:2610.00586v2

Contents

1. Introduction 1
2. The family of Dujella and Peral 4
3. A K3 surface and three of its twists 7
4. The curve C and six points 9
5. Independence and the rank over $\mathbb{Q}(C)$ 10
6. Proof of the theorems 12
7. Other bases for X 14
8. A second family 15
Appendix A. Computations 18
Declarations 18
References 18

1. Introduction

By Mazur's theorem [27], the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is one of fifteen groups. For each such group T one asks how large the rank of a curve with $E(\mathbb{Q})_{\text{tors}} \cong T$ can be, and which ranks occur infinitely often. Dujella maintains tables of the records [5, 6]: for each T, the largest known rank of a single curve, the largest known rank of a curve over $\mathbb{Q}(t)$, and the largest known rank that occurs for infinitely many curves. Dujella's list of open problems [7, Problem 2.6] asks:

> "Are there infinitely many elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (respectively $\mathbb{Z}/6\mathbb{Z}$) and rank ≥ 6?"

Date: November 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, Diophantine triples.

For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we show that there are (Theorem 1.1). The case $\mathbb{Z}/6\mathbb{Z}$ remains open.

The elliptic curves over $\mathbb{Q}$ whose torsion subgroup contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are, up to isomorphism, those of the form

$$E_{a,b}\colon\ y^2 = x(x+a^2)(x+b^2), \qquad a,b \in \mathbb{Q},\ ab(a^2-b^2) \neq 0$$

(see [2, Theorem 5.3], and [14, §6.7] for torsion exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$). On $E_{a,b}$ the points $(0,0)$, $(-a^2,0)$, $(-b^2,0)$ have order 2, and $(ab, ab(a+b))$ has order 4, with double $(0,0)$. Over $\mathbb{Q}(t)$, Lecacheux [25, Théorème 9], Elkies [16] and Eroshkin (see [11]) constructed families of rank at least 3, and Dujella and Peral [11] one of rank exactly 4, still the largest rank over $\mathbb{Q}(t)$ in Dujella's table. As of November 28, 2026 the largest known rank of a curve over $\mathbb{Q}$ with this torsion is 10, for a curve of Singh (see [8]), after curves of rank 9 of Dujella and Peral [11, 14] and of Klagsbrun.

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 [16, Lecture I]). With prescribed torsion they were used by Atkin and Morain [1] for the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, by Lecacheux and by Rabarison (see [12, §5.4]) and by Elkies [16, Lecture III]. In this way Dujella and Peral obtained infinitely many curves of rank at least 3 with torsion $\mathbb{Z}/8\mathbb{Z}$ and with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [12, §§5.4, 6.6]. Dujella, Kazalicki and Peral gave further such families for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [10, §9]. With no torsion prescribed, Elkies [16, Lectures II and III], [17] showed that pairs of quadratic base changes of an elliptic K3 surface of Mordell–Weil rank 17 give a family of rank at least 19 over an elliptic curve of positive rank, and hence infinitely many curves of rank at least 19. The author's preprint [21] uses the same mechanism for the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

For $\mathbb{Z}/4\mathbb{Z}$, Dujella and Peral made explicit a remark of Elkies [16, Lecture II, p. 9]: pairs of quadratic sections of his elliptic K3 surface with torsion $\mathbb{Z}/4\mathbb{Z}$ and Mordell–Weil rank 4 give several infinite families of rank at least 6 parametrized by elliptic curves of positive rank [14, §4]. Elkies obtained the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, as here, by a quadratic base change of a curve with torsion $\mathbb{Z}/4\mathbb{Z}$ [16, Lecture II], and rank at least 4 for an infinite family by a quadratic base change over an elliptic curve of positive rank [16, Lecture III, p. 13]. Before this paper, the largest rank known to occur infinitely often with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ was 5, due to Eroshkin (see [6]).

Theorem 1.1. *There are infinitely many elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\operatorname{rank} E(\mathbb{Q}) \geq 6$. Among them there are infinitely many distinct j-invariants.*

Theorem 1.1 bears on the heuristic of Park, Poonen, Voight and Wood [33], which suggests that ranks of elliptic curves over $\mathbb{Q}$ are bounded. Adapted to prescribed torsion as in [33, §8.3], the argument of [33, Theorem 7.3.3] predicts that if the number of curves with torsion T and height at most H is of order $H^{1/d}$, as Harron and Snowden prove [20, Theorem 1.1 and §1.2], then only finitely many of them have rank greater than $1 + 24/d$. This suggests that $b_T \leq 1 + \lfloor 24/d \rfloor$, where $b_T = \limsup\{\operatorname{rank} E(\mathbb{Q}) : E(\mathbb{Q})_{\mathrm{tors}} \cong T\}$ in the notation of [33]. The table of [33, §8.3] lists this bound next to the known lower bound for b_T, the largest rank known to occur infinitely often. Dujella and Peral noted that the two bounds coincide for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and for $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [13, 14]. For $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ one has $d = 6$, and the bound is 5, which Theorem 1.1 exceeds infinitely often.

Our curves are parametrized by the rational points of a curve of genus one and rank one. By Néron's count of points of bounded height [30, Ch. III, Théorème 4 and Corollaire 2], there are $(\log H)^{1/2+o(1)}$ of them with height at most H (Remark 6.2). As Elkies pointed out (see [33, Remark 1.1.3]), the model would have to be refined to predict the rank distribution in parametric families of high generic rank such as ours. Dujella, Kazalicki and Peral had

suggested, from root numbers in families of rank 3, that the heuristic needs some adjustment for $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [10]; for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, where the table of [33, §8.3] lists the rank bound 3, the author's preprint [21] gives a family of rank at least 4.

The idea. For an elliptic curve E over $\mathbb{Q}(m)$ and $q \in \mathbb{Q}(m)^\times$ not a square, the rank of E over $\mathbb{Q}(m)(\sqrt{q})$ is the sum of the ranks over $\mathbb{Q}(m)$ of E and of its quadratic twist E^q. Over $\mathbb{Q}(m)(\sqrt{q_1}, \sqrt{q_2})$ three twists contribute, by q_1, q_2 and q_1q_2, and when q_1 and q_2 are quadratic in m this field is in general the function field of a curve of genus one. Three twists of rank one then raise the rank by 3 over a base of genus one, which may have infinitely many rational points. In using twists we follow Dujella and Peral, who raised the rank of a curve with torsion $\mathbb{Z}/4\mathbb{Z}$ over a rational function field to 6 in this way [15, §4]; there each new point amounts to a square condition, and two such conditions with a common factor hold together over a curve of genus zero.

The curves of Theorem 1.1 are fibers of the following family. Let

$$a = 7(m-99)(m+1)(m-11)(m+9), \qquad b = -7(m+99)(m-1)(m+11)(m-9), \tag{1.1}$$

and let

$$X\colon\ y^2 = x(x+a^2)(x+b^2) \tag{1.2}$$

over $\mathbb{Q}(m)$. Its fiber X_{m_0} at $m_0 \in \mathbb{Q}$ is the curve $E_{a(m_0),b(m_0)}$, an elliptic curve with torsion containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ unless $m_0 \in \{0, \pm1, \pm9, \pm11, \pm99\}$ (Section 2). The family X is the one-parameter family of Dujella and Peral [14, §7.2] with their parameter $\tau = 1/7$, written in other coordinates (Lemma 2.1). On it they found a curve of rank 9 and seven curves of rank 8. We show in Proposition 2.4 that the rank of X over $\mathbb{Q}(m)$ is exactly 3.

Since $a(-m) = -b(m)$ and $b(-m) = -a(m)$, X is the base change by $n = m^2$ of an elliptic K3 surface Y over $\mathbb{Q}(n)$ (Lemma 3.1), and a twist of Y by a polynomial linear in n becomes a twist of X by one quadratic in m. Nagao's averages of traces of Frobenius [29] suggest positive rank for the twists of X by $q_1 = 5(3m^2 + 242)$ and $q_2 = 5(2m^2 + 243)$ (Section 3), and the twist by q_1q_2 has positive rank too. Let C be the affine curve

$$C\colon\quad u^2 = 5(3m^2 + 242), \qquad v^2 = 5(2m^2 + 243) \tag{1.3}$$

in the coordinates (m, u, v). Its function field is $\mathbb{Q}(C) = \mathbb{Q}(m)(\sqrt{q_1}, \sqrt{q_2})$, and for $c \in C(\mathbb{Q})$ we write $m(c)$ for its coordinate m. Three points P_1, P_2, P_3 of X are defined over $\mathbb{Q}(m)$, and three more, P_4, P_5, P_6, over $\mathbb{Q}(C)$ (Lemma 2.2 and Proposition 4.2).

Theorem 1.2. *(a) The smooth projective model $\overline{C}$ of C has genus one and infinitely many rational points. It is isomorphic over $\mathbb{Q}$ to the elliptic curve*

$$E_C\colon y^2 = x^3 + x^2 - 137620x - 10504000,$$

of conductor 9240 and rank one, and $C(\mathbb{Q}) = \overline{C}(\mathbb{Q})$.

(b) The six points $P_1, \dots, P_6 \in X(\mathbb{Q}(C))$ of Proposition 4.2 are linearly independent, and $\operatorname{rank} X(\mathbb{Q}(C)) = 6$.

(c) At every $c \in C(\mathbb{Q})$ except the sixteen points $(\pm1, \pm35, \pm35)$ and $(\pm99, \pm385, \pm315)$ the fiber $X_{m(c)}$ is an elliptic curve with torsion subgroup containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. For all but finitely many $c \in C(\mathbb{Q})$ the torsion subgroup of $X_{m(c)}(\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the rank of $X_{m(c)}(\mathbb{Q})$ is at least 6.

For example, $c_0 = (7401/2399,\ 88235/2399,\ 86835/2399) \in C(\mathbb{Q})$ gives, after scaling, the curve E_{a_0,b_0} with $(a_0, b_0) = (7037226227200,\ 3329722383911)$, which has torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank exactly 6 (Proposition 5.1 and Section 6).

To prove that the six points are independent, we specialize them at c_0 and reduce modulo six primes at which 3 divides the number of points of the reduced curve and the 3-primary part of its group of points is cyclic. Each reduction gives a homomorphism to $\mathbb{Z}/3\mathbb{Z}$ that kills the torsion, whose order is prime to 3, and the six homomorphisms take the six points to a matrix that is invertible modulo 3 (Proposition 5.1). The upper bound $\operatorname{rank} X(\mathbb{Q}(C)) \le 6$ comes from the injectivity criterion of Gusić and Tadić [19, Theorem 1.1] and 2-Selmer groups of single fibers of X and of its twists by q_2 and q_1q_2, which bound the rank of X over $\mathbb{Q}(m)$ by 3 and those of these two twists by 1; the map $m \mapsto 99/m$ carries the twist by q_2 to the twist by q_1 (Propositions 2.4 and 5.2). Over the other curves of genus one that Nagao's averages suggest, X has rank exactly 5 (Section 7).

By Silverman's specialization theorem [35, Theorem C], the six points stay independent at all but finitely many points of $C(\mathbb{Q})$, and by Faltings' theorem [18] the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ at all but finitely many (Theorem 1.2(c)). Proposition 6.1 gives an explicit infinite set of such points: at c_0 the torsion is seen at the prime 13 and the independence modulo the six primes, and both hold at every point of $C(\mathbb{Q})$ congruent to c_0 to sufficient order at these seven primes. The curves have infinitely many j-invariants because j is nonconstant on C.

In Section 8 we give a second family with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank at least 6, from the same model of Dujella and Peral, over a curve of genus one and rank two. It gives $(\log H)^{1+o(1)}$ curves of height at most H (Remark 6.2).

The numbered results are formalized in Lean 4 with Mathlib [22], with theorems of other authors taken as hypotheses; see Appendix A.

2. The family of Dujella and Peral

Dujella and Peral [14, §6.7] consider the curves $y^2 = (\xi x+1)(1-x/\xi)(\zeta x+1)$ induced by the Diophantine triples $\{\xi, -1/\xi, \zeta\}$ with $\xi = (\alpha\tau+1)/(\tau-\alpha)$ and $\zeta = 4\alpha\tau/((\alpha\tau+1)(\tau-\alpha))$. After a change of coordinates these are

$$y^2 = x(x + (A_+B_+)^2)(x + (A_-B_-)^2), \qquad A_\pm = \tau \pm \alpha,\ B_\pm = 1 \pm \alpha\tau, \tag{2.1}$$

which, multiplied out, is their model [14, (13)] and [11, (5)]:

$$y^2 = x^3 + 2(\alpha^2+\tau^2+4\alpha^2\tau^2+\alpha^4\tau^2+\alpha^2\tau^4)x^2 + (\tau+\alpha)^2(\alpha\tau-1)^2(\tau-\alpha)^2(\alpha\tau+1)^2x.$$

The model goes back to Dujella's study of the curves induced by Diophantine triples [9, §4], where it is used at $\alpha = 2$. Asking that $x = (\tau+\alpha)^2(\alpha\tau-1)(\alpha\tau+1)$, respectively $x = (\tau+\alpha)(\alpha\tau-1)^2(\tau-\alpha)$, be the abscissa of a point leads to their conditions, because at these divisors of the coefficient of x the right side of (2.1) is a square times $\tau^2+\alpha^2+2$, respectively $\alpha^2\tau^2+2\alpha^2+1$:

$$\tau^2+\alpha^2+2 = \square \quad [14, (14)], \qquad \alpha^2\tau^2+2\alpha^2+1 = \square \quad [14, (16)].$$

At $\alpha = 7$ the second condition reads $49\tau^2+99 = \square$, and $\tau = (99-m^2)/(14m)$ gives $49\tau^2+99 = \left((m^2+99)/(2m)\right)^2$. Then

$$14m\,A_+ = -(m-99)(m+1), \quad 14m\,B_+ = -7(m-11)(m+9),$$
$$14m\,A_- = -(m+99)(m-1), \quad 14m\,B_- = 7(m+11)(m-9),$$

so that $a=(14m)^2A_+B_+$ and $b=(14m)^2A_-B_-$ in (1.1), and X is (2.1) at $\alpha=7$, $\tau=(99-m^2)/(14m)$ after the substitution $x\mapsto(14m)^4x$. One has

$$a-b=14(m^4-2m^2+9801),\qquad a+b=-1400\,m(m^2-99),$$

so $ab(a^2-b^2)$ vanishes at $m_0\in\mathbb{Q}$ only for $m_0\in\{0,\pm1,\pm9,\pm11,\pm99\}$. The family of [14, §7.2] uses the first condition instead: writing

$$\tau^2+\alpha^2+2=\big((\tau^2+1)/\tau+(\alpha-1/\tau)t\big)^2$$

gives $\alpha=(t^2-2(\tau^2+1)t+1)/(\tau(t^2-1))$, and they take $\tau=1/7$, so that

$$\alpha_t:=(49t^2-100t+49)/(7(t^2-1)).$$

Lemma 2.1. *Let $m=(t+1)/(t-1)$. Then*

$$a=\frac{112\,t(5t-4)(5t-6)(49t-50)}{(t-1)^4},\qquad b=\frac{112\,(4t-5)(6t-5)(50t-49)}{(t-1)^4},$$

and $A_+B_+(\alpha_t,\frac17)=4a'/(343(t^2-1)^2)$, $A_-B_-(\alpha_t,\frac17)=-4b'/(343(t^2-1)^2)$, where $a'=t(5t-4)(5t-6)(49t-50)$ and $b'=(4t-5)(6t-5)(50t-49)$. Hence $a=\rho\cdot A_+B_+(\alpha_t,\frac17)$ and $b=-\rho\cdot A_-B_-(\alpha_t,\frac17)$ with $\rho=(98(t+1)/(t-1))^2$, and $(x,y)\mapsto(\rho^2x,\rho^3y)$ is an isomorphism over $\mathbb{Q}(t)=\mathbb{Q}(m)$ from the curve (2.1) at $(\alpha_t,1/7)$, the family of [14, §7.2], to X.

Proof. These are identities in $\mathbb{Q}(t)$. A curve $y^2=x(x+r^2)(x+s^2)$ depends only on r^2 and s^2, and scaling both by ρ^2 is the substitution $x\mapsto\rho^2x$. □

Lemma 2.1 reflects a symmetry of (2.1). Write $\sigma_1=\tau^2+\alpha^2+2$ and $\sigma_2=\alpha^2\tau^2+2\alpha^2+1$ for the expressions in the two conditions. The map $\psi(\alpha,\tau)=(1/\tau,\alpha)$ satisfies $(A_+B_+)\circ\psi=A_+B_+/\tau^2$, $(A_-B_-)\circ\psi=-A_-B_-/\tau^2$ and $\sigma_2\circ\psi=\sigma_1/\tau^2$. Hence ψ preserves (2.1) up to $x\mapsto\tau^4x$ and maps the points where the first condition holds to points where the second holds. It maps the line $\tau=1/7$ onto the line $\alpha=7$, and the substitution $m=(t+1)/(t-1)$ of Lemma 2.1 gives $(99-m^2)/(14m)=\alpha_t$. At $\tau=1/7$ the coefficient of x in their model, with $\alpha=(t^2-2(\tau^2+1)t+1)/(\tau(t^2-1))$, splits into linear factors in t [14, §7.2]. Under ψ this is the fact that $2(\alpha^2+1)=100$ is a square at $\alpha=7$. Their curve of rank 9 at $t=900/781$ is the fiber of X at $m=1681/119$, and their curves of rank 8 at $t=201/170$, $245/138$, $-800/459$, $1610/1417$, $1955/1754$, $2254/2215$, $2301/1670$ are the fibers at $m=371/31$, $383/107$, $341/1259$, $3027/193$, $3709/201$, $4469/39$, $3971/631$.

The torsion points of X over $\mathbb{Q}(m)$ include $(0,0)$, $(-a^2,0)$, $(-b^2,0)$ and the point $(ab,\,ab(a+b))$ of order 4, with double $(0,0)$. The next lemma gives three points of infinite order.

Lemma 2.2. *The points P_1,P_2,P_3 with the following coordinates lie in $X(\mathbb{Q}(m))$:*

$$\begin{aligned}x(P_1)&=-49(m-1)^2(m-11)^2(m+9)^2(m+99)^2,\\ x(P_1)+a^2&=-19208\,m(m^2-99)(m-11)^2(m+9)^2,\\ x(P_1)+b^2&=392\,m(m^2-99)(m-1)^2(m+99)^2,\\ y(P_1)&=-19208\,m(m^2-99)(m-1)^2(m-11)^2(m+9)^2(m+99)^2;\end{aligned}$$

$$\begin{aligned}
x(P_2) &= 49(m-99)(m-1)(m+1)(m+99)(m-9)^2(m+11)^2,\\
x(P_2)+a^2 &= 98(m-99)(m+1)(m^2-99)(m^2+99)^2,\\
x(P_2)+b^2 &= 98(m-1)(m+99)(m^2-99)(m-9)^2(m+11)^2,\\
y(P_2) &= -686\,(m-99)(m-1)(m+1)(m+99)(m^2-99)\\
&\qquad\cdot(m^2+99)(m-9)^2(m+11)^2;\\
x(P_3) &= -49(m-11)(m-9)(m+1)(m+99)(m+9)^2(m+11)^2,\\
x(P_3)+a^2 &= -3920\,m(m-11)(m+1)(m+9)^2(2m-33)^2,\\
x(P_3)+b^2 &= 3920\,m(m-9)(m+99)(m-6)^2(m+11)^2,\\
y(P_3) &= 27440\,m(m-6)(m-9)(m-11)(m+1)(m+99)\\
&\qquad\cdot(2m-33)(m+9)^2(m+11)^2.
\end{aligned}$$

Proof. In each case the product $x(x+a^2)(x+b^2)$ of the displayed factorizations is y^2; for instance $(-49)(-19208)\cdot 392 = 19208^2$. □

In the notation above, at $\alpha = 7$, $x(P_1) = -(14m)^4\big((\tau-\alpha)(1+\alpha\tau)\big)^2$ and $x(P_2) = (14m)^4(\tau+\alpha)(\alpha\tau-1)^2(\tau-\alpha)$. Thus P_1 is the point that every curve of the model carries, the image of the point $(0,1)$ of $y^2 = (\xi x+1)(1-x/\xi)(\zeta x+1)$ [14, §6.7] (the point P of [9, §4]). The point P_2 is the one whose existence is the second condition of Dujella and Peral. The point P_3 comes from the splitting of B_+ and B_- on the line $\alpha = 7$, where $\alpha^2+1 = 2\cdot 5^2$: the coordinate $x(P_3) = (14m)^2B_+B_-\,(m+1)(m+9)(m+11)(m+99)$ involves the linear factors $m+9$ of $14mB_+$ and $m+11$ of $14mB_-$.

For a curve $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with rational e_1, e_2, e_3 let

$$\kappa\colon E(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2, \qquad P \mapsto \big(x(P)-e_1,\, x(P)-e_2\big), \tag{2.2}$$

with the usual values at the points of order 2. This is the 2-descent homomorphism, with kernel $2E(\mathbb{Q})$ [36, Proposition X.1.4]. The torsion of the fibers is controlled by the following criterion, whose proof follows that of [31, Main Theorem 1].

Lemma 2.3. *Let $a, b \in \mathbb{Q}$ with $ab(a^2-b^2) \neq 0$. If neither ab nor $-ab$ is a square, then $E_{a,b}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.*

Proof. By Mazur's theorem [27] the only larger possibility is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, which needs a point of order 8, that is, a half of a point of order 4. On $E_{a,b}$ the points of order 4 are the halves of the points of order 2. The map κ of (2.2) (with $e_1 = 0$) has first component x and kills $2E_{a,b}(\mathbb{Q})$. The points $(-a^2, 0)$ and $(-b^2, 0)$ have no rational halves, since there the first component of κ is $-a^2$ or $-b^2$, which is negative and so not a square. The halves of $(0,0)$ are the points $(ab, \pm ab(a+b))$ and $(-ab, \pm ab(a-b))$, at which the first component of κ is ab or $-ab$. A half of such a point exists only if this component is a square, and therefore $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ requires ab or $-ab$ to be a square. □

Proposition 2.4. $\operatorname{rank} X(\mathbb{Q}(m)) = 3$, *and P_1, P_2, P_3 are linearly independent.*

Proof. Lower bound. At $m = 37/5$ the fiber is $E_{a,b}$ with $a = 198746352/625$ and $b = 87707648/625$. With $(e_1, e_2, e_3) = (0, -a^2, -b^2)$ in (2.2), in squarefree representatives

$$\kappa(P_1) = (-1,\ 5\cdot 7\cdot 37\cdot 79), \qquad \kappa(P_2) = (-2\cdot 3\cdot 19\cdot 229,\ 3\cdot 79\cdot 229),$$
$$\kappa(P_3) = (-2\cdot 3\cdot 19,\ 3\cdot 7\cdot 37), \quad \kappa(-a^2, 0) = (-1,\ 5\cdot 7\cdot 37\cdot 79\cdot 20233),$$

$$\kappa(0,0) = (1,1), \qquad \kappa(ab, ab(a+b)) = (3 \cdot 19 \cdot 23 \cdot 41 \cdot 229,\ 3 \cdot 5 \cdot 37 \cdot 41 \cdot 79 \cdot 229).$$

These five nontrivial vectors are independent: 20233 occurs only in $\kappa(-a^2, 0)$, 23 only in $\kappa(ab, ab(a+b))$, then 229 only in $\kappa(P_2)$, and 2 only in $\kappa(P_3)$. The fiber has torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \langle (-a^2, 0), (ab, ab(a+b)) \rangle$ by Lemma 2.3, since ab has squarefree part $3 \cdot 19 \cdot 23 \cdot 41 \cdot 229$ (the first entry of $\kappa(ab, ab(a+b))$) while $-ab < 0$. Hence κ maps the torsion subgroup onto $\langle \kappa(-a^2, 0), \kappa(ab, ab(a+b)) \rangle$. Suppose that $\sum n_i P_i$ is a torsion point with $n_i \in \mathbb{Z}$ not all zero. A point whose double is a torsion point is itself one, so we may halve the n_i until one of them is odd, and then the image of $\sum n_i P_i$ gives a relation among the five vectors. The specialized points are therefore independent, and so are P_1, P_2, P_3, since specialization at a smooth fiber is a homomorphism.

Upper bound. We use the criterion of Gusić and Tadić [19, Theorem 1.1]: for a nonconstant curve $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Z}[m]$ and $m_0 \in \mathbb{Q}$ with nonsingular fiber, if $g(m_0)$ is not a square for any nonconstant squarefree divisor $g \in \mathbb{Z}[m]$ of $(e_1 - e_2)(e_1 - e_3)$, of $(e_2 - e_1)(e_2 - e_3)$ or of $(e_3 - e_1)(e_3 - e_2)$, then specialization at m_0 is injective. For X, whose j-invariant is not constant, $(e_1, e_2, e_3) = (0, -a^2, -b^2)$, and these products are a^2b^2, $a^2(a^2 - b^2)$ and $-b^2(a^2 - b^2)$. Their nonconstant squarefree divisors are, up to sign, products of distinct factors among the eight linear factors of ab and the three polynomials m, $m^2 - 99$ and $m^4 - 2m^2 + 9801$, times a squarefree divisor of the content. The content is 7^4 for a^2b^2 and $2^4 \cdot 5^2 \cdot 7^4$ for the other two products. At $m = 14/3$ these eleven factors have the squarefree parts in the column $m = 14/3$ of Table 1. These and -1, 2, 5, 7 are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so no such divisor takes a square value at 14/3. The fiber at 14/3 is isomorphic to $E_{3747769,\,2090231}$, where $3747769 = 17 \cdot 19 \cdot 41 \cdot 283$ and $2090231 = 11 \cdot 13 \cdot 47 \cdot 311$. It has full rational 2-torsion and a 2-Selmer group of dimension 5 (computed with `mwrank` [3]), so its rank is at most 3; hence $\operatorname{rank} X(\mathbb{Q}(m)) \le 3$. □

TABLE 1. Squarefree parts of the irreducible factors at $m = 14/3$ and $m = 50/3$

Factor	$m = 14/3$	$m = 50/3$
$m - 99$	$-3 \cdot 283$	$-3 \cdot 13 \cdot 19$
$m + 1$	$3 \cdot 17$	$3 \cdot 53$
$m - 11$	$-3 \cdot 19$	$3 \cdot 17$
$m + 9$	$3 \cdot 41$	$3 \cdot 7 \cdot 11$
$m + 99$	$3 \cdot 311$	$3 \cdot 347$
$m - 1$	$3 \cdot 11$	$3 \cdot 47$
$m + 11$	$3 \cdot 47$	$3 \cdot 83$
$m - 9$	$-3 \cdot 13$	$3 \cdot 23$
m	$2 \cdot 3 \cdot 7$	$2 \cdot 3$
$m^2 - 99$	$-5 \cdot 139$	1609
$m^4 - 2m^2 + 9801$	$73 \cdot 11353$	$113 \cdot 241 \cdot 257$
$3m^2 + 242$		$2 \cdot 3 \cdot 1613$
$2m^2 + 243$		7187

3. A K3 SURFACE AND THREE OF ITS TWISTS

The family X is a base change of an elliptic K3 surface Y, and quadratic twists of Y are the source of its further points: a point on such a twist becomes a point of X over any

extension of $\mathbb{Q}(m)$ in which the twisting polynomial is a square. We give points on three twists in Lemma 3.2, and over the function field of the curve C of Section 4 they become the points P_4, P_5 and P_6 of Proposition 4.2.

Write $n = m^2$. Since $a(-m) = -b(m)$ and $b(-m) = -a(m)$, the polynomials

$$S := a^2 + b^2 = 98\,(n^4 + 9996n^3 - 1960394n^2 + 97970796n + 96059601),$$
$$w := ab = -49(n-1)(n-81)(n-121)(n-9801)$$

lie in $\mathbb{Q}[n]$, and X is the base change to $\mathbb{Q}(m)$ of

$$Y\colon\ y^2 = x(x^2 + Sx + w^2) \tag{3.1}$$

over $\mathbb{Q}(n)$. For $q \in \mathbb{Q}(n)^\times$ write $Y^q\colon y^2 = x(x^2 + qSx + q^2w^2)$ for the quadratic twist of Y by q. If $K \supseteq \mathbb{Q}(n)$ is a field containing a square root $\sqrt{q}$ of q, a point $(x, y) \in Y^q(K)$ gives the point $(x/q,\, y/(q\sqrt{q})) \in Y(K)$.

Lemma 3.1. *(a) $S - 2w = (a-b)^2 = 196(n^2 - 2n + 9801)^2$ and $S + 2w = (a+b)^2 = 1960000\,n(n-99)^2$. The point $(-w,\, w(a-b)) \in Y(\mathbb{Q}(n))$ has order 4, with double $(0, 0)$.*

(b) The discriminant $\Delta = 16w^4(S^2 - 4w^2)$ of (3.1) is a constant times

$$(n-1)^4(n-81)^4(n-121)^4(n-9801)^4\,n\,(n-99)^2(n^2-2n+9801)^2.$$

The singular fibers of Y are of type I_4 at $n = 1, 81, 121, 9801$, of type I_2 at $n = 99$ and at the two roots of $n^2 - 2n + 9801$, and of type I_1 at $n = 0$ and $n = \infty$; their Euler numbers sum to 24, and Y is a relatively minimal elliptic K3 surface.

(c) $S(9801/n) = (99/n)^4 S(n)$ and $w(9801/n) = (99/n)^4 w(n)$, so $n \mapsto 9801/n$ lifts to an automorphism of Y.

Proof. Parts (a) and (c) are polynomial identities, and $x = -w$ gives $x(x^2 + Sx + w^2) = w^2(S - 2w)$; doubling $(-w, w(a-b))$ gives $x = 0$. (b) The coefficients S and w^2 of x^2 and x have degrees 4 and 8 in n, so the substitution $n = 1/s$, $x = x'/s^4$, $y = y'/s^6$ gives the equation $y'^2 = x'(x'^2 + s^4S(1/s)x' + s^8w(1/s)^2)$ with coefficients in $\mathbb{Q}[s]$ and discriminant $s^{24}\Delta(1/s)$. Since Δ has degree 23, this discriminant vanishes to order 1 at $s = 0$, so the fiber at ∞ is of type I_1 and contributes 1 to the Euler number. At a zero of w, where $S = (a-b)^2 \neq 0$, the fiber is multiplicative of type I_4, and at the zeros of $S^2 - 4w^2 = (a-b)^2(a+b)^2$ of multiplicity 2 and 1, where the invariant $c_4 = 16(S^2 - 3w^2)$ of (3.1) is $16w^2 \neq 0$, it is of type I_2 and I_1 respectively [28, Table (IV.3.1)]. A relatively minimal elliptic surface over $\mathbb{P}^1$ with a section and Euler number 24 is a K3 surface [28, (III.4.2)–(III.4.6)]. □

The twists we use were found with averages of traces of Frobenius. For a twist Y^q of Y and a prime p, let $A_p(Y^q)$ be the average over $n_0 \in \mathbb{F}_p$ of the traces of Frobenius of the fibers of Y^q modulo p (with trace 0 at the singular fibers). Nagao [29] conjectured that $-\frac{1}{x}\sum_{p \le x} A_p \log p$ tends to the rank over $\mathbb{Q}(n)$. We computed the plain average of $-A_p(Y^q)$ over the primes $300 < p < 3000$ for the twists of Y by the linear polynomials in n of Appendix A and by their products with n. For Y and Y^n they are 1.00 and 1.99, in line with $\operatorname{rank} X(\mathbb{Q}(m)) = 3$. Only three other twists have averages above 0.45, all three close to 1: the twists by q_2, by nq_1 and by $n(4n+45)$, with averages 1.04, 1.04 and 1.06, where

$$q_1 = 5(3n + 242), \qquad q_2 = 5(2n + 243), \qquad q_{12} = q_1q_2/25 = (3n + 242)(2n + 243).$$

The automorphism of Lemma 3.1(c) exchanges the twists by q_2 and nq_1, up to squares. Over $\mathbb{Q}(C)$, where q_1 and q_2 become squares, these two twists become trivial together with the

twist by q_{12}, whose class is the product of theirs over $\mathbb{Q}(m)$. As q_{12} is quadratic in n and not divisible by n, this twist is not among those scanned, and its average is 1.00. The twist by $n(4n+45)$ leads to no better base: over the curves of genus one on which $4m^2+45$ and one of q_1, q_2 become squares, X has rank only 5 (Section 7). We found the points below by computing generators of the twists by q_2, nq_1 and q_{12} at the integers $2 \le n_0 \le 160$ at which these twists have rank one, and interpolating in n the values of $-x/(qw) - qw/x$, where x is the x-coordinate of the generator on Y^q, for $q = q_2$, nq_1, q_{12}. These values do not change when $(0,0)$ is added to the generator, and the interpolating functions have degree 4.

Lemma 3.2. *With $N = n^2 - 2n + 9801$, the points (x_i, y_i) with the following coordinates lie on Y^{q_2}, Y^{nq_1} and $Y^{q_{12}}$ over $\mathbb{Q}(n)$:*

$$\begin{aligned} x_4 &= 49(n-1)(n-81)(n-121)^2(2n+243)^2 && \text{on } Y^{q_2},\\ x_5 &= 49(n-9801)(n-121)(n-81)^2(3n+242)^2 && \text{on } Y^{nq_1},\\ x_6 &= 49(n-9801)(n-1)(n-121)^2(2n+243)^2 && \text{on } Y^{q_{12}}, \end{aligned}$$

and

$$\begin{aligned} y_4 &= -686\,(n-1)(n-36)(n-81)(n-121)^2(2n+243)^2N,\\ y_5 &= -686\,(n-9801)(n-121)(4n-1089)(n-81)^2(3n+242)^2N,\\ y_6 &= -1715\,(n-9801)(n-1)(n-99)(n-121)^2(2n+243)^2N. \end{aligned}$$

Up to sign, (x_5, y_5) is the image of (x_4, y_4) under the automorphism of Lemma 3.1(c).

Proof. Expanding gives

$$\begin{aligned} x_4^2 + q_2Sx_4 + q_2^2w^2 &= 9604\,(n-1)(n-81)(n-36)^2(n-121)^2(2n+243)^2N^2,\\ x_5^2 + nq_1Sx_5 + n^2q_1^2w^2 &= 9604\,(n-9801)(n-121)(n-81)^2(3n+242)^2(4n-1089)^2N^2,\\ x_6^2 + q_{12}Sx_6 + q_{12}^2w^2 &= 60025\,(n-9801)(n-1)(n-99)^2(n-121)^2(2n+243)^2N^2, \end{aligned}$$

so that $x_i(x_i^2 + qSx_i + q^2w^2) = y_i^2$ for $q = q_2$, nq_1, q_{12} and $i = 4$, 5, 6 respectively. The last assertion holds since

$$q_2(9801/n) = (9/n)^2\, nq_1(n) \qquad \text{and} \qquad x_4(9801/n) = (9/n)^2(99/n)^4\, x_5(n).$$

□

4. The curve C and six points

On C one has $u^2 = q_1(m^2)$ and $v^2 = q_2(m^2)$, so the twists of Lemma 3.2 become trivial over $\mathbb{Q}(C) = \mathbb{Q}(m,u,v)$: $q_2 = v^2$, $nq_1 = (mu)^2$ and $q_{12} = (uv/5)^2$.

Lemma 4.1. *Let $\overline{C} \subset \mathbb{P}^3$ be the closure of C, defined by $u^2 = 15m^2 + 1210z^2$ and $v^2 = 10m^2 + 1215z^2$.*

(a) $\overline{C}$ is a smooth curve of genus one, and $(m,u,v) = (1,35,35)$ is a rational point.

(b) $\overline{C}$ is isomorphic over $\mathbb{Q}$ to $E_C\colon y^2 = x^3 + x^2 - 137620x - 10504000$, which has conductor $9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ (LMFDB label 9240.bf4 [26]), torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, generated by $(-190, 2970)$ and $(-80, 0)$, and rank 1; the point $(-322, 726)$ has infinite order. In particular $\overline{C}(\mathbb{Q})$ is infinite, and $C(\mathbb{Q}) = \overline{C}(\mathbb{Q})$.

Proof. (a) The pencil $\lambda_1(u^2 - 15m^2 - 1210z^2) + \lambda_2(v^2 - 10m^2 - 1215z^2)$ has determinant $25\lambda_1\lambda_2(3\lambda_1 + 2\lambda_2)(242\lambda_1 + 243\lambda_2)$, so its four singular quadrics are distinct, and $\overline{C}$ is a smooth curve of genus one [4, Theorem 2.8(ii)]. (b) The lines $u = 35 + k(m-1)$ through

$(m,u)=(1,35)$ meet the conic $u^2=15m^2+1210$ again at $m=(k^2-70k+15)/(k^2-15)$, $u=-5(7k^2-6k+105)/(k^2-15)$, and then $v^2=5(2m^2+243)$ becomes

$$\eta^2=g(k):=49k^4-56k^3+514k^2-840k+11025,\qquad \eta=v(k^2-15)/5.$$

This gives a birational map from $\overline{C}$ to the smooth projective model of $\eta^2=g(k)$. As g has nonzero discriminant and the square leading coefficient 49, this curve is isomorphic over $\mathbb{Q}$ to its Jacobian, which has minimal model E_C [4, Theorem 2.8(iii)]. This is the curve 9240.bf4 of [26], with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and rank 1. The point $(-322,726)$ has infinite order, since $3\cdot(-322,726)$ has x-coordinate $-1901193922/2521^2$ and a torsion point of an integral Weierstrass equation has p-integral coordinates at every odd prime p [36, Theorem VII.3.4]. Finally, a rational point of $\overline{C}$ with $z=0$ would need $u^2=15m^2$ and $v^2=10m^2$ with $m\neq 0$, and 15 and 10 are not squares. □

Proposition 4.2. *With $n=m^2$, $q_1=u^2$, $q_2=v^2$ and x_i,y_i as in Lemma 3.2, the points*

$$P_4=\Big(\frac{x_4}{q_2},\ \frac{y_4}{q_2 v}\Big),\qquad P_5=\Big(\frac{x_5}{nq_1},\ \frac{y_5}{nq_1\,mu}\Big),\qquad P_6=\Big(\frac{x_6}{q_{12}},\ \frac{y_6}{q_{12}\,uv/5}\Big),$$

together with P_1,P_2,P_3 of Lemma 2.2, lie in $X(\mathbb{Q}(C))$. Explicitly,

$$\begin{aligned}x(P_4)&=\tfrac{49}{5}(m^2-1)(m^2-81)(m^2-121)^2(2m^2+243),\\ x(P_5)&=\tfrac{49}{5}\,m^{-2}(m^2-9801)(m^2-121)(m^2-81)^2(3m^2+242),\\ x(P_6)&=49\,(m^2-9801)(m^2-1)(m^2-121)^2(2m^2+243)/(3m^2+242).\end{aligned}$$

Proof. This follows from Lemma 3.2 and the map $(x,y)\mapsto(x/q,\ y/(q\sqrt{q}))$ defined before Lemma 3.1, applied with $\sqrt{q_2}=v$, $\sqrt{nq_1}=mu$ and $\sqrt{q_{12}}=uv/5$. □

Remark 4.3. The six points lie in four different eigenspaces of $X(\mathbb{Q}(C))\otimes\mathbb{Q}$. The extension $\mathbb{Q}(C)/\mathbb{Q}(m)$ is Galois with group $(\mathbb{Z}/2\mathbb{Z})^2$, generated by the sign changes of u and v, and $X(\mathbb{Q}(C))\otimes\mathbb{Q}$ is the sum of the eigenspaces of its four characters, $X(\mathbb{Q}(m))\otimes\mathbb{Q}$ and the parts on which only $u\mapsto -u$, only $v\mapsto -v$, or both act by -1. The points P_1,P_2,P_3 lie in the first, P_5 in the second, P_4 in the third and P_6 in the fourth.

5. Independence and the rank over $\mathbb{Q}(C)$

Proposition 5.1. *The points $P_1,\dots,P_6$ of Proposition 4.2 are linearly independent in $X(\mathbb{Q}(C))$.*

Proof. We specialize at one rational point of C and show that the six specialized points are independent by reducing them modulo six primes. Each reduction gives a homomorphism to $\mathbb{Z}/3\mathbb{Z}$ that kills the torsion, whose order is prime to 3. Evaluated at the six points, the six homomorphisms give a matrix that is invertible over $\mathbb{F}_3$.

Let $c_0=(m_0,u_0,v_0)=(7401/2399,\ 88235/2399,\ 86835/2399)\in C(\mathbb{Q})$. The fiber X_{m_0} is smooth, and all coordinates of the P_i are regular at c_0: their denominators are products of powers of 5, m, u and v. Specialization at c_0 is a group homomorphism $X(\mathbb{Q}(C))\to X_{m_0}(\mathbb{Q})$, since the Weierstrass model is smooth over the local ring of $\overline{C}$ at c_0. It therefore suffices to show that the points $P_i(c_0)$ are independent. Here

$$a(m_0)=8689566945346560000/2399^4,\qquad b(m_0)=4111541199653302800/2399^4,$$

and the scaling $(x, y) \mapsto (\nu^2 x, \nu^3 y)$ with $\nu = 2399^4/1234800$, which makes a and b coprime integers, maps X_{m_0} to $E_0 := E_{a_0,b_0}$, where

$$a_0 = 7037226227200 = 2^9 \cdot 5^2 \cdot 13 \cdot 47 \cdot 59 \cdot 101 \cdot 151,$$
$$b_0 = 3329722383911 = 7^2 \cdot 11 \cdot 17 \cdot 31 \cdot 41 \cdot 43 \cdot 61 \cdot 109.$$

Let R_i be the image of $P_i(c_0)$, with the y-coordinates of Lemma 2.2 and Proposition 4.2 and with $u_0, v_0 > 0$. Then

$$x(R_1) = -9134182662998624112839888896/625,$$
$$x(R_2) = -204090470295796923788950000,$$
$$x(R_3) = -19944153128696423007969280,$$
$$x(R_4) = -80466963140208120656325184314880/5755201,$$
$$x(R_5) = 68045531169574069706104995374489 60/6086089,$$
$$x(R_6) = -22494166745513310915537265584 8800/6355441.$$

The torsion subgroup of $E_0(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, so by Mazur's theorem [27] its order is 8 or 16. As this order is prime to 3, the torsion subgroup lies in $3E_0(\mathbb{Q})$. Let p be a prime of good reduction at which 3 divides $\#\widetilde{E}_0(\mathbb{F}_p)$ and the 3-primary part of $\widetilde{E}_0(\mathbb{F}_p)$ is cyclic. Then $P \mapsto (\#\widetilde{E}_0(\mathbb{F}_p)/3)\,\widetilde{P}$ is a homomorphism $E_0(\mathbb{Q}) \to \widetilde{E}_0(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$ with kernel containing $3E_0(\mathbb{Q})$, so it kills the torsion subgroup. The primes

$$p = 23,\ 37,\ 53,\ 83,\ 89,\ 113, \qquad \#\widetilde{E}_0(\mathbb{F}_p) = 24,\ 48,\ 48,\ 96,\ 96,\ 96,$$

are of this kind: they are odd and do not divide $a_0 b_0 (a_0^2 - b_0^2)$, and since $9 \nmid \#\widetilde{E}_0(\mathbb{F}_p)$ the 3-primary part is cyclic. With respect to a generator of $\widetilde{E}_0(\mathbb{F}_p)[3]$ (so up to sign), the images of $R_1, \dots, R_6$ at the j-th of these primes are the entries of the j-th row of

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 & 2 \\ 2 & 2 & 1 & 1 & 0 & 1 \\ 2 & 0 & 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 1 & 0 \end{pmatrix}, \qquad \det M \equiv 1 \pmod 3.$$

The points of order 3 of $\widetilde{E}_0(\mathbb{F}_p)$ have x-coordinate 9, 11, 40, 75, 79 and 4 at $p = 23$, 37, 53, 83, 89 and 113. If $\sum_i n_i R_i$ were a torsion point for some nonzero $(n_i) \in \mathbb{Z}^6$, we could divide the n_i by their greatest common divisor and assume $\gcd(n_i) = 1$. Then $(n_i \bmod 3)$ is a nonzero column vector with $M\,(n_i \bmod 3) = 0$, which is impossible. Thus $R_1, \dots, R_6$ are independent, and so are $P_1, \dots, P_6$. □

Proposition 5.2. *For $q \in \mathbb{Q}(m)^\times$ let $X^q\colon y^2 = x(x + qa^2)(x + qb^2)$ be the quadratic twist of X by q. With $n = m^2$, each of the twists X^{q_1}, X^{q_2} and $X^{q_{12}}$ has rank 1 over $\mathbb{Q}(m)$. Hence $\operatorname{rank} X(\mathbb{Q}(C)) = 6$, and $P_1, \dots, P_6$ generate a subgroup of finite index in $X(\mathbb{Q}(C))$.*

Proof. Since $\mathbb{Q}(C) = \mathbb{Q}(m)(u, v)$ with $u^2 = q_1$, $v^2 = q_2$ and $q_1 q_2 = 25 q_{12}$, the decomposition of Remark 4.3 gives

$$\operatorname{rank} X(\mathbb{Q}(C)) = \operatorname{rank} X(\mathbb{Q}(m)) + \operatorname{rank} X^{q_1}(\mathbb{Q}(m)) + \operatorname{rank} X^{q_2}(\mathbb{Q}(m)) + \operatorname{rank} X^{q_{12}}(\mathbb{Q}(m)),$$

because the part of $X(\mathbb{Q}(C)) \otimes \mathbb{Q}$ on which $u \mapsto -u$ acts by -1 and $v \mapsto -v$ trivially is the image of $X^{q_1}(\mathbb{Q}(m)) \otimes \mathbb{Q}$ under $(x, y) \mapsto (x/q_1,\ y/(q_1 u))$, and similarly for the other two

parts. By Propositions 2.4 and 5.1, $\operatorname{rank} X(\mathbb{Q}(m)) = 3$ and $\operatorname{rank} X(\mathbb{Q}(C)) \geq 6$, so the ranks of the three twists add up to at least 3. It suffices to show that each of them has rank at most 1 over $\mathbb{Q}(m)$, since then each has rank exactly 1 and $\operatorname{rank} X(\mathbb{Q}(C)) = 6$.

We apply [19, Theorem 1.1] as in Proposition 2.4 to X^q, with $(e_1, e_2, e_3) = (0, -qa^2, -qb^2)$, for $q = q_2, q_{12} \in \mathbb{Z}[m]$. The curve X^q has the same nonconstant j-invariant as X. The three products are now $q^2a^2b^2$, $q^2a^2(a^2 - b^2)$ and $-q^2b^2(a^2 - b^2)$. Their irreducible factors are the eleven of Proposition 2.4 and those of q, which are among $3m^2 + 242$ and $2m^2 + 243$, and their contents involve only the primes 2, 5 and 7. We take $m = 50/3$, where these factors have the squarefree parts listed in Table 1. In both cases these classes and -1, 2, 5, 7 are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so no nonconstant squarefree divisor of the three products takes a square value, which is the hypothesis of [19, Theorem 1.1]. The fibers of X^{q_2} and $X^{q_{12}}$ at $50/3$ have full rational 2-torsion and 2-Selmer groups of dimension 3 (computed with `mwrank` [3]). As the 2-torsion accounts for 2 of these dimensions, their ranks are at most 1, and that theorem gives $\operatorname{rank} X^q(\mathbb{Q}(m)) \leq 1$. Since $a(99/m) = -(99/m^2)^2 b(m)$, $b(99/m) = -(99/m^2)^2 a(m)$ and $q_2(99/m) = (9/m)^2 q_1(m)$, the automorphism $m \mapsto 99/m$ of $\mathbb{Q}(m)$, followed by a scaling of x and y, maps $X^{q_2}(\mathbb{Q}(m))$ isomorphically onto $X^{q_1}(\mathbb{Q}(m))$. Hence $\operatorname{rank} X^{q_1}(\mathbb{Q}(m)) = \operatorname{rank} X^{q_2}(\mathbb{Q}(m)) \leq 1$.

Finally, $X(\mathbb{Q}(C))$ is finitely generated [24], so its subgroup generated by the six independent points, which has rank 6, has finite index. □

6. Proof of the theorems

We prove Theorem 1.2 first, with the theorems of Silverman and Faltings, and then Theorem 1.1, by congruences that carry the computation at c_0 to infinitely many points of $C(\mathbb{Q})$ (Proposition 6.1).

Proof of Theorem 1.2. Part (a) is Lemma 4.1, and part (b) is Propositions 5.1 and 5.2.

(c) By Section 2, the fiber at $c \in C(\mathbb{Q})$ is an elliptic curve with torsion containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ unless $m(c) \in \{0, \pm 1, \pm 9, \pm 11, \pm 99\}$. Of these values only ± 1 and ± 99 occur on C, at the sixteen points listed, and by Lemma 4.1 the value $m(c) = \infty$ does not occur.

The j-invariant of X is $256(a^4 - a^2b^2 + b^4)^3/(a^4b^4(a^2 - b^2)^2)$, a quotient of polynomials in m of degrees 48 and 46 that are coprime because a and b are; so it has degree 48 in m. As m is nonconstant on C, so is j, and Silverman's specialization theorem [35, Theorem C] shows that the specialization map $X(\mathbb{Q}(C)) \to X_{m(c)}(\mathbb{Q})$ is injective for all but finitely many $c \in C(\mathbb{Q})$ with smooth fiber, and at those c we have $\operatorname{rank} X_{m(c)}(\mathbb{Q}) \geq 6$ by Theorem 1.2(b).

It remains to show that the torsion is exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for all but finitely many c. By Lemma 2.3, a larger torsion subgroup requires $ab(m(c))$ or $-ab(m(c))$ to be a nonzero square. The polynomial

$$ab = -49(m^2 - 1)(m^2 - 81)(m^2 - 121)(m^2 - 9801)$$

has degree 8 and distinct roots, so each of the hyperelliptic curves $r^2 = \pm ab(m)$ has genus 3. By Faltings' theorem [18, Satz 7] each has finitely many rational points, so $\pm ab(m)$ is a square for only finitely many $m \in \mathbb{Q}$. As at most four points of C lie over each value of m, $\pm ab(m(c))$ is a square for only finitely many $c \in C(\mathbb{Q})$. □

At c_0 the six points stay independent by Proposition 5.1. Since $13 \parallel a_0b_0$ and $-a_0b_0 < 0$, neither a_0b_0 nor $-a_0b_0$ is a square, and by Lemma 2.3 the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The rank of $E_{a_0,b_0}(\mathbb{Q})$ is exactly 6. With `mwrank` [3] we find that this curve has a 2-Selmer group of dimension 8, and its 2-torsion subgroup is $(\mathbb{Z}/2\mathbb{Z})^2$, so the rank is at most 6.

Proposition 6.1. *Let $c_0=(m_0,u_0,v_0)$ be the point of Proposition 5.1, and let $\mathcal{S}$ be the set of points $(m,u,v)\in C(\mathbb{Q})$ such that $\operatorname{ord}_{13}(m-m_0)\geq 2$ and, for each of the six primes $p=23,37,53,83,89,113$ of Proposition 5.1, the coordinates m, u, v are p-integral and congruent to m_0, u_0, v_0 modulo p. Then $\mathcal{S}$ is infinite. For every $c=(m,u,v)\in\mathcal{S}$ the fiber $X_m=X_{m(c)}$ is an elliptic curve with $X_m(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, and the specializations $P_1(c),\dots,P_6(c)$ of the points of Lemma 2.2 and Proposition 4.2 are linearly independent in $X_m(\mathbb{Q})$, so that $\operatorname{rank}X_m(\mathbb{Q})\geq 6$.*

Proof. Torsion. At $m_0=7401/2399$ the eight linear factors $m\pm1$, $m\pm9$, $m\pm11$, $m\pm99$ of $ab=-49(m^2-1)(m^2-81)(m^2-121)(m^2-9801)$ are 13-adic units except $m-99$, since $m_0\equiv 8 \pmod{13}$. As $m_0-99=-2^2\cdot3\cdot5^2\cdot13\cdot59/2399$, we have $\operatorname{ord}_{13}(m_0-99)=1$. If $\operatorname{ord}_{13}(m-m_0)\geq2$, then $\operatorname{ord}_{13}(m-99)=1$, and the other seven factors are congruent modulo 13^2 to their values at m_0, so they are 13-adic units and $\operatorname{ord}_{13}(ab(m))=1$. In particular $ab(m)\neq0$, and neither $ab(m)$ nor $-ab(m)$ is a square.

Good reduction. Let p be one of the six primes. The numbers m_0, $3m_0^2+242$, $a(m_0)$, $b(m_0)$, $a(m_0)-b(m_0)$ and $a(m_0)+b(m_0)$ are p-adic units, and u_0, v_0 are p-integral. Since $a,b\in\mathbb{Z}[m]$ and $m\equiv m_0 \pmod p$, the number $a(m)b(m)(a(m)^2-b(m)^2)$ is a p-adic unit. Thus X_m is an elliptic curve, and the model $y^2=x(x+a(m)^2)(x+b(m)^2)$ has good reduction at p and reduces to the same curve as X_{m_0}. By the first part and Lemma 2.3, $X_m(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

The six points. The coordinates of P_1, P_2, P_3 are polynomials in m with integer coefficients, and those of P_4, P_5, P_6 lie in $\mathbb{Z}[1/5,1/m,1/(3m^2+242)][m,u,v]$. For the x-coordinates this can be read off Proposition 4.2. For the y-coordinates, $u^2=q_1$ and $v^2=q_2$ give $y(P_4)=y_4v/q_2^2$, $y(P_5)=y_5u/(m^3q_1^2)$ and $y(P_6)=y_6uv/(5q_{12}^2)$, and y_4, y_5, y_6 of Lemma 3.2 are divisible by $(2n+243)^2$, $(3n+242)^2$ and $(2n+243)^2$ respectively. For $c\in\mathcal{S}$ the points $P_i(c)$ therefore have p-integral coordinates, congruent modulo p to those of $P_i(c_0)$, and they have the same reductions as the $P_i(c_0)$.

Independence. The scaling $\nu=2399^4/(2^4\cdot3^2\cdot5^2\cdot7^3)$ of Proposition 5.1 is a p-adic unit, so it induces an isomorphism from the reduction of X_{m_0} to that of E_0, which carries the reductions of the $P_i(c_0)$ to those of the R_i. Hence the six homomorphisms $X_m(\mathbb{Q})\to\mathbb{Z}/3\mathbb{Z}$ defined as in the proof of Proposition 5.1, one for each prime, kill the torsion subgroup and take on $P_1(c),\dots,P_6(c)$ the values given by the matrix M. Since $\det M\not\equiv0 \pmod3$, the points $P_1(c),\dots,P_6(c)$ are independent, as there.

$\mathcal{S}$ is infinite. Take c_0 as the origin of the group law on $\overline{C}$, a smooth curve of genus one by Lemma 4.1(a). By Lemma 4.1(b), $\overline{C}$ is isomorphic to E_C, which has rank one, and hence $\overline{C}(\mathbb{Q})$ contains a point c' of infinite order. For $p=13$ let $\Omega_p\subset\overline{C}(\mathbb{Q}_p)$ be the set of affine points with $m\in\mathbb{Z}_{13}$ and $\operatorname{ord}_{13}(m-m_0)\geq2$, and for each of the six other primes the set of affine points with $m,u,v\in\mathbb{Z}_p$ congruent to m_0,u_0,v_0 modulo p. Each Ω_p is an open neighborhood of c_0, so $\Omega=\prod_p\Omega_p$ is an open neighborhood of the identity in the compact group $\Gamma=\prod_p\overline{C}(\mathbb{Q}_p)$, the products running over the seven primes. For the diagonal embedding of $\overline{C}(\mathbb{Q})$ in Γ one has $\mathcal{S}=\overline{C}(\mathbb{Q})\cap\Omega$. Let Ω' be an open neighborhood of the identity with $\Omega'-\Omega'\subset\Omega$. Finitely many translates of Ω' cover Γ, so one of them contains kc' for infinitely many $k\geq1$, say for $k_1<k_2<\cdots$. Then the points $(k_j-k_1)c'$, $j\geq2$, lie in $\Omega'-\Omega'\subset\Omega$, hence in $\mathcal{S}$, and they are distinct because c' has infinite order. □

Proof of Theorem 1.1. By Proposition 6.1 the infinite set $\mathcal{S}$ consists of points c at which $X_{m(c)}$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and rank at least 6. The map $c\mapsto j(X_{m(c)})$ is a

nonconstant rational function on $\overline{C}$ of degree at most $48 \cdot 4 = 192$, since m has degree 4 on $\overline{C}$. This map takes each value at most 192 times, and infinitely many j-invariants occur. □

Remark 6.2. Here, as in [33, §5.1], the height of an elliptic curve over $\mathbb{Q}$ is $\max(|4A^3|, |27B^2|)$ for its model $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and no prime p with $p^4 \mid A$ and $p^6 \mid B$. For $m = x_1/x_0$ in lowest terms the invariants c_4, c_6 of the model $E_{x_0^4 a(m),\, x_0^4 b(m)}$ of X_m are binary forms in (x_0, x_1) of degrees 16 and 24 with no common zero, since every singular fiber of (1.2), including the one at $m = \infty$, is nodal. The height of X_m therefore lies between two positive constant multiples of $\max(|x_0|, |x_1|)^{48}$. Applying Néron's count [30, Ch. III, Théorème 4 and Corollaire 2] to the function m on $\overline{C}$, whose Jacobian has rank one, and using the bound 192, we obtain $(\log H)^{1/2+o(1)}$ curves $X_{m(c)}$, $c \in C(\mathbb{Q})$, of height at most H. In the same way, for the family F of Section 8 over the curve G_2, whose Jacobian has rank two, the invariants $c_4 = 16(U^2 - 3V^2)$ and $c_6 = -32U(2U^2 - 9V^2)$ of (8.1) are forms of degrees 4 and 6 in its parameter W with no common zero, since $c_4 \neq 0$ at the zeros $W = 1, \lambda^2, 0, -\lambda, \infty$ of the discriminant $16V^4(U^2 - 4V^2) = 256(1+\lambda)^2 W(W+\lambda)^2 V^4$; with the bound 96 proved there they give $(\log H)^{1+o(1)}$.

7. Other bases for X

We compare C with other bases for X. Over the conic $D\colon u^2 = 5(3m^2 + 242)$, on which only q_1 becomes a square, the points P_1, P_2, P_3 and P_5 are defined, since P_5 involves only m and $\sqrt{nq_1} = mu$. The conic is parametrized by $m = (k^2 - 70k + 15)/(k^2 - 15)$, $u = -5(7k^2 - 6k + 105)/(k^2 - 15)$, and at $k = 35/41$ one has $(m, u) = (m_0, u_0)$, so the four points specialize to four of the six independent points of Proposition 5.1; hence X has rank exactly 4 over $\mathbb{Q}(D) = \mathbb{Q}(k)$, namely $\operatorname{rank} X(\mathbb{Q}(m)) + \operatorname{rank} X^{q_1}(\mathbb{Q}(m)) = 3 + 1$ (Propositions 2.4 and 5.2). Dujella and Peral's curve of rank 9 is the fiber at $k = 25/11$, where $m = 1681/119$ (Section 2).

The map $(\alpha, \tau) \mapsto (\alpha, 1/\tau)$ preserves (2.1) up to $x \mapsto \tau^4 x$ and turns the second condition of Dujella and Peral into the condition that $2\alpha^2\tau^2 + \alpha^2 + \tau^2$ be a square; at $\alpha = 7$ and $\tau = (99 - m^2)/(14m)$ this is $99\tau^2 + 49 = h(m)/(14m)^2$ with $h = 99m^4 - 9998m^2 + 970299$. The curve $G\colon \eta^2 = h(m)$ has genus one and the rational point $(57, 31836)$, and its Jacobian $y^2 = x^3 + x^2 - 26097400x + 38851416548$, of conductor 683760 and torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, has rank 2, by a 2-descent [23]. Over $\mathbb{Q}(G) = \mathbb{Q}(m)(\sqrt{h})$ the curve X has rank exactly 5. The upper bound is $\operatorname{rank} X(\mathbb{Q}(G)) = \operatorname{rank} X(\mathbb{Q}(m)) + \operatorname{rank} X^h(\mathbb{Q}(m)) \leq 3 + 2$, where $X^h\colon y^2 = x(x + ha^2)(x + hb^2)$. The bound for X^h follows as in Proposition 5.2, from the criterion of Gusić and Tadić at $m = -80/3$, where the irreducible factors are those of Proposition 2.4 and h, and a 2-Selmer group of dimension 4 there. For the lower bound, the substitution $m \mapsto m' = (\eta - 98m)/(99 - m^2)$ satisfies $\tau(m') = 1/\tau(m)$, and with $\delta = (99 - m^2)/(14m')$ one has $a(m') = a(m)/\delta^2$ and $b(m') = b(m)/\delta^2$; so $(x, y) \mapsto (\delta^4 x(m'), \delta^6 y(m'))$ carries P_2 and P_3 to points P_2' and P_3' of $X(\mathbb{Q}(G))$, and $P_1, P_2, P_3, P_2', P_3'$ are independent, by a matrix of rank 5 over $\mathbb{F}_3$ computed as in Proposition 5.1 at $m = 291/53$ with the primes 37, 41, 61, 107 and 113. Since $G(\mathbb{Q})$ is infinite, Silverman's theorem and the argument of Section 6 give infinitely many curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank at least 5. This recovers Eroshkin's result. Over G one twist of rank 2 becomes trivial, whereas over C three twists of rank 1 do (Proposition 5.2). Over G the rank 6 appears at single fibers, such as the one at $m = 291/53$, which has rank 6, whereas over C it is the rank of $X(\mathbb{Q}(C))$.

Finally, the third twist found by the search of Section 3, by $n(4n + 45)$, gives over $\mathbb{Q}(m)$ the twist of X by $4m^2 + 45$, which has rank 1. The twist of Y by $n(4n + 45)$ has the point

with x-coordinate $49(n-121)(n-1)n^2(11n-1971)^2$, which gives a point of $X^{4m^2+45}(\mathbb{Q}(m))$. This point has infinite order, since at $m=42$ twice its specialization is not 13-integral on the integral model $y^2=x(x+(4m^2+45)a^2)(x+(4m^2+45)b^2)$ of that fiber [36, Theorem VII.3.4]. The upper bound follows as in Proposition 5.2 at $m=42$. The twists of X by $(4m^2+45)q_1$, $(4m^2+45)q_2$ and $(4m^2+45)q_{12}$ have rank 0 over $\mathbb{Q}(m)$, as in Proposition 5.2 at $m=-58/3$, $-58/3$ and $-46/7$, where the 2-Selmer groups have dimension 2. Hence X has rank 5 over each of the two curves of genus one on which $4m^2+45$ and one of q_1, q_2 become squares, and rank 7 over the curve of genus 5 on which all three do, which has only finitely many rational points by Faltings' theorem.

8. A second family

We give a second family with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and rank at least 6, over a curve of genus one and rank two.

Let $\mu=19/33$, $\lambda=\mu^2=361/1089$, $\beta=(161/1089)^2$ and $\gamma=\lambda^2/\beta=(361/161)^2$, and let

$$F\colon\ y^2=x(x^2+Ux+V^2),\qquad U=2(1+\lambda)^2W+2(W+\lambda)^2,\quad V=-(W-1)(W-\lambda^2),\tag{8.1}$$

over $\mathbb{Q}(W)$. Then $U-2V=4(W+\lambda)^2$ and $U+2V=4(1+\lambda)^2W$, so $(-V,\,2V(W+\lambda))$ is a point of order 4 with double $(0,0)$, and the other points of order 2 are defined over $\mathbb{Q}(s_1)$, where $W=s_1^2$. Over $\mathbb{Q}(s_1)$, F is the curve $E_{(s_1-1)(s_1-\lambda),\,(s_1+1)(s_1+\lambda)}$. Since $A_+B_+=\alpha^3(s_1+1)(s_1+\lambda)$ and $A_-B_-=-\alpha^3(s_1-1)(s_1-\lambda)$ at $(\alpha,\tau)=(33/19,\,33s_1/19)$, this is the model (2.1) of Dujella and Peral on the line $\alpha=33/19$, with no square condition imposed.

These parameters come from an exact computation with λ and β left free, in which we prescribe the shape of a section, as Dujella and Peral do to find new points [15, §4]. In the model F^q used below, the twist of F by a constant multiple of $W-\beta$ has a section whose x-coordinate is a constant times $(W-1)(W-\lambda^2)$ when (λ,β) lies on the curve

$$\lambda^4-16\lambda^3+(16\beta+30)\lambda^2+(160\beta-16)\lambda+64\beta^2+16\beta+1=0,$$

and one whose x-coordinate is a constant times $(W-1)(W-\beta)$ when it lies on the curve

$$16\lambda^4+32\lambda^3+(8-8\beta)\lambda^2-(24\beta+8)\lambda+\beta^2-18\beta+1=0.$$

This holds apart from degenerate cases: $\lambda=-1$, where F is singular, and the points $(1,0)$ of the first curve and $(1,1)$ of the second, where the constant multiple is 0. Other than $(-1,1)$ and $(1/9,1/81)$, where $\beta=\lambda^2$, the two curves meet at only one rational point of the (λ,β)-plane, $(361/1089,(161/1089)^2)$. There both multiples of $W-\beta$ are $29(W-\beta)$ up to squares, so the twist by $29(W-\beta)$ has the two points Q_2 and Q_3 below. The involution $W\mapsto\lambda^2/W$ gives two more, Q_4 and Q_5. The twist by $-(W-\beta)(W-\gamma)$, whose branch points $W=\beta$ and $W=\gamma=\lambda^2/\beta$ are exchanged by the involution, carries one more, Q_6. The remaining point, Q_1, lies on F itself.

Let G_2 be the curve

$$G_2\colon\quad W=s_1^2,\qquad 29(W-\beta)=s_2^2,\qquad -29\beta(W-\gamma)=s_3^2,$$

and set $q_A=29(W-\beta)$, $q_B=-29\beta(W-\gamma)$ and $q_H=-(W-\beta)(W-\gamma)$, so that $q_Aq_B/q_H=(4669/1089)^2$.

The points. For $q\in\mathbb{Q}(W)^\times$ let $F^q\colon y^2=x(x^2+qUx+q^2V^2)$. The points $Q_1\in F(\mathbb{Q}(W))$, $Q_2,Q_3\in F^{q_A}(\mathbb{Q}(W))$ and $Q_6\in F^{q_H}(\mathbb{Q}(W))$ with

$$\begin{aligned}x(Q_1)&=\mu^{-2}(W-\lambda^2)^2,&\qquad x(Q_2)&=\tfrac{1015}{1089})^2(W-1)(W-\lambda^2),\\ x(Q_3)&=\tfrac{928}{1089})^2(W-1)(W-\beta),&\qquad x(Q_6)&=\tfrac{240}{289})^2(W-\beta)^2(W-\gamma)^2\end{aligned}$$

satisfy

$$\begin{aligned} x^2+Ux+V^2 &= \tfrac{2102500}{130321}\,(W+\lambda)^2(W-\lambda^2)^2 && \text{at } x=x(Q_1),\\ x^2+q_AUx+q_A^2V^2 &= 841\,(W-1)(W-\lambda^2)\,f_2^2 && \text{at } x=x(Q_2),\\ x^2+q_AUx+q_A^2V^2 &= 841\,(W-1)(W-\beta)^3(W-\tfrac{625}{1089})^2 && \text{at } x=x(Q_3),\\ x^2+q_HUx+q_H^2V^2 &= \tfrac{671898241}{6975757441}\,(W-\beta)^2(W-\gamma)^2f_6^2 && \text{at } x=x(Q_6), \end{aligned}$$

where $f_2 = W^2 - \frac{648517}{1185921}W + \frac{3467044}{1291467969}$ and $f_6 = W^2 - \frac{14138244652530322}{796818233864961}W + \lambda^2$, so that in each case $x(x^2+qUx+q^2V^2)$ is a square in $\mathbb{Q}[W]$ ($671898241 = 161^4$ and $6975757441 = 289^4$). Since $U(\lambda^2/W) = (\lambda/W)^2U(W)$, $V(\lambda^2/W) = (\lambda/W)^2V(W)$ and $q_A(\lambda^2/W) = q_B/W$, the map

$$\iota\colon (x,y) \mapsto \big((W^2/\lambda)^2x(\lambda^2/W),\ (W^2/\lambda)^3y(\lambda^2/W)\big)$$

is an isomorphism of groups $F^{q_A}(\mathbb{Q}(W)) \to F^{Wq_B}(\mathbb{Q}(W))$, the composite of the field automorphism $W \mapsto \lambda^2/W$ with an isomorphism of curves. Let $Q_4 = \iota(Q_2)$ and $Q_5 = \iota(Q_3)$. On G_2 one has $q_A = s_2^2$, $Wq_B = (s_1s_3)^2$ and $q_H = (1089s_2s_3/4669)^2$, so, as in Proposition 4.2, the six points give points of F over $\mathbb{Q}(G_2)$, which we denote by the same names.

Theorem 8.1. *(a) G_2 is a curve of genus one with infinitely many rational points. Its Jacobian has conductor* 182747931661680*, torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and rank* 2*.*

(b) The points $Q_1,\dots,Q_6$ defined above lie in $F(\mathbb{Q}(G_2))$ and are linearly independent, so $\operatorname{rank} F(\mathbb{Q}(G_2)) \ge 6$*.*

(c) At the sixteen rational points of G_2 with $W \in \{1,\lambda^2\}$ the fiber of F is singular. At every other rational point it is an elliptic curve whose torsion subgroup contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, and for all but finitely many rational points of G_2 its torsion subgroup is exactly $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and its rank is at least 6*. Infinitely many of these curves are pairwise non-isomorphic.*

(d) At the point of G_2 with $s_1 = 23306521/20091929$ described below, the fiber is isomorphic to $E_{a,b}$ with $(a,b) = (460019200,\ 11180308689)$; its torsion subgroup is exactly $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, and the six points specialize to independent points.

Proof of Theorem 8.1. (a) Parametrizing the conic $29(s_1^2-\beta) = s_2^2$ through $(s_1,s_2) = (161/1089, 0)$ by $s_1 = \frac{161}{1089}\,(\theta^2+29)/(\theta^2-29)$, $s_2 = \theta(s_1 - \frac{161}{1089})$ turns the third equation into

$$\eta^2 = 1326538900\,\theta^4 - 77611154441\,\theta^2 + 1115619214900, \qquad \eta = \tfrac{1185921}{58}\,s_3(\theta^2-29),$$

which is squarefree (its discriminant is nonzero), so G_2 has genus one. Its Jacobian has the minimal model

$$y^2 = x^3 + x^2 - 7927479575830823114160\,x + 27165830539902981904087537980 4308,$$

of conductor $182747931661680 = 2^4\cdot3\cdot5\cdot7\cdot11\cdot17\cdot19\cdot23\cdot29\cdot197\cdot233$ and torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. It has full rational 2-torsion and a 2-Selmer group of dimension 4 (computed with `mwrank` [3]), so its rank is at most 2. Its points $(50796866898,\ 198589582959768)$ and $(389256165869/4,\ 164296202311285275/8)$ are independent, so the rank is 2. Indeed, the cubic has the roots -102809641014, 51068871386 and 51740769627, and the 2-descent map $P \mapsto (x(P)+102809641014,\ x(P)-51068871386)$ of (2.2) sends the two points to $(2,\ -2)$ and $(197,\ 7\cdot23\cdot197)$, and the generators $(41550472818,\ 3741958510639272)$ and $(51068871386,\ 0)$ of the torsion subgroup to $(2\cdot197\cdot233,\ -2\cdot197\cdot233)$ and $(29\cdot197\cdot233,\ -29\cdot197\cdot233)$. These four vectors are independent: 29 occurs only in the last, 7 only in the second, then

233 only in the third, and 2 in the first. Since G_2 has the rational point $\theta = 10/3$ and its Jacobian has rank 2, the set $G_2(\mathbb{Q})$ is infinite.

(b) Specialization at a rational point of G_2 at which the fiber is smooth is a homomorphism, as in Proposition 5.1. By (d) the six points specialize to independent points at such a point, so they are independent.

(c) The discriminant of (8.1) is $16V^4(U^2 - 4V^2)$, and $U^2 - 4V^2 = 16(1+\lambda)^2 W(W+\lambda)^2$. At a rational point of G_2 we have $W = s_1^2$ with $s_1 = \frac{161}{1089}(\theta^2 + 29)/(\theta^2 - 29) \neq 0$, so the fiber is singular if and only if $W \in \{1, \lambda^2\}$, that is, at the sixteen points with $\theta \in \{\pm 10/3, \pm 87/10, \pm 25/4, \pm 116/25\}$. At the other rational points the fiber is smooth, with torsion containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The j-invariant of F is a nonconstant function of W, of degree 12. As in Section 6, Silverman's theorem [35, Theorem C] shows that specialization is injective at all but finitely many points of $G_2(\mathbb{Q})$, which is infinite by (a), and at those points the rank is at least 6 by (b). Since W has degree 8 on G_2, each j-invariant occurs at most 96 times.

It remains to show that the torsion is exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ at all but finitely many rational points. Recall that over $\mathbb{Q}(s_1)$, F is the curve $E_{(s_1-1)(s_1-\lambda),(s_1+1)(s_1+\lambda)}$, for which $ab = -V$. By Lemma 2.3, torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ at a rational point P requires V or $-V$ to be a nonzero rational square at $W(P)$. The map $W\colon G_2 \to \mathbb{P}^1$ of degree 8 is branched only over 0, β, γ and ∞, so V has 16 simple zeros on G_2, the points over $W = 1$ and $W = \lambda^2$, and poles of order 4 at the four points over ∞, each with ramification index 2. The double covers $r^2 = \pm V$ of G_2 are therefore branched at exactly 16 points, and by the Riemann–Hurwitz formula they have genus 9. By Faltings' theorem [18, Satz 7] each has finitely many rational points, so $\pm V(W)$ is a nonzero square at only finitely many rational points of G_2.

(d) The quartic of (a) has the rational point $\theta = 857/140$, with $s_1 = 23306521/20091929$, $s_2 = 1120373240/180827361$ and $s_3 = 11142156700/7293370227$. There the six points are defined over $\mathbb{Q}$. Scaling x by $(3633170498469369/1046900)^2$ takes the fiber to $E = E_{a,b}$ with

$$(a, b) = (460019200,\ 11180308689) = (2^9 \cdot 5^2 \cdot 83 \cdot 433,\ 3^3 \cdot 11 \cdot 17 \cdot 31 \cdot 61 \cdot 1171),$$

where $Q_1, \dots, Q_6$ have, in this order by rows, the x-coordinates

$$\begin{array}{ll} 499284308691438490000/9, & 2215757908015311217546474200/19037652529, \\ 3395584751700492739215 36/3258025, & 2917855828463273573584336 32/113273449, \\ -4563185528671931392, & 3381199714987226818560000/83521. \end{array}$$

Since $83 \parallel ab$ and $-ab < 0$, the curve has torsion exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ by Lemma 2.3. It has squarefree conductor

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 53 \cdot 61 \cdot 83 \cdot 89 \cdot 137 \cdot 241 \cdot 401 \cdot 433 \cdot 457 \cdot 1171 \cdot 2089.$$

At the primes $p = 41, 47, 59, 67, 79, 97$ one has $\#\widetilde{E}(\mathbb{F}_p) = 48, 48, 72, 72, 96, 96$, and at $p = 59$ and 67 the group is $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with cyclic 3-primary part. The images of the six points at the j-th of these primes in $\widetilde{E}(\mathbb{F}_p)/3\widetilde{E}(\mathbb{F}_p)$ are the entries of the j-th row of

$$M' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 0 & 2 \end{pmatrix}, \qquad \det M' \equiv 2 \pmod 3.$$

Each row is defined up to sign by the choice of generator, and each column up to sign by that of the y-coordinate of its point, which is not fixed here. Hence the six points are independent, as in Proposition 5.1. □

We do not know whether rank 7 occurs infinitely often with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; the curve of Theorem 8.1(d) has rank exactly 7, since its 2-Selmer group has dimension 9 and its torsion, Q_1, Q_3, Q_5 and four further points [23] have images spanning a space of dimension 9 under the map κ of (2.2).

Appendix A. Computations

We used PARI/GP 2.17.3 [32] and SageMath 10.9 [34], which includes Cremona's `mwrank` [3]. The divisor tests of Gusić and Tadić were done in PARI, and the upper bounds for ranks from 2-Selmer groups were computed with `mwrank`.

The averages of Section 3 are plain averages over the 368 primes p with $300 < p < 3000$. The twists there are those by $s(n - r_0)$ and by $sn(n - r_0)$, where r_0 runs over the rationals whose numerator and denominator are at most 1000 in absolute value and s over the squarefree integers with $|s| \leq 100$ (so no s is divisible by p).

The programs and their outputs are deposited in [23], and the Lean formalization in [22]. The formalization proves all the numbered results, including the computations and the rank bounds from 2-Selmer groups. Eleven of the results take theorems of other authors as hypotheses, listed in its README. Among these hypotheses are Mazur's torsion theorem, the Lang–Néron theorem, Silverman's specialization theorem, Faltings' theorem, Néron's count of points of bounded height, the theorem of Gusić and Tadić and Theorem 2.8 of Cremona, Fisher and Stoll.

Declarations

Use of AI. This paper, its results and its Lean formalization 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 [23].

References

1. A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), no. 201, 399–405, doi:10.1090/S0025-5718-1993-1140645-1.
2. Boris M. Bekker and Yuri G. Zarhin, *Division by 2 of rational points on elliptic curves*, St. Petersburg Math. J. **29** (2018), no. 4, 683–713, doi:10.1090/spmj/1512; arXiv:1702.02255v2.
3. John E. Cremona, *Algorithms for Modular Elliptic Curves*, second ed., Cambridge University Press, Cambridge, 1997.
4. John E. Cremona, Tom A. Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820, doi:10.2140/ant.2010.4.763; arXiv:0908.1741v1.
5. Andrej Dujella, *High rank elliptic curves with prescribed torsion*, https://web.math.pmf.unizg.hr/~duje/tors/tors.html (accessed October 15, 2026).

6. ———, *Infinite families of elliptic curves with high rank and prescribed torsion*, https://web.math.pmf.unizg.hr/~duje/tors/generic.html (accessed October 15, 2026).
7. ———, *Open problems on Diophantine m-tuples and elliptic curves*, https://web.math.pmf.unizg.hr/~duje/pdf/open2.pdf, version of October 15, 2026.
8. ———, *Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, rank $= 10$*, https://web.math.pmf.unizg.hr/~duje/tors/z2z4.html (accessed November 28, 2026).
9. ———, *On Mordell–Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), no. 1, 3–18, doi:10.3336/gm.42.1.01; arXiv:0705.1875v1.
10. 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.
11. Andrej Dujella and Juan Carlos Peral, *High-rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples*, LMS J. Comput. Math. **17** (2014), no. 1, 282–288, doi:10.1112/S1461157014000023.
12. ———, *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, where §§5.4 and 6.6 are §§4.4 and 5.5.
13. ———, *Elliptic curves induced by Diophantine triples*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **113** (2019), no. 2, 791–806, doi:10.1007/s13398-018-0513-0; arXiv:1712.02082v2.
14. ———, *Construction of high rank elliptic curves*, J. Geom. Anal. **31** (2021), no. 7, 6698–6724, doi:10.1007/s12220-020-00373-7.
15. ———, *An elliptic curve over $\mathbb{Q}(u)$ with torsion $\mathbb{Z}/4\mathbb{Z}$ and rank 6*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **28** (2024), 185–192, doi:10.21857/y54jof4o2m; arXiv:2207.08206v2.
16. Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007, Preprint, arXiv:0709.2908v1.
17. ———, *An elliptic K3 surface $X/\mathbb{Q}(t)$ with Mordell–Weil rank 17, I: Formulas for X and base changes of ranks 18 and 19*, 2026, Preprint, arXiv:2608.25406v1.
18. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, doi:10.1007/BF01388432.
19. 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.
20. Robert Harron and Andrew Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170, doi:10.1515/crelle-2014-0107; arXiv:1311.4920v1.
21. Manvir Jaswal, *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.23364157.
22. ———, *Lean formalization: "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.23682551.
23. ———, *Programs and data for "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.23437115.
24. Serge Lang and André Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81** (1959), no. 1, 95–118, doi:10.2307/2372851.
25. 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.
26. The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, elliptic curve 9240.bf4 (accessed October 16, 2026).
27. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186, doi:10.1007/BF02684339.
28. Rick Miranda, *The Basic Theory of Elliptic Surfaces*, Dottorato di Ricerca in Matematica, ETS Editrice, Pisa, 1989.
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. André Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166, doi:10.24033/bsmf.1427.
31. Ken Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), no. 2, 101–123, doi:10.4064/aa-78-2-101-123.
32. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr/.

33. 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.
34. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026, https://www.sagemath.org.
35. 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.
36. ———, *The Arithmetic of Elliptic Curves*, second ed., Grad. Texts in Math., vol. 106, Springer, New York, 2009, doi:10.1007/978-0-387-09494-6.

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