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 we show has rank exactly 3 over the rational function field. The family is a base change of an elliptic K3 surface, and quadratic twists of that surface give it three further independent points over the function field of an elliptic curve of rank one. Congruences then carry the independence of the six points, and the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, from one rational point of that curve to infinitely many. The result is unconditional. It contradicts the prediction of Park, Poonen, Voight and Wood that only finitely many curves with this torsion have rank greater than 5, although the curves form a sparse family. A second family, over an elliptic curve of rank two, gives another proof.

Contents

1. Introduction 1
2. The family of Dujella and Peral 5
3. A K3 surface and three of its twists 8
4. The curve C and six points 10
5. Independence and the rank over $\mathbb{Q}(C)$ 11
6. Proof of the theorems 13
7. Other bases for X 15
8. A second family 18
Appendix A. Computations 22
Declarations 22
References 22

1. Introduction

By Mazur's theorem [29], 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, a lower bound for $b_T = \limsup\{\operatorname{rank} E(\mathbb{Q}) : E(\mathbb{Q})_{\text{tors}} \cong T\}$ in the notation of [35].

Date: October 27, 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.

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 [1, Theorem 5.3], and [15, §6.7] for torsion exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$): 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 [27, Théorème 9], Elkies [17] and Eroshkin (see [12]) constructed families of rank at least 3, and Dujella and Peral [12] one of rank exactly 4, still the largest rank over $\mathbb{Q}(t)$ in Dujella's table. Elkies obtained rank at least 4 for an infinite family by a quadratic base change over an elliptic curve of positive rank [17, Lecture III, p. 13]. As of October 15, 2026 the largest known rank of a curve over $\mathbb{Q}$ with this torsion is 9, for curves of Dujella and Peral [12, 15] and of Klagsbrun (see [8]), and the largest rank known to occur infinitely often is 5, which Dujella's table [6] credits to Eroshkin (2009, personal communication). 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?"

Theorem 1.1 answers the first part of this question. The case $\mathbb{Z}/6\mathbb{Z}$ remains open.

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.*

We obtain these curves as fibers of a one-parameter family X of Dujella and Peral [15] over $\mathbb{Q}(m)$, of rank 3, which is the base change by $n = m^2$ of an elliptic K3 surface Y over $\mathbb{Q}(n)$. Over a field obtained from $\mathbb{Q}(m)$ by adjoining square roots, the rank of X is the sum of the ranks over $\mathbb{Q}(m)$ of the quadratic twists of X by the corresponding square classes. So a quadratic twist Y^q of Y of positive rank, with q not a square in $\mathbb{Q}(m)$, gives new points of X over the function field of any cover of the m-line on which q becomes a square. For these points to give infinitely many curves over $\mathbb{Q}$, this cover must have infinitely many rational points, and so, by Faltings' theorem [19], genus at most one. The new ingredient is a curve C of genus one and rank one over whose function field X acquires three further independent points. To find it, we used averages of traces of Frobenius to decide which twists of Y to look at (see below). They led us to the twists by $5(2n+243)$ and by $5n(3n+242)$, which become trivial over the curve C given by $u^2 = 5(3m^2+242)$ and $v^2 = 5(2m^2+243)$ (since $n = m^2$, $5n(3n+242)$ and $5(3n+242)$ have the same square class). Over $\mathbb{Q}(C)$ three square classes of $\mathbb{Q}(m)$ become trivial, those of $5(3m^2+242)$, $5(2m^2+243)$ and their product. The twist of X by each of them has rank one over $\mathbb{Q}(m)$ (Proposition 5.2), and these three twists give the three new points.

To pass to curves over $\mathbb{Q}$, we specialize at one rational point c_0 of C, where the six points stay independent (Proposition 5.1): reduction modulo six primes gives six homomorphisms to $\mathbb{Z}/3\mathbb{Z}$, and their values on the six points form a matrix that is invertible over $\mathbb{F}_3$. These reductions depend only on the point of C modulo the six primes, so the same argument applies at every rational point c of C congruent to c_0 modulo them. The torsion is handled in the same way: a curve $E_{a,b}$ has torsion larger than $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ only if ab or $-ab$ is a square (Lemma 6.1), which a congruence modulo 13^2 rules out, since 13 divides ab exactly once at c_0. As C has positive rank, infinitely many of its rational points satisfy all these congruences (Proposition 6.2), and the fibers at these points form an explicit infinite set of curves as in Theorem 1.1, with infinitely many j-invariants because j is a nonconstant function on C. For the stronger statement of Theorem 1.2(c) below, which concerns all but finitely many points of $C(\mathbb{Q})$, we use instead Silverman's specialization theorem [38,

Theorem C] for the rank and, for the torsion, Faltings' theorem, applied to two double covers of C. They leave a finite set of exceptions that we have not determined (Section 6).

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 [17, Lecture I]). With prescribed torsion they were used by Lecacheux and by Rabarison (see [13, §5.4]) and by Elkies [17, 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [13, §§5.4, 6.6]. Dujella, Kazalicki and Peral gave further such families for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [11, §9]. For $\mathbb{Z}/4\mathbb{Z}$, Dujella and Peral made explicit a remark of Elkies [17, 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 [15, §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 $\mathbb{Z}/4\mathbb{Z}$ [17, Lecture II]. With no torsion prescribed, Elkies announced in [17, Lectures II and III], and proved in [18], 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 [23] describes a construction by the same mechanism for the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$: quadratic twists of positive rank, found with averages of traces of Frobenius, become trivial over the function field of a curve of genus one and rank one, and Silverman's theorem gives the specialization; for Theorem 1.1 we use congruences instead.

Theorem 1.1 bears on the heuristic of Park, Poonen, Voight and Wood [35], which suggests that ranks of elliptic curves over $\mathbb{Q}$ are bounded. Adapted to prescribed torsion as in [35, §8.3], the argument of [35, 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 [22, Theorem 1.1 and §1.2], then $H^{1/d-(r-1)/24+o(1)}$ of them have rank at least r when $1 \le r < 1 + 24/d$, at most $H^{o(1)}$ when $r = 1 + 24/d$, and only finitely many when $r > 1 + 24/d$. This suggests that $b_T \le 1 + \lfloor 24/d \rfloor$. For $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ one has $d = 6$, and the table of [35, §8.3] lists the rank bound 5 next to the known lower bound 5. Dujella and Peral noted that the two bounds coincide for this group and for $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [14, 15], and Dujella [10] that these lower bounds are then best possible if the heuristic is correct.

Theorem 1.1 gives $b_T \ge 6$ for $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, so for this group the known lower bound 5 is not best possible, and b_T exceeds the bound 5 that the heuristic suggests. Our curves form a sparse family, however: they are parametrized by the rational points of C, so by Néron's count of points of bounded height [32, Ch. III, Théorème 4 and Corollaire 2] only $(\log H)^{1/2+o(1)}$ of them have height at most H (Remark 6.3). This count is within the model's bound of $H^{o(1)}$ curves of rank at least 5, but the model predicts only finitely many curves of rank at least 6: what fails is the table's prediction for the family of all curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Park, Poonen, Voight and Wood note that special families of elliptic curves may behave differently for arithmetic reasons [35, Remark 1.1.2], and, as Elkies pointed out (see [35, Remark 1.1.3]), their 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [11]; for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, where the table of [35, §8.3] lists the rank bound 3, the author's preprint [23] gives a family of rank at least 4.

Theorem 1.1 follows from the more precise Theorem 1.2. 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 $\mathbb{Q}(m)$, the family of Dujella and Peral with $\tau = 1/7$ in other coordinates (see below). 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 $m_0 \in \{0, \pm 1, \pm 9, \pm 11, \pm 99\}$ (Section 2). 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). 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 the function field $\mathbb{Q}(C)$ (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 $(\pm 1, \pm 35, \pm 35)$ and $(\pm 99, \pm 385, \pm 315)$ 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).

The family X is the one-parameter family that Dujella and Peral obtained in [15, §7.2] from their model with two parameters α and τ by making $\tau^2 + \alpha^2 + 2$ a square through a parameter t and fixing $\tau = 1/7$, written in other coordinates (Lemma 2.1). The model goes back to Dujella's study of the curves induced by Diophantine triples [9, §4], where it is used at $\alpha = 2$, and appears as [12, (5)] and [15, (13)]. Dujella and Peral chose $\tau = 1/7$, motivated by experiments and by the splitting of one coefficient of their model into seven linear factors. On this family they found a curve of rank 9, at $t = 900/781$ in their coordinate (see Lemma 2.1), and seven curves of rank 8 [15, §7.2]; one of these, at $t = 245/138$, they had found before [14, §3.2]. They do not determine the rank of the family over $\mathbb{Q}(t)$; we show that it is exactly 3 (Proposition 2.3).

How the curve C was found. The polynomials a and b satisfy $a(-m) = -b(m)$ and $b(-m) = -a(m)$, so the coefficients of (1.2) are polynomials in $n = m^2$, and X is the base change to $\mathbb{Q}(m) = \mathbb{Q}(n)(\sqrt{n})$ of an elliptic surface Y over the n-line, an elliptic K3 surface with a point of order 4 (Lemma 3.1). 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 [31] conjectured that $-\frac{1}{x}\sum_{p \le x} A_p \log p$ tends to the rank over $\mathbb{Q}(n)$, and Rosen and Silverman showed that Tate's conjecture for the surface implies it if, in addition, the L-function L_2 of the surface has no zeros on the line $\operatorname{Re} s = 2$ [36, Theorem 1.3]. As a heuristic guide in the search for twists of positive rank, we computed plain averages of $-A_p(Y^q)$ over primes p for the twists by many linear polynomials in n and by their products with n (Appendix A). For Y and Y^n they are 1.00 and 1.99, in line with $\operatorname{rank} X(\mathbb{Q}(m)) = 3$, and only three other twists of this kind have averages near 1: the twists by $q_2 = 5(2n + 243)$, by nq_1 with $q_1 = 5(3n + 242)$, and by $n(4n + 45)$, with averages 1.04, 1.04 and 1.06. The first two are exchanged by the automorphism $n \mapsto 9801/n$ of Y, and the twist by $q_1 q_2/25 = (3n + 242)(2n + 243)$ has average 1.00. The third leads to no better base:

over the curves of genus one on which $4n + 45$ and one of q_1, q_2 become squares, X has rank only 5, and the curve on which all three become squares has genus 5 (Section 7).

The curve C is the cover of the m-line on which q_1 and q_2 become squares; over its function field the twists of Y by q_2, nq_1 and q_1q_2 become trivial, and each contributes a point (Lemma 3.2). Over the conic on which only q_1 becomes a square, X has rank at least 4, and Dujella and Peral's curve of rank 9 is a fiber of X over this conic (Proposition 7.1). The twist by $h = 99n^2 - 9998n + 970299$ has average 1.93; the polynomial h comes from the image, under the symmetry $(\alpha, \tau) \mapsto (\alpha, 1/\tau)$ of their model, of Dujella and Peral's condition that $\alpha^2\tau^2 + 2\alpha^2 + 1$ be a square (Section 7). Over the curve of genus one on which h becomes a square, the twist of X by h, of rank 2, becomes trivial, and X has rank exactly 5 (Proposition 7.2). So the choice of the base curve is what lifts the rank to 6.

A second family. The family of Section 8 comes from the model of Dujella and Peral on the line $\alpha = 33/19$, a value at which a quadratic twist of the model acquires two independent sections, found by an exact computation. Its base is a curve of genus one and rank two, over whose function field the family acquires six independent points: one on the family itself; two on its quadratic twist by $29(\tau^2 - (161/627)^2)$, together with their images under the involution $\tau \mapsto 1/\tau$ of the base line; and one on its twist by $-(\tau^2 - (161/627)^2)(\tau^2 - (627/161)^2)$, whose branch points are exchanged by the involution (Theorem 8.1). This family gives a second proof of Theorem 1.1.

Formalization. All the numbered results of this paper are formalized in Lean 4 with Mathlib [24]. The formal proofs follow the arguments of Sections 2 to 8 and prove the computations they use; where they differ from the paper, the documentation says how. Fourteen of the results, including Theorems 1.1, 1.2 and 8.1, take as hypotheses theorems of other authors in arithmetic and algebraic geometry, stated in general form and listed with their sources in the formalization.

2. The family of Dujella and Peral

The curve X is the family of Dujella and Peral with $\tau = 1/7$, which a symmetry of their model carries to the line $\alpha = 7$ used here (Lemma 2.1 and the paragraph after it). It has rank exactly 3 over $\mathbb{Q}(m)$ (Proposition 2.3).

Dujella and Peral [15, §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 [15, (13)] and [12, (5)]:

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

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 $\alpha^2\tau^2 + 2\alpha^2 + 1$:

$$\tau^2 + \alpha^2 + 2 = \square \quad [15, (14)], \qquad \alpha^2\tau^2 + 2\alpha^2 + 1 = \square \quad [15, (16)].$$

At $\alpha = 7$ the second condition reads $49\tau^2 + 99 = \square$, and $\tau = (99 - m^2)/(14m)$ gives $49\tau^2 + 99 = \big((m^2 + 99)/(2m)\big)^2$. 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 $a = (14m)^2 A_+ B_+$ and $b = (14m)^2 A_- B_-$ in (1.1), and X is (2.1) at $\alpha = 7$, $\tau = (99 - m^2)/(14m)$ after the substitution $x \mapsto (14m)^4 x$. 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 $m_0 \in \{0, \pm 1, \pm 9, \pm 11, \pm 99\}$. The family of [15, §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 $A_+B_+(\alpha_t, \frac{1}{7}) = 4a'/(343(t^2-1)^2)$, $A_-B_-(\alpha_t, \frac{1}{7}) = -4b'/(343(t^2-1)^2)$, where $a' = t(5t-4)(5t-6)(49t-50)$ and $b' = (4t-5)(6t-5)(50t-49)$. Hence $a = \rho \cdot A_+B_+(\alpha_t, \frac{1}{7})$ and $b = -\rho \cdot A_-B_-(\alpha_t, \frac{1}{7})$ with $\rho = (98(t+1)/(t-1))^2$, and $(x, y) \mapsto (\rho^2 x, \rho^3 y)$ is an isomorphism over $\mathbb{Q}(t) = \mathbb{Q}(m)$ from the curve (2.1) at $(\alpha_t, 1/7)$, the family of [15, §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 $x \mapsto \rho^2 x$. □

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 $\sigma_2 \circ \psi = \sigma_1/\tau^2$, so it preserves (2.1) up to $x \mapsto \tau^4 x$ 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 $(99 - m^2)/(14m) = \alpha_t$. Dujella and Peral had a further reason for $\tau = 1/7$ [15, §7.2]: at $\alpha = (t^2 - 2(\tau^2 + 1)t + 1)/(\tau(t^2 - 1))$ the coefficient of x in their model has two quadratic factors in t, the numerators of A_+ and A_-, which both have discriminant $8\tau^2(\tau^2+1)$, a square at $\tau = 1/7$. Under ψ this corresponds to 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 $X(\mathbb{Q}(m))$:*

$$\begin{aligned}
x(P_1) &= -49(m-1)^2(m-11)^2(m+9)^2(m+99)^2,\\
x(P_1)+a^2 &= -19208\,m(m^2-99)(m-11)^2(m+9)^2,\\
x(P_1)+b^2 &= 392\,m(m^2-99)(m-1)^2(m+99)^2,\\
y(P_1) &= -19208\,m(m^2-99)(m-1)^2(m-11)^2(m+9)^2(m+99)^2;\\
x(P_2) &= 49(m-99)(m-1)(m+1)(m+99)(m-9)^2(m+11)^2,\\
x(P_2)+a^2 &= 98(m-99)(m+1)(m^2-99)(m^2+99)^2,\\
x(P_2)+b^2 &= 98(m-1)(m+99)(m^2-99)(m-9)^2(m+11)^2,\\
y(P_2) &= -686\,(m-99)(m-1)(m+1)(m+99)(m^2-99)\\
&\qquad\cdot(m^2+99)(m-9)^2(m+11)^2;\\
x(P_3) &= -49(m-11)(m-9)(m+1)(m+99)(m+9)^2(m+11)^2,\\
x(P_3)+a^2 &= -3920\,m(m-11)(m+1)(m+9)^2(2m-33)^2,\\
x(P_3)+b^2 &= 3920\,m(m-9)(m+99)(m-6)^2(m+11)^2,\\
y(P_3) &= 27440\,m(m-6)(m-9)(m-11)(m+1)(m+99)\\
&\qquad\cdot(2m-33)(m+9)^2(m+11)^2.
\end{aligned}$$

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 $x(P_2) = (14m)^4(\tau+\alpha)(\alpha\tau-1)^2(\tau-\alpha)$. So P_1 is the point that every curve of the model carries, the image of the point $(0,1)$ of $y^2=(\xi x+1)(1-x/\xi)(\zeta x+1)$ [15, §6.7] (the point P of [9, §4]), and P_2 is the point 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 $\alpha^2+1=2\cdot 5^2$: one has $x(P_3) = (14m)^2B_+B_-\,(m+1)(m+9)(m+11)(m+99)$, which involves the linear factors $m+9$ of $14mB_+$ and $m+11$ of $14mB_-$.

Proposition 2.3. $\operatorname{rank} X(\mathbb{Q}(m)) = 3$*, 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 $b = 87707648/625$. For a curve $y^2=x(x-e_2)(x-e_3)$ with rational e_2, e_3 let

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

with the usual values at the points of order 2; it is the 2-descent homomorphism, with kernel $2E(\mathbb{Q})$ [39, Proposition X.1.4]. Here $e_2=-a^2$, $e_3=-b^2$, and in squarefree representatives

$$\begin{aligned}
\kappa(P_1) &= (-1,\ 5\cdot 7\cdot 37\cdot 79), & \kappa(P_2) &= (-2\cdot 3\cdot 19\cdot 229,\ 3\cdot 79\cdot 229),\\
\kappa(P_3) &= (-2\cdot 3\cdot 19,\ 3\cdot 7\cdot 37), & \kappa(-a^2,0) &= (-1,\ 5\cdot 7\cdot 37\cdot 79\cdot 20233),\\
\kappa(0,0) &= (1,1), & \kappa(ab, ab(a+b)) &= (3\cdot 19\cdot 23\cdot 41\cdot 229,\ 3\cdot 5\cdot 37\cdot 41\cdot 79\cdot 229).
\end{aligned}$$

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 Mazur's theorem [29] a larger torsion subgroup would contain a point of order 8, which would need ab or $-ab$ to be a square [33, Main

Theorem 1], and ab has squarefree part $3\cdot 19\cdot 23\cdot 41\cdot 229$ (the first entry of $\kappa(ab, ab(a+b))$) while $-ab<0$. So κ maps the torsion subgroup onto $\langle \kappa(-a^2,0), \kappa(ab, ab(a+b))\rangle$. Suppose that $\sum n_iP_i$ 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 $\sum n_iP_i$ gives a relation among the five vectors. So the specialized points, and hence P_1, P_2, P_3, are independent (specialization at a smooth fiber is a homomorphism).

Upper bound. In [12, §2], Dujella and Peral proved that their curve over $\mathbb{Q}(t)$ with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ has rank exactly 4, with an earlier form of the criterion of Gusić and Tadić. We use [21, 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. The proof uses that the group of points of the curve over $\mathbb{Q}(m)$ is finitely generated [21, §1], which holds here by the theorem of Lang and Néron [26]. 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, which is 7^4 for a^2b^2 and $2^4\cdot 5^2\cdot 7^4$ for the other two products. At $m=14/3$ the eleven factors $m-99$, $m+1$, $m-11$, $m+9$, $m+99$, $m-1$, $m+11$, $m-9$, m, m^2-99, m^4-2m^2+9801 have squarefree parts $-3\cdot 283$, $3\cdot 17$, $-3\cdot 19$, $3\cdot 41$, $3\cdot 311$, $3\cdot 11$, $3\cdot 47$, $-3\cdot 13$, $2\cdot 3\cdot 7$, $-5\cdot 139$, $73\cdot 11353$. 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` [2]), so its rank is at most 3; hence $\operatorname{rank} X(\mathbb{Q}(m))\le 3$. □

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. Lemma 3.2 gives points on three twists, 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. 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 [16, §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 0.

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

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

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; a point $(x,y)\in Y^q(K)$, for a field $K\supseteq\mathbb{Q}(n)$ containing a square root $\sqrt{q}$ of q, 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 $y'^2 = x'(x'^2 + s^4 S(1/s)x' + s^8 w(1/s)^2)$ 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 [30, Table (IV.3.1)]. A relatively minimal elliptic surface over $\mathbb{P}^1$ with a section and Euler number 24 is a K3 surface [30, (III.4.2)–(III.4.6)]. □

The twists we use were found with averages of traces of Frobenius, a heuristic guide to the rank: the average of a twist Y^q is the plain average of $-A_p(Y^q)$ over the primes $300 < p < 3000$, with A_p as in Section 1. We computed it for the twists of Y by the linear polynomials in n of Appendix A and by their products with n. Apart from Y and Y^n, whose averages are 1.00 and 1.99, only three of these twists have averages above 0.45, all three close to 1: the twists by q_2, by nq_1 and by $n(4n+45)$, where

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

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* $\mathbb{Q}(n)$*:*

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

and

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

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

$$x_4^2 + q_2 S x_4 + q_2^2 w^2 = 9604\,(n-1)(n-81)(n-36)^2(n-121)^2(2n+243)^2N^2,$$
$$x_5^2 + nq_1 S x_5 + n^2 q_1^2 w^2 = 9604\,(n-9801)(n-121)(n-81)^2(3n+242)^2(4n-1089)^2N^2,$$
$$x_6^2 + q_{12} S x_6 + q_{12}^2 w^2 = 60025\,(n-9801)(n-1)(n-99)^2(n-121)^2(2n+243)^2N^2,$$

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 [28]), 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 $\lambda_1(u^2 - 15m^2 - 1210z^2) + \lambda_2(v^2 - 10m^2 - 1215z^2)$ consists of diagonal quadrics with determinant $25\lambda_1\lambda_2(3\lambda_1 + 2\lambda_2)(242\lambda_1 + 243\lambda_2)$, which has four distinct roots in $\mathbb{P}^1$. So the binary quartic that [4, §2] attaches to the pair of quadrics has nonzero discriminant, and by [4, Theorem 2.8(ii)] the base locus $\overline{C}$ is a smooth curve of genus one. (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 $\eta^2 = g(k)$. The discriminant of g is $2^{16} \cdot 3^{12} \cdot 5^2 \cdot 7^4 \cdot 11^4 \neq 0$, and its leading coefficient is the square 49, so this curve has rational points at infinity and is isomorphic over $\mathbb{Q}$ to its Jacobian. The invariants of g in the sense of [3, §2] are $I(g) = 6605776$ and $J(g) = 18071642752$. By [4, Theorem 2.8(iii)] the Jacobian is $y^2 = x^3 - 27c_4x - 54c_6$ with $c_4 = 2^4 I(g)$ and $c_6 = 2^5 J(g)$, and the substitution $(x, y) \mapsto (4x, 8y)$ turns this into $y^2 = x^3 - 27I(g)x - 27J(g)$, with minimal model E_C. On E_C,

$$3 \cdot (-322, 726) = \Big(-\frac{1901193922}{2521^2},\ \frac{31980410728794}{2521^3}\Big)$$

is not 2521-integral, whereas a torsion point of an integral Weierstrass equation has p-integral coordinates at every odd prime p [39, Theorem VII.3.4]; so $(-322, 726)$ has infinite order. The curve E_C has full rational 2-torsion and a 2-Selmer group of dimension 3 (computed with `mwrank` [2]), so its rank is at most 1, hence 1. 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,

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

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. Proposition 5.1 proves their independence directly.

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, and the six homomorphisms, evaluated at the six points, give a matrix that is invertible over $\mathbb{F}_3$.

Let $c_0 = (m_0, u_0, v_0) = (7401/2399,\ 88235/2399,\ 86835/2399) \in C(\mathbb{Q})$, a point found by a search of the points of $C(\mathbb{Q})$ of small height (Appendix A). The fiber X_{m_0} is smooth, all coordinates of the P_i are regular at c_0 (their denominators are products of powers of 5, m, u and v), and 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. So it suffices 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

$$\begin{aligned}
x(R_1) &= -9134182662998624112839888896/625,\\
x(R_2) &= -204090470295796923788895000,\\
x(R_3) &= -19944153128696423007969280,\\
x(R_4) &= -80466963140208120656325184314880/5755201,\\
x(R_5) &= 68045531169574069706104995374489 60/6086089,\\
x(R_6) &= -22494166745513310915537265584880 0/6355441.
\end{aligned}$$

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 [29] its order is 8 or 16, prime to 3, so it lies in $3E_0(\mathbb{Q})$. For a prime p 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, $P \mapsto (\#\widetilde{E}_0(\mathbb{F}_p)/3)\,\widetilde{P}$ 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

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

We computed M in PARI by reducing the R_i modulo p (the denominators of the $x(R_i)$ are prime to the six primes), multiplying them by $\#\widetilde{E}_0(\mathbb{F}_p)/3$ and comparing the results with the points of order 3 of $\widetilde{E}_0(\mathbb{F}_p)$, which have x-coordinate 9, 11, 40, 75, 79 and 4 at $p = 23$, 37, 53, 83, 89 and 113. Up to the signs of its rows and columns, which change only the sign of $\det M$, the matrix M is determined by the printed $x(R_i)$. 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. So $R_1, \dots, R_6$ 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. As $\operatorname{rank} X(\mathbb{Q}(m)) = 3$ (Proposition 2.3) and $\operatorname{rank} X(\mathbb{Q}(C)) \geq 6$ (Proposition 5.1), the ranks of the three twists add up to at least 3, so it suffices to show that each of them has rank at most 1 over $\mathbb{Q}(m)$: then each has rank exactly 1, and $\operatorname{rank} X(\mathbb{Q}(C)) = 6$.

We apply [21, Theorem 1.1] as in Proposition 2.3 to X^q, with $(e_1, e_2, e_3) = (0, -qa^2, -qb^2)$, for $q = q_1, q_2, q_{12} \in \mathbb{Z}[m]$; 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 2.3 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. For X^{q_1} we take $m = 14/3$, where the eleven factors have the squarefree parts listed in Proposition 2.3 and $3m^2 + 242$ has squarefree part $2 \cdot 3 \cdot 461$. For X^{q_2} and $X^{q_{12}}$ we take $m = 50/3$, where the eleven factors, in the same order, have squarefree parts $-3 \cdot 13 \cdot 19$, $3 \cdot 53$, $3 \cdot 17$, $3 \cdot 7 \cdot 11$, $3 \cdot 347$, $3 \cdot 47$, $3 \cdot 83$, $3 \cdot 23$, $2 \cdot 3$, 1609 and $113 \cdot 241 \cdot 257$, and those of $2m^2 + 243$ and $3m^2 + 242$ are 7187 and $2 \cdot 3 \cdot 1613$. In each case 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 [21, Theorem 1.1]. The fibers of X^{q_1} at $14/3$ and 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` [2]); as the 2-torsion accounts for 2 of these dimensions, their ranks are at most 1, and that theorem gives $\operatorname{rank} X^q(\mathbb{Q}(m)) \le 1$.

Finally, $X(\mathbb{Q}(C))$ is finitely generated [26], 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 6.2). The torsion of the fibers is controlled by the following criterion, whose proof follows that of [33, Main Theorem 1].

Lemma 6.1. *Let $a, b \in \mathbb{Q}$ with $ab(a^2 - b^2) \ne 0$. 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 [29] 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 Proposition 2.3 (with $e_1 = 0$) has first component x and kills $2E_{a,b}(\mathbb{Q})$. At $(-a^2, 0)$ and $(-b^2, 0)$ its first component is $-a^2$ or $-b^2$, which is negative and so not a square, so these points have no rational halves. 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 $-ab$, and a half of such a point exists only if this component is a square. So $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ requires ab or $-ab$ to be a square. □

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 $m(c) \in \{0, \pm 1, \pm 9, \pm 11, \pm 99\}$, and of these values only ± 1 and ± 99 occur on C, at the sixteen points listed ($m(c) = \infty$ does not occur, by Lemma 4.1).

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 a nonconstant function on C, $X/\mathbb{Q}(C)$ is not isotrivial, and its $\mathbb{Q}(C)/\mathbb{Q}$-trace is zero. Silverman's specialization theorem [38, Theorem C] says that for a family of abelian varieties over a smooth projective curve, all defined over a number field, whose generic fiber has trace zero, specialization is injective at all but finitely many rational points of the curve with smooth fiber. We apply it to the Kodaira–Néron model of X over $\overline{C}$, whose sections are the points of $X(\mathbb{Q}(C))$ and whose fiber at c is $X_{m(c)}$ when that curve is smooth. So

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, $\operatorname{rank} X_{m(c)}(\mathbb{Q}) \geq 6$ 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 6.1, a larger torsion subgroup requires $ab(m(c))$ or $-ab(m(c))$ to be a nonzero square. On $\overline{C}$ the function

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

has 32 simple zeros, the four points above each of its eight rational roots, and poles of the even order 8 at the four points above $m = \infty$. Neither these roots nor ∞ is a branch point of $m\colon \overline{C} \to \mathbb{P}^1$, whose branch points are the roots of $(3m^2+242)(2m^2+243)$. So each of the double covers $r^2 = \pm ab$ of $\overline{C}$ is branched at exactly 32 points and has genus 17, by the Riemann–Hurwitz formula. By Faltings' theorem [19, Satz 7] each has finitely many rational points, so $\pm ab(m(c))$ is a square for only finitely many $c \in C(\mathbb{Q})$. □

We have not determined the finite set of points $c \in C(\mathbb{Q})$ at which the specialization map is not injective or the torsion subgroup is larger than $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$: the constants in Silverman's theorem can be computed in principle but are too large to be practical [21, §1], and Faltings' theorem is not effective. At c_0 the six points stay independent (Proposition 5.1) and the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$: since $13 \parallel a_0b_0$ and $-a_0b_0 < 0$, neither a_0b_0 nor $-a_0b_0$ is a square (Lemma 6.1). The rank of $E_{a_0,b_0}(\mathbb{Q})$ is exactly 6: `mwrank` [2] gives this curve 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.

The computation at c_0 carries over, by congruences, to an infinite set of rational points of C.

Proposition 6.2. *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 $m \pm 1$, $m \pm 9$, $m \pm 11$, $m \pm 99$ of $ab = -49(m^2-1)(m^2-81)(m^2-121)(m^2-9801)$ are 13-adic units except $m-99$, since $m_0 \equiv 8 \pmod{13}$, and $\operatorname{ord}_{13}(m_0 - 99) = 1$, since $m_0 - 99 = -2^2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 59/2399$. If $\operatorname{ord}_{13}(m-m_0) \geq 2$, 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 $ab(m) \neq 0$, 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. So X_m is an elliptic curve, the model $y^2 = x(x+a(m)^2)(x+b(m)^2)$ has good reduction at p, and its reduction is that of X_{m_0}. By the first part and Lemma 6.1, $X_m(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

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 $y(P_4) = y_4 v/q_2^2$, $y(P_5) = y_5 u/(m^3 q_1^2)$ and $y(P_6) = y_6 uv/(5q_{12}^2)$, 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. So for $c \in \mathcal{S}$ the points

$P_i(c)$ 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 $\nu = 2399^4/(2^4 \cdot 3^2 \cdot 5^2 \cdot 7^3)$ 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 $\det M \not\equiv 0 \pmod 3$, 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 $\overline{C}$. By Lemma 4.1(b), $\overline{C}$ is then isomorphic to E_C, so $\overline{C}(\mathbb{Q})$ 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 $\operatorname{ord}_{13}(m - m_0) \geq 2$, 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 $k \geq 1$, say for $k_1 < k_2 < \cdots$. Then the points $(k_j - k_1)c'$, $j \geq 2$, 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 6.2 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 $\overline{C}$; so each value is taken at most 192 times, and infinitely many j-invariants occur. □

Remark 6.3. Here, as in [35, §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; so the height of X_m lies between two positive constant multiples of $\max(|x_0|, |x_1|)^{48}$. Then [32, Ch. III, Théorème 4 and Corollaire 2], applied to the function m on $\overline{C}$, whose Jacobian has rank one, together with the bound 192 gives $(\log H)^{1/2+o(1)}$ 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 forms of degrees 4 and 6 in its parameter W and the bound 96 proved there give $(\log H)^{1+o(1)}$.

7. Other bases for X

We compare C with other bases for X, none of which is needed for Theorem 1.1: over a conic through Dujella and Peral's curve of rank 9, X has rank at least 4 (Proposition 7.1), and over a curve of genus one that comes from a symmetry of their model, it has rank exactly 5 (Proposition 7.2).

The curve C is the fiber product over the m-line of the conics $u^2 = 5(3m^2 + 242)$ and $v^2 = 5(2m^2 + 243)$, which the involution $m \mapsto 99/m$ of the family (the involution $n \mapsto 9801/n$ of Lemma 3.1(c)) exchanges up to squares. Over each conic alone two of the twists of Section 3 stay nontrivial and one becomes trivial.

Proposition 7.1. *Let $D\colon u^2 = 5(3m^2 + 242)$, parametrized by $m = (k^2 - 70k + 15)/(k^2 - 15)$, $u = -5(7k^2 - 6k + 105)/(k^2 - 15)$.*

(a) *The points* P_1, P_2, P_3, P_5 *lie in* $X(\mathbb{Q}(D)) = X(\mathbb{Q}(k))$ *and are independent, so* X *over* $\mathbb{Q}(k)$ *has rank at least* 4.

(b) *Its fiber at* $k = 25/11$ *is the fiber of* X *at* $m = 1681/119$*, the curve of rank* 9 *of Dujella and Peral* [15, §7.2] *at* $t = 900/781$*, with minimal model*

$$y^2 + xy = x^3 - 1443705842368492991301675445569878391286260\,x + 5185245341269541163221532255116623986091375865258779782416196 00.$$

Proof. (a) P_5 involves only m and $\sqrt{nq_1} = mu$, which lie in $\mathbb{Q}(k)$. At $k_0 = 35/41$ one has $(m, u) = (7401/2399,\ 88235/2399)$, the first two coordinates of c_0, so the four points specialize to four of the six independent points of Proposition 5.1. (b) $m(25/11) = 1681/119 = (t+1)/(t-1)$ at $t = 900/781$, and the minimal model is computed from (1.2); it is the model printed in [15, §7.2]. □

In the coordinate t of Lemma 2.1, D is the conic $u'^2 = 1225t^2 - 2390t + 1225$, with $u' = u(t-1)$, and at $t = 900/781$ one has $1225t^2 - 2390t + 1225 = (7715/781)^2$. So Dujella and Peral's curve of rank 9 is a fiber of a family of rank at least 4 over $\mathbb{Q}(k)$.

Another base of genus one comes from a symmetry of the model. The map $(\alpha, \tau) \mapsto (\alpha, 1/\tau)$ preserves (2.1) up to $x \mapsto \tau^4 x$ and carries $\alpha^2\tau^2 + 2\alpha^2 + 1$ to $(2\alpha^2\tau^2 + \alpha^2 + \tau^2)/\tau^2$, so it 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 $\tau = (99 - m^2)/(14m)$,

$$2\alpha^2\tau^2 + \alpha^2 + \tau^2 = 99\tau^2 + 49 = h(m)/(14m)^2, \qquad h(m) = 99m^4 - 9998m^2 + 970299.$$

Let $G\colon \eta^2 = h(m)$. The twist of Y by h, a quadratic polynomial in n, is the one with average 1.93 in the search described in the introduction.

Proposition 7.2. *(a)* G *is a curve of genus one with the rational point* $(m, \eta) = (57, 31836)$*; its Jacobian is* $y^2 = x^3 + x^2 - 26097400x + 38851416548$*, of conductor* 683760*, with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *and rank* 2.

(b) The quadratic twist $X^h\colon y^2 = x(x + ha^2)(x + hb^2)$ *has rank* 2 *over* $\mathbb{Q}(m)$*, and* $\operatorname{rank} X(\mathbb{Q}(G)) = 5$.

Proof. (a) h is squarefree of degree 4 (its discriminant is $2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^8 \cdot 11^4 \cdot 37^2$) and $h(57) = 31836^2$; the Jacobian is computed from the invariants of h as in Lemma 4.1. With `mwrank` [2] one finds a 2-Selmer group of dimension 4 (with full rational 2-torsion), so the rank is at most 2. The points $(-5194, 185220)$ and $(-4249, 270270)$ are independent, so the rank is 2. Indeed, the cubic has the roots -5734, 1666 and 4067, and the 2-descent map $P \mapsto (x(P) + 5734,\ x(P) - 1666)$ of Proposition 2.3 sends the two points to $(3 \cdot 5,\ -5 \cdot 7)$ and $(3 \cdot 5 \cdot 11,\ -5 \cdot 7)$; it sends the generators $(-784, 242550)$ and $(1666, 0)$ of the torsion subgroup to $(2 \cdot 11,\ -2)$ and $(2 \cdot 37,\ -2 \cdot 37)$. These four vectors are independent: 37 occurs only in the last, then 2 only in the third and 11 only in the second, and the first is nontrivial.

(b) Since $\mathbb{Q}(G) = \mathbb{Q}(m)(\sqrt{h})$, $\operatorname{rank} X(\mathbb{Q}(G)) = \operatorname{rank} X(\mathbb{Q}(m)) + \operatorname{rank} X^h(\mathbb{Q}(m)) = 3 + \operatorname{rank} X^h(\mathbb{Q}(m))$ (Proposition 2.3). *Upper bound.* For X^h, $(e_1, e_2, e_3) = (0, -ha^2, -hb^2)$; the nonconstant squarefree divisors in $\mathbb{Z}[m]$ of $h^2a^2b^2$, $h^2a^2(a^2 - b^2)$ and $-h^2b^2(a^2 - b^2)$ are now built from the factors of Proposition 2.3 and h. At $m = -80/3$ these twelve factors have squarefree parts $-3 \cdot 13 \cdot 29$, $-3 \cdot 7 \cdot 11$, $-3 \cdot 113$, $-3 \cdot 53$, $3 \cdot 7 \cdot 31$, $-3 \cdot 83$, $-3 \cdot 47$, $-3 \cdot 107$, $-3 \cdot 5$, $7 \cdot 787$, $593 \cdot 1433$, $3 \cdot 1291 \cdot 2083$. With -1, 2, 5, 7 they are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so no such divisor takes a square value at $-80/3$. The fiber of X^h at $-80/3$ has full rational 2-torsion and a 2-Selmer group of dimension 4, so its rank is at most 2, and by [21, Theorem 1.1] $\operatorname{rank} X^h(\mathbb{Q}(m)) \le 2$. *Lower bound.* The substitution $m \mapsto m' = (\eta - 98m)/(99 - m^2)$ satisfies

$\tau(m') = 1/\tau(m)$. Put $\delta = (99 - m^2)/(14m')$, so that $a(m') = a(m)/\delta^2$ and $b(m') = b(m)/\delta^2$, and write $x(m')$ and $y(m')$ for the coordinates x and y with m replaced by m'. Then the map $(x, y) \mapsto (\delta^4 x(m'), \delta^6 y(m'))$ carries points of X over $\mathbb{Q}(m')$ to points of X over $\mathbb{Q}(G)$. Let P_2' and P_3' be the images of P_2 and P_3. At $m = 291/53$, $\eta = 2447004/2809$, scaling x by $(7890481/7056)^2$ takes the fiber to $E = E_{379291648,\,212565977}$, with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ by Lemma 6.1 ($43 \parallel ab$ and $-ab < 0$), and takes $P_1, P_2, P_3, P_2', P_3'$ to points with x-coordinates

$$-85985831567294464, \quad -58444996670344024, \quad -2248161523739262976/49,$$
$$-62331445860559616, \quad -48899358183829504.$$

We use the primes $p = 37, 41, 61, 107, 113$, where $\#\widetilde{E}(\mathbb{F}_p) = 48, 48, 72, 96, 120$; at $p = 61$ the group is $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with cyclic 3-primary part. Computed as in Proposition 5.1, the images of these points at the j-th of these primes in $\widetilde{E}(\mathbb{F}_p)/3\widetilde{E}(\mathbb{F}_p) \cong \mathbb{Z}/3\mathbb{Z}$ are the entries of the j-th of the rows

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

of a matrix of rank 5 over $\mathbb{F}_3$, each row defined up to sign by the choice of generator. So the five points are independent, and $\operatorname{rank} X(\mathbb{Q}(G)) \geq 5$. The upper bound gives $\operatorname{rank} X(\mathbb{Q}(G)) \leq 5$, so the five independent points $P_1, P_2, P_3, P_2', P_3'$ span a subgroup of finite index, and the image P_1' of P_1 is linearly dependent on them. □

The fiber at $m = 291/53$, isomorphic to $E_{379291648,\,212565977}$, has rank 6, one more than $\operatorname{rank} X(\mathbb{Q}(G))$, and its Tate–Shafarevich group has no element of order 2. Indeed, its 2-Selmer group has dimension 8 (computed with `mwrank`), and its points with the x-coordinates of P_1, P_2, P_3, P_3' listed above and with x-coordinates 585506734092845056 and 109341229015218525384601 6/17732521 have images under the map κ of Proposition 2.3 which, with those of the torsion, span a space of dimension 8. This fiber shows what C adds: over G the rank 6 occurs at single fibers such as this one, whereas over C it is the rank of $X(\mathbb{Q}(C))$ (Theorem 1.2(b)).

Since G has the rational point $(57, 31836)$ and its Jacobian has rank 2, the set $G(\mathbb{Q})$ is infinite. Silverman's theorem and the argument of Section 6, now with double covers $r^2 = \pm ab$ of G of genus 9, then give infinitely many curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank at least 5 from $G(\mathbb{Q})$; this recovers the bound credited to Eroshkin in [6]. Over G one twist of rank 2 becomes trivial, whereas over C three twists of rank 1 do (Proposition 5.2).

The third twist found by the search of Section 1, by $n(4n + 45)$, gives over $\mathbb{Q}(m)$ the twist of X by $4m^2 + 45$, which has rank 1, but 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 $\mathbb{Q}(m)$. So 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 (by the Riemann–Hurwitz formula) on which all three become squares, which has only finitely many rational points by Faltings' theorem. These ranks follow as in Proposition 5.2. 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 has infinite order since its specialization at $m = 42$ does. The upper bounds come from the criterion of Gusić and Tadić at $m = 42$ for the twist by $4m^2 + 45$, at $m = -58/3$ for the twists by $(4m^2 + 45)q_1$ and $(4m^2 + 45)q_2$, and at $m = -46/7$ for the twist by $(4m^2 + 45)q_{12}$, where the fibers have 2-Selmer groups of dimensions 3, 2, 2 and 2. At $m = 42$ the eleven factors of Proposition 2.3, in the same order, have squarefree parts $-3 \cdot 19$, 43, 31, $3 \cdot 17$, $3 \cdot 47$, 41, 53, $3 \cdot 11$, $2 \cdot 3 \cdot 7$, $5 \cdot 37$ and 346441, and $4m^2 + 45$ has squarefree part $3 \cdot 263$. At $m = -58/3$ they have squarefree parts $-3 \cdot 5 \cdot 71$, $-3 \cdot 5 \cdot 11$, $-3 \cdot 7 \cdot 13$, $-3 \cdot 31$, $3 \cdot 239$, $-3 \cdot 61$, -3, $-3 \cdot 5 \cdot 17$, $-2 \cdot 3 \cdot 29$, 2473 and $97 \cdot 4969$, and those of $4m^2 + 45$, $3m^2 + 242$ and

$2m^2+243$ are $83\cdot167$, $2\cdot3\cdot5\cdot409$ and $5\cdot1783$. At $m=-46/7$ they are $-7\cdot739$, $-3\cdot7\cdot13$, $-3\cdot7\cdot41$, $7\cdot17$, $7\cdot647$, $-7\cdot53$, $7\cdot31$, $-7\cdot109$, $-2\cdot7\cdot23$, $-5\cdot547$ and $1153\cdot24113$, and those of $4m^2+45$, $3m^2+242$ and $2m^2+243$ are $47\cdot227$, $2\cdot9103$ and 16139. In each case these classes and -1, 2, 5, 7 are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times2}$, and the contents of the three products again involve only the primes 2, 5 and 7, so no nonconstant squarefree divisor of the three products takes a square value.

8. A second family

We give a second proof of Theorem 1.1, independent of the first, with a family over a curve of genus one and rank two. Since the base has rank two rather than one, the family gives $(\log H)^{1+o(1)}$ curves of height at most H, against $(\log H)^{1/2+o(1)}$ for C (Remark 6.3).

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 $\mathbb{Q}(s_1)$ with $W=s_1^2$. Over $\mathbb{Q}(s_1)$, F is the curve $E_{(s_1-1)(s_1-\lambda),\,(s_1+1)(s_1+\lambda)}$, and since $A_+B_+=\alpha^3(s_1+1)(s_1+\lambda)$ and $A_-B_-=-\alpha^3(s_1-1)(s_1-\lambda)$ at $(\alpha,\tau)=(33/19,\,33s_1/19)$, it 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 [16, §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

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

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, $\bigl(361/1089,(161/1089)^2\bigr)$. 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, and 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 put $q_A=29(W-\beta)$, $q_B=-29\beta(W-\gamma)$ 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

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

satisfy

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

with $f_2=W^2-\frac{648517}{1185921}W+\frac{3467044}{1291467969}$ 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. Put $Q_4=\iota(Q_2)$ 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

$$y^2=x^3+x^2-7927479575830823114160\,x+27165830539902981904087537 9804308,$$

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` [2]), so its rank is at most 2. Its points (50796866898, 198589582959768) and (389256165869/4, 164296202311285275/8) are independent, so the rank is 2: the cubic has the roots -102809641014, 51068871386 and 51740769627, and the 2-descent map $P\mapsto(x(P)+102809641014,\ x(P)-51068871386)$ of Proposition 2.3 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. As a check, twice the point (50796866898, 198589582959768)

has x-coordinate with denominator $7^2 \cdot 13^2$. 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) The field $\mathbb{Q}(G_2)$ is $\mathbb{Q}(W)(\sqrt{W}, \sqrt{q_A}, \sqrt{q_B})$, and W, q_A, q_B are independent modulo squares in $\mathbb{Q}(W)$, since their divisors modulo 2 are supported on $\{0, \infty\}$, $\{\beta, \infty\}$ and $\{\gamma, \infty\}$. So $\mathbb{Q}(G_2)/\mathbb{Q}(W)$ is Galois with group $(\mathbb{Z}/2\mathbb{Z})^3$, and $F(\mathbb{Q}(G_2)) \otimes \mathbb{Q}$ is the sum of the eigenspaces of the eight characters. The eigenspace of the character attached to a square class q is $F^q(\mathbb{Q}(W)) \otimes \mathbb{Q}$. The points lie in the eigenspaces of the four distinct classes 1, q_A, Wq_B and $q_Aq_B \equiv q_H$. So they are independent as soon as Q_1 and Q_6 have infinite order and Q_2, Q_3 are independent in $F^{q_A}(\mathbb{Q}(W))$ (then so are $Q_4 = \iota(Q_2)$ and $Q_5 = \iota(Q_3)$). We specialize at $W = 4$, where F, F^{q_A} and F^{q_H} are smooth, and write $F_4^{q_A}$ and $F_4^{q_H}$ for their fibers there. The curve $F_4^{q_A}$ has torsion subgroup $(\mathbb{Z}/2\mathbb{Z})^2$, since its reductions at the good primes 7 and 13 have 8 and 12 points and its cubic has the three rational roots 0, $e_2 = -881981589323167/156267624249$ and $e_3 = -451693636824103/1406408618241$. With $\kappa(P) = (x(P), x(P) - e_2)$ as in Proposition 2.3,

$$\kappa(Q_2) = (3 \cdot 23 \cdot 79 \cdot 2539,\ 3 \cdot 29 \cdot 2539), \qquad \kappa(Q_3) = (3 \cdot 2017 \cdot 2339,\ 3 \cdot 29 \cdot 2017),$$
$$\kappa(0,0) = (1,\ 29 \cdot 2017 \cdot 2339), \qquad \kappa(e_2, 0) = (-29 \cdot 2017 \cdot 2339,\ 29 \cdot 53 \cdot 89),$$

which are independent (23 and 53 each occur once, and then 3); so, as in Proposition 2.3, $Q_2(4)$ and $Q_3(4)$ are independent modulo torsion, and so are Q_2 and Q_3. The point $Q_1(4)$, with

$$x(Q_1(4)) = 21283118169769/466219936809,$$

is not 19-integral on the integral model $y^2 = x^3 + 1089^2Ux^2 + 1089^4V^2x$ (at $W = 4$), where its x-coordinate has denominator $3^2 \cdot 11^2 \cdot 19^2$; so it has infinite order [39, Theorem VII.3.4]. Likewise $Q_6(4)$, with

$$x(Q_6(4)) = 1123001473244171824850560 0/974374006659413003857521,$$

is not 7-integral on the integral model of $F_4^{q_H}$ obtained by scaling x by 190933281^2.

(c) The discriminant of (8.1) is $16V^4(U^2 - 4V^2)$, and $U^2 - 4V^2 = 16(1 + \lambda)^2W(W + \lambda)^2$. At a rational point of G_2, $W = s_1^2$ with $s_1 = \frac{161}{1089}(\theta^2 + 29)/(\theta^2 - 29) \neq 0$, so the fiber is singular exactly when $W \in \{1, \lambda^2\}$, 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, so as in Section 6 Silverman's theorem [38, Theorem C] shows that specialization is injective at all but finitely many points of $G_2(\mathbb{Q})$, which is infinite by (a); there 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. Over $\mathbb{Q}(s_1)$, F is the curve $E_{(s_1-1)(s_1-\lambda),(s_1+1)(s_1+\lambda)}$, for which $ab = -V$. So, by Lemma 6.1, whose proof follows [33, Main Theorem 1], 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. So the double covers $r^2 = \pm V$ of G_2 are branched at exactly 16 points and have genus 9, by the Riemann–Hurwitz formula. By Faltings' theorem [19, 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

$$\begin{array}{ll} 499284308691438490000/9, & 22157579080153112175464742 00/19037652529, \\ 3395584751700492739215 36/3258025, & 29178558284632735735843 3632/113273449, \\ -4563185528671931392, & 33811997149872268185600 00/83521. \end{array}$$

The curve has torsion exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, since $83 \parallel ab$ and $-ab < 0$ (Lemma 6.1), and 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 of the rows

$$(1,1,1,1,1,2),\ (1,0,1,2,1,0),\ (0,2,2,0,0,0),\ (2,2,1,0,0,1),\ (2,1,0,1,1,1),\ (1,2,1,1,0,2)$$

of a matrix with determinant 2 modulo 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. So the six points are independent, as in Proposition 5.1. □

The curve $E_{460019200,\,11180308689}$ of (d) has rank 7, and its Tate–Shafarevich group has no element of order 2. Indeed, its 2-Selmer group has dimension 9 (computed with `mwrank`), and the points Q_1, Q_3, Q_5 of (d), together with its points with x-coordinates

$$\begin{array}{ll} -3478949377821720000, & -1520527880418835200, \\ -39841413054999928093920 00/32041, & 1805886560331729100 80/169, \end{array}$$

have images under the map κ of Proposition 2.3 which, with those of the torsion, span a space of dimension 9. The six points of (d) would not do here: with the torsion, their images under κ span a space of dimension 5 only, even though the six points are independent. This curve bears on the question, raised at the end of this section, whether rank 7 occurs infinitely often with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Remark 8.2. Without Faltings' theorem one still obtains infinitely many of these curves with torsion exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank at least 6, by a 3-adic analogue of the 13-adic condition of Proposition 6.2. At $\theta = 857/140$ one has $\mathrm{ord}_3(V(W)) = -1$. The same holds at every rational point of G_2 with $\mathrm{ord}_3(\theta - 857/140) \geq 6$, since $V(W)$ is a constant times a product of eight linear polynomials in θ with integer coefficients, divided by $(\theta^2 - 29)^4$, and each of these nine polynomials has 3-adic valuation at most 5 at $857/140$. So $\pm V(W)$ is not a square in $\mathbb{Q}_3$ at these points, and by the proof of (c) the torsion there is exactly $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since G_2 has a rational point and its Jacobian has positive rank, this 3-adic neighborhood of $\theta = 857/140$ contains infinitely many rational points of G_2: if P is a rational point of infinite order on the Jacobian and $N \geq 1$ is such that NP lies in the kernel of reduction modulo 3, a pro-3 group, then the translates of the point with $\theta = 857/140$ by $3^k NP$, for $k = 1, 2, \dots$, are distinct and tend to it 3-adically. By Silverman's theorem, as in the proof of (c), the rank is at least 6 at all but finitely many of them.

The case $\mathbb{Z}/6\mathbb{Z}$ of [7, Problem 2.6] remains open. We do not know whether rank 7 occurs infinitely often with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Appendix A. Computations

We used PARI/GP 2.17.3 [34] and SageMath 10.9 [37], which includes Cremona's `mwrank` [2]. The divisor tests of Gusić and Tadić were done in PARI and again with python-flint [20]. Apart from the one noted below, the upper bounds for ranks from 2-Selmer groups were computed with `mwrank` and again with PARI's `ellrank`, with the same results. The independence of the six points at c_0, proved in PARI with the matrix M of Proposition 5.1, was proved again in SageMath by a 2-descent, with the program listed under Proposition 5.1 in [25]. There the images under the map κ of Proposition 2.3 of $P_1(c_0), \dots, P_6(c_0)$ and of the two generators of the torsion of X_{m_0} span a space of dimension 6 only. The two relations come from two combinations of these points and of torsion points that lie in $2X_{m_0}(\mathbb{Q})$, and replacing two of the six points by halves of these combinations, that is, by points whose doubles are these combinations, gives points whose images, with those of the torsion, span a space of dimension 8. The proof of Theorem 1.1 needs no upper bound for a rank: its computational inputs are polynomial identities and factorizations (including the degree of j), the point $(-322, 726)$ of infinite order on E_C, and the valuations and the matrix M at c_0.

The point c_0, at $k = 35/41$ in the parameter of the proof of Lemma 4.1, came from a search of the points of $C(\mathbb{Q})$ of height at most 10^5 in k; its fiber is one of the two smooth fibers, up to isomorphism, found there, both of rank 6 [25]; for the other, the upper bound 6 was computed with `ellrank` only.

The averages of Section 1 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 $|s| \le 100$ (so no s is divisible by p). Apart from $r_0 = 0$ and $s = 1$, where the twists are Y and Y^n, exactly three averages exceed 0.45, those of the three twists named there. Among the eighteen twists by q and by nq with q one of $4n + 45$, q_1, q_2, $(4n+45)q_1$, $(4n+45)q_2$, $q_1q_2/25$, h, $(4n+45)h$ and q_1h, the twists by $q_1q_2/25$ and by h have averages 1.00 and 1.93, the three twists above reappear, and the other thirteen lie between -0.09 and 0.07.

The programs and their outputs are deposited in [25], and the Lean formalization in [24].

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 [25].

References

1. 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.

2. John E. Cremona, *Algorithms for Modular Elliptic Curves*, second ed., Cambridge University Press, Cambridge, 1997.
3. ———, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1–2, 71–87, doi:10.1006/jsco.1998.1004.
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 $= 9$*, https://web.math.pmf.unizg.hr/~duje/tors/z2z4.html (accessed October 15, 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. ———, *High-rank elliptic curves with given torsion group and some applications*, Banach Center Publ. **126** (2023), 9–26, doi:10.4064/bc126-1.
11. 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.
12. 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.
13. ———, *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.
14. ———, *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.
15. ———, *Construction of high rank elliptic curves*, J. Geom. Anal. **31** (2021), no. 7, 6698–6724, doi:10.1007/s12220-020-00373-7.
16. ———, *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.
17. Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007, Preprint, arXiv:0709.2908v1.
18. ———, *An elliptic K3 surface $X/\mathbb{Q}(t)$ with Mordell–Weil rank 17, I: Formulas for X and base changes of rank 18 and 19*, 2026, Preprint, arXiv:2608.25406v1.
19. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, doi:10.1007/BF01388432.
20. The FLINT team, *FLINT: Fast Library for Number Theory*, 2025, https://flintlib.org, version 3.3.1, with the Python interface python-flint 0.8.0.
21. 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.
22. 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.
23. 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.
24. ———, *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.23682552.
25. ———, *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.
26. 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.
27. 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.

28. The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, elliptic curve 9240.bf4 (accessed October 16, 2026).
29. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186, doi:10.1007/BF02684339.
30. Rick Miranda, *The Basic Theory of Elliptic Surfaces*, Dottorato di Ricerca in Matematica, ETS Editrice, Pisa, 1989.
31. 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.
32. 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.
33. Ken Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), no. 2, 101–123, doi:10.4064/aa-78-2-101-123.
34. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr/.
35. 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.
36. 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.
37. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026, https://www.sagemath.org.
38. 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.
39. ———, *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