INFINITELY MANY ELLIPTIC CURVES WITH TORSION $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ AND RANK AT LEAST FOUR

MANVIR JASWAL

Abstract. We show that there are infinitely many elliptic curves over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 4, one more than the largest rank previously known to occur infinitely often with this torsion. The universal elliptic curve with this torsion acquires four independent points over the function field of an explicit elliptic curve of rank one, and Silverman's specialisation theorem gives the family. Three of the points come from quadratic twists by polynomials that become squares on that curve, as in the rank-3 constructions of Dujella and Peral and of Dujella, Kazalicki and Peral. The fourth comes from the twist by the product of two of them; it is pulled back from a quadratic twist of a rational elliptic surface, of which the universal curve is a base change along a double cover of the line. The family is sparse, but it contradicts the prediction of Park, Poonen, Voight and Wood that only finitely many curves with this torsion have rank greater than 3.

1. Introduction

By Mazur's theorem [20], 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 [9, 10]. For each T the tables in [10] give lower bounds for the largest rank of an elliptic curve over $\mathbb{Q}(t)$ with torsion T and for the largest rank that occurs for infinitely many curves, $b_T = \limsup\{\operatorname{rank} E(\mathbb{Q}) : E(\mathbb{Q})_{\text{tors}} \cong T\}$ in the notation of [24, §8.3]. For $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ these lower bounds are 2 and 3, and the largest known rank of a single curve is 6 [9]. Theorem 1.1 below raises the second of these bounds to 4; it does not change the first, since our family is parametrised by a curve of genus one.

The bound $b_T \geq 3$ for $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ comes from families of curves of rank at least 3 parametrised by the rational points of elliptic curves of positive rank, constructed by Dujella and Peral [5, §6.6] (§5.5 of the arXiv version) and by Dujella, Kazalicki and Peral [4, §9]. Rank 2 over $\mathbb{Q}(t)$ is due to Dujella and Peral [5, 6], MacLeod [19, §5] and Dujella, Kazalicki and Peral [4, Theorem 2]. Families of rank at least 1 over $\mathbb{Q}(t)$ with this torsion were constructed earlier by Campbell, Kulesz, Lecacheux, Dujella and Rabarison, and by Woo [31]; Lecacheux used elliptic fibrations of the corresponding surfaces, and Woo quadratic sections of K3 surfaces (see [5, §1] and [4, §§1.2–1.3]). Theorem 1.1 below answers the case $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ of a question in Dujella's list of open problems [11, Problem 2.4], which asks whether there are infinitely many elliptic curves over $\mathbb{Q}$ with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (respectively $\mathbb{Z}/8\mathbb{Z}$) and rank at least 4.

Park, Poonen, Voight and Wood [24] proposed a heuristic which suggests that ranks of elliptic curves over $\mathbb{Q}$ are bounded. In their model a curve $y^2 = x^3 + a_4x + a_6$, with $a_4, a_6 \in \mathbb{Z}$ and no prime p such that $p^4 \mid a_4$ and $p^6 \mid a_6$, has height $H = \max(4|a_4|^3, 27a_6^2)$ [24, §5.1],

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 14J27, 11G35.

Key words and phrases. Elliptic curves, Mordell–Weil rank, torsion subgroup, specialisation, elliptic surfaces.

and it has rank at least r with probability $H^{-(r-1)/24+o(1)}$ for each fixed $r \geq 1$ [24, §1]. In [24, §8.3] they adapt it to families with prescribed torsion. If the number of curves with torsion T and height at most H is of order $H^{1/d}$, as Harron and Snowden [14] prove, the model suggests that $b_T \leq 1 + \lfloor 24/d \rfloor$. In the tables of Park, Poonen, Voight and Wood the rank bound is "an integer such that our model predicts that the family contains only finitely many elliptic curves of strictly higher rank" [24, §8.3]. For $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ one has $d = 12$, and their table lists the rank bound 3 next to the known lower bound 3. They observe that for each T the conjectured upper bound is at least as large as the proven lower bound. The bound for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is quoted in [6, §1], in a table in [7, §1] and in [4, §1]. Dujella, Kazalicki and Peral observed in [4, §11] that if the parity conjecture and this bound both hold, then only finitely many curves in their rank-3 families can have root number $+1$, since such a curve has even rank and hence rank at least 4. They computed root numbers in a rank-3 family with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, found the two signs about equally often, and suggested that the heuristic needs some adjustment for this torsion group; Dujella and Peral repeat this observation in [8, §5].

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

The result is unconditional. Under the parity conjecture, the observation of [4, §11] above already suggested it. Theorem 1.1 shows that $b_T \geq 4$ for $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, which contradicts the entry 3 for this torsion group in the table of [24, §8.3]. That entry rests on a count. There are of order $H^{1/12}$ curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and height at most H [14], against $H^{20/24}$ elliptic curves in all. Summing the probabilities above over these curves, as in the proof of [24, Theorem 7.3.3] but with this count in place of the total, gives an expected number $H^{(3-r)/24+o(1)}$ of such curves of rank at least r for $1 \leq r \leq 3$, and a bounded one for $r \geq 4$. So the model predicts only finitely many curves of rank at least 4 with this torsion. At rank 3 the expected number is $H^{o(1)}$ and the model is inconclusive: since $24/d = 2$ is an integer, rank 3 is a borderline case, and rank 4 lies strictly beyond it.

The family of Theorem 1.2 below is sparse. Its curves are parametrised by the rational points of an elliptic curve of rank one, so the number of isomorphism classes of its curves of height at most H is only of the order of $(\log H)^{1/2} = H^{o(1)}$ (Remark 6.2), against $H^{1/12}$ for all curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ [14]; this count is consistent with the model's $H^{o(1)}$ curves of rank at least 3, though not with its bounded number at rank at least 4. It is also a family of generic rank 4 (Proposition 5.3). Park, Poonen, Voight and Wood note that special families of elliptic curves may behave differently for arithmetic reasons, as special subvarieties can in the Batyrev–Manin conjectures [24, Remark 1.1.2], and that their model would have to be refined to predict the ranks in parametric families of high generic rank [24, Remark 1.1.3]. What fails is the table's prediction for the family of all curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In our case the universal curve is itself the base change of a rational elliptic surface along a double cover of the line (Section 2), and two of the four points constructed below, P_3 and P_4 of Proposition 4.2, are pull-backs of points on quadratic twists of that surface (Remark 7.1).

Theorem 1.1 follows from the more precise Theorem 1.2. Let

$$E\colon\ y^2 = f(x) := x(x-a)(x-b), \qquad a = (v+1)^3(3v-5), \quad b = 32(v-1)^3, \tag{1}$$

over $\mathbb{Q}(v)$. This is the universal curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, in the model of [4, §2] (see also [5]). Its fibre E_{v_0} at $v_0 \in \mathbb{Q}$ is an elliptic curve unless $v_0 \in \{-1, 1, 3, \frac{1}{3}, \frac{5}{3}\}$ (Section 2).

Let C be the $(\mathbb{Z}/2\mathbb{Z})^3$-cover of the v-line on which the polynomials

$$D_1 = 3v(7v-5), \qquad D_2 = 3(v-2)(7v-9), \qquad D_3 = 3v(v-2)$$

become squares (their choice is explained in "How the family was found" below). It is the affine curve

$$C\colon \quad r^2 = 10s^2 + 54, \qquad t^2 = 6s^2 + 10 \tag{2}$$

in the coordinates (s, r, t), with the map $v = 6/(3-s^2)$ to the v-line. The quadratic twists of E by D_1, D_2, D_3 and D_1D_2 have points over $\mathbb{Q}(v)$, which give four points $P_1, \dots, P_4$ of E over the function field $\mathbb{Q}(C)$ (Lemmas 3.1 and 4.1 and Proposition 4.2).

Theorem 1.2. *(a) The smooth projective model of C has genus one and infinitely many rational points; it is isomorphic over $\mathbb{Q}$ to the elliptic curve $E'\colon y^2 = x^3 + x^2 - 1720x + 16100$ (conductor 1680, $E'(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$), and $(-40, 150) \in E'(\mathbb{Q})$ has infinite order.*

(b) The four points $P_1, \dots, P_4 \in E(\mathbb{Q}(C))$ of Proposition 4.2 are linearly independent, so $\operatorname{rank} E(\mathbb{Q}(C)) \geq 4$.

(c) For every $c \in C(\mathbb{Q})$ other than the sixteen points $(\pm 1, \pm 8, \pm 4)$ and $(\pm 3, \pm 12, \pm 8)$, which lie over the singular fibres at $v = 3$ and $v = -1$, the specialisation $E_{v(c)}$ is an elliptic curve with $E_{v(c)}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and for all but finitely many $c \in C(\mathbb{Q})$ it has rank at least 4.

For example, $c_0 = (129, 408, 316) \in C(\mathbb{Q})$ gives $v = -1/2773$, and $E_{-1/2773}$ is a curve of rank 5 found by Dujella and Lecacheux in 2002 [12] (Example 6.1).

How the family was found. For a quadratic twist $E^D\colon Dy^2 = f(x)$ of (1) by $D \in \mathbb{Q}[v]$ and a prime $p \geq 5$, let $A_p(E^D) = \frac{1}{p}\sum_{z \in \mathbb{F}_p} a_p(E^D_z)$ be the average of the traces of Frobenius of the fibres modulo p. Here $a_p(E^D_z) = -\sum_{x \in \mathbb{F}_p}(\frac{D(z)f(x)}{p})$, a sum of Legendre symbols with the coefficients of f evaluated at z. At a smooth fibre it is the trace of Frobenius, and at the others it is defined by this sum. Nagao [22] conjectured that the sum $-\frac{1}{X}\sum_{5 \leq p \leq X} A_p(E^D)\log p$ tends to $\operatorname{rank} E^D(\mathbb{Q}(v))$ as $X \to \infty$, and Rosen and Silverman [25, Theorem 1.3] related this conjecture to Tate's conjecture for the surface E^D. To find twists of positive rank, we computed approximations to this limit, using the primes $5 \leq p \leq 1000$, for the twists by $k\ell_1\ell_2$, where k is a squarefree integer with $|k| \leq 60$ and $\ell_1, \ell_2 \in \mathbb{Z}[v]$ are distinct primitive linear polynomials with coefficients of absolute value at most 40, and also for the twists by $k\ell$ with ℓ one such polynomial.

If three polynomials in $\mathbb{Q}[v]$ are independent in $\mathbb{Q}(v)^\times/\mathbb{Q}(v)^{\times 2}$, the twists of E by them have positive rank, and the polynomials become squares on a curve of genus one, then E has three independent points over the function field of that curve: they lie in different eigenspaces of the Galois group $(\mathbb{Z}/2\mathbb{Z})^3$ (Proposition 5.1). MacLeod [19, §3] describes the method behind such constructions. For three general quadratic polynomials the $(\mathbb{Z}/2\mathbb{Z})^3$-cover of the v-line on which they become squares is branched over six points and has genus 5 by the Riemann–Hurwitz formula. Here D_3 shares its roots 0 and 2 with D_1 and D_2, so the cover is branched only over $\{0, \frac{5}{7}, 2, \frac{9}{7}\}$ and has genus one. It is the curve C of (2), where $v = 6/(3-s^2)$ parametrises the conic $w^2 = D_3(v)$.

We found this configuration as follows. The search above finds 43 twists with an approximation above 0.5, all between 0.86 and 1.00 and all by products $k\ell_1\ell_2$. The substitutions $v \mapsto 2-v$ and $v \mapsto (5v-3)/(3v-5)$ generate a group of six substitutions of v that leave E_v unchanged up to isomorphism (Section 2); with their images under these six substitutions,

the 43 twists give 54 twists by quadratic polynomials. Of the triples of these 54 polynomials, 216 have exactly four distinct roots in total, so that their cover has genus one, and up to the substitutions these triples form 46 classes. For a triple in each class we computed the same approximations, with the primes up to 10^4, for the twists by all seven nonempty products of its three polynomials. Only one class has a product of two or three of the polynomials close to 1: the class of D_1, D_2, D_3, where the twist by D_1D_2 gives 0.94. All other products lie between -0.08 and 0.05. The twist by D_1D_2 does have a point over $\mathbb{Q}(v)$, and so E has a fourth point over the same function field (Lemma 3.1 and Proposition 5.1). Only afterwards did we notice that D_3 and $D_1D_2/9$ (which gives the same twist as D_1D_2, since 9 is a square) are polynomials in $u = (v-1)^2$ (Remark 7.1). For the four twists of Section 3, by D_1, D_2, D_3 and $D_1D_2/9$, the weighted average $-\sum_p A_p(E^D)\log p/\sum_p \log p$ over the primes $5 \le p \le 3000$ is 0.968, 0.968, 0.969 and 0.998. Dividing by $\sum_p \log p$ rather than by X makes it a mean of the numbers $-A_p(E^D)$, with weights $\log p$; it has the same limit as Nagao's sum, and these primes up to 3000 already separate these twists from the controls: for $D = 1$ and for four polynomials taken at random (v^2+3, $2v^2-v+5$, $(v+4)(3v-2)$ and $5v+7$) it lies between -0.017 and 0.014. Like the approximations above, these averages are only a heuristic guide.

The nearest earlier constructions use two of the same three polynomials. The curve E over the conic $w^2 = D_3(v)$, with this parametrisation and the point P_3 (up to a point of order 2), is the first curve of rank one in the list of [4, §7], and E over the cover on which D_2 and D_3 are squares, with the points P_2 and P_3 (the latter up to a point of order 2), is the second Dujella–Peral curve of rank two [4, §8.2]. The first Dujella–Peral curve [4, §8.1] is E over the cover on which D_3 and $3v(5v-7)$ are squares, and the first of the rank-3 families of [4, §9] is E over the cover on which, in addition, D_2 is a square. The rank-3 family of [5, §6.6] is E over the cover on which D_1, D_3 and $v(5v-3)$ are squares, and these two families correspond under $v \mapsto 2-v$. Our curve C is the cover on which D_1, D_2 and D_3 are all squares: it adds the condition that D_1 be a square to the base of the second Dujella–Peral curve. Since D_1 is the image $D_2(2-v)$ of D_2 under $v \mapsto 2-v$, the product D_1D_2 is a polynomial in u, and the twist by it has a point over $\mathbb{Q}(v)$: this one further condition gives two independent points, P_1 and P_4. Remark 7.1 explains heuristically why this twist has a point: it is the pull-back of a twist of the rational elliptic surface of Section 2; that twist is a K3 surface, and by a count of Hodge classes a section of infinite order on such a twist is expected to cost one condition on the twisting polynomial, against three for the twist of E by a general squarefree polynomial of degree 4 in v.

Plan of the paper. Section 2 recalls the torsion of the universal curve and shows that it is a base change of a rational elliptic surface. Section 3 gives the four twists and their points. Section 4 shows that the twisting polynomials become squares on C and that the smooth projective model of C is an elliptic curve of positive rank. Section 5 proves that the four points are independent, using the 2-descent map at the fibre over c_0 to show that each has infinite order, and that $\operatorname{rank} E(\mathbb{Q}(C)) = 4$: $E(\mathbb{Q}(C)) \otimes \mathbb{Q}$ splits into eight eigenspaces, one for E and one for each of its twists by the seven nonempty products of D_1, D_2 and D_3, and a 2-descent at one fibre of each of these eight curves, chosen so that specialisation is injective there by the criterion of Gusić and Tadić [13], bounds its rank. Section 6 deduces Theorems 1.2 and 1.1, identifies the Dujella–Lecacheux curve in the family and estimates the number of its curves of bounded height. Section 7 discusses the origin of the fourth point, other torsion groups and parity, and Section 8 describes the computations.

2. The universal curve

Every smooth rational fibre of E has torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ (Lemma 2.1), which gives the torsion statement of Theorem 1.2(c). For E as in (1) one has $a-b=(v-3)^3(3v-1)$ and

$$\Delta(E)=16\,a^2b^2(a-b)^2=16\,(v+1)^6(3v-5)^2\cdot 2^{10}(v-1)^6\cdot(v-3)^6(3v-1)^2,$$

so for $v_0\in\mathbb{Q}$ the specialisation E_{v_0} is an elliptic curve unless $v_0\in\{-1,1,3,\frac{1}{3},\frac{5}{3}\}$. Writing $f(x)=x^3+Ax^2+Bx$ one has $A=-(a+b)=37-84v+102v^2-36v^3-3v^4$ and $B=ab=32(v-1)^3(v+1)^3(3v-5)$, as in [4, §2] and [5]. The j-invariant is

$$j(E)=\frac{(3v^2-6v+7)^3\,(3v^6-18v^5+345v^4-1260v^3+1605v^2-738v+127)^3}{4\,(v-3)^6(v-1)^6(v+1)^6(3v-5)^2(3v-1)^2},$$

a rational function of degree 24 in v.

Lemma 2.1. *(a) The points $(0,0)$, $(a,0)$, $(b,0)$ and*

$$T_3=\big(4(v^2-1)^2,\ 4(v-3)^2(v-1)^2(v+1)^2\big)$$

lie in $E(\mathbb{Q}(v))$; T_3 has order 3, so $E(\mathbb{Q}(v))\supseteq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

(b) For $v_0\in\mathbb{Q}\setminus\{-1,1,3,\frac{1}{3},\frac{5}{3}\}$, $E_{v_0}(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

(c) Every elliptic curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ is isomorphic over $\mathbb{Q}$ to E_{v_0} for some $v_0\in\mathbb{Q}$.

Proof. (a) One checks $f(4(v^2-1)^2)=16(v-3)^4(v-1)^4(v+1)^4$, and that $4(v^2-1)^2$ is a root of the 3-division polynomial $3x^4+4Ax^3+6Bx^2-B^2$ of E. So T_3 has order 3. (b) For such v_0 the curve E_{v_0} is smooth, the three points of order 2 remain distinct, and the specialisation of T_3 is an affine point P with $3P=O$. Hence $E_{v_0}(\mathbb{Q})$ contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, and $E_{v_0}(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ because no group in Mazur's list [20] properly contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. (c) This is the classical parametrisation of curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ (Kubert [17]; see [4, §2] and [5] for the model (1)): Kubert's curve with parameter $\alpha=(3v+1)/(v-1)$ (the parameter is called α in [19, §5]) is isomorphic to E_v over $\mathbb{Q}(v)$. Kubert's curve is $Y^2+(1-\gamma)XY-(\gamma+\gamma^2)Y=X^3-(\gamma+\gamma^2)X^2$ with $\gamma=(10-2\alpha)/(\alpha^2-9)$, and $\gamma=(v-1)(v-3)/(2(3v-1))$ at $\alpha=(3v+1)/(v-1)$. The substitution

$$x=(4-12v)^2X+8(v-1)(v+1)^2,$$
$$y=(4-12v)^3Y+(4-12v)^2(v^2-10v+5)X+8(v-3)(v-1)(v+1)^2(3v-1)$$

takes $y^2-x(x-a)(x-b)$ to $(4-12v)^6(Y^2+(1-\gamma)XY-(\gamma+\gamma^2)Y-X^3+(\gamma+\gamma^2)X^2)$. As α runs over the rational numbers other than ±3, 1, 5 and 9, at which Kubert's curve is undefined or singular, $v=(\alpha+1)/(\alpha-3)$ runs over $\mathbb{Q}\setminus\{-1,1,3,\frac{1}{3},\frac{5}{3}\}$, and at each such v the substitution is an isomorphism over $\mathbb{Q}$, since $4-12v\neq0$. □

The substitution $v\mapsto 2-v$ gives $a(2-v)=a-b$ and $b(2-v)=-b$, so $(x,y)\mapsto(x+b,y)$ is an isomorphism $E_{2-v}\to E_v$ over $\mathbb{Q}(v)$. Similarly, for $\bar v=(5v-3)/(3v-5)$ one has $a(\bar v)=\mu^2b$ and $b(\bar v)=\mu^2a$ with $\mu=16/(3v-5)^2$, so $(x,y)\mapsto(\mu^2x,\mu^3y)$ is an isomorphism $E_v\to E_{\bar v}$ over $\mathbb{Q}(v)$. The substitutions $v\mapsto 2-v$ and $v\mapsto\bar v$ generate a group of order 6, whose five nontrivial elements are those that [4, §2] lists as leaving $j(E)$ unchanged, and $E_{g(v)}\cong E_v$ over $\mathbb{Q}(v)$ for each g in it. Put $u=(v-1)^2$ and $\xi=x-16(v-1)^3=x-b/2$. Then (1) becomes

$$y^2=(\xi^2-256u^3)\,(\xi-3u^2-24u+16),\tag{3}$$

whose coefficients lie in $\mathbb{Q}(u)$: E is the base change, along the double cover $v \mapsto u = (v-1)^2$, of the elliptic surface $\mathcal{F} \to \mathbb{P}^1_u$ defined by (3). Its discriminant is $\Delta(\mathcal{F}) = 2^{14}u^3(u-4)^6(9u-4)^2$, with singular fibres of type I_6 at $u=4$, I_3 at $u=0$, I_2 at $u=4/9$ and I_1 at $u=\infty$ (Euler numbers summing to 12), so $\mathcal{F}$ is a rational elliptic surface. It has the point $(4u^2+16u,\ 4u(u-4)^2)$ of order 3 (the image of T_3) and the point $(3u^2+24u-16,\ 0)$ of order 2, hence a point T_6 of order 6. Moving T_6 to $(0,0)$ puts (3) into Kubert's normal form $y^2+(1-\delta)xy-(\delta+\delta^2)y = x^3-(\delta+\delta^2)x^2$ for a point of order 6 [17], with $\delta = (4-u)/(9u-4)$. Since δ is a fractional linear function of u, $\mathcal{F}$ is the universal elliptic curve with a point of order 6 over the modular curve $X_1(6)$, the δ-line. Equivalently, its classifying map to $X_1(6)$ has degree 1, as it must, since $j(\mathcal{F})$ has degree $12 = [\mathrm{PSL}_2(\mathbb{Z}) : \pm\Gamma_1(6)]$ in u. It is one of Beauville's semistable elliptic surfaces with four singular fibres [1]. Let $X_1(2,6)$ be the modular curve of elliptic curves with a point of order 6 and a point of order 2 outside the subgroup that it generates. The double cover $v \mapsto u = (v-1)^2$ adjoins the two other points of order 2, $\xi = \pm 16(v-1)^3$, so it is the forgetful map $X_1(2,6) \to X_1(6)$. This structure is already implicit in [4, §2] (and in §2.2 of the arXiv version of [5]), where the model (1) is obtained from the universal curve with a point of order 6, over a line with coordinate d, by making $(d+1)(9d+1)$ a square; that double cover of the d-line is the quotient by $v \mapsto \bar{v}$, which is conjugate to $v \mapsto 2-v$ in the group of order 6. It is also visible in MacLeod's model [19, (5.1)] of the universal curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, whose coefficients are polynomials in the square of its parameter ρ (r in [19]). For $v = 1+2/\rho$, so that $\rho^2 = 4/u$, the map $(x,y) \mapsto (\rho^4 x/16 + (\rho+1)^3(\rho-3),\ \rho^6 y/64)$ is an isomorphism over $\mathbb{Q}(\rho)$ from E_v to this model.

3. Four points over quadratic extensions

Each of the points $P_1, \dots, P_4$ of Theorem 1.2(b) comes from a point over $\mathbb{Q}(v)$ on a quadratic twist of E. Put

$$D_1 = 3v(7v-5), \qquad D_2 = 3(v-2)(7v-9), \qquad D_3 = 3v(v-2),$$
$$D_4 = v(v-2)(7v-5)(7v-9) = \tfrac{1}{9}D_1D_2.$$

Then $D_2(v) = D_1(2-v)$, and $D_3 = 3(u-1)$ and $D_4 = (u-1)(49u-4)$ are polynomials in $u = (v-1)^2$, the coordinate on the base of the surface $\mathcal{F}$ of (3).

Lemma 3.1. *For $i = 1, \dots, 4$ let $x_i, y_i \in \mathbb{Q}[v]$ be*

$$\begin{aligned} x_1 &= (v+1)^2(7v-5), & y_1 &= (v-3)(v+1)^2(5v-3),\\ x_2 &= (v+1)(5v-7)^2, & y_2 &= (v-3)^2(v+1)(5v-7),\\ x_3 &= \tfrac{16}{3}\,v(v+1)(3v-5), & y_3 &= \tfrac{16}{9}\,(v-3)(v+1)(3v-5)(3v-1),\\ x_4 &= (v-1)^2(v+1)(7v-5), & y_4 &= 2(v-3)(v-1)^2(v+1). \end{aligned}$$

Then $f(x_i) = D_i\, y_i^2$ in $\mathbb{Q}[v]$; that is, (x_i, y_i) is a point of the quadratic twist $D_i\, y^2 = f(x)$ of E.

Proof. Since $f(x) = x(x-a)(x-b)$, it suffices to factor $x_i - a$ and $x_i - b$:

$$\begin{aligned} x_1 - a &= 3v(v+1)^2(3-v), & x_1 - b &= -(v-3)(5v-3)^2,\\ x_2 - a &= -3(v+1)(v-2)(v-3)^2, & x_2 - b &= -(v-3)^2(7v-9),\\ x_3 - a &= -\tfrac{1}{3}(v+1)(3v-5)(3v-1)(v-3), & x_3 - b &= -\tfrac{16}{3}(v-3)(3v-1)(v-2),\\ x_4 - a &= 4v(v+1)(v-2)(v-3), & x_4 - b &= (v-1)^2(v-3)(7v-9). \end{aligned}$$

Multiplying,

$$\begin{aligned} f(x_1) &= 3v(7v-5)\,(v+1)^4(v-3)^2(5v-3)^2,\\ f(x_2) &= 3(v-2)(7v-9)\,(v+1)^2(5v-7)^2(v-3)^4,\\ f(x_3) &= \tfrac{256}{27}\,v(v-2)(v+1)^2(3v-5)^2(3v-1)^2(v-3)^2,\\ f(x_4) &= 4\,v(v-2)(7v-5)(7v-9)\,(v-1)^4(v+1)^2(v-3)^2, \end{aligned}$$

which are the stated identities. □

The point (x_2,y_2) is the image of $(x_1(2-v),y_1(2-v))$ under the isomorphism $E_{2-v}\to E_v$ of Section 2: indeed $x_2(v)=x_1(2-v)+b(v)$ and $y_2(v)=y_1(2-v)$. For the relation to [4, §§7 and 8.2] see Section 1.

4. The curve of genus one

On the curve C of (2) the four polynomials D_i become squares, so the points of Lemma 3.1 give points of E over $\mathbb{Q}(C)$, and C has infinitely many rational points (Lemma 4.3). Let $v=6/(3-s^2)$ on C, and put

$$w_1=\frac{3r}{3-s^2},\qquad w_2=\frac{3st}{3-s^2},\qquad w_3=\frac{6s}{3-s^2},\qquad w_4=\frac{w_1w_2}{3}.$$

Lemma 4.1. *On C one has $D_i(v)=w_i^2$ for $i=1,\dots,4$.*

Proof. From $v=6/(3-s^2)$: $7v-5=(5s^2+27)/(3-s^2)$, $v-2=2s^2/(3-s^2)$ and $7v-9=3(3s^2+5)/(3-s^2)$. Hence $D_1=18(5s^2+27)/(3-s^2)^2=9(10s^2+54)/(3-s^2)^2=w_1^2$, $D_3=36s^2/(3-s^2)^2=w_3^2$ and $D_2=18s^2(3s^2+5)/(3-s^2)^2=9s^2(6s^2+10)/(3-s^2)^2=w_2^2$, using (2). Finally $D_4=D_1D_2/9=w_4^2$. □

Proposition 4.2. *The points*

$$P_i=(x_i,\ y_iw_i)\qquad (i=1,\dots,4),$$

with x_i,y_i as in Lemma 3.1 evaluated at $v=6/(3-s^2)$, lie in $E(\mathbb{Q}(C))$.

Proof. By Lemmas 3.1 and 4.1, $f(x_i)=D_iy_i^2=(y_iw_i)^2$. □

Lemma 4.3. *Let $\overline{C}\subset\mathbb{P}^3$ be the closure of C, defined by $r^2=10s^2+54z^2$ and $t^2=6s^2+10z^2$.*

(a) $\overline{C}$ is a smooth curve of genus one, and $(s,r,t)=(1,8,4)$ is a rational point.

(b) $\overline{C}$ is isomorphic over $\mathbb{Q}$ to $E'\colon y^2=x^3+x^2-1720x+16100$, which has conductor 1680 and $E'(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$; the point $P_0=(-40,150)$ has infinite order. In particular $\overline{C}(\mathbb{Q})$ is infinite. Moreover $C(\mathbb{Q})=\overline{C}(\mathbb{Q})$.

Proof. (a) The pencil $\lambda_1(r^2-10s^2-54z^2)+\lambda_2(t^2-6s^2-10z^2)$ consists of diagonal quadrics with determinant $\lambda_1\lambda_2(10\lambda_1+6\lambda_2)(54\lambda_1+10\lambda_2)$, which has four distinct roots in $\mathbb{P}^1$. This determinant is 2^{-4} times the binary quartic that [3, §2] attaches to the pair of quadrics, so the discriminant of the pair is nonzero, and by [3, Theorem 2.8(ii)] the base locus $\overline{C}$ is a smooth curve of genus one, a complete intersection of two quadrics in $\mathbb{P}^3$. (b) The lines $r=8+m(s-1)$ through $(s,r)=(1,8)$ meet the conic $r^2=10s^2+54$ again at $s=(m^2-16m+10)/(m^2-10)$, and then $t^2=6s^2+10$ becomes

$$\eta^2=G(m):=16m^4-192m^3+1456m^2-1920m+1600,\qquad \eta=t\,(m^2-10).$$

This gives a birational map from $\overline{C}$ to the smooth projective model of $\eta^2=G(m)$. The discriminant of G is $2^{30}3^85^47^2\neq0$, so G has no repeated roots. Its leading coefficient 16

is a square, 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 [2, §2] are $I(G) = 1321216$ and $J(G) = -1843945472$. By [3, 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 $y^2 = x^3 + x^2 - 1720x + 16100$. On this curve, $3P_0 = (-57160/73^2,\ 71127450/73^3)$ is not 73-integral, whereas a torsion point $P \neq O$ of an integral Weierstrass equation has p-integral coordinates at every odd prime p by [28, Theorem VII.3.4] (as $\lfloor 1/(p^n - p^{n-1}) \rfloor = 0$); so $3P_0$, and hence P_0, has infinite order. The conductor and the torsion subgroup are standard computations (PARI/GP [23]). A 2-descent shows that the curve E' (Cremona's label 1680h3, LMFDB label 1680.p2) has rank 1: its 2-Selmer group has dimension 3 and $E'(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, so the rank is at most 1, hence equal to 1. Finally, $C(\mathbb{Q}) = \overline{C}(\mathbb{Q})$, since a rational point of $\overline{C}$ with $z = 0$ would need $r^2 = 10s^2$ and $t^2 = 6s^2$ with $s \neq 0$, and 10 and 6 are not squares. □

5. Independence

Proposition 5.1. *The points P_1, P_2, P_3, P_4 of Proposition 4.2 are linearly independent in $E(\mathbb{Q}(C))$.*

Proof. Galois action. The function field $\mathbb{Q}(C) = \mathbb{Q}(s, r, t)$ equals $\mathbb{Q}(v)(w_1, w_2, w_3)$, since $s = w_3/v$, $r = 2w_1/v$ and $t = 2w_2/(sv)$. The classes of D_1, D_2, D_3 in $\mathbb{Q}(v)^\times/\mathbb{Q}(v)^{\times 2}$ are independent: every nonempty product of them has a root of odd multiplicity (the roots of D_1, D_2, D_3 are $\{0, \frac{5}{7}\}$, $\{2, \frac{9}{7}\}$ and $\{0, 2\}$). Hence $\mathbb{Q}(C)/\mathbb{Q}(v)$ is Galois with group $\mathcal{G} \cong (\mathbb{Z}/2\mathbb{Z})^3$, and for $\sigma \in \mathcal{G}$ we may write $\sigma(w_i) = \chi_i(\sigma) w_i$ with characters χ_1, χ_2, χ_3 that form a basis of the character group. Also $\sigma(w_4) = \chi_1\chi_2(\sigma) w_4$. Since E is defined over $\mathbb{Q}(v)$ and $x_i, y_i \in \mathbb{Q}(v)$,

$$\sigma(P_i) = (x_i,\ \chi(\sigma)\, y_i w_i) = \chi(\sigma)\, P_i, \qquad \chi = \chi_1, \chi_2, \chi_3, \chi_1\chi_2 \text{ for } i = 1, 2, 3, 4,$$

where $-(x, y) = (x, -y)$. Write ψ_i for the character attached to P_i in this display. Suppose $\sum_j n_j P_j = T$ with $n_j \in \mathbb{Z}$ and $T \in E(\mathbb{Q}(C))_{\mathrm{tors}}$. Applying $\sum_{\sigma \in \mathcal{G}} \psi_i(\sigma)\, \sigma$ and using the orthogonality of the four distinct characters $\psi_1, \ldots, \psi_4$, we get $8 n_i P_i = \sum_\sigma \psi_i(\sigma)\sigma(T)$, a torsion point. So $n_i = 0$ as soon as P_i has infinite order.

Each P_i has infinite order. Let $c_0 = (129, 408, 316) \in C(\mathbb{Q})$. Then $v(c_0) = -1/2773$, and the fibre $E_{-1/2773}$ is smooth. All coordinates of the P_i are regular at c_0, and specialisation at a point with smooth fibre is a group homomorphism $E(\mathbb{Q}(C)) \to E_{-1/2773}(\mathbb{Q})$, since the Weierstrass model is an elliptic curve over the local ring of $\overline{C}$ at c_0. So it suffices that the specialised points $R_i := P_i(c_0)$ have infinite order. Let a_0, b_0 be the values of a, b at $-1/2773$. These values and the x-coordinates of the R_i are

$$\begin{aligned} &x(R_1) = -106592226048/2773^3, && x(R_2) = 1044991487232/2773^3, \\ &x(R_3) = 205024512/2773^3, && x(R_4) = -295900173321984/2773^4, \\ &a_0 = -295388450590464/2773^4, && b_0 = -683076506368/2773^3. \end{aligned}$$

Let

$$\kappa\colon E_{-1/2773}(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2, \qquad P \mapsto (x(P),\, x(P) - a_0),$$

with $\kappa(O) = (1, 1)$ and the usual values $\kappa(0, 0) = (a_0 b_0, -a_0)$ and $\kappa(a_0, 0) = (a_0, a_0(a_0 - b_0))$. This is the 2-descent homomorphism, with kernel $2E_{-1/2773}(\mathbb{Q})$ [28, Proposition X.1.4]. Its

values on $R_1,\dots,R_4$ and on the three points of order 2 are, in squarefree representatives,

$$\begin{aligned}
&\kappa(R_1)=(-8319,\,-390), && \kappa(R_2)=(213521,\,77),\\
&\kappa(R_3)=(2220831921,\,18063780735), && \kappa(R_4)=(-231,\,-30030),\\
&\kappa(0,0)=(1026764624809,\,266959), && \kappa(a_0,0)=(-266959,\,-6021260245),\\
&\kappa(b_0,0)=(-3846151,\,-22555).
\end{aligned}$$

Only the primes $2,3,5,7,11,13,19,47,59,73,347$ and 3467 occur in these values; for example $2220831921=3\cdot7\cdot11\cdot47\cdot59\cdot3467$, $18063780735=3\cdot5\cdot7\cdot11\cdot13\cdot347\cdot3467$, $1026764624809=7\cdot11\cdot19\cdot47\cdot59\cdot73\cdot3467$ and $6021260245=5\cdot7\cdot11\cdot13\cdot347\cdot3467$. The values follow from the factorisations of a, b and $a-b$ in Section 2 and of x_i and x_i-a in Lemma 3.1 and its proof, evaluated at $-1/2773$; for instance, $x(R_1)=-2772^2\cdot2^4\cdot3\cdot17^2/2773^3$ and $x(R_1)-a_0=-2772^2\cdot2^7\cdot3\cdot5\cdot13/2773^4$, so $\kappa(R_1)=(-3\cdot2773,\,-2\cdot3\cdot5\cdot13)$. By Lemma 2.1(b), $E_{-1/2773}(\mathbb{Q})_{\mathrm{tors}}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, so every torsion point is the sum of a point of $E_{-1/2773}[2]=\{O,(0,0),(a_0,0),(b_0,0)\}$ and a point of order dividing 3, which lies in $2E_{-1/2773}(\mathbb{Q})$. Hence κ maps $E_{-1/2773}(\mathbb{Q})_{\mathrm{tors}}$ onto the group $\{(1,1),\kappa(0,0),\kappa(a_0,0),\kappa(b_0,0)\}$. None of the $\kappa(R_i)$ lies in this group. Therefore $R_i\notin E_{-1/2773}(\mathbb{Q})_{\mathrm{tors}}+2E_{-1/2773}(\mathbb{Q})$, and in particular R_i has infinite order. □

Remark 5.2. A 2-descent at the fibre over c_0 alone also proves Proposition 5.1, without the Galois action: the same data show that $R_1,\dots,R_4$ are independent in $E_{-1/2773}(\mathbb{Q})$. The six vectors $\kappa(R_1),\dots,\kappa(R_4),\kappa(0,0),\kappa(a_0,0)$ have $\mathbb{F}_2$-rank 5, the only relation being $\kappa(R_1)+\kappa(R_2)+\kappa(R_4)=0$ in the group $(\mathbb{Q}^\times/\mathbb{Q}^{\times2})^2$, written additively. Accordingly $R_1+R_2-R_4=2Q$ for the point $Q\in E_{-1/2773}(\mathbb{Q})$ with $y(Q)<0$ and

$$x(Q)=-1761551909998848/61644977784047.$$

Since $\kappa(Q)=(-717079,\,-38170)$, the images of $Q,R_2,R_3,R_4,(0,0),(a_0,0)$ have $\mathbb{F}_2$-rank 6. If Γ is the subgroup generated by Q,R_2,R_3,R_4 and $E_{-1/2773}(\mathbb{Q})_{\mathrm{tors}}$, then $\kappa(\Gamma)$ is a quotient of $\Gamma/2\Gamma$, so $6\le\operatorname{rank}\Gamma+2$. Thus Q,R_2,R_3,R_4, and hence $R_1,\dots,R_4$, are independent.

The four points also span $E(\mathbb{Q}(C))\otimes\mathbb{Q}$.

Proposition 5.3. $\operatorname{rank}E(\mathbb{Q}(C))=4$.

Proof. As in the proof of Proposition 5.1, $\mathbb{Q}(C)/\mathbb{Q}(v)$ is Galois with group $(\mathbb{Z}/2\mathbb{Z})^3$, and $E(\mathbb{Q}(C))\otimes\mathbb{Q}$ is the sum of its eigenspaces. The eigenspace of the character attached to a class $D\in\langle D_1,D_2,D_3\rangle\subset\mathbb{Q}(v)^\times/\mathbb{Q}(v)^{\times2}$ is $E^D(\mathbb{Q}(v))\otimes\mathbb{Q}$, where $E^D\colon Dy^2=f(x)$, since $(x,y)\mapsto(x,y\sqrt{D})$, with $\sqrt{D}\in\mathbb{Q}(C)$, maps $E^D(\mathbb{Q}(v))$ isomorphically onto the group of points of $E(\mathbb{Q}(C))$ on which the Galois group acts through that character. Hence $\operatorname{rank}E(\mathbb{Q}(C))=\sum_D\operatorname{rank}E^D(\mathbb{Q}(v))$, the sum over the eight classes, whose representatives D are listed in Table 1.

Write E^D as $Y^2=X(X-aD)(X-bD)$ with $aD,bD\in\mathbb{Z}[v]$. This curve is not constant, since its j-invariant is $j(E)$, a nonconstant function of v, so [13, Theorem 1.1] applies to it. With $e_1=0$, $e_2=aD$ and $e_3=bD$, the products $(e_1-e_2)(e_1-e_3)$, $(e_2-e_1)(e_2-e_3)$ and $(e_3-e_1)(e_3-e_2)$ of [13, Theorem 1.1] are $ab\,D^2$, $a(a-b)D^2$ and $-b(a-b)D^2$. For each class the table gives a value $v_D\in\mathbb{Q}$ such that, for every nonconstant squarefree divisor $g\in\mathbb{Z}[v]$ of $ab\,D^2$, $a(a-b)D^2$ or $-b(a-b)D^2$, the number $g(v_D)$ is not a square (in particular not 0, so the fibre $E^D_{v_D}$ is smooth), and the specialisation $E^D(\mathbb{Q}(v))\to E^D_{v_D}(\mathbb{Q})$ is injective by [13, Theorem 1.1]. Such a divisor is $\pm d$ times a product of distinct primitive irreducible factors of the product, where d is a squarefree divisor of its content, and the contents of $ab\,D^2$, $a(a-b)D^2$ and $-b(a-b)D^2$ are 32, 1 and 32, or 288, 9 and 288 for the four classes

whose representative has content 3. The table gives the number of divisors g for each class, counted once for each of the three products (5352 in all).

The curve $E^D_{v_D}$ has full rational 2-torsion, so $\operatorname{rank} E^D_{v_D}(\mathbb{Q}) + 2$ is the dimension over $\mathbb{F}_2$ of $E^D_{v_D}(\mathbb{Q})/2E^D_{v_D}(\mathbb{Q})$, which injects into the 2-Selmer group $\mathrm{Sel}_2(E^D_{v_D})$; so the rank is at most $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^D_{v_D}) - 2$. Here Sel_2 is the group of the classical complete 2-descent [28, Proposition X.1.4]: for the model $Y^2 = X(X-e)(X-e')$ of Table 2, it consists of the pairs (b_1, b_2) of squarefree divisors of $2ee'(e-e')$, of either sign, for which the curve $b_1z_1^2 - b_2z_2^2 = e$, $b_1z_1^2 - b_1b_2z_3^2 = e'$ has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime $p \mid 2ee'(e-e')$, a finite computation. Table 1 gives these dimensions and bounds, and Table 2 gives an integral model of each curve $E^D_{v_D}$ and generators of its 2-Selmer group. All the 2-descents in this paper are on curves with full rational 2-torsion, so they use no class groups and do not depend on GRH. For each class we chose a v_D of small height at which no $g(v_D)$ is a square and this bound equals the rank to be proved (1 for the classes of D_1, D_2, D_3 and D_1D_2, and 0 for the other four). Hence $\operatorname{rank} E(\mathbb{Q}(C)) \le 4$, and equality holds by Proposition 5.1. The values $g(v_D)$ and the 2-Selmer groups are machine computations with PARI/GP: the 2-Selmer groups are computed with `ell2cover` [23]. □

TABLE 1. The eight classes in the proof of Proposition 5.3: a representative D, the value v_D, the dimension of the 2-Selmer group of $E^D_{v_D}$, the resulting bound for its rank and the number of divisors g tested.

class	representative D	v_D	$\dim_{\mathbb{F}_2} \mathrm{Sel}_2$	rank bound	divisors g
1	1	$-2/7$	2	0	86
D_1	D_1	$-11/4$	3	1	748
D_2	D_2	$-3/10$	3	1	748
D_3	D_3	$-3/10$	3	1	748
D_1D_2	D_4	$-3/10$	3	1	1526
D_1D_3	$(7v-5)(v-2)$	$-1/10$	2	0	374
D_2D_3	$v(7v-9)$	$-11/10$	2	0	374
$D_1D_2D_3$	$3(7v-5)(7v-9)$	$-11/6$	2	0	748

6. Proof of the theorems

Proof of Theorem 1.2. Part (a) is Lemma 4.3 and part (b) is Proposition 5.1. For (c), the torsion statement is Lemma 2.1(b) ($v(c) = \infty$ would need $s^2 = 3$). The j-invariant of E is a nonconstant function of v, and v is a nonconstant function on C, so $E/\mathbb{Q}(C)$ is not isotrivial, and its $\mathbb{Q}(C)/\mathbb{Q}$-trace, an abelian subvariety of E in characteristic 0 [15, §3.1], is trivial. Silverman's specialisation theorem [27, Theorem C] applies to an abelian variety with trivial trace over the function field of a curve over a number field, through a smooth projective model over the curve; here we take the Kodaira–Néron model of E over $\overline{C}$, whose fibre at c is $E_{v(c)}$ when that curve is smooth. By the second statement of that theorem (with $d = 1$), the specialisation map $E(\mathbb{Q}(C)) \to E_{v(c)}(\mathbb{Q})$ is injective for all but finitely many $c \in C(\mathbb{Q})$ with smooth fibre. For other forms of the theorem see [29, Theorem III.11.4] and [15, Theorem 1.1(2), Corollary 1.2, Proposition 3.1], whose Corollary 1.2 states the consequence for ranks used here and whose Proposition 3.1 removes the hypothesis on the trace. At every $c \in C(\mathbb{Q})$ with smooth fibre at which the specialisation map is injective, $\operatorname{rank} E_{v(c)}(\mathbb{Q}) \ge \operatorname{rank} E(\mathbb{Q}(C)) \ge 4$ by (b). The fibre is singular at the sixteen points

TABLE 2. Integral models $Y^2 = X(X-e)(X-e')$ of the eight curves $E^D_{v_D}$ of Table 1. For the four classes of rank 1 the last column gives $\kappa(P) = (X(P), X(P)-e)$, in squarefree representatives, for the point P that the point of Lemma 3.1 gives at $v = v_D$; with the images of the points of order 2, it spans $\mathrm{Sel}_2(E^D_{v_D})$. For the other four classes, $\mathrm{Sel}_2(E^D_{v_D})$ is the image of $E^D_{v_D}[2]$.

class	e	e'	$\kappa(P)$
1	-5125	-163296	
D_1	58190979	-1382832000	$(-33, -2231)$
D_2	-17221687	-598287040	(59570, 777)
D_3	-465451	-16169920	(94990, 1985291)
D_1D_2	-1222739777	-42478379840	$(-5957, -202279)$
D_1D_3	-5138721	-56647360	
D_2D_3	152471	-5443986240	
$D_1D_2D_3$	36794625	-4407393344	

$(\pm1, \pm8, \pm4)$, over $v = 3$, and $(\pm3, \pm12, \pm8)$, over $v = -1$, and at no other point of $C(\mathbb{Q})$, since $v = 6/(3-s^2)$ takes the values 1, $\frac{1}{3}$ and $\frac{5}{3}$ only where $s^2 = -3$, -15 and $-\frac{3}{5}$. □

We have not determined the finite set of points $c \in C(\mathbb{Q})$ with smooth fibre at which the specialisation map is not injective: the constants in Silverman's theorem can be computed in principle, but they are too large to be practical [13, §1], and the criterion of [13, Theorem 1.1] is for curves over $\mathbb{Q}(t)$, whereas C has genus one. This set contains neither the point c_0 of Example 6.1 nor the point c_1 of Remark 7.3: at both, the points $P_1(c), \dots, P_4(c)$ are independent (Remarks 5.2 and 7.3), $\mathrm{rank}\, E(\mathbb{Q}(C)) = 4$ (Proposition 5.3), and torsion specialises injectively. For the same reasons, a point $c \in C(\mathbb{Q})$ with smooth fibre lies in this set exactly when $P_1(c), \dots, P_4(c)$ are dependent.

Proof of Theorem 1.1. By Lemma 4.3(b) the set $C(\mathbb{Q})$ is infinite, and by Theorem 1.2(c) all but finitely many of its points give curves $E_{v(c)}$ with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 4. The map $c \mapsto j(E_{v(c)})$ is a nonconstant rational function on $\overline{C}$ (of degree $24 \cdot 8 = 192$, since v has degree 8 on $\overline{C}$), so each value is taken at most 192 times, and infinitely many j-invariants occur. □

Example 6.1. The point $c_0 = (129, 408, 316)$ gives $v = -1/2773$. The global minimal model of $E_{-1/2773}$ is

$$y^2 + xy = x^3 - 9904296902409602038661 70\, x + 34384426638818733249978188708060 4900,$$

of conductor 138952056675401970. It is the first of the two curves of rank 5 with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ that [12] attributes to Dujella and Lecacheux (2002). Dujella [12] lists five points on this model, with $x =$ 39632200740, 376196308530, -387729217260, 233546798100 and 276487413090; they are independent, since with two points of order 2 their images under the 2-descent map have $\mathbb{F}_2$-rank 7. The curve has full rational 2-torsion and a 2-Selmer group of dimension 7, so its rank is at most 5, and the fibre at c_0 has rank 5, one more than the generic rank 4 (Proposition 5.3).

Remark 6.2. Write $H(E_v)$ for the height of the curve E_v, defined in Section 1. There are constants $\gamma_1, \gamma_2 > 0$ such that for large H the elliptic curves $E_{v(c)}$ with $c \in C(\mathbb{Q})$ and

$H(E_{v(c)}) \le H$ fall into at most $\gamma_2(\log H)^{1/2}$ isomorphism classes, and at least $\gamma_1(\log H)^{1/2}$ of these classes consist of curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 4. Indeed, identify $\overline{C}$ with E' (Lemma 4.3), which has rank one: $E'(\mathbb{Q})$ is generated by P_0 and its torsion subgroup, of order 8 (a computation with Cremona's `mwrank` in SageMath [26]; the LMFDB [18] lists this curve as 1680.p2, with the generator $(8, 54) = (35, 0) - P_0$), so that $\overline{C}(\mathbb{Q}) = \{kP_0+T : k \in \mathbb{Z},\ T \in E'(\mathbb{Q})_{\mathrm{tors}}\}$. Let $\hat{h}$ be the canonical height on E' for the divisor (O), and let h be the logarithmic height on $\mathbb{P}^1(\mathbb{Q})$. The function $c \mapsto h(v(c))$ is a height on $\overline{C}$ for the divisor $v^*(\infty)$, of degree 8; it differs from $8\hat{h}(c)$ by $O(\hat{h}(c)^{1/2}+1)$, since the divisor $v^*(\infty) - 8(O)$ has degree 0. Also $\hat{h}(kP_0) = k^2\hat{h}(P_0)$. Moreover $\log H(E_v) = 24\,h(v) + O(1)$ for every $v \in \mathbb{Q}$ with smooth fibre. For $v = m/n$ in lowest terms, E_v has the integral model $Y^2 = X(X - \alpha)(X - \beta)$ with $\alpha = (m + n)^3(3m - 5n)$ and $\beta = 32n(m - n)^3$. Since α and β have no common zero, the invariants $c_4 = 16(\alpha^2 - \alpha\beta + \beta^2)$ and $c_6 = 32(\alpha+\beta)(2\alpha-\beta)(\alpha-2\beta)$ of this model are coprime binary forms in m, n of degrees 8 and 12, and c_4 is positive definite; so a minimal model differs from this one by a bounded scaling, and $\log H(E_v) = 24 \log \max(|m|, |n|) + O(1)$. Together, since $\hat{h}(kP_0 + T) = \hat{h}(kP_0)$, these give $\log H(E_{v(c)}) = 192\,\hat{h}(P_0)\,k^2+O(|k|+1)$ for $c = kP_0+T$ with smooth fibre, so for large H the bound $H(E_{v(c)}) \le H$ holds when $|k| \le \gamma_3(\log H)^{1/2}$ and fails when $|k| > \gamma_4(\log H)^{1/2}$, for some constants $\gamma_3, \gamma_4 > 0$. The count then follows from Theorem 1.2(c), since each isomorphism class contains at most 192 of the curves $E_{v(c)}$ (proof of Theorem 1.1).

7. Remarks

Remark 7.1 (Where the fourth point comes from). The fourth point comes from the twist by D_1D_2, which, unlike the twists by D_1 and D_2, is the pull-back of a twist of the rational elliptic surface $\mathcal{F}$ of (3).

The polynomials $D_3 = 3(u-1)$ and $D_4 = (u-1)(49u-4)$ lie in $\mathbb{Q}[u]$, where $u = (v-1)^2$, so the twists of E by them are the pull-backs to the v-line of twists of $\mathcal{F}$. Likewise, P_3 and P_4 are the pull-backs of the points $\xi = \frac{16}{3}(7u - 4)$ of the twist of $\mathcal{F}$ by $3(u - 1)$ and $\xi = u(7u + 4)$ of the twist by $(u - 1)(49u - 4)$ (indeed $x_3 - 16(v - 1)^3 = \frac{16}{3}(7u - 4)$, $y_3 = \frac{16}{9}(u - 4)(9u - 4)$ and $x_4 - 16(v - 1)^3 = u(7u + 4)$). The involution $v \mapsto 2 - v$ fixes the classes of D_3 and D_4 and exchanges those of D_1 and D_2. Accordingly, P_2 is the image of P_1 under it, up to sign (Section 3).

The surface $E \to \mathbb{P}^1_v$ is a K3 surface, as noted in [4, §1]: the double cover $v \mapsto u$ is branched over $u = 0$ and $u = \infty$, where the fibres I_3 and I_1 of $\mathcal{F}$ become I_6 and I_2, so that E has the fibres I_6 at $v = -1, 1, 3$ and I_2 at $v = \frac{1}{3}, \frac{5}{3}, \infty$, with Euler numbers summing to 24. Its trivial lattice has rank $2+3\cdot5+3\cdot1 = 20$, the largest Picard number of a K3 surface in characteristic 0 ($\rho \le h^{1,1} = 20$), so $E(\overline{\mathbb{Q}}(v))$ is finite by the Shioda–Tate formula [21, Corollary (VII.2.4)]: E is an extremal elliptic K3 surface, and its points of infinite order, such as $P_1, \dots, P_4$, are defined only over nontrivial extensions of $\overline{\mathbb{Q}}(v)$. A quadratic twist of a rational elliptic surface that is ramified at exactly two points of $\mathbb{P}^1$, at each of which the fibre is smooth or of type I_n, is a K3 surface ($p_g = 1$): the two fibres become of type I_0^* or I_n^*, which raises the Euler number from 12 to 24 [21, (III.4.2)–(III.4.6), Tables (IV.3.1) and (V.4.1)]. This covers the twist of $\mathcal{F}$ by $D_4 = (u - 1)(49u - 4)$, ramified at $u = 1$ and $u = 4/49$, and the twist by $D_3 = 3(u - 1)$, ramified at $u = 1$ and at $u = \infty$, where the fibre I_1 of $\mathcal{F}$ becomes I_1^*. In the same way, quadratic twists of the K3 surface E by a squarefree quadratic polynomial in v have $p_g = 2$, and those by a squarefree polynomial of degree 4 in v have $p_g = 3$.

Finally, in the plane of quadratic polynomials in u taken up to scalars, D_4 lies on the curve of the polynomials $q_\lambda(u) = (\lambda^2 u - 4(8-\lambda)^2)((\lambda-3)u-4)$, and the twist of $\mathcal{F}$ by each q_λ has the point $\xi = u(\lambda u + 32 - 4\lambda)$: for this ξ one has $(\xi^2 - 256u^3)(\xi - 3u^2 - 24u + 16) = q_\lambda(u)\, u^2 (u-4)^2$, and $\lambda = 7$ gives $q_7 = 4D_4$. (We found q_λ by trying $\xi = u(\lambda u + \mu)$, for which the right-hand side of (3) is u^2 times two quadratic polynomials in u; for $\mu = 32 - 4\lambda$ both vanish at $u = 4$.) For $\lambda = 7$ the point gives P_4, which has infinite order (Proposition 5.1). Hence it has infinite order for all but finitely many $\lambda \in \mathbb{Q}$: a torsion point of the twist of $\mathcal{F}$ by q_λ over $\mathbb{Q}(u)$ has order at most 12, since torsion specialises injectively to a smooth fibre over $\mathbb{Q}$, where Mazur's theorem [20] applies, and for each $N \leq 12$ the condition $NP = O$ on the point P is polynomial in λ and fails at $\lambda = 7$. (It holds at $\lambda = 4$ and $\lambda = 12$, where q_λ is 16 times a square and the point is a torsion point of $\mathcal{F}$.)

Heuristically, one counts conditions: in a family of surfaces, the locus where a given class in H^2 stays of type $(1,1)$ is cut out locally by at most $h^{2,0} = p_g$ equations, the vanishing of its $(0,2)$-component [30, §5.3], and a section of infinite order of a twist gives such a class, outside the span of the zero section and the fibre components (the Shioda–Tate formula [21, Theorem (VII.2.1) and Corollary (VII.2.4)]). So, over $\mathbb{C}$, in the two-dimensional space of quadratic twists of $\mathcal{F}$ by quadratic polynomials in u, taken up to scalars ($p_g = 1$), each twist with a section of infinite order should lie on a curve of such twists, as the twist by D_4 lies on the curve of twists by q_λ. For quadratic twists of E by squarefree quadratic polynomials in v ($p_g = 2$), such as those by D_1 and D_2, the same count allows positive rank at isolated parameters, and heuristically only there. Since $v \mapsto 2 - v$ exchanges D_1 and D_2, their product $D_1 D_2 = 9D_4$ is a quadratic polynomial in u, so by this count a point on the twist of E by it is expected to cost one condition, as for the twists of $\mathcal{F}$ ($p_g = 1$), instead of the three that a twist of E by a squarefree polynomial of degree 4 in v ($p_g = 3$) would need. This suggests why the twist of E by $D_1 D_2$ can have positive rank here.

Remark 7.2 (Other torsion groups). The table of [24, §8.3] gives the same borderline rank bound 3 for $T = \mathbb{Z}/8\mathbb{Z}$, where $b_{\mathbb{Z}/8\mathbb{Z}} \geq 3$ is known [4, 5, 10]. In terms of a parameter τ, the universal curve $y^2 = x^3 + A_8 x^2 + B_8 x$ with torsion $\mathbb{Z}/8\mathbb{Z}$ of [4, §2] has $A_8 = 8\theta^2 - 8\theta + 1$ and $B_8 = 16\theta^4$ with $\theta = \tau(1-\tau)$, so it too is the base change of an elliptic surface along a double cover of the line (its j-invariant is unchanged under $\tau \mapsto 1 - \tau$, as noted loc. cit.). Does the mechanism of Remark 7.1 also give $b_{\mathbb{Z}/8\mathbb{Z}} \geq 4$?

Remark 7.3 (Parity). If the root number of $E_{v(c)}$ equals -1 for infinitely many $c \in C(\mathbb{Q})$, the parity conjecture would give infinitely many curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 5. Both signs occur. The root number is -1 at c_0, where the rank is 5 (Example 6.1), and $+1$ at $c_1 = (83157/88747,\ 703176/88747,\ 346772/88747) \in C(\mathbb{Q})$, where $v = 7876030009/2785500563$. At c_1 the rank is 4. The points $P_1(c_1), \ldots, P_4(c_1)$ are independent: as at c_0 (Remark 5.2), their images under the 2-descent map and those of two points of order 2 have $\mathbb{F}_2$-rank 5, the only relation showing that $P_1(c_1) + P_2(c_1) + P_4(c_1)$ is twice a rational point Q, and replacing $P_1(c_1)$ by Q raises the $\mathbb{F}_2$-rank to 6. A 2-descent gives a 2-Selmer group of dimension 8, on which the Cassels–Tate pairing has rank 2, so that the rank is at most $8 - 2 - 2 = 4$; the rank 2 of the pairing is the third entry of the output of PARI's `ellrank` [23], which computes the 2-part of the Cassels–Tate pairing unconditionally. We do not know whether each sign occurs infinitely often. Park, Poonen, Voight and Wood suggest a refinement of their model for a family of generic rank r_0 and varying root number, in which a curve of height about H in the family has rank $r_0 + \nu$ with probability comparable, up to a factor $H^{o(1)}$, to that of rank ν for an arbitrary curve [24, Remark 1.1.3]. Since the family of Theorem 1.2 has generic rank 4 and only of the

order of $(\log H)^{1/2}$ curves of height at most H, this refinement predicts only finitely many curves of rank at least 6 in it, and is inconclusive at rank 5. Dujella [11, Problem 2.5] asks for a heuristic that predicts the distribution of parities of ranks in the known families with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (or $\mathbb{Z}/8\mathbb{Z}$) and rank at least 3; for the rank-3 families, see the experiments of [4, §11].

8. Computations

Table 3 lists the computations behind Sections 2–7. Theorems 1.1 and 1.2 rest only on exact computations: the polynomial identities of Sections 2–4, the curve E' of Lemma 4.3 with its conductor, its torsion and the point $3P_0$, the points of $C(\mathbb{Q})$ over singular fibres, and the values at c_0 printed in the proof of Proposition 5.1. Everything else in Table 3, including the rank of E', serves only Proposition 5.3, Example 6.1 and the remarks. The computations were done with PARI/GP 2.17.3 [23], apart from one with Cremona's `mwrank` in SageMath 10.9 [26] (Remark 6.2). The programs and their outputs are deposited in [16], together with those for the averages, for the search for twists of positive rank and for the search over triples of twists in Section 1. Nearly all of these computations were repeated with separately written programs, which are also in [16]. On one core of an AMD EPYC 4484PX each program takes at most 19 seconds, apart from the averages and the two searches of Section 1, which take 57, 269 and 127 seconds.

Table 3. The computations behind Sections 2–7.

statement	computed
Section 2, Lemma 2.1	T_3, $3T_3 = O$, a point of order 6, $j(E)$, equation (3), the singular fibres of $\mathcal{F}$
Section 2	Kubert's normal form of $\mathcal{F}$; MacLeod's model and E_v; Kubert's curve at $(3v+1)/(v-1)$ and E_v; the isomorphism $E_v \to E_{\bar{v}}$ and the group of order 6
Lemmas 3.1, 4.1	the polynomial identities
Lemma 4.3	G, $\operatorname{disc}(G)$, $I(G)$, $J(G)$, the Jacobian, $3P_0$, the order of P_0, the conductor and torsion of E', $E'(\mathbb{Q})[2]$, $\mathrm{Sel}_2(E')$, rank $E'(\mathbb{Q})$
Proposition 5.1, Remark 5.2	$v(c_0)$, $x(R_i)$, a_0, b_0, the values of κ, the point Q
Theorem 1.2(c)	the points of $C(\mathbb{Q})$ over singular fibres
Proposition 5.3	the values $g(v_D)$, the 2-Selmer groups of the $E^D_{v_D}$, the models and the values $\kappa(P)$ of Table 2
Example 6.1	minimal model, conductor, rank bounds
Remark 6.2	$E'(\mathbb{Q})$ generated by P_0 and $E'(\mathbb{Q})_{\mathrm{tors}}$, with `mwrank`
Remark 7.1	the singular fibres of E and of the twists of $\mathcal{F}$ by D_3 and D_4, the points P_3 and P_4 as pull-backs, the identity for q_λ, $\lambda = 4$ and 12
Remark 7.3	c_1, conductors, root numbers, the independence of $P_1(c_1), \dots, P_4(c_1)$, the 2-Selmer group and the Cassels–Tate pairing at c_1

Declarations

Use of AI. This paper was produced by a multi-agent AI research system that the author built and ran, using Anthropic Claude Opus 5.5: apart from the work of others that it cites, the ideas, proofs, computations and text are due to the system. Its results were checked by separate agents, and the computations that its proofs use by second programs (Section 8 and [16]). The author takes full responsibility for the paper, including its correctness and the integrity and accuracy of its citations.

Funding. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interests. The author declares no competing interests.

References

[1] A. Beauville, Les familles stables de courbes elliptiques sur $\mathbb{P}^1$ admettant quatre fibres singulières, *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), 657–660.
[2] J. E. Cremona, Classical invariants and 2-descent on elliptic curves, *J. Symbolic Comput.* **31** (2001), 71–87.
[3] J. E. Cremona, T. A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Algebra Number Theory* **4** (2010), 763–820; arXiv:0908.1741.
[4] A. Dujella, M. Kazalicki and J. C. 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), Paper No. 169; arXiv:2105.06215.
[5] A. Dujella and J. C. Peral, Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, in: *Trends in Number Theory*, Contemp. Math. **649**, Amer. Math. Soc., Providence, RI, 2015, 47–62; arXiv:1306.0027.
[6] A. Dujella and J. C. Peral, Elliptic curves induced by Diophantine triples, *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM* **113** (2019), 791–806; arXiv:1712.02082.
[7] A. Dujella and J. C. Peral, Construction of high rank elliptic curves, *J. Geom. Anal.* **31** (2021), 6698–6724.
[8] A. Dujella and J. C. Peral, 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; arXiv:2207.08206.
[9] A. Dujella, High rank elliptic curves with prescribed torsion, https://web.math.pmf.unizg.hr/~duje/tors/tors.html (accessed 13 October 2026).
[10] A. Dujella, Infinite families of elliptic curves with high rank and prescribed torsion, https://web.math.pmf.unizg.hr/~duje/tors/generic.html (accessed 13 October 2026).
[11] A. Dujella, Open problems on Diophantine m-tuples and elliptic curves, version of 13 October 2026, https://web.math.pmf.unizg.hr/~duje/pdf/open2.pdf.
[12] A. Dujella, Some curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and rank $= 5$, https://web.math.pmf.unizg.hr/~duje/tors/z2z6old5.html (accessed 13 October 2026).
[13] I. Gusić and P. Tadić, Injectivity of the specialization homomorphism of elliptic curves, *J. Number Theory* **148** (2015), 137–152; arXiv:1409.7189.
[14] R. Harron and A. Snowden, Counting elliptic curves with prescribed torsion, *J. Reine Angew. Math.* **729** (2017), 151–170; arXiv:1311.4920.
[15] M. Hindry and C. Salgado, Lower bounds for the rank of families of abelian varieties under base change, *Acta Arith.* **189** (2019), 263–282; arXiv:1712.05858.
[16] M. Jaswal, Programs and data for "Infinitely many elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least four", Zenodo, 2026, https://doi.org/10.5281/zenodo.23364151.
[17] D. S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3)* **33** (1976), 193–237.
[18] The LMFDB Collaboration, The L-functions and modular forms database, https://www.lmfdb.org, elliptic curve 1680.p2 (accessed 14 October 2026).
[19] A. J. MacLeod, A simple method for high-rank families of elliptic curves with specified torsion, arXiv:1410.1662 (2014).
[20] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHÉS* **47** (1977), 33–186.

[21] R. Miranda, *The Basic Theory of Elliptic Surfaces*, Dottorato di Ricerca in Matematica, ETS Editrice, Pisa, 1989.
[22] K. Nagao, $\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points, *Manuscripta Math.* **92** (1997), 13–32.
[23] The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
[24] J. Park, B. Poonen, J. Voight and M. M. Wood, A heuristic for boundedness of ranks of elliptic curves, *J. Eur. Math. Soc.* **21** (2019), 2859–2903; arXiv:1602.01431.
[25] M. Rosen and J. H. Silverman, On the rank of an elliptic surface, *Invent. Math.* **133** (1998), 43–67.
[26] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026, https://www.sagemath.org.
[27] J. H. Silverman, Heights and the specialization map for families of abelian varieties, *J. Reine Angew. Math.* **342** (1983), 197–211.
[28] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2009.
[29] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. **151**, Springer, 1994.
[30] C. Voisin, *Hodge Theory and Complex Algebraic Geometry II*, Cambridge Stud. Adv. Math. **77**, Cambridge Univ. Press, 2003.
[31] J. Woo, *Arithmetic of elliptic curves and surfaces: descents and quadratic sections*, Ph.D. thesis, Harvard University, 2010.

Toronto, Canada
Email address: manvirjaswal@icloud.com