involve

a journal of mathematics

Infinite family of elliptic curves of rank at least 4

Bartosz Naskręcki

mathematical sciences publishers

2010 vol. 3, no. 3

Infinite family of elliptic curves of rank at least 4

Bartosz Naskręcki

(Communicated by Bjorn Poonen)

We investigate $\mathbb{Q}$-ranks of the elliptic curve E_t: $y^2+txy=x^3+tx^2-x+1$, where t is a rational parameter. We prove that for infinitely many values of t the rank of $E_t(\mathbb{Q})$ is at least 4.

1. Introduction

In this paper we investigate the family of curves

$$E_t : y^2+txy=x^3+tx^2-x+1, \tag{1-1}$$

with parameter $t \in \mathbb{Q}$, and prove:

Main Theorem. *For infinitely many $u \in \mathbb{Q}$, the elliptic curve over $\mathbb{Q}$ given by the affine equation $E_{(u^2-u-3)} : y^2+(u^2-u-3)xy = x^3+(u^2-u-3)x^2-x+1$ has Mordell–Weil group of rank at least 4. More precisely, the group $E_{(u^2-u-3)}(\mathbb{Q})$ contains the subgroup spanned by the linearly independent points*

$$(0, 1),\ (1, 1),\ (u, u+1),\ \bigl(\tfrac{1}{9}, \tfrac{1}{54}(9+3u-3u^2+v)\bigr),$$

where the point (u, v) lies on the elliptic curve given by the equation

$$2569+18u-9u^2-18u^3+9u^4=v^2.$$

The latter curve has Weierstrass model

$$y_0^2=x_0^3-92835x_0+1389150, \tag{1-2}$$

which defines an elliptic curve over $\mathbb{Q}$ with Mordell–Weil group of rank 2 and torsion group $\mathbb{Z}/2\mathbb{Z}$, spanned by the points

$$(-309, 756),\ (-45, 2340),\ (15, 0).$$

MSC2000: 11D25, 11G05.

Keywords: elliptic curves, Mordell–Weil group, ranks in families.

This work was completed as a part of an undergraduate project at the Department of Mathematics and Computer Science in Poznań. We used the open source computer package Sage for almost all numerical computations.

The curves $E_{(u^2-u-3)}$ have different j-invariants for all but finitely many $u \in \mathbb{Q}$ as in the statement of the theorem.

Brown and Myers [2002] constructed an infinite family of elliptic curves over $\mathbb{Q}$ with quadratic growth of parameter and the rank of the Mordell–Weil group at least three. They asked whether one can find similar families of elliptic curves with higher ranks. Our Main Theorem resulted from attempts to answer the question. The method developed in this paper is modeled on the approach of [Brown and Myers 2002]. It naturally leads to computations with curves of high genera (instead of using specializations [Silverman 1986; 1983] as in the well-known method of Mestre).

It is of fundamental interest to find families of elliptic curves parametrized by a rational parameter with ranks higher than a prescribed constant [Kowalski 2007; Silverberg 2007; Rubin and Silverberg 2007; Kihara 1997; Mestre 1991; Nagao 1994]. The method of Mestre based on specialization theorems and computer search gives several infinite families of elliptic curves over $\mathbb{Q}$ of ranks as high as 14. Recent work by Elkies [2007] revealed elliptic curves with rank 18 over $\mathbb{Q}(t)$ and 19, parametrized by an elliptic curve of positive rank. Weierstrass equations of these families are rather complicated rational expressions of high order.

The family in Main Theorem provides quadratic polynomials as coefficients of the Weierstrass equation and four linearly independent points of a simple form. In addition, we obtain a general algorithm which can provide more such simple families with similar properties, and of rank at least 4. The main obstruction to obtaining higher ranks with our method is the base change from the projective line to a curve of higher genus — the best choice being a curve of genus 1 with infinite set of rational points over $\mathbb{Q}$ (as suggested after Lemma 2.2).

Rubin and Silverberg [2007] have obtained other infinite families of elliptic curves over $\mathbb{Q}$ of rank 4, constructed by twisting a curve given in the Legendre form. The families in that work are parametrized the by projective line or by an elliptic curve of rank 1 with twists parametrized by another elliptic curve of rank 1.

The choice of a particular family E_t was motivated by the study of more general families of elliptic curves with polynomial coefficients of degree at most one in the variable t. We first choose two rational constant sections with small coefficients. This method is likely to give rational elliptic surfaces with those two sections being independent. Then we look for a subfamily which contains a section with nonconstant x-coordinate, for example linear in variable t. Computations reveal what base change (e.g., quadratic base change from $\mathbb{P}^1$ to $\mathbb{P}^1$) shall increase the rank from 2 to 3 for particular values of t. Finally, we look for a suitable fourth point with constant x-coordinate. This provides a new base change to curve of higher genus (infinitely many curves of rank 4 occur only with elliptic curve with positive rank as a base). Similar computations gave us one more family of the type described in

Main Theorem, namely

$$F_{t(u)} : y^2 - t(u)xy = x^3 - t(u)x^2 - t(u)x + 1,$$

where $t(u) = 1 - u/2 + u^2/2$ and

$$v^2 = 361 + 198u - 189u^2 - 18u^3 + 9u^4$$

is the elliptic curve in a quartic form with rank 4 over $\mathbb{Q}$. For all but finitely many $u \in \mathbb{Q}$ the points

$$(0, 1),\ (2, 3),\ (u, u-1),\ \left(\tfrac{4}{9}, \tfrac{1}{27}(6 - 3u + 3u^2 + v)\right)$$

on the curve $F_{t(u)}$ are linearly independent.

The result stated in Main Theorem can be extended, if the parity conjecture holds true for E [Rohrlich 1994]. Let $\Lambda(E/\mathbb{Q}, s)$ be the complete L-series of the elliptic curve over $\mathbb{Q}$. Denote by $w(E) \in \{\pm 1\}$ the root number in the functional equation

$$\Lambda(E, 2-s) = w(E)\Lambda(E, s). \tag{1-3}$$

The parity conjecture predicts that

$$(-1)^{\text{rank } E(\mathbb{Q})} = w(E). \tag{1-4}$$

We can compute the root number $w(E_t)$ for the specific curves E_t and determine the parity of the rank of group $E_t(\mathbb{Q})$. Computations can be done explicitly using Sage [Stein et al. 2005], by choosing primes of bad reduction of E_t. We state numerical results in Section 4.2. In particular, assuming parity conjecture we constructed several elliptic curves over $\mathbb{Q}$ that have Mordell–Weil rank at least 5 (see Table 2).

2. Description of the algorithm

There are two obvious points lying on the curve (1-1), namely:

$$(0, 1), (1, 1) \in E_t(\mathbb{Q}(t)).$$

We produce with them several other points with coordinates in the ring $\mathbb{Z}[t]$:

$$\begin{aligned}
-(0, 1) &= (0, -1),\\
-(1, 1) &= (1, -t-1),\\
(0, 1) + 2(1, 1) &= (-t+1, -1),\\
(0, 1) + (1, 1) &= (-t-1, t^2+t-1),\\
(0, 1) - (1, 1) &= (t+3, 2t+5),\\
-(0, 1) + (1, 1) &= (t+3, -t^2-5t-5),\\
-(0, 1) + 2(1, 1) &= (t+5, 2t+11),\\
2(1, 1) &= (-1, t+1).
\end{aligned}$$

The following lemma describes the structure of the group $E_t(\mathbb{Q}(t))$.

Lemma 2.1. *The group* $E_t(\mathbb{Q}(t))$ *has rank* 2 *and has trivial torsion. It is generated by the points* $(0, 1)$ *and* $(1, 1)$.

Proof. Consider the elliptic curve

$$E_t : y^2 + txy = x^3 + tx^2 - x + 1$$

over $\mathbb{Q}(t)$ as the elliptic surface $\mathscr{E}$ over $\mathbb{P}^1$. The discriminant of E_t is equal to

$$-(t+2)^2(t^4+8t^3+11t^2-20t+92),$$

and the surface $\mathscr{E}$ has 6 singular fibers (in Kodaira classification):

- a fiber of type I_6 over $t = \infty$,
- a fiber of type I_2 over $t = -2$,
- four fibers of type I_1 over $t = \alpha_i$ for $i = 1, 2, 3, 4$, where

$$t^4+8t^3+11t^2-20t+92 = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4).$$

Let S be the set of bad places, namely $S = \{\infty, -2, \alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. From the Shioda–Tate formula [Shioda 1990, Corollary 5.3] we get

$$\operatorname{rank} E_t(\overline{\mathbb{Q}}(t)) = \rho(\mathscr{E}) - 2 - \sum_{v \in S}(m_v - 1),$$

where $\rho(\mathscr{E})$ is the Picard number of surface $\mathscr{E}$ and m_v is the number of components of singular fiber over place v. After [Shioda 1990, Equation 10.14] we find that the elliptic surface $\mathscr{E}$ is rational since the coefficients of the defining equation in Weierstrass form satisfy the condition:

$$\deg a_i(t) \leq i,$$

and the discriminant is nonconstant. This implies that $\rho(\mathscr{E}) = 10$ [Shioda 1990, Lemma 10.1] and we get from the Shioda–Tate formula:

$$\operatorname{rank} E_t(\overline{\mathbb{Q}}(t)) = 2.$$

Computation of the height pairing matrix for the points $P_1 = (0, 1)$ and $P_2 = (1, 1)$ gives the matrix:

$$(\langle P_i, P_j \rangle)_{1 \leq i, j \leq 2} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{6} \end{pmatrix}.$$

This shows that points P_1 and P_2 span the free part of the group $E_t(\overline{\mathbb{Q}}(t))$. Since they are both rational points over $\mathbb{Q}(t)$, it follows that they span the free part of the group $E_t\ (\mathbb{Q}(t))$.

The map

$$\phi : E_t(\overline{\mathbb{Q}}(t)) \to \prod_{v\in S} G(F_v)$$

takes a section to the respective fiber component of F_v that it meets. The group $G(F_v)$ is generated by simple components of the fiber F_v. The map ϕ is an injection on the torsion part. From the Néron model structure we know that for the multiplicative fibers I_n the group $G(I_n) \cong \mathbb{Z}/n\mathbb{Z}$. In case of the family E_t we get the injection

$$E_t(\overline{\mathbb{Q}}(t))_{\text{tors}} \hookrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Let $P = (x, y) \in E_t(\overline{\mathbb{Q}}(t))$ be a 2-torsion point. The condition $P = -P$ implies that x-coordinate must satisfy:

$$0 = 4 - 4x + 4tx^2 + t^2x^2 + 4x^3.$$

The polynomial on the right side is irreducible over $\overline{\mathbb{Q}}(t)$. Similarly, let P satisfy $P = -2P$. It follows that

$$0 = -1 + 4t + t^2 + 12x - 6x^2 + 4tx^3 + t^2x^3 + 3x^4.$$

Again the polynomial is irreducible over $\overline{\mathbb{Q}}(t)$. This clearly implies that only the point at infinity has finite order:

$$E_t(\overline{\mathbb{Q}}(t))_{\text{tors}} = \{\mathbb{O}\}. \qquad \square$$

In order to find more points on the curve (1-1) we specialize parameter t to a polynomial function of another parameter u:

$$t(u) = a_n u^n + \cdots + a_1 u + a_0,$$

where $a_i \in \mathbb{Q}$. To get a rational point on the curve (1-1) with x-coordinate equal to $au + b$, for $a, b \in \mathbb{Q}$, it is necessary and sufficient that

$$\Delta(u) = 4(-1 + b + au)^2(1 + b + au) + (2 + t(u))^2(b + au)^2 \qquad (2\text{-}1)$$

be a perfect square.

Lemma 2.2. *Let $P = (x, y)$ be a rational point on the curve $E_{t(u)}$ over $\mathbb{Q}(u)$, where $t(u) = a_n u^n + \cdots + a_1 u + a_0 \in \mathbb{Q}[u]$ of positive degree. Let $x = au + b \in \mathbb{Q}[u]$. Suppose that $a \neq 0$.*

(i) *If* $\deg t = 1$, *then $P = k(0, 1) + l(1, 1)$ for some $k, l \in \mathbb{Z}$.*

(ii) *If* $\deg t = 2$, *then $P = (x, x + 1)$ and $t(u) = x^2 - x - 3$ or $P = (x, x - 1)$ and $t(u) = -x^2 + x + 1$.*

If, *in addition*, $\deg t > 2$, *there is no rational point whose x-coordinate is equal to $au + b \in \mathbb{Q}[u]$.*

Proof. (i) Assume $t(u)=a_1u+a_0$ and $a_1\neq 0$. Put $P(u)=q_2u^2+q_1u+q_0$. Since P is a rational point on $E_{t(u)}$, the discriminant $\Delta(u)$ as in (2-1) is a perfect square:

$$\Delta(u)=P(u)^2;$$

moreover, for some $\varepsilon\in\{1,-1\}$, we have $q_2=\varepsilon aa_1$, $q_1=\dfrac{2a^2+2aa_1+aa_0a_1+ba_1^2}{\varepsilon a_1}$, and

$$q_0=\frac{-2a^3-4a^2a_1-2a^2a_0a_1-2aa_1^2+4aba_1^2+2ba_1^3+ba_0a_1^3}{\varepsilon a_1^3}.$$

Equating the last two coefficients of $\Delta(u)$ and $P(u)^2$ gives two equations in the variables a_1, a_0, a, b:

$$\begin{aligned}R_1(a,b,a_0,a_1)&=-a^6-4a^5a_1-2a^5a_0a_1-6a^4a_1^2+4a^4ba_1^2-4a^4a_0a_1^2-a^4a_0^2a_1^2\\&\quad-4a^3a_1^3+10a^3ba_1^3-2a^3a_0a_1^3+5a^3ba_0a_1^3-a^2a_1^4+8a^2ba_1^4\\&\quad-4a^2b^2a_1^4+4a^2ba_0a_1^4+a^2ba_0^2a_1^4+2aba_1^5-4ab^2a_1^5+aba_0a_1^5\\&\quad-2ab^2a_0a_1^5+a_1^6-ba_1^6-b^2a_1^6+b^3a_1^6\\&=0,\end{aligned}$$

$$\begin{aligned}R_2(a,b,a_0,a_1)&=2a^4+6a^3a_1+3a^3a_0a_1+6a^2a_1^2-3a^2ba_1^2+4a^2a_0a_1^2+a^2a_0^2a_1^2\\&\quad+2aa_1^3-4aba_1^3+aa_0a_1^3-2aba_0a_1^3-a_1^4-ba_1^4+b^2a_1^4\\&=0.\end{aligned}$$

The ideal $I=I(R_1,R_2)$ of these equations can be rearranged in the form of the Gröbner basis $I=I(a^9-2a^7a_1^2+a^5a_1^4, R'_1,\dots,R'_{18})$, with $R'_i=R'_i(a,b,a_0,a_1)$. The first polynomial of the new basis factors as $a^5(a-a_1)^2(a+a_1)^2$. The equation $a^5(a-a_1)^2(a+a_1)^2=0$ can only have solutions $a=\pm a_1$ since we assumed $a\neq 0$. For $a=a_1$ the equations reduce to

$$a_0=b-3 \quad\text{or}\quad a_0=b-5.$$

For $t(u)=au+(b-3)$ or $t(u)=au+(b-5)$, we get respectively the points

$$\begin{gathered}\bigl(t(u)+3,5+2t(u)\bigr),\ \bigl(t(u)+3,-5-5t(u)-t(u)^2\bigr),\\ \bigl(t(u)+5,11+2t(u)\bigr),\ \bigl(t(u)+5,-11-7t(u)-t(u)^2\bigr).\end{gathered}$$

They are linear combinations of (0, 1) and (1, 1) in the group $E_t(\mathbb{Q}(u))$.

For $a=-a_1$ the equations reduce to

$$a_0=-1-b \quad\text{or}\quad a_0=1-b.$$

For $t(u) = -au - b - 1$ and $t(u) = -au - b + 1$ we get the points

$$\big(-t(u)-1, 1\big),\ \big(-t(u)-1, -1+t(u)+t(u)^2\big),$$
$$\big(-t(u)+1, -1\big),\ \big(-t(u)+1, 1-t(u)+t(u)^2\big),$$

respectively. Again both points are the linear combinations of (0, 1) and (1, 1).

We can now proceed analogously to the proof of (i) and show property (ii). Let $t(u) = a_2u^2 + a_1u + a_0$ and $a_1 \neq 0$. Put $P(u) = q_3u^3 + q_2u^2 + q_1u + q_0$. Comparing coefficients of (2-1) and $P(u)^2$ implies

$$q_3 = \varepsilon a a_2, \quad q_2 = \frac{aa_1 + ba_2}{\varepsilon}, \quad q_1 = \frac{2a + aa_0 + ba_1}{\varepsilon}, \quad q_0 = \frac{2a^2 + 2ba_2 + ba_0a_2}{\varepsilon a_2},$$

with $\varepsilon = \pm 1$. By comparing the three lowest terms in $P(u)^2$ and $\Delta(u)$ we obtain

$$a_1 = \frac{(-1+2b)a_2}{a}, \quad a^3(2+a_0) + a(1+b-b^2)a_2 = 0, \quad a^2 = \lambda a_2,$$

with $\lambda = \pm 1$. This implies that $t(u) = -2 - \lambda - (au+b)\lambda + (au+b)^2\lambda$. In this way — assuming $x(u) = au + b$ — we get the two distinct families

	point	parameter $t(u)$
Family A	$(x, x+1)$	$x^2 - x - 3$
Family B	$(x, x-1)$	$-x^2 + x + 1$

To show the last case we proceed by induction on degree of the polynomial $t(u)$. Consider $t(u)$ as a polynomial in u of degree $n > 2$; then $\deg \Delta = 2n + 2$, so we look for the polynomial $P(u)$ of degree $n+1$ such that $\Delta(u) = P(u)^2$. We put

$$a_i^* = \begin{cases} a_i & \text{if } 0 < i \le n, \\ a_0 + 2 & \text{if } i = 0, \\ 0 & \text{otherwise,} \end{cases} \qquad \text{and} \qquad q_j^* = \begin{cases} q_j & \text{if } 0 \le j \le n+1, \\ 0 & \text{otherwise.} \end{cases}$$

We prove by induction the formula

$$q_j^* = \varepsilon(aa_{j-1}^* + bb_j^*),$$

using the identities

$$c_j(\Delta) = a^2 \sum_{j=\alpha+\beta} a_\alpha^* a_\beta^* + 2ab \sum_{j+1=\alpha+\beta} a_\alpha^* a_\beta^* + b^2 \sum_{j+2=\alpha+\beta} a_\alpha^* a_\beta^*, \quad c_j(P^2) = \sum_{j=\alpha+\beta} q_\alpha^* q_\beta^*,$$

for $j = n+1, \dots, 2n+2$, where $c_j(a_0 + a_1x + \cdots + a_nx^n) = a_j$. It follows from $\Delta = P^2$ that

$$c_j(\Delta) = c_j(P^2).$$

We substitute the coefficients $q_0=\varepsilon(2b+ba_0)$ and $q_1=\varepsilon(a(a_0+2)+ba_1)$ into the identities above with $j=0, 1, 2$ and we get $b^2=1$ and finally $a=0$, a contradiction. This completes the proof of the lemma. □

By Lemma 2.2, we can specialize to one of the quadratic parameters, since the families A and B (see previous page) have similar properties. For the rest of the paper we choose the specialization $t(u)=u^2-u-3$:

$$E_{(u^2-u-3)}: y^2+(u^2-u-3)xy=x^3+(u^2-u-3)x^2-x+1.$$

For notational simplicity, we write $f(x, y, u)=0$ for this equation. The point $(u, u+1)$ lies on these curves and gives several new integral points over $\mathbb{Q}[u]$:

$$\begin{aligned} -(u, u+1) &= (u, -u^3+u^2+2u-1),\\ (0, 1)+(u, u+1) &= (-u+1, u^3-2u^2-u+1),\\ (1, 1)-(u, u+1) &= (u^3-2u, u^4+u^3-3u^2-2u+1),\\ 2(1, 1)+(u, u+1) &= (-u^3+4u^2-6u+4, u^5-6u^4+14u^3-17u^2+10u-1). \end{aligned}$$

To find the fourth linearly independent rational point on the curve $E_{(u^2-u-3)}$, we consider the following general algorithm:

(1) Choose two rational functions $a(x), b(x)\in\mathbb{Q}(x)$.

(2) Form the simultaneous equations $f(a(u), y_a(u), u)=0$, $f(b(u), y_b(u), u)=0$.

(3) Find $a(x), b(x)$ such that $y_a(x), y_b(x)\in\mathbb{Q}(x)$.

(4) A sufficient and necessary condition for y_a, y_b to be rational is that the discriminant of the quadratic equation $f(a(x), y_a, x)=0$ in y_a be a perfect square. The same condition holds for the equation in y_b.

(5) Find all rational points, i.e., the triples $(u, s, w)\in\mathbb{Q}^3$ on the affine curve:

$$\Delta_{f(a(x),y_a,x)=0}(u)=s^2, \qquad \Delta_{f(b(x),y_b,x)=0}(u)=w^2, \tag{2-2}$$

where $\Delta_{f(a(x),y_a,x)=0}(x)$ and $\Delta_{f(b(x),y_b,x)=0}(x)$ belong to $\mathbb{Q}(x)$.

We now pick $a(x)=x$ and $b(x)=c$. Then the first equation in (2-2) reduces to $(2-u-u^2+u^3)^2=s^2$, while the second gives

$$4-4c-3c^2+4c^3+2c^2u-c^2u^2-2c^2u^3+c^2u^4=w^2.$$

We choose $c\in\mathbb{Q}$ so that it defines the elliptic curve in a quartic form with infinitely many points (u, w). A direct search with $u\in\mathbb{N}$ reveals that for $u=7$ we have on the curve E_{39} the four linearly independent points

$$(0, 1),\ (1, 1),\ (7, 8),\ \left(\tfrac{1}{9}, \tfrac{8}{27}\right);$$

hence we put $c=\frac{1}{9}$, as in the statement of Main Theorem.

3. Proofs

To prove Main Theorem, we will need the following elementary lemma.

Lemma 3.1. *Let $b \in M$, where M is a left $\mathbb{Z}$-module. Suppose $a_1, \dots, a_k \in M$ are linearly independent over $\mathbb{Z}$ and the nonzero cosets $[a_1], \dots, [a_k] \in M/2M$ are linearly independent over $\mathbb{F}_2$. If $[b] \notin \langle [a_1], \dots, [a_k] \rangle$ and the 2-torsion of M is trivial, then $b, a_1, \dots, a_k$ are independent over $\mathbb{Z}$ in M.*

Proof. Suppose, contrary to our claim, that there exists $\alpha_1, \dots, \alpha_k, \beta \in \mathbb{Z}$, not all zero, such that $\beta b + \alpha_1 a_1 + \cdots + \alpha_k a_k = 0$. We can assume that β is the least positive integer for which this holds. If β is odd, we have $[\beta b] = [b]$ and $[b] = [\alpha_1 a_1 + \cdots + \alpha_k a_k]$, a contradiction. If β is even, we have $[0] = [\alpha_1 a_1 + \cdots + \alpha_k a_k]$; but the linear independence of cosets $[a_i]$ over $\mathbb{F}_2$ implies that all α_i are even, so it is possible to write $\beta' b = \alpha'_1 a_1 + \cdots + \alpha'_k a_k$, where $2\beta' = \beta$ and $2\alpha'_i = \alpha_i$. This contradicts the minimality of β. □

We now establish the structure of the torsion subgroup of the curve E_t for all but finitely many $t \in \mathbb{Q}$.

Lemma 3.2. *Let $t_1(u) = u$ and $t_2(u) = u^2 - u - 3$. The structure of the torsion subgroup of groups $E_{t_i(u)}(\mathbb{Q})$ for $u \in \mathbb{Q}$ is as follows:*

Group T	$\#\{u \in \mathbb{Q} : E_{t_1(u)}(\mathbb{Q})_{\text{tors}} \cong T\}$	$\#\{u \in \mathbb{Q} : E_{t_2(u)}(\mathbb{Q})_{\text{tors}} \cong T\}$
$\mathbb{Z}/2\mathbb{Z}$	∞	0
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ $N = 1, 2, 3, 4$	0	0
$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$	$<\infty$	0
$\mathbb{Z}/3N\mathbb{Z}$ $N = 1, 2, 3, 4$	0	0
$\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$	$<\infty$	$<\infty$
$\mathbb{Z}/7\mathbb{Z}$	$<\infty$	$<\infty$

Proof. Mazur [Mazur 1978] showed that the group $E_t(\mathbb{Q})_{\text{tors}}$ is isomorphic either to $\mathbb{Z}/N\mathbb{Z}$ with $1 \le N \le 10$ or $N = 12$, or to $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with $N = 2, 4, 6$ or 8. We prove below that for $t = u^2 - u - 3$, with $u \in \mathbb{Q}$, the groups $E_t(\mathbb{Q})_{\text{tors}}[2]$ and $E_t(\mathbb{Q})_{\text{tors}}[3]$ are trivial for all u. The triviality of rational 5-torsion and 7-torsion subgroups is proved only for all but finitely many u. The 2-torsion is computed also for the general parameter t, which leads to curve of genus zero with rational parametrization. These facts, combined with Mazur's theorem, will suffice to finish the proof of the lemma.

Let $P = (x, y)$ be a 2-torsion point on the curve $y^2 + txy = x^3 + tx^2 - x + 1$. Its negative is $-P = (x, -tx - y)$. From the condition $P = -P$ it follows that

$$y = -\frac{tx}{2}.$$

Substitution into the Weierstrass equation of E_t gives the equation

$$0 = 4 - 4x + 4tx^2 + t^2x^2 + 4x^3, \tag{3-1}$$

which defines the curve of genus zero with the parametrization

$$t = \frac{-8 - 8s - 2s^2 - s^3}{4 + s^2}, \quad x = -1 - \frac{s^2}{4}.$$

When this is substituted in (3-1), the only nontrivial 2-torsion point is obtained:

$$\left(-1 - \tfrac{1}{4}s^2, \tfrac{1}{8}(-8 - 8s - 2s^2 - s^3)\right).$$

Therefore the groups $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$ cannot occur as torsion subgroups of $E_t(\mathbb{Q})$. Specialization of the parameter $t(u) = u^2 - u - 3$ gives the curve of genus two

$$C_1 : 4 - 4x + 4(-3 - u + u^2)x^2 + (-3 - u + u^2)^2x^2 + 4x^3 = 0,$$

which has the normal form

$$C_2 : Y^2 = (-5 - 2X - X^2)(11 + 34X + 7X^2 + 4X^3).$$

where

$$X = \frac{1 + ux - u^2x}{x - 1}, \quad Y = -4x + 8ux. \tag{3-2}$$

We define $\operatorname{Jac}(C_2)$ to be the Jacobian variety of the curve C_2 over $\mathbb{Q}$. The group $\operatorname{Jac}(C_2)(\mathbb{Q})$ of rational points of this variety has the torsion subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and 2-Selmer group $\operatorname{Sel}(\operatorname{Jac}(C_2)/\mathbb{Q})[2]$ over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (computed with the Magma commands TorsionSubgroup and TwoSelmerGroup). This enables us to perform a two-descent and compute that the rank $\operatorname{Jac}(C_2)(\mathbb{Q}) = 0$.

The only rational points on the curve C_2 might come from the torsion points of the Jacobian. We compute (with the Magma Chabauty0 procedure) that actually only the point at infinity is the rational point on C_2. The affine points on the curve C_1 come from the affine part of C_2 via the map defined in (3-2), except for the points $(x, u) = (1, \frac{1}{2}(1 \pm \sqrt{5}))$; hence there are only two rational points on C_1: the points at infinity (the parameter $u = \infty$ defines a singular curve). This shows that $E_{u^2-u-3}(\mathbb{Q})_{\text{tors}}[2] = \{\mathbb{O}\}$ for all $u \in \mathbb{Q}$ such that E_{u^2-u-3} is nonsingular.

Let $P = (x, y)$ be a 3-torsion point on the curve $y^2 + txy = x^3 + tx^2 - x + 1$. The condition $P = -2P$ implies that the pair (x, t) must satisfy the equation

$$C_3 : 1 - 4t - t^2 - 12x + 6x^2 - 4tx^3 - t^2x^3 - 3x^4 = 0.$$

The curve C_3 has genus two and has the normal form

$$C_4 : Y^2 = (1-X)(5+3X)(1+X^3),$$

where

$$X = x, \quad Y = \frac{2+t+2x^3+tx^3}{1-x}.$$

Similarly to the case of 2-torsion we compute that the rank of $\mathrm{Jac}(C_4)(\mathbb{Q})$ is zero because $\mathrm{Sel}(\mathrm{Jac}(C_4)/\mathbb{Q})[2] \cong \mathbb{Z}/8\mathbb{Z}$ and $\mathrm{Jac}(C_4)(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/8\mathbb{Z}$. We obtain four rational points on C_3: two at infinity, plus

$$(x,t) = \left(-\tfrac{5}{3}, -2\right) \quad \text{and} \quad (x,t) = (1,-2).$$

The parameter $t = -2$ gives a singular nodal curve; hence $E_t(\mathbb{Q})_{\mathrm{tors}}[3] = \{\mathbb{O}\}$, for all $t \in \mathbb{Q}$ such that E_t is nonsingular.

Let $P = (x, y) \in E_t(\mathbb{Q})$ be the point of order 4. The conditions $2P = -2P$ and $2P \neq \mathbb{O}$ imply that the pair (x,t) satisfies the equation

$$-14-8t-2t^2+8x-4tx+15t^2x+8t^3x+t^4x-10x^2+40tx^2+10t^2x^2 \\ +40x^3-10x^4+4tx^5+t^2x^5+2x^6=0,$$

which defines a curve of genus 3. From Faltings' theorem [1983] we see that for all but finitely many $t \in \mathbb{Q}$ groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$ cannot occur as torsion subgroups of $E_t(\mathbb{Q})$.

The cases of rational 5-torsion and 7-torsion do not generate hyperelliptic curves so we use again Faltings' theorem.

The condition $3P = -2P$ for $P = (x, y) \in E_t(\mathbb{Q})$ implies that the pair (x,t) lies on the curve of genus 13 given by

$$\begin{aligned}223&+140t-13t^2+40t^3+45t^4+12t^5+t^6-540x-480tx+200t^2x+160t^3x+20t^4x\\ &+190x^2+1680tx^2+900t^2x^2+240t^3x^2+30t^4x^2+1520x^3-820tx^3-685t^2x^3\\ &-560t^3x^3-270t^4x^3-60t^5x^3-5t^6x^3-1795x^4-120tx^4-430t^2x^4+440t^3x^4+455t^4x^4\\ &+120t^5x^4+10t^6x^4+696x^5+112tx^5+1372t^2x^5+736t^3x^5-124t^4x^5-244t^5x^5\\ &-95t^6x^5-16t^7x^5-t^8x^5-60x^6+720tx^6+420t^2x^6-840t^3x^6-705t^4x^6-180t^5x^6\\ &-15t^6x^6+240x^7+360tx^7-1350t^2x^7-720t^3x^7-90t^4x^7+105x^8-1140tx^8-285t^2x^8\\ &-380x^9+80tx^9+20t^2x^9+62x^{10}-16t^2x^{10}-8t^3x^{10}-t^4x^{10}-20tx^{11}-5t^2x^{11}-5x^{12}\\ &=0.\end{aligned}$$

The condition $4P = -3P$ for $P = (x, y) \in E_t(\mathbb{Q})$ implies that the pair (x,t) lies on a curve of genus 31 (equation omitted).

Applying the theorem of Faltings, we deduce that, for all but finitely many t, the rational 5-torsion and 7-torsion are trivial. Mazur's structure theorem now implies the statement of the lemma. □

Proof of Main Theorem. In order to prove Main Theorem we check if the appropriate points and their linear combinations belong to $2E_{(u^2-u-3)}(\mathbb{Q})$. Given a $\mathbb{Q}$-rational point $P=(x,y)$ on the curve $E_{(u^2-u-3)}$ over $\mathbb{Q}$ we have the following formula for the x-coordinate of the point $2P$:

$$x(2P)=\frac{4-2u+u^2+2u^3-u^4-8x+2x^2+x^4}{4-4x+(-3+2u-u^2-2u^3+u^4)x^2+4x^3}.$$

To simplify the notation, define:

$$P_{\varepsilon_1,\varepsilon_2,\varepsilon_3}=\varepsilon_1(0,1)+\varepsilon_2(1,1)+\varepsilon_3(u,u+1).$$

If for $u\in\mathbb{Q}$ there exists a rational point $\left(\frac{1}{9},y\right)$ on the curve $E_{(u^2-u-3)}$ and y is one of two possible values

$$y=\tfrac{1}{54}\left(9+3u-3u^2\pm\sqrt{2569+18u-9u^2-18u^3+9u^4}\right),$$

then we put

$$Q_{\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4}=\varepsilon_1(0,1)+\varepsilon_2(1,1)+\varepsilon_3(u,u+1)+\varepsilon_4\left(\tfrac{1}{9},y\right), \tag{3-3}$$

where $\varepsilon_i\in\{-1,0,1\}$.

The proof falls naturally into two parts. In the first part we establish the criteria for which the equations $P_{\varepsilon_1,\varepsilon_2,\varepsilon_3}=x(2P)$ and $Q_{\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4}=x(2P)$ have solutions in pairs of rational numbers (u,x) (recall that $P=(x,y)$ lies on $E_{(u^2-u-3)}$). In the second part of the proof we gather information to find the infinite subset of $\mathbb{Q}$ of parameters u for which the rank is at least 4. To use Lemma 3.1 we must consider the tuples $(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ in

$$\{(1,0,0),\ (0,1,0),\ (0,0,1),\ (1,1,0),\ (0,1,-1),\ (1,0,1),\ (1,1,1)\}. \tag{3-4}$$

Assume that $\left(\frac{1}{9},y\right)$ is $\mathbb{Q}$-rational. Consider $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4)$ in the set

$$\{(0,0,0,1),\ (1,0,0,1),\ (0,1,0,1),\\ (0,0,1,1),\ (1,1,0,1),\ (0,1,-1,1),\ (1,0,1,1),\ (1,1,1,1)\}.$$

The tuples with negative entries were chosen to lower the genera of corresponding curves. Since we work mod $2E_{(u^2-u-3)}(\mathbb{Q})$ the tuples can be chosen with a fair amount of freedom. We compute genera of curves using the *genus* command from the *algcurves* package in Maple 12. We consider in detail three specific cases.

$\boldsymbol{(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(1,0,0)}$. This tuple implies the equation

$$\frac{4-2u+u^2+2u^3-u^4-8x+2x^2+x^4}{4-4x+(-3+2u-u^2-2u^3+u^4)x^2+4x^3}=0. \tag{3-5}$$

Since (0, 1) is not the point at infinity, the denominator is nonvanishing and

$$4-2u+u^2+2u^3-u^4-8x+2x^2+x^4=0.$$

It defines an elliptic curve of rank 1. By means of the formulas

$$\begin{aligned} x_0 = \frac{1}{3(u^2-u-1)}(&12u^4-12u^3x-36u^3+12u^2x^2+30u^2x+35u^2 \\ &-12ux^3-24ux^2-42ux+61u+18x^3+6x^2+36x-113), \\ y_0 = -\frac{2}{u^2-u-1}(&8u^5-8u^4x-32u^4+8u^3x^2+28u^3x+44u^3-8u^2x^3-24u^2x^2 \\ &-39u^2x+9u^2+20ux^3+20ux^2+43ux-101u-19x^3-11x^2-54x+122), \end{aligned}$$

we can transform the equation into short Weierstrass form:

$$y_0^2 = x_0^3 + \tfrac{359}{3}x_0 + \tfrac{3130}{27}.$$

The Mordell–Weil group of this elliptic curve is generated by the point $\left(\frac{53}{3}, 88\right)$. Hence in the original form the generator is equal to $(u, x) = \left(\frac{1}{2}, \frac{1}{2}\right)$. The remaining cases for $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ in (3-4) are summarized in the first table below; the genera were computed with Maple.

ε_1	ε_2	ε_3	genus
1	0	0	1
0	1	0	3
0	0	1	2
1	1	0	3
0	1	−1	4
1	0	1	2
1	1	1	4

ε_1	ε_2	ε_3	ε_4	genus
0	0	0	1	5
1	0	0	1	9
0	1	0	1	13
0	0	1	1	19
1	1	0	1	13
0	1	−1	1	15
1	0	1	1	11
1	1	1	1	28

Now assume that we are given a rational point $\left(\frac{1}{9}, y\right)$ lying on the curve $E_{(u^2-u-3)}$ for a suitable $u \in \mathbb{Q}$.

$(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (0, 0, 0, 1)$. In this case

$$\frac{-u^4+2u^3+u^2-2u+x^4+2x^2-8x+4}{(u^4-2u^3-u^2+2u-3)x^2+4x^3-4x+4} = \frac{1}{9}. \tag{3-6}$$

This equation defines an affine curve of genus 5.

$(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (1, 0, 0, 1)$. Here we have

$$\frac{-u^4+2u^3+u^2-2u+x^4+2x^2-8x+4}{(u^4-2u^3-u^2+2u-3)x^2+4x^3-4x+4} = -9u^2+9u-162y+180. \tag{3-7}$$

From the equation of the curve $E_{(u^2-u-3)}$ we can find the formula

$$y = \tfrac{1}{54}(-3u^2+3u+v+9), \tag{3-8}$$

with $v = \pm\sqrt{2569+18u-9u^2-18u^3+9u^4}$. Using these relations we can assume that if a point (u, x) lies on the curve given by (3-7), it also lies on the curve

$$\begin{aligned}&9(9u^4-18u^3-9u^2+18u+2569)(u^4x^2-2u^3x^2-u^2x^2+2ux^2+4x^3-3x^2-4x+4)^2\\ &-(153u^4x^2+u^4-306u^3x^2-2u^3-153u^2x^2-u^2+306ux^2+2u-x^4\\ &\qquad\qquad\qquad\qquad\qquad\qquad +612x^3-461x^2-604x+608)^2=0.\end{aligned}$$

This curve has genus 9. The rest is computed in a similar way; the results are given in the second table on the previous page.

In the last step of the proof we show for which $u \in \mathbb{Q}$ the point $\left(\frac{1}{9}, y\right)$ is $\mathbb{Q}$-rational. By formula (3-8) $y \in \mathbb{Q}$ if and only if $2569+18u-9u^2-18u^3+9u^4$ is a full square. This condition defines the elliptic curve in a quartic form. It is birational to elliptic curve in the Weierstrass form:

$$y_0^2 = x_0^3-92835x_0+1389150. \tag{3-9}$$

The Mordell–Weil group of the curve has rank 2. The torsion subgroup is isomorphic to $\mathbb{Z}/2$. Generators of the free part are $(x_0, y_0) = (-309, -756)$, and $(x_0, y_0) = (390, -4950)$ and the generator of the torsion subgroup is $(15, 0)$. In the quartic form they correspond respectively to

$$\left(\tfrac{1}{9}, \tfrac{1369}{27}\right),\ \left(\tfrac{27}{10}, -\tfrac{5173}{100}\right),\ (-6, -133).$$

The birational map between models of elliptic curve provides a method to generate a suitable infinite set S of parameters $u \in \mathbb{Q}$ (see Section 4.2 for details). In fact $\{u \in \mathbb{Q} : \text{rank } (E_{(u^2-u-3)}(\mathbb{Q})) \geq 4\} \subset S$ and the difference between sets correspond precisely to the set of u-coordinates of rational points on the curves listed in the tables on the previous page. Except for the case $(\varepsilon_1, \varepsilon_2, \varepsilon_3) = (1, 0, 0)$, all curves have finitely many rational points due to Faltings' theorem. Consider the curve $E_t : y^2+txy = x^3+tx^2-x+1$, and assume the point $\left(\frac{1}{9}, y\right)$ on the curve E_t is $\mathbb{Q}$-rational. Solving the quadratic equation gives

$$y = \tfrac{1}{54}\left(-3t \pm \sqrt{2596+36t+9t^2}\right).$$

The point (0, 1) is a double in $E_t(\mathbb{Q})$ and $\left(\frac{1}{9}, y\right)$ is a rational point when there exists a triple $(t, x, s) \in \mathbb{Q}^3$ on

$$s^2 = 2596 + 36t + 9t^2, \quad 0 = 1 - 4t - t^2 - 8x + 2x^2 + x^4.$$

The parametrization of the first equation gives

$$t = \frac{2596 - f^2}{6f - 36}, \qquad s = \frac{f^2 - 12t + 2596}{2f - 12},$$

with a new parameter $f \in \mathbb{Q}\backslash\{6\}$. Substituting into the second equation gives the curve:

$$-6364096 - 62736f + 5084f^2 + 24f^3 - f^4 - 10368x + 3456fx - 288f^2x \\ + 2592x^2 - 864fx^2 + 72f^2x^2 + 1296x^4 - 432fx^4 + 36f^2x^4 = 0.$$

This curve has genus 3, so it has finitely many rational points by Faltings' theorem. Specializing to a parameter $t(u) = u^2 - u - 3$ we obtain that there are only finitely many $u \in \mathbb{Q}$ for which (0, 1) is a double in $E_{(u^2-u-3)}(\mathbb{Q})$ while $\left(\frac{1}{9}, y\right)$ is $\mathbb{Q}$-rational. So in fact the difference $S\backslash B$ is a finite set.

It remains to show that the j-invariant of the curve $E_t : y^2 + txy = x^3 + tx^2 - x + 1$ repeats itself for finitely many $t \in \mathbb{Q}$. We compute

$$j(E_t) = -\frac{(48 + t^2(4+t)^2)^3}{(2+t)^2(92 + (-1+t)t(4+t)(5+t))}. \tag{3-10}$$

Hence the equation

$$j(E_{t_1}) = j(E_{t_2})$$

defines an affine curve with coordinates (t_1, t_2) which has genus 11 according to computations in Maple. This implies that specializing the parameter t to $u^2 - u - 3$ gives a curve with finitely many rational points. □

4. Numerical results

4.1. ***General statistics.*** We show in Figure 1, left, the rank of the curves

$$y^2 + txy = x^3 + tx^2 - x + 1, \tag{4-1}$$

with positive integers $t < 230$. All computations were performed with Sage 3.4 [Stein et al. 2005] using the `mwrank` procedure. In some 6% of cases the value shown is conjectural, since it was not possible to prove an upper bound for the rank. Here is the percentage of curves of each rank:

rank	1	2	3	4	?
fraction	1%	41%	45%	7%	6%

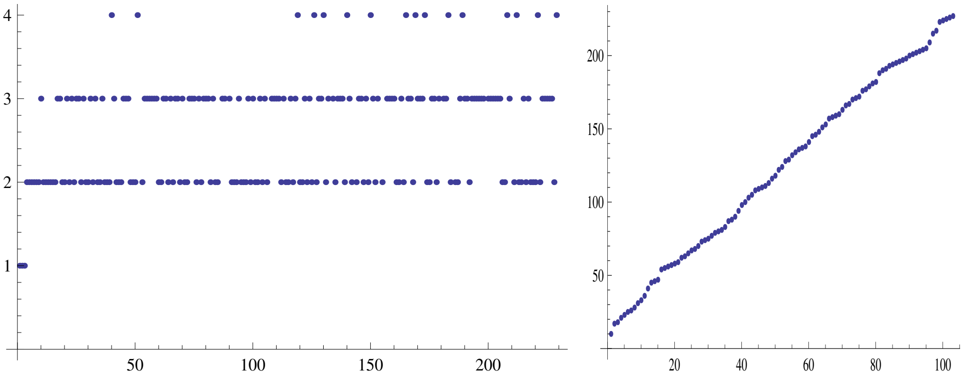

Figure 1. Left: Rank of curves of the form (4-1). Right: Growth of t for curves of rank 3 (abscissa: number of curves of rank 3 up to a certain t).

Also interesting is the plot of curves of rank 3 in Figure 1, right. It suggests that the progression for curves of rank 3 is almost linear, and hence that we can use the general algorithm from the introduction to state another version of the main Main Theorem and find many more infinite families of elliptic curves over $\mathbb{Q}$.

4.2. ***Explicit version of the main theorem.*** The statement of the theorem requires removing a finite subset of "bad rational points" due to Faltings' theorem (Mordell's conjecture). The upper bound of heights of this points is hard to obtain. We shall give an explicit and effective version of the main result of this paper. For rational points on the curve (1-2) with low height we can compute the explicit table of corresponding elliptic curves $E_{(u^2-u-3)}$ over $\mathbb{Q}$ of rank at least 4. The curve

$$C_1 : y_0^2 = x_0^3 - 92835x_0 + 1389150 \tag{4-2}$$

is mapped to the curve

$$C_2 : 2569 + 18u - 9u^2 - 18u^3 + 9u^4 = v^2 \tag{4-3}$$

via the map

$$\phi : C_1 \to C_2,$$

where $\phi(x_0, y_0) = (u, v)$ is given by the formulas

$$u = \frac{565605 + x_0(-948 + 7x_0) + 266y_0}{(-1551 + x_0)(45 + x_0)},$$

$$v = \frac{1}{(-1551 + x_0)^2(45 + x_0)^2}\big(133(92385 + (-30 + x_0)x_0)(-115425 + x_0(1536 + x_0)) \\ +234(-3922935 + x_0(9010 + 41x_0))y_0\big);$$

the map is defined at each of the points $(-45, 2340)$, $(-45, -2340)$, $(1551, 59904)$, $(1551, -5990)$, and ∞_{C_1}:

$$\phi(-45, 2340) = \phi(1551, 59904) = \infty_{C_2}, \quad \phi(\infty_{C_1}) = (7, 133),$$
$$\phi(-45, -2340) = \big(-\tfrac{10898}{5187}, -\tfrac{477412081}{8968323}\big), \quad \phi(1551, -59904) = \big(\tfrac{16085}{5187}, \tfrac{477412081}{8968323}\big),$$

Here ∞_{C_1} is the point at infinity on C_1 and analogously for C_2. The map is regular at every point of C_1, so it is a morphism of curves. The inverse mapping is

$$\psi : C_1 \to C_2,$$

where $\psi(u, v) = (x_0, y_0)$ is given by

$$x_0 = \frac{5117 - 948u + 753u^2 + 266v}{(-7+u)^2},$$
$$y_0 = \frac{266\big(5201 + 9u(-4 + u(-22 + 13u))\big) + 2(1799 + 4797u)v}{(-7+u)^3},$$

which is not regular at the point ∞_{C_2} and is defined at the points $(7, 133)$ and $(7, -133)$:

$$\psi(7, 133) = \infty_{C_1}, \quad \psi(7, -133) = \big(-\tfrac{3628425}{17689}, \tfrac{8081948160}{2352637}\big).$$

With the notation $A = C_1 \backslash \{(-45, 2340), (1551, 59904)\}$, $B = C_2 \backslash \{\infty_{C_2}\}$, we have

$$\phi \circ \psi = \mathrm{id}_A, \quad \psi \circ \phi = \mathrm{id}_B\ .$$

We now give an explicit table of curves of rank at least 4 as stated in the Main Theorem. If we assume the parity conjecture we can show that some of them have actually the rank at least 5. Let

$$E_{(u^2-u-3)} : y^2 + (u^2 - u - 3)xy = x^3 + (u^2 - u - 3)x^2 - x + 1,$$

and $P_1 = (-309, 756)$, $P_2 = (-45, 2340)$, $T = (15, 0)$ — the points spanning the group $C_1(\mathbb{Q})$. From the computations above we can associate uniquely a pair (u, v) on C_2 corresponding to the point $\alpha T + \beta_1 P_1 + \beta_2 P_2$. We abbreviate this as $(u, v) \leftrightarrow (\alpha, \beta_1, \beta_2)$. We define the following functions:

- $R(u)$ is the regulator of the points
$$(0, 1),\ (1, 1),\ (u, u+1),\ \big(\tfrac{1}{9}, \tfrac{1}{54}(9 + 3u - 3u^2 + v)\big);$$
- $N(u)$ is the conductor of the curve $E_{(u^2-u-3)}$;
- $j(u)$ is the j-invariant of $E_{(u^2-u-3)}$;
- $w(u)$ is equal to the global root number $w(E_{(u^2-u-3)}/\mathbb{Q})$.

All the computations were performed for the minimal model of each curve.

For the last tuple the regulator is equal to 0 because the tuple corresponds to $u=\frac{1}{9}$ for which the fourth point from the statement of the Main Theorem coincides with the third point. For the tuple $(0,-1,1)$ (when $u=8/9$) the fourth point is linearly dependent on the other three points. Moreover the curves corresponding to these tuples are isomorphic over $\mathbb{Q}$.

Remark. We can find in the family $E_{(u^2-u-3)}$ curves of unconditional rank at least five. The curve $E_{239}: y^2+239xy=x^3+239x^2-x+1$ is a curve of unconditional rank five. The set of generators of the nontorsion part is given by

$$(0,1),\ (1,1),\ (16,17),\ \left(-\tfrac{14}{25},\tfrac{16661}{125}\right),\ \left(\tfrac{52}{81},\tfrac{469}{729}\right).$$

We can show that for $c=-\frac{14}{25}$ the associated auxiliary elliptic curve from the Main Theorem,

$$4-4c-3c^2+4c^3+2c^2u-c^2u^2-2c^2u^3+c^2u^4=w^2,$$

has rank 4 over $\mathbb{Q}$. Applying the technique of the proof of the Main Theorem we can actually prove a similar result to the one stated there. Precisely, we would have

α	β_1	β_2	$R(u)$	$N(u)$	$j(u)$	$W(u)$	rank
0	−2	−2	253637.08	7.42×10^{117}	−4382.17	−1	≥ 5
0	−2	−1	53400.57	4.79×10^{79}	-1.39×10^{6}	1	≥ 4
0	−2	0	16681.20	5.69×10^{59}	-4.14×10^{11}	−1	≥ 5
0	−2	1	23528.39	1.89×10^{64}	-1.11×10^{16}	1	≥ 4
0	−1	−2	117347.77	1.22×10^{95}	-4.66×10^{19}	1	≥ 4
0	−1	−1	6398.35	2.46×10^{46}	-7.42×10^{8}	1	≥ 4
0	−1	0	28.40	4.13×10^{12}	−1255.79	1	≥ 4
0	−1	1	0	6.54×10^{11}	−1264.95	1	–
0	0	−2	138113.04	6.46×10^{98}	−912.11	−1	≥ 5
0	0	−1	4697.68	1.21×10^{43}	−20742.18	1	≥ 4
0	0	0	8.61	57482738.0	-4.72×10^{9}	1	≥ 4
0	1	−2	608830.99	3.64×10^{145}	-4.45×10^{19}	1	≥ 4
0	1	−1	56796.71	1.80×10^{81}	-3.75×10^{10}	−1	≥ 5
0	1	0	1301.45	8.98×10^{31}	−200862.89	−1	≥ 5
0	1	1	0	6.54×10^{11}	−1264.95	1	–

Table 2. Curves of rank 4 and 5. See previous page for the meaning of the columns.

four linearly independent points for infinitely many rational parameters $u \in \mathbb{Q}$:

$$(0,1),\ (1,1),\ (u,u+1),\ \bigl(-\tfrac{14}{25},\tfrac{1}{125}(-105-35u+35u^2+v)\bigr),$$

where

$$v^2 = 17956+2450u-1225u^2-2450u^3+1225u^4.$$

Acknowledgments

The author thanks Wojciech Gajda for suggesting the problem; Sebastian Petersen, for helpful comments concerning root numbers and the parity conjecture; and Adam Lipowski, for the computational resources supporting Sage 3.4 [Stein et al. 2005]. The author also thanks the referee for several helpful suggestions on the mathematical content of the paper and the exposition.

References

[Brown and Myers 2002] E. Brown and B. T. Myers, "Elliptic curves from Mordell to Diophantus and back", *Amer. Math. Monthly* **109**:7 (2002), 639–649. MR 2003d:11080 Zbl 1083.11037

[Elkies 2007] N. D. Elkies, "Three lectures on elliptic surfaces and curves of high rank", preprint, 2007. arXiv 0709.2908

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. Erratum in **75** (1984), 381. MR 85g:11026a Zbl 0588.14026

[Kihara 1997] S. Kihara, "On an infinite family of elliptic curves with rank $\geq$ 14 over $\mathbf{Q}$", *Proc. Japan Acad. Ser. A Math. Sci.* **73**:2 (1997), 32. MR 98d:11059 Zbl 0906.11023

[Kowalski 2007] E. Kowalski, *Elliptic curves, rank in families and random matrices*, edited by J. B. Conrey et al., London Math. Soc. Lecture Note Series **341**, Cambridge University Press, 2007. MR 2008j:11073

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Mestre 1991] J.-F. Mestre, "Courbes elliptiques de rang $\geq$ 12 sur $\mathbf{Q}(t)$", *C. R. Acad. Sci. Paris Sér. I Math.* **313**:4 (1991), 171–174. MR 92m:11052 Zbl 0749.14026

[Nagao 1994] K.-i. Nagao, "An example of elliptic curve over $\mathbf{Q}(T)$ with rank $\geq$ 13", *Proc. Japan Acad. Ser. A Math. Sci.* **70**:5 (1994), 152–153. MR 95e:11064 Zbl 0848.14015

[Rohrlich 1994] D. E. Rohrlich, "Elliptic curves and the Weil–Deligne group", pp. 125–157 in *Elliptic curves and related topics*, edited by H. Kisilevsky and M. R. Murty, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994. MR 95a:11054 Zbl 0852.14008

[Rubin and Silverberg 2007] K. Rubin and A. Silverberg, "Twists of elliptic curves of rank at least four", pp. 177–188 in *Ranks of elliptic curves and random matrix theory*, edited by J. B. Conrey et al., London Math. Soc. Lecture Note Ser. **341**, Cambridge Univ. Press, 2007. MR 2008e:11065 Zbl 05190710

[Shioda 1990] T. Shioda, "On the Mordell–Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240. MR 91m:14056 Zbl 0725.14017

[Silverberg 2007] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*, edited by J. B. Conrey et al., London Math. Soc. Lecture Note Series **341**, Cambridge University Press, 2007. MR 2008c:11087

[Silverman 1983] J. H. Silverman, “Heights and the specialization map for families of abelian varieties”, *J. Reine Angew. Math.* **342** (1983), 197–211. MR 84k:14033 Zbl 0505.14035

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Stein et al. 2005] W. Stein et al., Sage open-source mathematical software system, 2005, available at http://sagemath.org.

Received: 2010-01-30 Revised: 2010-08-25 Accepted: 2010-09-04

bartnas@amu.edu.pl *Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland*

involve

pjm.math.berkeley.edu/involve

PRODUCTION

Silvio Levy, Scientific Editor Sheila Newbery, Senior Production Editor Cover design: ©2008 Alex Scorpan

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2010 is US $100/year for the electronic version, and $120/year (+$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://www.mathscipub.org
A NON-PROFIT CORPORATION
Typeset in LaTeX

involve

2010 vol. 3 no. 3

1944-4176(2010)3:3;1-E