Proc. Indian Acad. Sci. (Math. Sci.) (2018) 128:54
https://doi.org/10.1007/s12044-018-0433-0

On the family of elliptic curves $y^2 = x^3 - m^2x + p^2$

ABHISHEK JUYAL and SHIV DATT KUMAR*

Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad 211 004, India
*Corresponding author.
E-mail: abhinfo1402@gmail.com; sdt@mnnit.ac.in

MS received 2 February 2017; revised 17 July 2017; accepted 5 October 2017; published online 25 October 2018

Abstract. In this paper, we study the torsion subgroup and rank of elliptic curves for the subfamilies of $E_{m,p} : y^2 = x^3 - m^2x + p^2$, where m is a positive integer and p is a prime. We prove that for any prime p, the torsion subgroup of $E_{m,p}(\mathbb{Q})$ is trivial for both the cases $\{m \geq 1,\ m \not\equiv 0 \pmod 3\}$ and $\{m \geq 1,\ m \equiv 0 \pmod 3$, with $gcd(m, p) = 1\}$. We also show that given any odd prime p and for any positive integer m with $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod{32}$, the lower bound for the rank of $E_{m,p}(\mathbb{Q})$ is 2. Finally, we find curves of rank 9 in this family.

Keywords. Elliptic curve; rank; torsion subgroup.

2010 Mathematics Subject Classification. 11G05.

1. Introduction

Brown and Myers [2] constructed an infinite family $E_m : y^2 = x^3 - x + m^2$ of elliptic curves over $\mathbb{Q}$ with quadratic growth of parameter and the rank of the Mordell–Weil group at least two. Antoniewicz [1] produced another family of elliptic curves $C_m : y^2 = x^3 - m^2x + 1$ over $\mathbb{Q}$ with the rank of Mordell–Weil group at least three. Ekinberg [4], in his Ph.D. thesis, studied the families E_m and C_m and found some subfamilies of E_m and C_m of high rank. He also considered the family $D_m : y^2 = x^3 - m^2x + m^2$, and has shown that the Mordell–Weil rank of D_m is 2 over $\mathbb{Q}(m)$ with generators (m, m), $(0, m)$. Petra Tadić carried out an interesting study of previously mentioned families E_m and C_m over function fields. In [15], Tadić proved that the torsion subgroup of $C_m : y^2 = x^3 - m^2x + 1$ over the function field $\mathbb{C}(m)$ is trivial, and rank of C_m is 3 and 4 over the function fields $\mathbb{Q}(m)$ and $\mathbb{C}(m)$ respectively. Furthermore, Tadić derived a parametrization of C_m of rank at least four over the function field $\mathbb{Q}(a, i, s, n, k)$, where $s^2 = i^3 - a^2i$. Tadić [14] found a subfamily of elliptic curves E_m having rank ≥ 3 over the function field $\mathbb{Q}(a, i, s, n, k, l)$, where $s^2 = i^3 + a^2$. Additionally, Tadić applied the results of [14] to prove the existence of two more families; the first with ranks ≥ 3 and ≥ 4 over the field of rational functions in four variables and the second is a family of rank ≥ 5 parametrized by an elliptic curve of positive rank.

It is of particular interest to specifically study the family $E_{m,p} : y^2 = x^3 - m^2x + p^2$ of elliptic curves parametrized by two rational parameters. The work of Brown–Myers and Antoniewicz [1,2] is the source of inspiration for the problem of the presented work and methodology developed in this article. The main object of this paper is to prove the following results.

Theorem 1.1. *Let*

$$E_{m,p} : y^2 = x^3 - m^2x + p^2,$$

be a family of elliptic curves, where p is a prime number and m is a positive integer. Then

$$\text{Tors } E_{m,p}(\mathbb{Q}) = \{\mathcal{O}\}$$

if

(1) $m \not\equiv 0 \pmod 3$,
(2) $m \equiv 0 \pmod 3$ *and* $gcd(m, p) = 1$.

Theorem 1.2. *Let*

$$E_{m,p} : y^2 = x^3 - m^2x + p^2$$

be a family of elliptic curves, where m is a positive integer such that $m \not\equiv 0 \pmod 3$ *and* $m \equiv 2 \pmod{32}$ *with p an odd prime. Then*

$$\text{Rank } E_{m,p}(\mathbb{Q}) \geq 2.$$

Before we proceed for the proof of the above stated theorems, in the next section we develop necessary background material needed for better exposition and clarity of presentation in this paper.

2. Preliminaries: Notations, definitions and related known results

In reference to the notional convention, throughout this article, we denote the families of elliptic curves $y^2 = x^3 - m^2x + p^2$ by $E_{m,p}$. For the convenience of the reader, we describe some related material from [13] that includes some basic concepts of elliptic curves over rational field $\mathbb{Q}$ and well-known results.

An elliptic curve over the field $\mathbb{Q}$ of rational numbers is a curve E defined by a Weierstrass equation

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$, and

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

In other words, the above condition is equivalent to the cubic equation $x^3 + ax + b = 0$, having three distinct complex roots. In essence, an elliptic curve E can be thought of as a curve in projective space $\mathbb{P}^2$, with homogeneous equation $y^2z = x^3 + axz^2 + bz^3$ and a point, namely [0, 1, 0], at 'infinity' which we denote by ∞. Note that all the vertical lines meet at the point ∞. Let

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

One can define the law of addition for the points on the elliptic curve which, in literature, is known as chord-tangent law of addition (for details, see [13]). The set of all points of an elliptic curve E forms an abelian group, of which $E(\mathbb{Q})$ is a subgroup. In particular, the point at ∞ is the identity element and inverse of $A = (x, y) \in E(\mathbb{Q})$ is $-A := (x, -y)$.

The fundamental Mordell theorem [9] says that the group $E(\mathbb{Q})$ of all rational points of an elliptic curve E is a finitely generated abelian group, which means that

$$E(\mathbb{Q}) = \mathbb{Z}^r + \text{Tors } E(\mathbb{Q}),$$

where r is an uniquely determined non-negative integer called the rank of elliptic curve and Tors $E(\mathbb{Q})$ is the finite abelian group consisting of all elements of finite order in $E(\mathbb{Q})$.

The torsion subgroup of $E(\mathbb{Q})$ is 'well-understood'. Nagell–Lutz theorem [6,11] and Mazur theorem [7] gave complete classification of a torsion subgroup of an elliptic curve over the rational field. The notion of the rank of an elliptic curve has been studied. However, its characterization is, in general, a difficult task. A primary reason of this difficulty is that the rank can not be obtained effectively from the coefficients a, b of the curve's equation. Now in search of either an exact rank of $E(\mathbb{Q})$ or a lower bound on rank of $E(\mathbb{Q})$, in literature, plenty of computational ways have been developed, many of them being either computationally complex or exploit heavy mathematical machinery.

3. Torsion subgroup of $E_{m,p}$

In this section, our main aim is to prove Theorem 1.1. A technique that we use here is to reduce $E_{m,p}$ over finite fields. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, where $a, b \in \mathbb{Z}$. For a given prime p, E is treated as a 'curve' over the finite field $\mathbb{F}_p$, where $a, b, x, y \in \mathbb{F}_p$. Let $\Delta(E) = -16(4a^3 + 27b^2)$ be the discriminant of elliptic curve E. Now if $p \nmid \Delta(E)$, then the roots of cubic equation $x^3 + ax + b$ are all distinct and in that case E becomes an elliptic curve over $\mathbb{F}_p$. Essentially this is an instance when one says that at p, E has a good reduction and $E(\mathbb{F}_p)$ is known as the group of $\mathbb{F}_p$-points of E. Now given a good reduction of E at p, the application of Theorem 3.1 gives an injective map from the group of rational torsion points Tors $E(\mathbb{Q})$ into the group $E(\mathbb{F}_p)$.

The following theorem and lemmas will be the main ingredients for proving Theorem 1.1.

Theorem 3.1 ([5], Theorem 5.1). *The restriction of the reduction homomorphism* $r_{p|\text{Tors } E(\mathbb{Q})} : \text{Tors } E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$ *is injective for any odd prime* p, *where* E *has a good reduction and* $r_{2|\text{Tors } E(\mathbb{Q})} : \text{Tors } E(\mathbb{Q}) \longrightarrow E_2(\mathbb{F}_2)$ *has kernel at most* $\mathbb{Z}/2\mathbb{Z}$ *when* E *has a good reduction at* 2.

Lemma 3.2. *There is no point of order two in $E_{m,p}(\mathbb{Q})$ for every positive integer m and every prime p.*

Proof. Let $A = (x, y)$ be a point in $E_{m,p}(\mathbb{Q})$ of order two. Then $2A = 0 \Leftrightarrow A = -A \Leftrightarrow y = 0$ and $x \neq 0$. Thus

$$x^3 - m^2x + p^2 = 0.$$

Since A has finite order, x must be an integer (by Nagell–Lutz theorem). Therefore the above equation gives

$$m^2 = x^2 + \frac{p^2}{x},$$

which implies that $x \in \{\pm 1, \pm p, \pm p^2\}$. Hence $m^2 \in \{1 \pm p^2, p^2 \pm p, p^4 \pm 1\}$, which contradicts that m is an integer. □

By doubling a point on the elliptic curve, we mean adding the point to itself (see [13]). On $E_{m,p}$, if $P = (x, y)$ is any point, then by the addition law, we get the doubling of P, denoted $2P = (x', y')$, and is given by

$$x' = \frac{x^4 + 2m^2x^2 + m^4 - 8xp^2}{4(x^3 - m^2x + p^2)} \tag{1}$$

and

$$y' = -y - \frac{3x^2 - m^2}{2y}(x' - x). \tag{2}$$

Lemma 3.3. *$E_{m,p}(\mathbb{Q})$ does not contain any point of order 3 for any positive integer m with $m \not\equiv 0 \pmod 3$ and for any prime p.*

Proof. Assume, on the contrary that, there exists a point $A = (x, y) \in E_{m,p}(\mathbb{Q})$ such that $3A = \mathcal{O} \Leftrightarrow 2A = -A \Leftrightarrow x$-coordinate of $2A = x$-coordinate of A. Therefore

$$\frac{x^4 + 2x^2m^2 + m^4 - 8xp^2}{4(x^3 - m^2x + p^2)} = x,$$

equivalently

$$3x^4 - 6m^2x^2 + 12p^2x - m^4 = 0. \tag{3}$$

If $m \not\equiv 0 \pmod 3$, then under modulo 3, equation (3) has no solution, which implies that equation (3) has no rational solution. Thus $E_{m,p}(\mathbb{Q})$ has no point of order 3 for $m \not\equiv 0 \pmod 3$ and for any prime p. □

Lemma 3.4. *$E_{m,p}(\mathbb{Q})$ does not contain a point of order* 3 *for any positive integer m with $m \equiv 0 \pmod 3$, and for any prime p with $\gcd(m, p) = 1$.*

Proof. The initial part of the proof of this lemma is quite similar to the proof of Lemma 3.3 till equation (3). From equation (3), it is clear that $x|m^4$. Now here two cases arise:

Case 1. *When $x \equiv 0 \pmod 3$.* Suppose the prime factorization of x contains 3^a and the prime factorization of m contains 3^b. Then it is clear that $b \geq a$. Now, write equation (3) as

$$3^{4a+1}(a_1) - 3^{2b+a+1}(a_2) + 3^{a+1}(a_3) - 3^{4b}(a_4) = 0, \tag{4}$$

where a_1, a_2, a_3 and a_4 are some integers. Under modulo $3^{(a+2)}$, (4) has no solution which implies that (3) too has no rational solution.

Case 2. *When $x \not\equiv 0 \pmod 3$.* Equation (3) can be written as

$$(m^2)^2 + (6x^2)m^2 - (3x^4 + 12p^2x) = 0, \tag{5}$$

which is quadratic in m^2 with discriminant

$$\Delta = 48x(x^3 + p^2).$$

Equation (5) also gives

$$m^2 = \frac{-6x^2 + \sqrt{\Delta}}{2},$$

a further simplification leads to $\Delta = (2m^2 + 6x^2)^2$. By comparing both values of Δ, we get

$$(2m^2 + 6x^2)^2 = 48x(x^3 + p^2). \tag{6}$$

Equation (6) implies that there exists $n \in \mathbb{N}$ such that $x(x^3 + p^2) = 3n^2$. Now $\gcd(x, x^3 + p^2) = 1$ or p or p^2. If $\gcd(x, x^3 + p^2) = p$ or p^2, then from (3), $p|m$ contradicts that $\gcd(m, p) = 1$. Therefore, $\gcd(x, x^3 + p^2) = 1$ and we can factor the right-hand side of equation (6) as

Case (*a*).

$$\begin{cases} x = \alpha^2, \\ x^3 + p^2 = 3\beta^2, \end{cases}$$

or

Case (*b*).

$$\begin{cases} x = 3\alpha^2, \\ (\alpha^3)^2 + p^2 = 3\beta^2. \end{cases}$$

Case (a) can be rewritten as

$$(\alpha^3)^2 + p^2 = 3\beta^2. \tag{7}$$

Since equation (7) has no solution under modulo 3, hence equation (3) too has no rational solution. Given that $x \not\equiv 0 \pmod 3$, Case (b) is impossible. Hence we conclude that $E_{m,p}(\mathbb{Q})$ does not have a point of order 3 for $m \equiv 0 \pmod 3$, and for any prime p with $\gcd(m, p) = 1$. □

We are now equipped with much of the needed machinery and ready to prove Theorem 1.1.

Proof of Theorem 1.1. We split the proof into two cases which together complete the proof of this theorem.

Case 1. *When* $p \neq 5$. In this case, $5 \nmid \Delta = -16(-4m^6 + 27p^4)$, hence $E_{m,p}$ has a good reduction at 5. Reducing $E_{m,p}$ over $\mathbb{F}_5$, results in the following:

(i) If $p^2 \equiv 1 \pmod 5$. Depending upon whether $m^2 \equiv 0, 1$ or $4 \pmod 5$, $E_{m,p}$ reduces to $y^2 = x^3+1$, $y^2 = x^3-x+1$, $y^2 = x^3-4x+1$ respectively with the corresponding cardinality of $E_{m,p}(\mathbb{F}_5)$ being 6, 8, 9.

(ii) If $p^2 \equiv 4 \pmod 5$. $E_{m,p}$ reduces to $y^2 = x^3+4$, $y^2 = x^3-x+4$, $y^2 = x^3-4x+4$ according to $m^2 \equiv 0, 1$ or $4 \pmod 5$ respectively with the corresponding cardinality of $E_{m,p}(\mathbb{F}_5)$ being 6, 8, 9.

An application of Theorem 3.1 and Lagrange theorem, furnishes the complete list of possible orders of Tors $E_{m,p}(\mathbb{Q})$ as 1, 2, 3, 6, 8 and 9 only. Lemmas 3.2, 3.3 and 3.4 guarantee that the curve $E_{m,p}$ does not have points of order 2 and 3. Thus we conclude that Tors $E_{m,p}(\mathbb{Q}) = \{\mathcal{O}\}$.

Case 2. When $p = 5$. Note that $3 \nmid \Delta$ and $7 \nmid \Delta$, hence $E_{m,5} : y^2 = x^3 - m^2x + 25$ has good reductions at 3 and 7. Reducing $E_{m,p}$ over $\mathbb{F}_3$ and $\mathbb{F}_7$, we have

(iii) Over $\mathbb{F}_3$, we get $E_{m,5} : y^2 = x^3 + 1$ or $y^2 = x^3 - x + 1$, depending upon whether $m^2 \equiv 0$ or $1 \pmod 3$ and in that case the corresponding cardinality of $E_{m,5}(\mathbb{F}_3)$ is 4 and 7 respectively. Thus in this case, we have $|\text{Tors } E_{m,5}(\mathbb{Q})| = 1, 2, 4$ or 7 of which the only probable values are 1 and 7 because of Lemma 3.2.

(iv) Over $\mathbb{F}_7$, we get $y^2 = x^3 + 4$, $y^2 = x^3 - x + 4$, $y^2 = x^3 - 2x + 4$ or $y^2 = x^3 - 4x + 4$ according as $m^2 \equiv 0, 1, 2$, or $4 \pmod 7$ respectively, with the cardinality of $E_{m,5}(\mathbb{F}_7)$ being 3, 10, 10, 10 respectively. Thus the possible values for the cardinality of Tors $E_{m,p}(\mathbb{Q})$ are 1, 2, 3, 5 or 10 of which 2, 3 and 10 are again not possible by the same reasoning as in the previous cases. Thus $|\text{Tors } E_{m,p}(\mathbb{Q})| = 1$ or 5.

The two subcases (iii) and (iv) together imply that 5 and 7 cannot be the cardinality of Tors $E_{m,p}(\mathbb{Q})$ because in the former case, all the non-trivial points must have order 5, whereas the same in the latter case would be 7, leading to a contradiction. We thus conclude that Tors $E_{m,p}(\mathbb{Q}) = \{\mathcal{O}\}$. □

Remark. The condition $\gcd(m, p) = 1$ has been imposed in the proof of Theorem 1.1 because we have an example of an elliptic curve, namely $y^2 = x^3 - 9x + 9$, which has its torsion subgroup isomorphic to $\mathbb{Z}_3$. However, we did not find any other example for which the torsion subgroup is non-trivial.

4. The rank of $E_{m,p}$

In this section, we produce a subfamily of minimum rank 2. To achieve this, it is sufficient to find at least two independent points, say $A_{m,p}$ and $B_{m,p}$ on each curve in $E_{m,p}$.

First, we note that the point $B_{m,p} = (m, p)$ lies on every curve $E_{m,p}$ and the x-coordinate of $2B_{m,p}$ is $(m^4 - 2mp^2)/p^2$. Thus if $\gcd(m, p) = 1$, then the order of $B_{m,p}$ is infinite, and hence we get a subfamily of $E_{m,p}$ of rank at least one. To get a subfamily of minimum rank two, we will use the following result.

Theorem 4.1 ([3], p. 78). *Let $E(\mathbb{Q})$ (respectively $2E(\mathbb{Q})$) be the group of rational points (respectively, double of rational points) on an elliptic curve E, and suppose E has trivial rational torsion. Then the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is an elementary abelian 2-group of order 2^r, where r is the rank of $E(\mathbb{Q})$.*

On each curve in $E_{m,p}$, one can find the obvious points namely,

$$A_{m,p} = (0, p),\ B_{m,p} = (m, p).$$

We will now construct a subfamily of $E_{m,p}$ for which the above two points will be linearly independent. We first prove few results which will help us in achieving this.

Lemma 4.2. *Let $A = (x', y')$ and $B = (x, y)$ be points in $E_{m,p}(\mathbb{Q})$ such that $A = 2B$ and $x' \in \mathbb{Z}$. Then*

(1) $x \in \mathbb{Z}$,
(2) $x \equiv m \pmod 2$.

Proof. Substituting $x = \frac{u}{s}$, $\gcd(u, s) = 1$ in (1) and after simplifying, we get

$$(m^4 - 4p^2x')s^4 + (4m^2x' - 8p^2)us^3 + 2m^2u^2s^2 - 4x'u^3s + u^4 = 0. \tag{8}$$

From (8), it is clear that $s|u^4$, so $s \in \{-1, 1\}$, and hence $x \in \mathbb{Z}$.

Again, we can write equation (1) as

$$(x^2 + m^2)^2 = 4(x'(x^3 - m^2x + p^2) + 2xp^2),$$

which implies that $2|(x^2 + m^2)$, i.e., $x \equiv m \pmod 2$. □

Lemma 4.3. *The point $A_{m,p} = (0, p)$ is an element of $E_{m,p}(\mathbb{Q}) \setminus 2E_{m,p}(\mathbb{Q})$ for any positive integer m with $m \equiv 2 \pmod{32}$ and any odd prime p.*

Proof. Suppose $A_{m,p} = 2C$ for some $C = (x, y) \in E_{m,p}(\mathbb{Q})$. Then we have

$$\frac{x^4 + 2m^2x^2 + m^4 - 8xp^2}{4(x^3 - m^2x + p^2)} = 0$$

or

$$x^4 + 2m^2x^2 + m^4 - 8xp^2 = 0. \tag{9}$$

The simplification of the above equation leads to

$$(x^2 + m^2)^2 = 8xp^2. \tag{10}$$

From equation (10), we observe that $x = 2k^2$ for some $k \in \mathbb{Z}$, i.e., x is an even number. Substituting the value of x in equation (9), we get

$$16k^8 + 8m^2k^4 + m^4 - 16k^2p^2 = 0. \tag{11}$$

It follows that for any integer k, under modulo 32, equation (11) has no solution. Consequently, equation (11) has no rational solution. Therefore, $A_{m,p} \notin 2E_{m,p}$. □

Lemma 4.4. *The point* $B_{m,p} = (m, p)$ *is an element of* $E_{m,p}(\mathbb{Q}) \setminus 2E_{m,p}(\mathbb{Q})$ *for any positive integer* m *with* $m \equiv 2 \pmod 4$ *and for any prime* p.

Proof. Suppose $B_{m,p} = (m, p) = 2C$ for some $C = (x, y) \in E_{m,p}(\mathbb{Q})$. Then

$$\frac{x^4 + 2m^2x^2 + m^4 - 8xp^2}{4(x^3 - m^2x + p^2)} = m.$$

Simplifying it, we get

$$x^4 - 4mx^3 + 2m^2x^2 + (4m^3 - 8p^2)x + m^4 - 4p^2m = 0,$$

which can be rewritten as

$$(x - m)^4 - 4(x - m)^2m^2 - 8(x - m)p^2 - 12p^2m + 4m^4 = 0. \tag{12}$$

Taking Lemma 4.2 into consideration, we substitute $x - m = 2s$, which results in simplification of (12) as

$$(2s^2 - m^2)^2 = (4s + 3m)p^2.$$

The above equation holds only if $(4s+3m) = w^2$ for some $w \in \mathbb{Z}$. Since $m \equiv 2 \pmod 4$, $4s + 3m \equiv 2 \pmod 4$ leads to a contradiction that it is a perfect square. This completes the proof. □

Lemma 4.5. *The point* $A_{m,p} + B_{m,p} = (-m, p)$ *is an element of* $E_{m,p}(\mathbb{Q}) \setminus 2E_{m,p}(\mathbb{Q})$ *for any positive integer* m *with* $m \equiv 2 \pmod 4$ *and for any prime* p.

Proof. With arguments similar to Lemma 4.4, we can say that $A_{m,p} + B_{m,p} = (-m, p) \notin 2E_{m,p(\mathbb{Q})}$ for $m \equiv 2 \pmod 4$ and for any prime p. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. To show that Rank $E_{m,p}(\mathbb{Q}) \geq 2$, we first claim that $H = \{[\mathcal{O}], [A_{m,p}], [B_{m,p}], [A_{m,p}] + [B_{m,p}]\}$ is a subgroup of $E_{m,p}/2E_{m,p}$ of order 4, for the values

Table 1. Ranks of some $E_{m,p}$:$y^2 = x^3 - m^2x + p^2$.

Rank	$[m, p]$
7	[4, 1931][8, 3299], [13, 7589], [17, 2003], [37, 1481], [53, 2087], [79, 2713], [89, 4933], [92, 4591], [107, 1427], [107, 3257], [118, 2309], [121, 3613], [134, 3109], [157, 811], [167, 1559], [172, 1811], [181, 1709], [182, 881], [188, 2063], [188, 5737], [194, 1721], [197, 2393], [202, 467], [206, 1699], [218, 1481], [233, 1669], [245, 4799], [248, 2311], [248, 8861], [257, 1597], [278, 2521], [312, 1063], [332, 5167], [338, 3877], [342, 593], [353, 911], [312, 1063], [332, 5167], [338, 3877], [342, 593], [353, 911], [356, 4363], [382, 4871], [409, 5503], [419, 2801], [443, 6917], [444, 5669], [476, 6833], [479, 5503], [482, 3457], [485, 2633], [488, 5113], [602, 8861], [624, 9649], [713, 7589], [1033, 1151], [1123, 9029], [1194, 2683], [1204, 8081], [1237, 2063], [1431, 5167], [1226, 2633], [2077, 8389], [3787, 9281], [8321, 8377], [4649, 1453],
8	[58, 8581], [278, 9437], [461, 281], [548, 1559], [673, 7351], [689, 7529], [718, 2309], [721, 8317], [761, 4451], [872, 1759], [898, 6673], [913, 659], [919, 7253], [922, 7517], [992, 6343], [1069, 9043], [1297, 8269], [1400, 7489], [1402, 6299], [1403, 5441], [1427, 6737], [1468, 6271], [1468, 3697], [1482, 2213], [1502, 7573], [1576, 8681], [1613, 1483], [1646, 9311], [1718, 2646], [1733, 3607], [1774, 6883], [1778, 6733], [1823, 8273], [1838, 2143], [1847, 6791], [1876, 3037], [1913, 5711], [1940, 229], [2113, 7541], [2353, 5783], [2977, 4787], [3242, 1009], [2042, 5881], [2107, 2953], [2246, 5849], [2257, 8863], [2459, 8273], [3083, 8219], [3188, 5903], [3419, 9397], [3463, 1009], [3523, 7537], [3595, 3571], [3733, 1117], [4133, 1483], [4738, 8887], [4773, 8837], [5191, 2011], [5612, 7937], [6247, 2801], [6397, 3191], [6607, 3671], [8432, 2953], [6743, 631], [7823, 9539]
9	[2212, 7727], [2557, 3767], [3517, 9239], [3533, 8429], [6053, 3541], [7484, 1049], [7484, 7817], [7189, 7309], [8644, 4337], [9319, 967], [9343, 1951], [4975, 6691], [5093, 1913], [5383, 6917], [5692, 3769], [5915, 1289], [6053, 3541], [6271, 4133], [6299, 2281], [8509, 4943], [6719, 619]

of m and p satisfying the conditions of Theorem 1.2. We have to show that the elements of H are all distinct. To this end, we first observe that $[A_{m,p}] \neq [\mathcal{O}]$, $[B_{m,p}] \neq [\mathcal{O}]$ and $[A_{m,p} + B_{m,p}] \neq [\mathcal{O}]$. Now suppose $[A_{m,p}] = [B_{m,p}]$. Then $[A_{m,p} + B_{m,p}] = [A_{m,p}] + [B_{m,p}] = [2A_{m,p}] = [\mathcal{O}]$, which is a contradiction. Similarly, it can be shown that $[A_{m,p}] \neq [A_{m,p} + B_{m,p}]$ and $[B_{m,p}] \neq [A_{m,p} + B_{m,p}]$. Hence H is a subgroup of $E_{m,p}/2E_{m,p}$ of order 4.

Secondly, we claim that $A_{m,p}$ and $B_{m,p}$ are linearly independent points in $E_{m,p}(\mathbb{Q})$. Suppose, on the contrary, there exist integers u and v such that $uA_{m,p} + vB_{m,p} = \mathcal{O}$. Without loss of generality, we may further assume that u is the smallest positive integer with this property. Now we have the following cases:

(1) If u is even and v is odd, then $[\mathcal{O}] = [uA_{m,p} + vB_{m,p}] = u[A_{m,p}] + v[B_{m,p}]$ or $[\mathcal{O}] = [B_{m,p}]$, which contradicts Lemma 4.4.

(2) If u is odd and v is even, then $[\mathcal{O}] = [uA_{m,p} + vB_{m,p}] = u[A_{m,p}] + v[B_{m,p}]$ or $[\mathcal{O}] = [A_{m,p}]$, again contrary to what Lemma 4.3 asserts.
(3) If u and v are both odd, then $[\mathcal{O}] = [A_{m,p} + B_{m,p}]$, and this contradicts Lemma 4.5.
(4) If u and v are even, then $u = 2u'$, $v = 2v'$ for some u', v'. We have $2[u'A_{m,p} + v'B_{m,p}] = [\mathcal{O}]$. This implies that $u'A_{m,p} + v'B_{m,p}$ is a rational point of order 2. But $E_{m,p}(\mathbb{Q})$ has only trivial torsion point. Therefore, $u'A_{m,p} + v'B_{m,p} = \mathcal{O}$, but then this contradicts the minimality of u.

We have thus shown that $A_{m,p}$ and $B_{m,p}$ are linearly independent points in $E_{m,p}(\mathbb{Q})$. Now by Theorem 4.1, the cardinality of $E_{m,p}/2E_{m,p}$ is 2^r, where r is the rank of $E_{m,p}(\mathbb{Q})$. By our first claim, $E_{m,p}(\mathbb{Q})$ has at least 4 points which means that the rank r of $E_{m,p}(\mathbb{Q})$ is at least 2 for any positive integer m, with $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod{32}$ and p an odd prime. This concludes the theorem. □

5. Examples of curves with high rank

Over the rational field $\mathbb{Q}$, one typical way to find elliptic curves with high rank is to construct the families of elliptic curves with high generic rank and thereafter, we search for an adequate specialization together with effective sieving tools. The Mestre–Nagao sum is used very often [8,10]. Over $\mathbb{Q}$, let E be an elliptic curve and p be a prime. Set $a_p = a_p(E) = p + 1 - |E(\mathbf{F}_p)|$. Given a fixed integer N, the Mestre–Nagao sum is defined as

$$S(N, E) = \sum_{p \le N, p \text{ prime}} \left(1 - \frac{p-1}{E(\mathbf{F_p})}\right) \log(p)$$
$$= \sum_{p \le N, p \text{ prime}} \frac{-a_p + 2}{p + 1 - a_p} \log(p).$$

There do exist experimental verification that one generally expect that those are the larger values of $S(N, E)$ to which high rank curves correspond. In this hope, we searched for curves $E = E_{m,p}$ in the range $1 \le m \le 10000$; $1 \le p \le 10000$, for which $S(523, E) > 32$, $S(1979, E) > 42$.

After this initial sieving, we calculated the rank of the remaining curves with SAGE [12]. Table 1 comprehensively summarizes the results.

Acknowledgements

The authors are grateful to the reviewer for constructive feedback which has helped in improving the expositions and technical quality of the manuscript. The first author sincerely thanks the Harish-Chandra Research Institute, Allahabad for providing research facilities to pursue his research work and is indebted to Prof. Kalyan Chakraborty (HRI, Allahabad) for his continuous support and encouragement.

References

[1] Antoniewicz A, On a family of elliptic curves, *Universitatis Iagellonicae Acta Mathematica*, **1285(43)** (2005) 21–32

[2] Brown E and Myers B T, Elliptic curves from Mordell to diophantus and back, *Amer. Math. Monthly*, **109(7)** (2002) 639–649
[3] Cremona J E, Algorithms for modular elliptic curves, 2nd ed. (1997) (New York: Cambridge University Press)
[4] Eikenberg E V, Rational points on some families of elliptic curves, Ph.D. thesis (2004) (University of Maryland)
[5] Husemöller D, Elliptic Curves (1987) (New York: Springer-Verlag)
[6] Lutz E, Sur l'equation $y^2 = x^3 - Ax_B$ dans les corps p-adic, *J. Reine Angew. Math.*, **177** (1937) 237–247
[7] Mazur B, Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.*, **47** (1977) 33–186
[8] Mestre J F, Construction de courbes elliptiques sur $\mathbb{Q}$ de rang $\geq$12, *C. R. Acad. Sci. Paris Ser. I*, **295** (1982) 643–644
[9] Mordell L J, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Camb. Philos. Soc.*, **21** (1922) 179–192
[10] Nagao K, An example of elliptic curve over $\mathbb{Q}$ with rank $\geq$20, *Proc. Japan Acad. Ser. A Math. Sci.*, **69** (1993) 291–293
[11] Nagell T, Solution de quelque problémes dans la théorie arithmétique des cubiques planes du premier genre, Wid. Akad. Skrifter Oslo I (1935) Nr. 1
[12] SAGE software, version 4.5.3, http://www.sagemath.org
[13] Silverman J H and Tate J, Rational points on elliptic curves, Undergraduate Texts in Mathematics (1992) (New York: Springer-Verlag)
[14] Tadić P, The rank of certain subfamilies of the elliptic curve $Y^2 = X^3 - X + T^2$, *Ann. Math. et Informaticae*, **40** (2012) 145–153
[15] Tadić P, On the family of elliptic curve $Y^2 = X^3 - T^2X + 1$, *Glasnik Matematicki*, **47(67)** (2012) 81–93

COMMUNICATING EDITOR: C S Rajan