Kalyan Chakraborty; Richa Sharma

On a family of elliptic curves of rank at least 2

Czechoslovak Mathematical Journal, Vol. 72 (2022), No. 3, 681–693

Persistent URL: `http://dml.cz/dmlcz/150610`

Czechoslovak Mathematical Journal, 72 (147) (2022), 681–693

ON A FAMILY OF ELLIPTIC CURVES OF RANK AT LEAST 2

Kalyan Chakraborty, Richa Sharma, Kerala

Received March 22, 2021. Published online June 6, 2022.

Abstract. Let $C_m\colon\ y^2 = x^3 - m^2x + p^2q^2$ be a family of elliptic curves over $\mathbb{Q}$, where m is a positive integer and p, q are distinct odd primes. We study the torsion part and the rank of $C_m(\mathbb{Q})$. More specifically, we prove that the torsion subgroup of $C_m(\mathbb{Q})$ is trivial and the $\mathbb{Q}$-rank of this family is at least 2, whenever $m \not\equiv 0 \pmod 3$, $m \not\equiv 0 \pmod 4$ and $m \equiv 2 \pmod{64}$ with neither p nor q dividing m.

Keywords: elliptic curve; torsion subgroup; rank

MSC 2020: 11G05, 14G05

1. Introduction

The arithmetic of elliptic curves is one of the most fascinating branches in mathematics which has exciting practical applications, too. In 2002, Brown and Myers in [2] showed that $E_m\colon\ y^2 = x^3 - x + m^2$ has trivial torsion when $m \geqslant 1$, rank $(E_m(\mathbb{Q})) \geqslant 2$ if $m \geqslant 2$, and rank $(E_m(\mathbb{Q})) \geqslant 3$ for infinitely many values of m. Antoniewicz in [1] considered the family $C_m\colon\ y^2 = x^3 - m^2x + 1$ and derived a lower bound on the rank. He showed that rank $(C_m(\mathbb{Q})) \geqslant 2$ for $m \geqslant 2$ and rank $(C_{4k}(\mathbb{Q})) \geqslant 3$ for the infinite subfamily with $k \geqslant 1$. Later Petra in [9] gave a parametrization on $E\colon\ Y^2 = X^3 - T^2X + 1$ of rank at least 4 over the function fields and with the help of this he found a family of rank not less than 5 over the field of rational functions and a family of rank not less than 6 over an elliptic curve. Petra again in another work (see [10]) considered $E\colon\ Y^2 = x^3 - x + T^2$, a parametrization of rank not less than 3 over the function fields and using this he found families of rank not less than 3, 4 over fields of rational functions. He also obtained a particular elliptic curve with rank $r \geqslant 11$. More recently, Juyal and Kumar in [5] considered the family $E_{m,p}\colon\ y^2 = x^3 - m^2x + p^2$ and showed that the lower bound for the rank of $E_{m,p}(\mathbb{Q})$ is 2.

DOI: 10.21136/CMJ.2022.0106-21

Extending the study further, we generalize the family $E_{m,p}\colon\ y^2 = x^3 - m^2x + p^2$ by including one more prime q with some conditions on the integer m.

2. Preliminaries

In this section we recall some basic facts in the theory of elliptic curves and fix the notations along the way.

Throughout this article, we denote by C_m the family of elliptic curves

$$y^2 = x^3 - m^2x + p^2q^2.$$

2.1. Elliptic curve.

Definition 2.1. Let K be a number field with the characteristic not equal to 2 or 3. An elliptic curve E over K is defined to be an algebraic curve given by

$$E\colon\ y^2 = x^3 + bx + c \quad \text{with } b, c \in K \quad \text{and} \quad \Delta = -(4b^3 + 27c^2) \neq 0.$$

It is a smooth curve which is encoded in the discriminant $\Delta \neq 0$ and this also signifies that $x^3 + bx + c$ has 3 distinct roots. This ensures that the curve is nonsingular.

Let $E(K)$ denote the set of all K-rational points on E with an additional point $\mathcal{O}$, 'the point of infinity', i.e.,

$$E(K) = \{(x, y) \in K \times K\colon\ y^2 = x^3 + bx + c\} \cup \{\mathcal{O}\}.$$

Proposition 2.1 ([7]). *The set $E(K)$ forms a finitely generated abelian group under $\oplus$. The point $\mathcal{O}$ is the identity under this operation.*

The group $E(K)$ is known as the Mordell-Weil group of E over K. The above result over $\mathbb{Q}$ is due to Mordell and that over any number field is due to Weil.

The *Mordell-Weil theorem* states that

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r.$$

Here $E(K)_{\text{tors}}$ (the torsion part of E) is finite. It consists of the elements of finite order on E and the nonzero positive number r is called the *rank* of E which gives us the information of how many independent points of infinite order E has. It is exactly the number of copies of $\mathbb{Z}$ in the above theorem.

The structure of the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is well understood. The Mazur in [6] and Nagell-Lutz theorems in [7] provide a complete description of the torsion subgroup of any elliptic curve over $\mathbb{Q}$. The rank of an elliptic curve is a measure of the size of the set of rational points. The rank is very difficult to compute and it is quite mysterious, too. There exists no known procedure which can compute the rank with surety.

3. Main result

Now we state the first main result of the paper.

Theorem 3.1. *Let*

$$C_m\colon\ y^2 = x^3 - m^2x + p^2q^2 \tag{3.1}$$

be a family of elliptic curves with p, q are distinct primes and m being a positive integer. Then

$$C_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$$

and the $\mathbb{Q}$-rank of this family is at least 2, whenever $m \not\equiv 0 \pmod 3$, $m \not\equiv 0 \pmod 4$ and $m \equiv 2 \pmod{64}$ with neither p nor q dividing m.

Here are the main steps that are used to prove this theorem. Firstly we use the technique of reduction modulo a prime of an elliptic curve at good reduction primes, i.e., the primes which do not divide the discriminant of the curve. Then the application of Theorem 3.2 gives an injective map from the group of rational torsion points $E(\mathbb{Q})_{\text{tors}}$ into the group $E(\mathbb{F}_p)$ to arrive onto the result on the torsion part. Further we show that our family of concern, C_m, has at least two independent rational points, showing the rank is at least 2. If $P = (x, y)$ is any point on C_m then the law for doubling a point on an elliptic curve, denoted $2P = (x', y')$, is given by

$$x' = \frac{x^4 + m^4 + 2m^2x^2 - 8p^2q^2x}{4y^2}, \quad y' = -y - \frac{3x^2 - m^2}{2y}(x' - x). \tag{3.2}$$

The following result regarding the restriction of the reduction modulo p map to the torsion part will be of our use.

Theorem 3.2 ([4], Theorem 5.1)**.** *Let E be an elliptic curve over $\mathbb{Q}$. The restriction of the reduction homomorphism $r_{p|E(\mathbb{Q})_{\text{tors}}}\colon E(\mathbb{Q})_{\text{tors}} \to E_p(\mathbb{F}_p)$ is injective for any odd prime p, where E has a good reduction and $r_{2|E(\mathbb{Q})_{\text{tors}}}\colon E(\mathbb{Q})_{\text{tors}} \to E_2(\mathbb{F}_2)$ has the kernel at most $\mathbb{Z}/2\mathbb{Z}$ when E has a good reduction at 2.*

We begin the journey towards the proof of the above result by proving a couple of lemmas dealing with points of order 2, 3, 5 and 7 of the family of elliptic curves under consideration. Here for us $m \not\equiv 0 \pmod 4$ is a positive integer and p, q will always be distinct odd primes.

Lemma 3.1. *The family $C_m(\mathbb{Q})$ does not have a point of order 2.*

P r o o f. Suppose $C_m(\mathbb{Q})$ has a point $A = (x, y)$ of order 2, then

$$2A = \{\mathcal{O}\} \Leftrightarrow A = -A \Leftrightarrow y = 0, \quad x \neq 0.$$

Therefore, $x^3 - m^2x + p^2q^2 = 0$. Since the order of A is finite, so x must be an integer (by the Nagell-Lutz theorem, see[7]). Thus,

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

This implies that

$$x \in \{\pm 1, \pm p, \pm p^2, \pm q, \pm q^2, \pm pq, \pm pq^2, \pm p^2q, \pm p^2q^2\}.$$

Therefore, the possible choices of m^2 fall in

$$\{1 \pm p^2q^2, p^2 \pm pq^2, p^4 \pm q^2, q^2 \pm p^2q, q^4 \pm p^2, p^2q^2 \pm pq, p^2q^4 \pm p\} \quad \text{and} \quad \{p^4q^2 \pm q, p^4q^4 \pm 1\},$$

which is a contradiction to the fact that m is an integer. □

Lemma 3.2. *The family $C_m(\mathbb{Q})$ does not contain a point of order* 3.

P r o o f. Suppose on the contrary that it has a point of order 3 and call it A. Then $3A = \{\mathcal{O}\}$, or equivalently, $2A = -A$ or x-coordinate of $(2A) = x$-coordinate of $(-A)$, where $A = (x, y)$, $2A = (x', y')$ (x' and y' are given in (3.2)). Simplifying the value of x' gives

$$m^4 + 6m^2x^2 - 3x^4 - 12p^2q^2x = 0. \tag{3.3}$$

Reducing (3.3) at mod 3, we obtain $m^4 \equiv 0 \pmod 3$ and hence $m \equiv 0 \pmod 3$, so we get a contradiction via $m \not\equiv 0 \pmod 3$. □

Let $P \in C_m(\mathbb{Q}) = (x, y)$, $2P = (x', y')$ (the notations are as before) and then double $2P$, i.e., $4P = (x'', y'')$, where

$$x'' = \frac{x'^4 + m^4 + 2m^2x'^2 - 8p^2q^2x'}{4y'^2}, \quad y'' = -y' - \frac{3x'^2 - m^2}{2y'}(x'' - x'). \tag{3.4}$$

Lemma 3.3. *The family $C_m(\mathbb{Q})$ does not contain a point of order* 5.

P r o o f. Suppose C_m has an order 5 point A. Then $5A = \{\mathcal{O}\}$, or equivalently $4A = -A$, or x-coordinate of $(4A) = x$-coordinate of $(-A)$, where $A = (x, y)$, $4A = (x'', y'')$ (x'' and y'' are given in (3.4)). Upon simplification after inserting the value of x'', we get

$$\begin{aligned}(3.5)\quad &(x^4 + m^4 + 2m^2x^2 - 8p^2q^2x)^4 + 256m^4y^8 \\ &\quad + 32m^2y^4(x^4 + m^4 + 2m^2x^2 - 8p^2q^2x)^2 \\ &\quad - 512p^2q^2y^6(x^4 + m^4 + 2m^2x^2 - 8p^2q^2x) \\ &= 256xy^6\Big[-2y^2 - (3x^2 - m^2)\Big(\frac{x^4 + m^4 + 2m^2x^2 - 8p^2q^2x}{4y^2} - x\Big)\Big]^2.\end{aligned}$$

If x is even and we read (3.5) modulo 4, that would give $m \equiv 0, 2 \pmod 4$. The case $m \equiv 0 \pmod 4$ is not possible as we have assumed $m \not\equiv 0 \pmod 4$. If $m \equiv 2 \pmod 4$, reducing (3.5) at mod 32 we get a contradiction. In the case when x is odd, again reducing (3.5) modulo 4 gives

$$(m^2 + 1)^8 \equiv 0 \pmod 4.$$

This implies $m \equiv 1, 3 \pmod 4$, which is again not possible as we have assumed $m \equiv 2 \pmod 4$. □

Appealing to the addition law on C_m once more,

$$6P = 2P \oplus 4P = (x''', y''') \quad \text{(say)} \quad \text{with } x''' = \frac{(y'' - y')^2}{(x'' - x)^2} - x' - x''.$$

Here x'' and y'' are given in (3.4).

We now proceed to rule out the existence of an order 7 point on C_m.

Lemma 3.4. *The family $C_m(\mathbb{Q})$ does not have a point of order 7.*

P r o o f. Let $A = (x, y) \in C_m(\mathbb{Q})$ be of order 7. Then $7A = \{\mathcal{O}\} \Leftrightarrow 6A = -A \Leftrightarrow$ x-coordinate of $(6A) = x$-coordinate of $(-A)$.

Thereafter performing some elementary simplifications we arrive at

$$\begin{aligned}(3.6)\quad &16y^2y'^4[4y'^2 + (3x'^2 - m^2)(x'' - x')]^2 \\ &\quad - (x'^4 + m^4 + 2m^2x'^2 - 8p^2q^2x' - 4xy'^2)^2 \\ &\quad \times [y'^2(x^4 + m^4 + 2m^2x^2 - 8p^2q^2x) + y^2(x'^4 + m^4 + 2m^2x'^2 - 8p^2q^2x')] \\ &= 4xy^2y'^2(x'^4 + m^4 + 2m^2x'^2 - 8p^2q^2x' - 4xy'^2)^2.\end{aligned}$$

We reduce (3.6) modulo 4 to get

$$(3.7)\quad -(x'^4 + m^4 + 2m^2x'^2)^2[y'^2(x^4 + m^4 + 2m^2x^2) + y^2(x'^4 + m^4 + 2m^2x'^2)] \equiv 0 \pmod 4.$$

Now two cases can occur:

Case 1: $x \equiv 0 \pmod 2$. In this case, $m \equiv 0, 2 \pmod 4$. Here we consider two subcases:

Subcase 1.1: $m \equiv 0 \pmod 4$. This is not possible because by assumption $m \not\equiv 0 \pmod 4$.

Subcase 1.2: $m \equiv 2 \pmod 4$. As we know x is even and $m \equiv 2 \pmod 4$, then reducing (3.6) modulo 256, we get a contradiction. Since $\mathbb{Z}/256\mathbb{Z}$ is not an integral domain, so for nilpotent elements we also get a contradiction.

Case 2: $x \not\equiv 0 \pmod 2$. In this case $x^2 \equiv 1 \pmod 8$ as x is odd. Now reducing (3.6) modulo 8, we obtain

$$\begin{aligned}(3.8)\qquad -(x'^4+m^4+2m^2x'^2)^2[y'^2(1+m^4+2m^2)+y^2(x'^4+m^4+2m^2x'^2)]\\ = 4xy^2y'^2(x'^4+m^4+2m^2x'^2)^2 \pmod 8.\end{aligned}$$

Further from (3.2) we see that

$$x' = \frac{1+m^4+2m^2}{4y^2} \pmod 8, \quad x'^2 = \frac{(1+m^4)^2+4m^4+4m^2(1+m^4)}{16y^4} \pmod 8,$$
$$x'^4 = \frac{(1+m^4)^4}{16^2y^8} \pmod 8, \quad y' = -\frac{1}{8y^3}(3-m^2)(m^4+6m^2-4x-3) \pmod 8,$$
$$y'^2 = \frac{1}{64y^6}(3-m^2)^2(1+m^4+2m^2)^2 \pmod 8.$$

Now substituting the values of x', x'^2, x'^4, y' and y'^2 into (3.8), we get

$$(3.9)\qquad (1+m^4)^8[4(3-m^2)^2(1+m^4+2m^2)^3+(1+m^4)^4] \equiv 0 \pmod 8.$$

Using $m \equiv 2 \pmod{64}$ in (3.9) gives $5 \equiv 0 \pmod 8$, which is not possible. □

4. Proof of Theorem 3.1

We are now in a position to complete the proof of Theorem 3.1.

Proof. Before proceeding towards the proof let us recall that $3 \bmod p$ is not a square in $(\mathbb{Z}/p\mathbb{Z})^*$ for $p = 5, 7$ and 17. The discriminant of C_m is

$$\Delta(C_m) = 16(4m^6 - 3^3p^4q^4).$$

(I) If $p, q \neq 5$ and $m \not\equiv 0 \pmod 4$ then $5 \nmid \Delta(C_m)$ and thus C_m has a good reduction at 5. Now two cases may occur while reducing C_m to $\mathbb{F}_5$.

(a) If $p^2 \equiv 1 \pmod 5$ then q is $q^2 \equiv 1, 4 \pmod 5$ and that implies $p^2q^2 \equiv 1, 4 \pmod 5$.

(i) When $p^2q^2 \equiv 1 \pmod 5$, the curve C_m reduces to $y^2 = x^3 + 1$, $y^2 = x^3 - x + 1$ and $y^2 = x^3 - 4x + 1$ according to $m^2 \equiv 0, 1$ or $4 \pmod 5$, respectively. The corresponding size of $C_m(\mathbb{F}_5)$ would be 6, 8 and 9.

(ii) When $p^2q^2 \equiv 4 \pmod 5$, depending upon whether $m^2 \equiv 0, 1$ or $4 \pmod 5$, the curve C_m reduces to $y^2 = x^3 + 4$, $y^2 = x^3 - x + 4$ and $y^2 = x^3 - 4x + 4$, respectively, with the corresponding cardinality of $C_m(\mathbb{F}_5)$ being 6, 8 and 9.

(b) Let $p^2 \equiv 4 \pmod 5$. This case is analogous to the previous one.

Theorem 3.2 and Lagrange's theorem tell us that the possible orders of $C_m(\mathbb{Q})_{\text{tors}}$ are 1, 2, 3, 4, 6, 8 and 9 only. Lemmas 3.1 and 3.2 show that $C_m(\mathbb{Q})$ does not have points of order 2 and 3. Thus, in this case

$$C_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}.$$

(II) Let $p = 5$ or $q = 5$ (and $p \neq q$). Let $p = 5$, then the defining equation of C_m is

$$y^2 = x^3 - m^2x + 25q^2 \quad \text{and} \quad \Delta(C_m) = 16(4m^6 - 3^3 5^4 q^4), \text{ respectively.}$$

(a′) If $q \neq 7$, then utilising the condition $m \not\equiv 0 \pmod 4$ would imply $7 \nmid \Delta(C_m)$, and thus C_m has a good reduction at 7. Now three cases may occur while reducing C_m to $\mathbb{F}_7$.

(i) If $q^2 \equiv 1 \pmod 7$: depending on $m^2 \equiv 0, 1, 2$ or $4 \pmod 7$, the curve C_m reduces to $y^2 = x^3 + 4$, $y^2 = x^3 - x + 4$, $y^2 = x^3 - 4x + 4$ and $y^2 = x^3 - 2x + 4$ with the corresponding cardinality of $C_m(\mathbb{F}_7)$ being 3, 10, 10 and 10, respectively.

(ii) If $q^2 \equiv 2 \pmod 7$: in this case C_m reduces to $y^2 = x^3 + 1$, $y^2 = x^3 - x + 1$, $y^2 = x^3 - 2x + 1$ and $y^2 = x^3 - 4x + 1$ according to $m^2 \equiv 0, 1, 2$ or $4 \pmod 7$ with the corresponding cardinality of $C_m(\mathbb{F}_7)$ being 12, 12, 12 and 12, respectively.

(iii) If $q^2 \equiv 4 \pmod 7$: depending upon whether $m^2 \equiv 0, 1, 2$ or $4 \pmod 7$, C_m reduces to $y^2 = x^3 + 2$, $y^2 = x^3 - x + 2$, $y^2 = x^3 - 2x + 2$ and $y^2 = x^3 - 4x + 2$ with the corresponding cardinality of $C_m(\mathbb{F}_7)$ being 9, 9, 9 and 9, respectively.

Thus, the possible orders of $C_m(\mathbb{Q})_{\text{tors}}$ are 1, 2, 3, 4, 5, 6, 9, 10 and 12. The results of Lemmas 3.1, 3.2 and 3.3 show that C_m does not have points of order 2, 3 and 5. Thus, in this case also

$$C_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}.$$

(b′) Let $q = 7$. In this case, since $17 \nmid \Delta$, the curve C_m has good reductions at 17. Now reducing C_m to $\mathbb{F}_{17}$, the curve C_m has various possibilities: $C_m\colon\ y^2 \equiv x^3 + 1$, $y^2 \equiv x^3 - x + 1$, $y^2 \equiv x^3 - 2x + 1$, $y^2 \equiv x^3 - 4x + 1$, $y^2 \equiv x^3 - 8x + 1$, $y^2 \equiv x^3 - 9x + 1$, $y^2 \equiv x^3 - 13x + 1$, $y^2 \equiv x^3 - 15x + 1$ or $y^2 \equiv x^3 - 16x + 1$ according to $m^2 \equiv 0, 1, 2, 4, 8, 9, 13, 15$ or $16 \pmod{17}$, respectively, with the cardinality of $C_m(\mathbb{F}_{17})$ being 18, 14, 16, 25, 21, 19, 24, 24 or 18, respectively.

Hence, the possible orders of $C_m(\mathbb{Q})_{\text{tors}}$ are 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 14, 16, 18, 19, 21, 24 or 25. (Mazur's theorem tells that 14, 18, 19, 21, 24 and 25 cannot be a possible order, see [6].) Among the rest the only probable value is 1 because of Lemmas 3.1 3.2, 3.3 and 3.4. Thus,

$$C_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}.$$

□

5. The rank of C_m

The rank of an elliptic curve is a major topic of research for many years now but it is yet to be understood well. In this section we show that our family of concern, C_m, has at least two independent rational points, showing the rank is at least 2. These two points are in fact $A_m = (0, pq)$ and $B_m = (m, pq)$, and they are in $C_m(\mathbb{Q})$. We need to show that A_m and B_m are linearly independent, i.e., there do not exist nonzero integers a and b such that

$$[a]A_m + [b]B_m = \mathcal{O},$$

where $[a]A_m$ denotes the a-times addition of A_m.

Points of order 2 satisfy $y = 0$, while points of order 4 satisfy $x = 0$, so any rational point (x, y) on C_m such that $xy \neq 0$ must be of infinite order. Therefore, in our case the rank of C_m must be at least 1. To show that the rank is 2 we need to recall the following result.

Theorem 5.1 ([3]). *Let $E(\mathbb{Q})$ (or $2E(\mathbb{Q})$) be the group of rational points (or doubles of rational points, respectively) on an elliptic curve E, and suppose that 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 $E(\mathbb{Q})$.*

Lemma 5.1. *Let $A = (x', y')$ and $B = (x, y)$ be points in $C_m(\mathbb{Q})$ such that $A = 2B$ and $x' \in \mathbb{Z}$. Then*

▷ $x \in \mathbb{Z}$,

▷ $x \equiv m \pmod 2$.

P r o o f. Substituting $x = u/s$ with $(u, s) = 1$ into (3.2) and after elementary simplification,

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

This relation implies that $s \mid u^4$, and therefore $s = 1$. Thus, $x \in \mathbb{Z}$. Again, (3.2) can be written as

$$(x^2 + m^2)^2 = 4[x'x^3 - m^2x + 25p^2 + 50p^2x],$$

which implies that $2 \mid (x^2 + m^2)$. Thus, $x \equiv m \pmod 2$. □

Lemma 5.2. *The equivalence class* $[A_m] = [(0, pq)]$ *is a nonzero element of* $C_m(\mathbb{Q})/2C_m(\mathbb{Q})$ *for any positive integers* m *with* $m \equiv 2 \pmod{64}$ *and for odd primes* p *and* q.

P r o o f. Assume $A_m = 2C$ for some $C = (x, y) \in C_m(\mathbb{Q})$. Thus,

$$\frac{x^4 + m^4 + 2m^2x^2 - 8p^2q^2x}{4y^2} = 0.$$

Upon simplification it becomes

$$x^4 + m^4 + 2m^2x^2 - 8p^2q^2x = 0. \tag{5.1}$$

Thus,

$$(x^2 + m^2)^2 = 8p^2q^2x. \tag{5.2}$$

The left hand side of (5.2) is a square and so the right hand side would also be a square. This implies $x = 2(k)^2$ for some $k \in \mathbb{Z}$, where $(2, k) = 1$.

Proof of the fact that $(2, k) = 1$: Suppose $(2, k) \neq 1$, then $k = 2k_1$. Now substituting the value of $x = 8k_1^2$ into (5.2), we obtain

$$8^4k_1^8 + 16m^4 + 128k_1^4m^2 = 64k_1^2p^2q^2. \tag{5.3}$$

The equation (5.3) implies m is a multiple of 4 which is a contradiction to the fact that $m \not\equiv 0 \pmod 4$.

Putting the value of x into equation (5.1), we obtain

$$16k^8 + m^4 + 8k^4m^2 - 16k^2p^2q^2 = 0. \tag{5.4}$$

When $m \equiv 2 \pmod{64}$ this implies $m^2 \equiv 4 \pmod{64}$ and $m^4 \equiv 16 \pmod{64}$. We read (5.4) modulo 64 to get

$$k^8 + 1 + 2k^4 - k^2p^2q^2 \equiv 0 \pmod 4.$$

Since k is odd and p, q are odd primes, so $p^2 \equiv 1 \pmod 4$ and $q^2 \equiv 1 \pmod 4$. Using this we get a contradiction that $3 \equiv 0 \pmod 4$. Therefore, the above equation has no solution modulo 64. Hence, this equation has no solution. Therefore, $A_m \notin 2C_m(\mathbb{Q})$. □

Lemma 5.3. *The equivalence class* $[B_m] = [(m, pq)]$ *is a nonzero element of* $C_m(\mathbb{Q})/2C_m(\mathbb{Q})$ *for positive integers* $m \equiv 2 \pmod 4$ *and for odd primes* p, q.

Proof. Assume $B_m = (m, pq) = 2C$ for some $C = (x, y) \in C_m(\mathbb{Q})$. Thus, we get

$$\frac{x^4 + m^4 + 2m^2x^2 - 8p^2q^2x}{4y^2} = m.$$

Since $x \equiv m \pmod 2$ (using Lemma 5.1), we can write $x - m = 2s$ and after simplifying we get

$$(x - m)^4 - 4m^2(x - m)^2 - 8p^2q^2(x - m) - 12mp^2q^2 + 4m^4 = 0.$$

Now using $x - m = 2s$, we have

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

Since the left hand side is a square this implies the right hans side would also be square so $(4s + 3m) = w^2$ for some $w \in \mathbb{Z}$. Since $m \equiv 2 \pmod 4$, this implies $4s + 3m \equiv 2 \pmod 4$. So we get into a contradiction by $2 \equiv 0$ or $1 \pmod 4$. □

Lemma 5.4. *The equivalence class* $[A_m + B_m] = [(-m, -pq)]$ *is a nonzero element of* $C_m(\mathbb{Q})/2C_m(\mathbb{Q})$ *for positive integers* $m \equiv 2 \pmod{16}$ *and odd primes* p, q.

Proof. Suppose $A_m + B_m = (-m, -pq) = 2C$ for some $C = (x, y) \in C_m(\mathbb{Q})$. Thus,

$$\frac{x^4 + m^4 + 2m^2x^2 - 8p^2q^2x}{4y^2} = -m.$$

As $x \equiv m \pmod 2$, we can write $x - m = 2s$ and, after simplifying,

$$(x - m)^4 + 8m(x - m)^3 + 20m^2(x - m)^2 + 16m^3(x - m) \\ - 8p^2q^2(x - m) + 4m^4 - 8p^2q^2m + 4mp^2q^2 = 0.$$

Now using $x - m = 2s$, we have

$$4s^4 + 16ms^3 + 20m^2s^2 + 8m^3s - 4p^2q^2s + m^4 - p^2q^2m = 0. \tag{5.5}$$

When $m \equiv 2 \pmod{16}$ this implies $m^2 \equiv 4 \pmod{16}$ and $m^4 \equiv 0 \pmod{16}$. Now reducing (5.5) modulo 16 gives

$$4s^4 - 4p^2q^2s - 2p^2q^2 \equiv 0 \pmod{16}.$$

This in turn implies that $2s^4 - 2p^2q^2s - p^2q^2 \equiv 0 \pmod 8$. Since p and q are odd primes so $p^2 \equiv 1 \pmod 8$, and $q^2 \equiv 1 \pmod 8$ and using this we arrive at a contradiction. □

If we show that $\{[\mathcal{O}], [A_m], [B_m], [A_m] + [B_m]\}$ is a subgroup of $C_m/2C_m$ and A_m, B_m are linearly independent points then the proof that rank of $C_m(\mathbb{Q}) \geqslant 2$ will be completed.

Theorem 5.2. *Let m is a positive integer such that $m \not\equiv 0 \pmod 3$, $m \not\equiv 0 \pmod 4$ and $m \equiv 2 \pmod{64}$ with p, q being odd primes then the set*

$$\{[\mathcal{O}], [A_m], [B_m], [A_m] + [B_m]\}$$

is a subgroup of $C_m/2C_m$ of order 4 with $A_m = (0, pq)$, $B_m = (m, pq)$.

Proof. From the above we know that $[A_m] \neq [\mathcal{O}]$, $[B_m] \neq [\mathcal{O}]$ and $[A_m + B_m] \neq [\mathcal{O}]$. We now assume $[A_m] = [B_m]$, then $[A_m + B_m] = [A_m] + [B_m] = [2A_m] = [\mathcal{O}]$, which is not possible. It is easy to show that $[A_m]$ and $[A_m + B_m]$ are distinct. Similarly $[B_m]$ and $[A_m + B_m]$ are also distinct. Hence, $[\mathcal{O}]$, $[A_m]$, $[B_m]$ and $[A_m] + [B_m]$ are distinct classes in $C_m/2C_m$. Thus, this set is a subgroup of order 4 in $C_m/2C_m$. □

Theorem 5.3. *The points A_m and B_m are linearly independent in $C_m\colon y^2 = x^3 - m^2x + p^2q^2$ with $A_m = (0, pq)$, $B_m = (m, pq)$ and m is a positive integer such that $m \not\equiv 0 \pmod 3$, $m \not\equiv 0 \pmod 4$ and $m \equiv 2 \pmod{64}$ with p, q being two odd primes.*

Proof. Assume, on the contrary, $aA_m + bB_m = \mathcal{O}$, where a and b are integers and a is minimal. Four cases needed to be considered.

- ▷ If a is even and b is odd, then $[aA_m + bB_m] = [\mathcal{O}]$ and in the group $C_m/2C_m$, we obtain $[B_m] = [\mathcal{O}]$. Thus, we get a contradiction by Lemma 5.3.
- ▷ If a is odd and b is even, then $[aA_m + bB_m] = [\mathcal{O}]$ implies that $[A_m] = [\mathcal{O}]$ which is not possible by Lemma 5.2.
- ▷ When both a and b are odd, we get $[A_m + B_m] = \mathcal{O}$, which contradicts Lemma 5.4.
- ▷ If a and b are both even, then writing $a = 2a'$, $b = 2b'$, we get

$$2[a'A_m + b'B_m] = [\mathcal{O}].$$

This implies that $[a'A_m + b'B_m]$ is a point of order 2. From Lemma 3.1, we get $[a'A_m + b'B_m] = [\mathcal{O}]$ and this contradicts the fact that a is minimal. □

Thus, we have proved that A_m and B_m are linearly independent points and $C_m/2C_m$ contains a subgroup of order 4. Now by Theorem 5.1, the rank r of $C_m(\mathbb{Q})$ is at least 2 for any positive integer m, with $m \not\equiv 0 \pmod 3$, $m \not\equiv 0 \pmod 4$, $m \equiv 2 \pmod{64}$ and p, q being two odd primes.

Table 1 confirms the results up to certain values of m, p and q. The table shows that the rank of the elliptic curves considered is not less than 2.

All the computations have been done with the help of SAGE, see [8].

Rank	[m,pq]
2	$(2,21)(2,33)(194,33)(2,39)(194,51)(2,57)(194,57)(2,55)(2,65)$, $(2,85)(2,95)(194,91)(130,119)$, $(2,133)(130,133)(130,187)(130,209)$, $(194,209)$, $(2,247)(194,247)$
3	$(2,15)(130,21)(194,21)(194,39)(2,51)(130,51)(2,35)(194,65)$, $(194,85)(194,95)(130,77)(194,77)$, $(194,133)(2,143)(2,187)(2,209)$, $(2,91)(2,221)$, $(130,323)$
4	$(194,15)(130,33)(130,57)(194,35)(194,55)(194,35)(2,77)$, $(2,119)(194,119)(194,143)$, $(194,221)(194,323)$
5	$(194,187)(2,323)$

Table 1. Rank of $C_m(\mathbb{Q})\colon\ y^2 = x^3 - m^2x + p^2q^2$ for some values of m, p and q.

6. Concluding remarks

If we consider a larger family of elliptic curves (say)

$$D_m\colon\ y^2 = x^3 - m^2x + (pqr)^2,$$

then following our method the number of cases that have to be dealt becomes quite large and to handle so many cases will be cumbersome to say the least. Another interesting phenomena, that we observed while computing the ranks, are, that many curves come out with rank 3. A natural query would be: Does there exist a subfamily consisting of infinitely many members amongst the members in C_m with the rank at least 3? Now proving that a certain set of three points is independent amounts to showing that 7 distinct points are not doubles of rational points, see [1].

References

[1] *A. Antoniewicz*: On a family of elliptic curves. Zesz. Nauk. Uniw. Jagiell. 1285, Univ. Iagell. Acta Math. *43* (2005), 21–32. zbl MR

[2] *E. Brown, B. T. Myers*: Elliptic curves from Mordell to Diophantus and back. Am. Math. Mon. *109* (2002), 639–649. zbl MR doi

[3] *J. E. Cremona*: Algorithms for Modular Elliptic Curves. Cambridge University Press, New York, 1997. zbl MR

[4] *D. Husemöller*: Elliptic Curves. Graduate Texts in Mathematics 111. Springer, New York, 2004. zbl MR doi

[5] *A. Juyal, S. D. Kumar*: On the family of elliptic curves $y^2 = x^3 - m^2x + p^2$. Proc. Indian Acad. Sci., Math. Sci. *128* (2018), Article ID 54, 11 pages. zbl MR doi

[6] *B. Mazur*: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Étud. Sci. *47* (1977), 33–186. zbl MR doi

[7] *J. H. Silverman, J. T. Tate*: Rational Points on Elliptic Curves. Undergraduate Texts in Mathematics. Springer, Cham, 2015. zbl MR doi

[8] *W. Stein, D. Joyner, D. Kohel, J. Cremona, E. Burçin*: SageMath software, version 4.5.3. Available at `https://www.sagemath.org/` (2010). sw

[9] *P. Tadić*: On the family of elliptic curve $Y^2 = X^3 - T^2X + 1$. Glas. Mat., III. Ser. *47* (2012), 81–93. zbl MR doi

[10] *P. Tadić*: The rank of certain subfamilies of the elliptic curve $Y^2 = X^3 - X + T^2$. Ann. Math. Inform. *40* (2012), 145–153. zbl MR

Authors' address: Kalyan Chakraborty, Richa Sharma (corresponding author), Kerala School of Mathematics, Kunnamangalam PO, Kozhikode-673571, Kerala, India, e-mail: `kalychak@ksom.res.in`, `richa@ksom.res.in`.