MATHEMATICA, 67 (90), N° 2, 2025, pp. 213–225

ON THE FAMILY OF ELLIPTIC CURVES $y^2 = x^3 - m^2x + (pqr)^2$

ARKABRATA GHOSH

Abstract. In this article, we consider a family of elliptic curves defined by $E_m : y^2 = x^3 - m^2x + (pqr)^2$ where m is a positive integer and $p, q,$ and r are distinct odd primes and study the torsion as well the rank of $E_m(\mathbb{Q})$. More specifically, we proved that if $m \not\equiv 0 \pmod 3, m \equiv 2 \pmod{2^k}$ where $k \geq 5$, and none of the prime numbers p, q and r divide m, then the torsion subgroup of $E_m(\mathbb{Q})$ is trivial and a lower bound of the $\mathbb{Q}$ rank of this family of elliptic curves is 2.

MSC 2020. 11G05, 14G05.

Key words. Elliptic curve, rank, torsion subgroup.

1. INTRODUCTION

The arithmetic of the elliptic curve is one of the most fascinating branches of mathematics as it connects number theory to algebraic geometry.

Brown and Myers [2] constructed an infinite family $E_m : y^2 = x^3 - x + m^2$ of elliptic curves over $\mathbb{Q}$ and proved that the family has trivial torsion. Moreover, they showed that $\text{rank}(E_m(\mathbb{Q})) \geq 2$ if $m \geq 2$ and $\text{rank}(E_m(\mathbb{Q})) \geq 3$ for infinitely many values of m.

Antoniewiez [1] considered another family of elliptic curves $C_m : y^2 = x^3 - m^2x + 1$ and showed that $\text{rank}(C_m(\mathbb{Q})) \geq 2$ for $m \geq 2$ and $\text{rank}(C_{4k}(\mathbb{Q})) \geq 3$ for the infinite sub-family with $k \geq 1$.

Ekinberg [5], in his Ph.D. thesis, studied the family $D_m : y^2 = x^3 - m^2x + m^2$, and showed that $\text{rank}(D_m(\mathbb{Q})) = 2$ for all $m \geq 2$. Later Tadic [11] gave a parametrization on a family of the elliptic curve $C : Y^2 = X^3 - T^2X + 1$ over function fields. He proved that the torsion subgroup of E over the function field $\mathbb{C}(m)$ is trivial and rank of E is 3 and 4 over the function fields $\mathbb{Q}(m)$ and $\mathbb{C}(m)$ respectively. Later, Tadic [12] found a family of elliptic curves $E_m : Y^2 = x^3 - x + T^2$ having rank ≥ 3 over the function field $\mathbb{Q}(a, i, s, n, k, l)$, where $s^2 = i^3 + a^2$. In addition, using the results of [12], he proved the existence of families with rank ≥ 3 and rank ≥ 4 over the fields of rational functions in four variables.

The author thanks the referee for his/her helpful comments and suggestions.

DOI: 10.24193/mathcluj.2025.2.06

Later Juyal and Kumar [7] considered the family $E_{m,p} : y^2 = x^3 - m^2x + p^2$ and showed the lower bound for the rank of $E_{m,p}(\mathbb{Q})$ is 2. Finally Chakraborty and Sharma [3] considered the family $E_{pq} : y^2 = x^3 - m^2x + (pq)^2$ where p and q are distinct odd primes and showed that it has trivial torsion and rank at least two.

In this article, we consider the family of elliptic curves defined by $E_m : y^2 = x^3 - m^2x + (pqr)^2$ for distinct odd primes p, q and r and certain conditions on the integer m. The main aim of this article is to prove the following theorems.

THEOREM 1.1. *Let*

$$E_m : \ y^2 = x^3 - m^2x + (pqr)^2$$

be a family of elliptic curves where m is a positive integer such that $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod{2^k}$, where $k \geq 5$, $p, q,$ and r are distinct odd primes and none of them divide m. Then $E_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$, where $E_m(\mathbb{Q})_{\text{tors}}$ denotes the torsion of $E_m(\mathbb{Q})$ and $\mathcal{O}$ is the identity element of the group $E_m(\mathbb{Q})$.

THEOREM 1.2. *Let*

$$E_m : \ y^2 = x^3 - m^2x + (pqr)^2$$

be a family of elliptic curves, where m is a positive integer such that $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod{2^k}$ where $k \geq 5$, and $p, q,$ and r are distinct odd primes. Then rank $(E_m(\mathbb{Q})) \geq 2$.

2. PRELIMINARIES

In this section, we shall recall some basic facts regarding elliptic curves. Throughout this article, we shall consider the following family of elliptic curves

$$y^2 = x^3 - m^2x + (pqr)^2 \tag{1}$$

and we denote it by E_m.

2.1. ELLIPTIC CURVES

Let K be a number field. An elliptic curve E over K is an algebraic curve defined by the Weierstrass equation

$$E : y^2 = x^3 + bx + c, \quad \text{with } b, c \in K,$$

and $\Delta = -(4a^3 + 27b^2) \neq 0$. In other words, the above condition is the same as the cubic equation $x^3 + bx + c = 0$ having three distinct roots in K. Moreover, an elliptic curve can be thought of as a smooth (non-singular at every point) algebraic curve of genus one in the projective space $\mathbb{P}^2(K)$, defined by the homogeneous equation $y^2z = x^3 + bxz^2 + cz^3$ and the point $[0 : 1 : 0]$ on the curve is denoted by $\mathcal{O}$. Let $E(K)$ denote the set of all K-rational points on E with the "point at infinity" $\mathcal{O}$. In other words,

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

Now we can state the following proposition regarding $E(K)$, which is as follows.

PROPOSITION 2.1 ([10, Chapter III, Section 5, page 88]). *$E(K)$-the set of K rational points form a finitely generated abelian group, where we denote the group law with $\bigoplus$ (see* [10, Chapter I, Section 4, page 30]*), and the additive identity $\mathcal{O}$.*

The abelian group $E(K)$ is known as the Mordell-Weil group of E over K. When $K = \mathbb{Q}$, a result was proved by Mordell regarding $E(\mathbb{Q})$ which Weil then improved for any number field. Together, this result is known as the Mordell-Weil Theorem which states that $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$. Here $E(K)_{\text{tors}}$ is the torsion part of E which is a finite abelian group consisting of elements of finite order and the non-negative integer r is called the rank of the elliptic curve which gives us the information about the number of independent points of infinite order of E over K.

The structure of a torsion subgroup of an elliptic curve over $\mathbb{Q}$ is well-understood. Mazur [8] and Nagel-Lutz [10] theorems provide a comprehensive knowledge of the torsion subgroup of an elliptic curve over $\mathbb{Q}$. On the other hand, it is challenging to compute the rank of an elliptic curve and as of today, there is no well-defined algorithm to find it. There are plenty of computational ways that have been developed to find the rank but most of them are either computationally complex or involve heavy mathematical machinery. So an efficient way to compute the rank of an elliptic curve is still unknown.

3. THE TORSION SUBGROUP OF E_n

The principal aim of this section is to prove some results that will be used to prove Theorem 1.1 in Section 4. So to achieve our goal, we use the technique of reduction modulo a prime which does not divide the discriminant of an elliptic curve say E. If any prime p' does not divide $\Delta(E)$, then all the roots of the cubic x^3+bx+c in $\overline{\mathbb{F}}_{p'}$ are distinct and we can say E is an elliptic curve over $\mathbb{F}_{p'}$ or in other words, at p', E has a good reduction. 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 $E(\mathbb{Q})_{\text{tors}}$ into the group $E(\mathbb{F}_{p'})$.

THEOREM 3.1 ([6, Theorem 5.1]). *Let E be an elliptic curve over $\mathbb{Q}$. The restriction of reduction homomorphism $r_p|_{E(\mathbb{Q})_{\text{tors}}} : E(\mathbb{Q})_{\text{tors}} \to E_p(\mathbb{F}_p)$ is injective for any odd prime p where E has a good reduction and $r_2|_{E(\mathbb{Q})_{\text{tors}}} : E(\mathbb{Q})_{\text{tors}} \to E_2(\mathbb{F}_2)$ has the kernel at most $\mathbb{Z}/2\mathbb{Z}$ when E has a good reduction at 2.*

We need the following remark before going for tools that will help prove the Theorem 1.2.

REMARK 3.2. If $P = (x, y)$ is any point on E_m, then by the law of addition for doubling a point on an elliptic curve, we denote $2P = (x', y')$ where the

values of x' and y' are as follows,

$$\begin{cases} x' = \frac{(x^2+m^2)^2-8x(pqr)^2}{4y^2}, \\ y' = -y - \frac{3x^2-m^2}{2y}(x-x'). \end{cases} \tag{2}$$

We will introduce a couple of lemmas and prove them.

LEMMA 3.3. *There is no point of order* 2 *in* $E_m(\mathbb{Q})$ *for every positive integer* m *and distinct odd primes* p, q *and* r.

Proof. Suppose that $E_m(\mathbb{Q})$ contains a point of order two, namely $P = (x, y)$. Then $2P = \{\mathcal{O}\} \iff P \iff -P \iff y = 0$ and $x \neq 0$. Therefore,

$$x^3 - m^2x + (pqr)^2 = 0. \tag{3}$$

Since the order of P is finite, x must be an integer by the Nagell-Lutz Theorem ([10, Chapter II, Section 5, page 56]). Thus, from equation (3), we have

$$m^2 = x^2 + \frac{(pqr)^2}{x}.$$

Now the above expression implies that

$$x \in \{\pm 1, \pm p, \pm q, \pm r, \pm p^2, \pm q^2, \pm r^2, \pm pq, \pm pr, \pm qr, \pm pq^2,$$

$$\pm p^2q, \pm (pq)^2, \pm pr^2, \pm p^2r, \pm (pr)^2\}$$

or

$$x \in \{\pm q^2r, \pm qr^2, \pm (qr)^2, \pm pqr, \pm p^2qr, \pm pq^2r, \pm pqr^2, \pm (pq)^2r,$$

$$\pm p(qr)^2, \pm (pr)^2q, \pm (pqr)^2\}.$$

Now $x = \pm 1 \iff m^2 = 1 \pm (pqr)^2$ which is impossible. Similarly, $x = \pm pqr \iff m^2 = (pqr)^2 \pm pqr$ which is again impossible. Using easy computations involving divisibility, one can show that other resulting equations in m, p, q, and r do not have solutions. This is a contradiction to our claim and hence $E_m(\mathbb{Q})$ has no point of order 2. □

LEMMA 3.4. *There is no point of order* 3 *in* $E_m(\mathbb{Q})$ *for every positive integer* $m \not\equiv 0 \pmod 3$ *and for distinct odd primes* p, q *and* r.

Proof. Assume, on the contrary that, $E_m(\mathbb{Q})$ has a point of order 3 say $P = (x, y)$. Then $3P = \{\mathcal{O}\}$, or equivalently, $2P = -P$, which implies that the x-coordinate of $(2P)$=x-coordinate of $(-P)$, where $P = (x, y)$ and $2P = (x', y')$ (values of x' and y' are given by equation (2)). Therefore after putting the values of x' and upon simplification, we have

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

Using the Nagel-Lutz Theorem ([10, Chapter II, Section 5, page 56]), one obtains that x is an integer. If we consider the equation (4) modulo 3, we get $m^4 \equiv 0 \pmod 3$, which implies $m \equiv 0 \pmod 3$. This contradicts our hypothesis and hence, we can say that $E_m(\mathbb{Q})$ has no point of order 3. □

Let $P = (x, y)$ and $2P = (x', y')$ be points of $E_m(\mathbb{Q})$. Then the double of the point $2P$ is denoted by $4P = (x'', y'')$, where

$$\begin{cases} x'' = \frac{(x'^2+m^2)^2-8x'(pqr)^2}{4y'^2}, \\ y'' = -y' - \frac{3x'^2-m^2}{2y'}(x'' - x'). \end{cases} \tag{5}$$

LEMMA 3.5. *$E_m(\mathbb{Q})$ has no point of order 5 for $m \equiv 2 \pmod 4$, and for distinct odd primes p, q and r.*

Proof. Suppose E_m has a point of order 5 say P. Then $5P = \{\mathcal{O}\} \iff 4P = -P$. So the x coordinate of $4P$ is the same as x coordinate of $(-P)$, where $P = (x, y)$ and $4P = (x'', y'')$ (x'' and y'' are given in equation (5)). Upon simplification after putting the value of x'' we obtain

$$\begin{aligned} &(C^2 - 8xD^2)^4 + 32m^2y^4(C^2 - 8xD^2)^2 - 512D^2y^6(C^2 - 8xD^2) \\ &\quad + 256m^4y^8 = 256xy^6[-2y^2 - (3x^2 - m^2)(\frac{D^2 - 8xC^2}{4y^2} - x)]^2, \end{aligned} \tag{6}$$

where $C = (x^2 + m^2)$ and $D = pqr$.

Now if x is even, then by considering equation (6) modulo 4, we get $m \equiv 0 \pmod 4$ which is a contradiction to our assumption that $m \not\equiv 0 \pmod 4$. On the other hand, if we assume x is odd, then again reducing the equation (6) modulo 4, we have $(x^2 + m^2)^8 \equiv 0 \pmod 4$. As x is odd, we have $x^2 \equiv 1 \pmod 4$. So we get the following equation

$$(m^2 + 1)^8 \equiv 0 \pmod 4. \tag{7}$$

From equation (7), we can conclude that $m \equiv 1, 3 \pmod 4$, and this contradicts the hypothesis $m \equiv 2 \pmod 4$. So our assumption is wrong and hence, we can say that $E_m(\mathbb{Q})$ does not contain any point of order 5. □

LEMMA 3.6. *$E_m(\mathbb{Q})$ has no point of order 7 for $m \equiv 2 \pmod 8$, and for distinct odd primes p, q and r.*

Proof. Let $P = (x, y) \in E_m(\mathbb{Q})$ be a point of order 7. Then $7P = \{\mathcal{O}\} \iff 6P = -P \iff x-$coordinate of $(6P) \iff x-$coordinate of $(-P)$. Therefore, after implementing some elementary simplification, we arrive at the following equation.

$$\begin{aligned} &16y^2y'^4[4y'^2 + (3x'^2 - m^2)(x'' - x')]^2 \\ &\quad - (C'^2 - 8D^2x' - 4xy'^2)^2[y'^2(C^2 - 8D^2x) + y^2(C'^2 - 8D'^2x)] \\ &= 4x^2y^2y'^2(C'^2 - 8D^2x' - 4xy'^2)^2, \end{aligned} \tag{8}$$

where $C = (x^2 + m^2),\ C' = (x'^2 + m^2)$ and $D = pqr$.

We reduce the equation (8) modulo 4 to get

$$-C'^4(y'^2C^2 + y^2C'^2) \equiv 0 \pmod 4. \tag{9}$$

Now we consider two cases.

Case 1. At first, we consider $x \equiv 0 \pmod 2$. Now by putting the values of C, C' and D in equation (9) and simplifying, we get

$$m \equiv 0 \pmod 4.$$

This contradicts our assumption that $m \equiv 2 \pmod 8 \not\equiv 0 \pmod 4$.

Case 2. Now we take $x \equiv 1 \pmod 2$. As x is odd, we have $x^2 \equiv 1 \pmod 8$. Reducing equation (9) modulo 8, we obtain

$$-C'^4(y'^2C^2 + y^2C'^2) \equiv 4xy^2y'^2C'^4 \pmod 8. \tag{10}$$

Furthermore, from equation (2), we get

$$\begin{cases} x' = \frac{(m^2+1)^2}{4y^2} \pmod 8, \\ x'^2 = \frac{(1+m^2)^4}{16y^4} \pmod 8, \\ x'^4 = \frac{(1+m^2)^8}{256y^8} \pmod 8, \\ y' = -\frac{(3-m^2)(m^4+6m^2-4x-3)}{8y^3} \pmod 8, \\ y'^2 = \frac{(3-m^2)^2(m^2+1)^2}{64y^6} \pmod 8. \end{cases} \tag{11}$$

Now by substituting the values of x', x'^2, x'^4, y' and y'^2 in equation (10), we get

$$(1 + m^2)^{16}[4(3 - m^2)^2(1 + m^2)^6 + (1 + m^2)^8] \equiv 0 \pmod 8. \tag{12}$$

By assumption, we have $m \equiv 2 \pmod 8$. Using this, we can deduce from equation (12) that $5 \equiv 0 \pmod 8$, which is impossible. □

4. PROOF OF THEOREM 1.1

We will now complete the proof of the Theorem 1.1 using the results discussed in Section 3.

Proof. We know that the discriminant of the family of elliptic curves E_m given by the equation (1) is

$$\Delta(E_m) = 16[4m^6 - 27(pqr)^4].$$

We now split the proof into a couple of different cases and they are as follows.

Case 1. Firstly, we consider $p, q, r \neq 5$. Then we claim that 5 does not divide $\Delta(E_m)$ and prove it in the following way: Suppose our assumption is wrong. Hence, $4m^6 \equiv 27(pqr)^4 \equiv 2(pqr)^4 \pmod 5$. Being odd primes

different than 5, by Fermat's little theorem, we can deduce that $p^4 \equiv q^4 \equiv r^4 \equiv 1 \pmod 5$. So, $4m^6 \equiv 2 \pmod 5$. On the other hand, for any integer m, $m^6 \equiv 0, 1, \text{ or } 4 \pmod 5$ and hence, $4m^6 \equiv 0, 1, 4 \pmod 5$. So our assumption is wrong and so $5 \nmid \Delta(E_m)$. Hence we can say that E_m has a good reduction at 5. Now while we try to reduce E_m in $\mathbb{F}_5$, we get two different scenarios.

(a) If $p^2 \equiv 1 \pmod 5$, then $q^2 \equiv 1, 4 \pmod 5$ and $r^2 \equiv 1, 4 \pmod 5$. It implies that $(pqr)^2 \equiv 1, 4 \pmod 5$.
   (i) When $(pqr)^2 \equiv 1 \pmod 5$, then depending upon whether $m^2 \equiv 0, 1 \text{ or } 4 \pmod 5$, E_m reduces into the equations $y^2 = x^3 + 1$, $y^2 = x^3 - x + 1$ and $y^2 = x^3 + 4x + 5$ respectively. So the corresponding size of the cardinality of $E_m(\mathbb{F}_5)$ would be $6, 8$ and 8.
   (ii) When $(pqr)^2 \equiv 4 \pmod 5$, then the curve E_m reduces to $y^2 = x^3 + 4$, $y^2 = x^3 - x + 4$ and $y^2 = x^3 + 4x + 4$ accordingly as $m^2 \equiv 0, 1 \text{ or } 4 \pmod 5$ respectively, with the corresponding cardinality of $E_m(\mathbb{F}_5)$ being $6, 8$ and 8.

(b) If $p^2 \equiv 4 \pmod 5$, then depending upon the choices of $q^2, r^2 \pmod 5$, we will have $(pqr)^2 \equiv 1, 4 \pmod 5$. This is completely analogous to the previous one.

By Theorem 3.1 and Lagrange's theorem, we can say that the possible orders of $E_m(\mathbb{Q})_{\text{tors}}$ are $1, 2, 3, 4, 6, 8$ and 9 only. Now Lemmas 3.3 and 3.4 ensure that $E_m(\mathbb{Q})$ does not have any points of order 2 and 3. Thus we can conclude that

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

Case 2. We consider the scenario when $p = 5$ or $q = 5$ or $r = 5$ (as $p \neq q \neq r$). At first, let $p = 5$. Then equation (1) of E_m can be re-written as

$$y^2 = x^3 - m^2x + 25q^2r^2,$$

with

$$\Delta(E_m) = 16[4m^6 - 3^3 5^4 (qr)^4].$$

(a) if both $q \neq 7 \neq r$, then it would imply 7 does not divide $\Delta(E_m)$, and thus it is evident that E_m has a good reduction at 7. Now as both q and r are odd, so $q^2 \equiv r^2 \equiv 1, 2 \text{ or } 4 \pmod 7$. Hence, based on different choices of q and r, $(qr)^2 \equiv 1, 2 \text{ or } 4 \pmod 7$. Hence, there are three cases to consider while we reduce E_m in $\mathbb{F}_7$.
   (i) $(qr)^2 \equiv 1 \pmod 7$:
   Depending on whether $m^2 \equiv 0, 1, 2 \text{ or } 4 \pmod 7$, the curve E_m reduces to $y^2 = x^3+4$, $y^2 = x^3-x+4$, $y^2 = x^3-4x+4$ or $y^2 = x^3-2x+4$ respectively. So the corresponding cardinality of $E_m(\mathbb{F}_7)$ would be $3, 10, 10$ and 10 respectively.

(ii) $(qr)^2 \equiv 2 \pmod 7$:
In this case, the curve E_m reduces to $y^2 = x^3+1$, $y^2 = x^3-x+1$, $y^2 = x^3-2x+1$ or $y^2 = x^3-4x+1$ accordingly as $m^2 \equiv 0, 1, 2$ or $4 \pmod 7$ with the corresponding cardinality of $E_m(\mathbb{F}_7)$ being $12, 12, 12$ and 12 respectively.

(iii) $(qr)^2 \equiv 4 \pmod 7$:
Depending upon whether $m^2 \equiv 0, 1, 2$ or $4 \pmod 7$, the curve E_m reduces to $y^2 = x^3 + 2$, $y^2 = x^3 - x + 2$, $y^2 = x^3 - 2x + 2$ or $y^2 = x^3 - 4x + 2$ respectively. So the corresponding cardinality of $E_m(\mathbb{F}_7)$ would be $9, 9, 9$ and 9 respectively.

So from the above three scenarios, it is clear that the possible orders of $E_m(\mathbb{Q})_{\text{tors}}$ are $1, 2, 3, 4, 5, 6, 9, 10$ and 12. Now using the results of Lemmas 3.3, 3.4 and equation (4), we can say that E_m does not have any points of order $2, 3$ and 5. Thus in this case too

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

(b) If $q = 7$, then the equation (1) of E_m can be re-written as

$$y^2 = x^3 - m^2x + 5^2 7^2 r^2,$$

with

$$\Delta(E_m) = 16(4m^6 - 3^3 5^4 7^4 r^4) = 3(21m^6 - 3^2 5^4 7^4 r^4) + m^6. \tag{13}$$

Now as r is an odd prime, we have $r^2 \equiv 1 \pmod 3$, and from our assumption that $m \not\equiv 0 \pmod 3$, we can say $m^2 \equiv 1 \pmod 3$, which, when combined with equation (13), gives that 3 does not divide $\Delta(E_m)$. So E_m has a good reduction at 3.

Now while reducing E_m to $\mathbb{F}_3$, we have two scenarios that are described below.

(a) At first, when we take $q \not\equiv 0 \pmod 3$, we have $q^2 \equiv 1 \pmod 3$. Hence, based on the choice of m, curve E_m reduces to $y^2 = x^3 - x + 1$ with the corresponding cardinality of $E_m(\mathbb{F}_3)$ being 7.

(b) When $q = 3$, then the curve E_m reduces to $y^2 = x^3-x$. Now the cardinality of $E_m(\mathbb{F}_3)$ is 4.

From the above two scenarios, we can say the possible orders of

$$E_m(\mathbb{Q})_{\text{tors}}$$

are $1, 2, 4$ and 7. Using the results of Lemmas 3.3, 3.4, 3.5 and 3.6, we can say that E_m does not have any points of order $1, 2, 4$ and 7. Thus in this case too

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

So by combining all the different scenarios, we can conclude that when m is an integer such that $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod 8$, and p, q, r are distinct odd primes, then $E_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$. □

5. THE RANK OF E_m

The rank of an elliptic curve is a topic of major importance in number theory and as of today, it is yet to be understood fully. In this section, we will show that the family of the concerned elliptic curve E_m has rank at least two by showing the existence of two linearly independent rational points.

We will consider two points, namely $A_m = (0, pqr)$ and $B_m = (m, pqr)$ on $E_m(\mathbb{Q})$ and we need to show that they are linearly independent, i.e, there does not exist two non-zero integers a and b such that

$$[a]A_m + [b]B_m = \mathcal{O} \tag{14}$$

where $[a]A_m$ denotes a-times addition of A_m in $E_m(\mathbb{Q})$.

At first, we claim that the point $B_m = (m, pqr) \in E_m(\mathbb{Q})$ is a point of infinite order because if not, then the order of B_m must be finite and hence, it must be in the torsion of $E_m(\mathbb{Q})$. But as we have already proved that

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

we can conclude that the order of $B_m = (m, pqr)$ must be infinite. Hence, we can say the rank of E_m is at least one. We need to use the following result to show the rank is at least two.

THEOREM 5.1 ([4, Section 3.6, Page 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 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 $E(\mathbb{Q})$.*

Now to accomplish our aim, we need to prove the following four auxiliary results.

LEMMA 5.2. *Let $A = (x'.y')$ and $B = (x, y)$ be points on $E_m(\mathbb{Q})$ such that $A = 2B$ and $x' \in \mathbb{Z}$. Then*

- $x \in \mathbb{Z}$,
- $x \equiv m \pmod 2$.

Proof. Substituting $x = \frac{u}{v}$, with $\gcd(u, v) = 1$ in the expression of x' of equation (2) and after simplification, we get

$$(m^4 - 4p^2q^2r^2x')v^4 + (4m^2x' - 8p^2q^2r^2)uv^3 + 2m^2u^2v^2 - 4x'u^3v + u^4 = 0. \tag{15}$$

From equation (15), it is evident that $v|u^4$ and therefore $v = \pm 1$. Thus $x \in \mathbb{Z}$.

Now the equation (2) can be written as

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

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

LEMMA 5.3. *The equivalence class* $[A_m] = [(0, pqr)]$ *is a non-zero element of* $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ *for any positive integer* $m \equiv 2 \pmod{2^5}$ *and for odd primes* $p, q,$ *and* r.

Proof. Suppose $A_m = 2C$ for some $C = (x, y) \in E_m(\mathbb{Q})$. From equation (2), we have

$$\frac{(x^2 + m^2)^2 - 8x(pqr)^2}{4y^2} = 0,$$

which upon simplification, becomes

$$(x^2 + m^2)^2 = 8x(pqr)^2. \tag{16}$$

The left-hand side of equation (16) is a perfect square and so the right-hand side must be too. This implies that $x = 2k_1^2$ for some $k_1 \in \mathbb{Z}$.

Now we claim that $\gcd(2, k_1) = 1$. We prove our claim in the following way: Suppose our claim is false. Then $k_1 = 2^\alpha k_2$ where $\alpha, k_2 \in \mathbb{Z}$ and $\alpha \geq 1$. Substituting $x = 2k_1^2 = 2^{2\alpha+1}k_2^2$ in equation (16), we obtain

$$2^{8\alpha+4}k_2^8 + m^4 + 2^{4\alpha+3}k_2^4m^2 = 2^{2\alpha+4}k_2^2(pqr)^2$$

which can be rewritten as

$$m^4 + 8 \times 2^{4\alpha}k_2^4m^2 + 16 \times 2^{8\alpha}k_2^4 = 16 \times 2^{2\alpha}k_2^2(pqr)^2. \tag{17}$$

Now if we consider equation (17) modulo 32, we get $m^4 \equiv 0 \pmod{32}$. From our assumption, we can say $m \equiv 2 \pmod{32}$ from which we can deduce that $m^4 \equiv 16 \pmod{32}$. Hence we arrive at a contradiction.

By putting the value of x in the equation (16) and simplifying, we obtain

$$16k_1^8 + m^4 + 8k_1^4m^2 = 16k_1^2(pqr)^2. \tag{18}$$

From the hypothesis, we get $m \equiv 2 \pmod{32}$, which implies $m^2 \equiv 4 \pmod{32}$ and $m^4 \equiv 16 \pmod{32}$. So when we consider equation (18) modulo 32, we get that

$$k_1^8 + 1 - k_1^2(pqr)^2 \equiv 0 \pmod{2}.$$

As k_1 is odd and p, q and r are odd primes, we have $k_1^2 \equiv 1 \pmod{2}$, $p^2 \equiv 1 \pmod{2}$, $q^2 \equiv 1 \pmod{2}$ and $r^2 \equiv 1 \pmod{2}$. Substituting these values in the above equation, we get a contradiction: $1 \equiv 0 \pmod{2}$. So we can say that equation (18) has no solution. Therefore, $A_m \notin 2E_m(\mathbb{Q})$. □

LEMMA 5.4. *The equivalence class* $[B_m] = [(m, pqr)]$ *is a non-zero element of* $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ *for positive integers* $m \equiv 2 \pmod{2^5}$ *and for odd primes* p, q *and* r.

Proof. Assume $B_m = (m, pqr) = 2C$ for some $C = (x, y) \in E_m(\mathbb{Q})$. Now from equation (2), we can say

$$\frac{(x^2 + m^2)^2 - 8x(pqr)^2}{4y^2} = m.$$

From Lemma 5.2, we get $x \equiv m \pmod 2$. By putting $x - m = 2s$ in the above equation and simplifying, we get

$$(2s^2 - m^2)^2 = (pqr)^2[4s + 3m]. \tag{19}$$

As the left-hand side of equation (19) is a perfect square, so will the right-hand side be. So, we have $(4s + 3m) = w^2$ for some $w \in \mathbb{Z}$ which in turn implies $3m \equiv 0, 1 \pmod 4$. Now as $m \equiv 2 \pmod{2^5}$, we have $m \equiv 2 \pmod 4$. So from here, we get $3m \equiv 2 \pmod 4$ which is a contradiction to the fact that $(4s + 3m)$ is a perfect square. Hence, $B_m \notin 2E_m(\mathbb{Q})$. □

LEMMA 5.5. *The equivalence class $[A_m + B_m] = [-m, pqr]$ is a non-zero element of $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ for positive integers $m \equiv 2 \pmod{2^5}$ and for odd primes p, q and r.*

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

$$\frac{(x^2 + m^2)^2 - 8x(pqr)^2}{4y^2} = -m.$$

As $x \equiv m \pmod 2$, we can write $x - m = 2s$. Substituting this value in the above equation and after simplification, we have

$$4s^4 + 16ms^3 + 20m^2s^2 + 8m^3s - 4s(pqr)^2 + m^4 - (pqr)^2m = 0 \tag{20}$$

Now as $m \equiv 2 \pmod{2^5}$, we can say $m \equiv 2 \pmod{16}$. Next as $m \equiv 2 \pmod{16}$, we have $m^2 \equiv 4 \pmod{16}$, $m^3 \equiv 8 \pmod{16}$ and $m^4 \equiv 0 \pmod{16}$. Substituting these values in equation (20), we get

$$4s^4 - 4s(pqr)^2 - 2(pqr)^2 \equiv 0 \pmod{16},$$

which can be simplified into the equation

$$2s^4 - 2s(pqr)^2 - (pqr)^2 \equiv 0 \pmod 8. \tag{21}$$

Because p, q and r are odd primes, we have $p^2 \equiv q^2 \equiv r^2 \equiv 1 \pmod 8$. Then, from equation (20), we have $2s[s^3 - (pqr)^2] \equiv 1 \pmod 8$ which is a contradiction. □

Onward, if we can show that $\{\mathcal{O}, [A_m], [B_m], [A_m + B_m]\}$ is a subgroup of $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ and A_m, B_m are linearly independent, then we can prove that rank of $E_m(\mathbb{Q})$ is at least 2. To prove Theorem 1.2, we will state and prove the following propositions.

PROPOSITION 5.6. *Let m be a positive integer such that $m \not\equiv 0 \pmod 3$ and $m \equiv 2 \pmod{2^k}$ where $k \geq 5$ with odd primes p, q and r. Then the set*

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

is a subgroup of $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ of order 4, with $A_m = (0, pqr)$, $B_m = (m, pqr)$.

Proof. Given Lemma 5.3, Lemma 5.4 and Lemma 5.5, we can say that all of $[A_m], [B_m]$ and $[A_m + B_m]$ are not equal to $\{\mathcal{O}\}$. Now if $[A_m] = [B_m]$, then $[A_m + B_m] = [2B_m] = [\{\mathcal{O}\}]$, which is not possible. Now, if $[A_m] = [A_m + B_m]$, then we have $[\{\mathcal{O}\}] = [2A_m] = [B_m]$, which is again a contradiction. Similarly, we can show $[B_m]$ and $[A_m + B_m]$ are also distinct. Hence, $\mathcal{O}, [A_m], [B_m]$ and $[A_m + B_m]$ are distinct classes in $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$. Thus the set S is a subgroup of order 4 in $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$. □

PROPOSITION 5.7. *Points $A_m = (0, pqr)$ and $B_m = (m, pqr)$ are two linearly independent points in $E_m : y^2 = x^3 - m^2x + (pqr)^2$ where $m \neq 0 \pmod 3$ and $m \equiv 2 \pmod{2^k}$, $k \geq 5$ and for odd primes p, q and r.*

Proof. From the discussion at the beginning of this section, we know that if the points A_m and B_m are linearly independent, then there do not exist non-zero integers a and b such that they satisfy equation (14). Suppose, on the contrary, we have $aA_m + bB_m = \mathcal{O}$ where a and b are defined as above with a minimal. We need to consider four different cases and they are as follows:

- If a is even and b is odd and $[aA_m + bB_m] = [\mathcal{O}]$, then in the group $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$, we have $[B_m] = [\mathcal{O}]$. This is a contradiction by Lemma 5.4.
- If a is odd and b is even, then $[aA_m + bB_m] = [\mathcal{O}]$ implies that $[A_m] = [\mathcal{O}]$. This is impossible due to the Lemma 5.3.
- When both a and b are odd we get $[A_m + B_m] = [\mathcal{O}]$, which contradicts Lemma 5.4.
- Now if both a and b are even, then we may assume $a = 2a'$ and $b = 2b'$. Then from $[aA_m + bB_m] = [\mathcal{O}]$, we get that $2[a'A_m + b'B_m] = [\mathcal{O}]$, which implies that $(a'A_m + b'B_m)$ is a point of order 2 in $E_m(\mathbb{Q})$. But this is a contradiction due to the Lemma 3.3. □

Now we are ready to prove Theorem 1.2.

Proof. From Proposition 5.6, we have two linearly independent points, A_m and B_m in $E_m(\mathbb{Q})$. From Theorem 5.1, we can say that the cardinality of the group $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ is 2^r, where r is the rank of the group $E_m(\mathbb{Q})$. Using Proposition 5.7, we can say that $E_m(\mathbb{Q})$ has at least 4 points which means the rank r of $E_m(\mathbb{Q})$ is at least 2. This concludes the proof of the theorem. □

Now we give an example related to the Theorems 1.1 and 1.2.

EXAMPLE 5.8. Let us take $m = 2$, $p = 3$, $q = 7$ and $r = 11$. As these values satisfy the hypothesis of the Theorem 1.1, we can say $E_2(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$. Moreover, the rank of $E_2(\mathbb{Q}) = 2$, which verifies Theorem 1.2. The computation was done using SAGE [9].

6. CONCLUDING REMARKS

In this article, we have taken a certain family of elliptic curves E_m given by equation (1) and shown that they are of rank at least 2. Now using computations, it can be verified that some of these curves have rank at least 3. So the natural question would be the following: Does there exist a subfamily of E_m that has a rank at least 3 or higher? It would make an interesting problem.

REFERENCES

[1] A. Antoniewicz, *On a family of elliptic curves*, Univ. Iagel. Acta Math., **1285** (2005), 21–32.
[2] E. Brown and B. T. Myers, *Elliptic curves from Mordell to Diophantus and back*, Amer. Math. Monthly, **109** (2002), 639–649.
[3] K. Chakraborty and R. Sharma, *On a family of elliptic curves of rank at least 2*, Czechoslovak Math. J., **72** (2022), 681–693.
[4] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, New York, 1997.
[5] E. V. Ekinberg, *Rational points on some families of elliptic curves*, PhD Thesis, University of Maryland, College Park, MD, 2004.
[6] D. Husemoller, *Elliptic Curves*, Springer-Verlag, New York, NY, 1987.
[7] A. Juyal and S. D. Kumar, *On the family of elliptic curve* $Y^2 = X^3 - m^2X + p^2$, Proc. Indian Acad. Sci. Math. Sci., **128** (2018), 1–11.
[8] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci., **47** (1977), 33–186.
[9] SAGE Software, version 9.3, https://www.sagemath.com.
[10] J. H. Silverman and J. H. Tate, *Rational points on elliptic curve*, Undergraduate Text in Mathematics, Springer-Verlag, New York, NY, 1992.
[11] P. Tadić, *On the family of elliptic curves* $Y^2 = X^3 - T^2X + 1$, Glas. Mat. Ser. III, **47** (2012), 81–93.
[12] P. Tadić, *The rank of certain subfamilies of elliptic curve* $Y^2 = X^3 - X + T^2$, Ann. Math. Inform., **40** (2012), 145–153.

Received April 4, 2024
Accepted October 14, 2024

SRM University–AP
Department of Mathematics
Mangalgiri Mandal, Neerukonda, Amravati
Andhra Pradesh, 522502, India
E-mail: arka2686@gmail.com
https://orcid.org/0009-0005-8970-4307