Malaysian Journal of Mathematical Sciences 17(1): 67–76(2023)
https://doi.org/10.47836/mjms.17.1.06

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

Elliptic Curves of Type $y^2 = x^3 - 3pqx$ Having Ranks Zero and One

Mina, R. J. S.[1] and Bacani, J. B. *[2]

[1,2]*Department of Mathematics and Computer Science, University of the Philippines Baguio*
[2]*Mathematical Sciences Division, National Research Council of the Philippines*

E-mail: jbbacani@up.edu.ph
**Corresponding author*

Received: 8 February 2022
Accepted: 24 November 2022

Abstract

The group of rational points on an elliptic curve over $\mathbb{Q}$ is always a finitely generated Abelian group, hence isomorphic to $\mathbb{Z}^r \times G$ with G a finite Abelian group. Here, r is the rank of the elliptic curve. In this paper, we determine sufficient conditions that need to be set on the prime numbers p and q so that the elliptic curve $E : y^2 = x^3 - 3pqx$ over $\mathbb{Q}$ would possess a rank zero or one. Specifically, we verify that if distinct primes p and q satisfy the congruence $p \equiv q \equiv 5 \pmod{24}$, then E has rank zero. Furthermore, if $p \equiv 5 \pmod{12}$ is considered instead of a modulus of 24, then E has rank zero or one. Lastly, for primes of the form $p = 24k + 17$ and $q = 24\ell + 5$, where $9k + 3\ell + 7$ is a perfect square, we show that E has rank one.

Keywords: elliptic curve; rank of elliptic curve; torsor

1 Introduction

Elliptic curves (ECs) are structured as $C : y^2 = x^3 + Ax + B$ with an additional property that its discriminant $\Delta := -16(4A^3 + 27B^2)$ is non-zero. Its collection of rational points $C(\mathbb{Q})$ has a well-defined addition law making it as a commutative group, with the additive identity $\mathcal{O}$ (known as 'point of infinity'). A celebrated result of Mordell (and Weil) states that $C(\mathbb{Q})$ can be generated finitely. Hence,

$$C(\mathbb{Q}) \cong C(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $C(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of $C(\mathbb{Q})$; that is, the collection of points with finite order, and $r > 0$ is called the rank of C. There are ways on how to compute $C(\mathbb{Q})_{\text{tors}}$. One of which is by utilizing the theorem of Nagell-Lutz. However, an algorithm that can compute the rank of any elliptic curve is yet to be created or discovered. Hence, finding the ranks of families of elliptic curves is of interest to many number theorists.

Recently, there are research studies on families of ECs $y^2 = x^3 + bx$ where finding their ranks is one of the goals. In 2007, Spearman [9] determined the values of prime p for which the elliptic curve (EC) $y^2 = x^3 - px$ has rank two. In the same year, he also gave conditions on $2p$, where p is prime, so that the EC $y^2 = x^3 - 2px$ will have a rank of three [10]. In 2010, Hollier et al. [4] considered ECs $y^2 = x^3 + pqx$, where primes p and q are distinct. In 2011, Fujita and Terai [3] considered $y^2 = x^3 - p^k x$, where p is prime and $k = 1, 2, 3$. They provided sufficient as well as necessary conditions for the rank of the given curve to be equal to one or two. In 2014, Daghigh and Didari [1] determined the ranks of ECs of type $y^2 = x^3 - 3px$. In 2015, they studied the ECs $y^2 = x^3 - pqx$, where primes p and q are of different values [2]. In the same year, Kim [6] studied ECs $y^2 = x^3 \pm 4px$, where p is a prime number.

We are motivated to contribute to the literature of finding ranks of elliptic curves. In this work, we focus on elliptic curves having the structure

$$y^2 = x^3 - 3pqx, \tag{1}$$

where the primes p and q have different values. We provide conditions on p and q so that (1) will have a rank equal to zero. Moreover, we provide values of p and q so that the rank of (1) is exactly one. The main results are stated in the third section.

Here is the method that we used in finding ranks of elliptic curves.

Consider an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, where a and b are rational numbers. $a, b \in \mathbb{Q}$. Note that $T := (0, 0)$ is a rational point on E of order 2, i.e., $2T = \mathcal{O}$. Given another elliptic curve $\overline{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$, there exists an isogeny $\phi : E \to \overline{E}$ of degree 2 given by

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right).$$

Thus, E and $\overline{E}$ are 2-isogenous curves. Let Γ and $\overline{\Gamma}$ be the groups of rational points on E and $\overline{E}$, respectively. Let $\mathbb{Q}^\times$ be the multiplicative group of non-zero rational numbers. Also, let $\mathbb{Q}^{\times 2}$ the subgroup of $\mathbb{Q}^\times$ of squares of rational numbers; that is,

$$\mathbb{Q}^{\times 2} = \{u^2 \mid u \in \mathbb{Q}^\times\}.$$

Then, there is a group homomorphism $\alpha : \Gamma \longrightarrow \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ defined as

$$\begin{cases} \alpha(\mathcal{O}) = 1 \pmod{\mathbb{Q}^{\times 2}} \\ \alpha(T) = b \pmod{\mathbb{Q}^{\times 2}} \\ \alpha(x, y) = x \pmod{\mathbb{Q}^{\times 2}} \quad \text{if } x \neq 0, \end{cases}$$

where $\mathcal{O}$ is the identity in Γ. Similarly, there is a group homomorphism $\overline{\alpha} : \overline{\Gamma} \longrightarrow \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ given by

$$\begin{cases} \overline{\alpha}(\overline{\mathcal{O}}) = 1 \pmod{\mathbb{Q}^{\times 2}} \\ \overline{\alpha}(T) = a^2 - 4b \pmod{\mathbb{Q}^{\times 2}} \\ \overline{\alpha}(x, y) = x \pmod{\mathbb{Q}^{\times 2}} \quad \text{if } x \neq 0, \end{cases}$$

where $\overline{\mathcal{O}}$ is the identity in $\overline{\Gamma}$.

The group $\alpha(\Gamma)$ comprises 1, b and all factors b_1 of b, all modulo $\mathbb{Q}^{\times 2}$. Here, $b_1 \not\equiv 1 \pmod{\mathbb{Q}^{\times 2}}$, such that a triple $(N, M, e) \in \mathbb{Z}^3$, where $M \neq 0, e \neq 0$, solves the Diophantine equation (also called 'torsors')

$$\mathcal{T} : N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4, \quad \text{with } b_1 b_2 = b,$$

and satisfies the following divisibility criteria:

$$\gcd(N, e) = \gcd(M, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1.$$

Similarly, the group $\overline{\alpha}(\overline{\Gamma})$ comprises 1, $a^2 - 4b$ and all factors b_1 of $a^2 - 4b \pmod{\mathbb{Q}^{\times 2}}$, with $b_1 \not\equiv 1 \pmod{\mathbb{Q}^{\times 2}}$, such that a triple $(N, M, e) \in \mathbb{Z}^3$, where $M \neq 0$, $e \neq 0$, satisfies the Diophantine equation

$$\mathcal{T}' : N^2 = b_1 M^4 - 2aM^2 e^2 + b_2 e^4, \quad \text{with } b_1 b_2 = a^2 - 4b,$$

and the gcd criteria mentioned above. Then, we have the following formula involving the rank r of E:

$$2^r = \frac{1}{4}(|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|),$$

where $|\cdot|$ denotes the order of the finite group. For more details about this method, we refer the reader to [8].

For some applications of elliptic curves, we refer the reader to [7] and [5].

2 Results

The main theorem will now be stated and proven in this section.

Theorem 2.1. *Suppose distinct primes p and q satisfy the congruence $p \equiv q \equiv 5 \pmod{24}$. Then $E : y^2 = x^3 - 3pqx$ is an elliptic curve with rank equal to zero.*

Proof. We have $E : y^2 = x^3 - 3pqx$ and $\overline{E} : y^2 = x^3 + 12pqx$. We first determine $|\alpha(\Gamma)|$. Note that $1, -3pq \in \alpha(\Gamma)$ by definition of α. We also have all the possible divisors of $-3pq$ modulo $\mathbb{Q}^{\times 2}$ in the following set

$$\{3pq,\ -1,\ \pm 3q,\ \pm p,\ \pm pq,\ \pm 3,\ \pm 3p,\ \pm q\}.$$

We then consider the solvability of the following torsors over the set of integers.

$$\mathcal{T}_1 : \quad N^2 = 3pqM^4 - e^4$$

$$\mathcal{T}_2 : \quad N^2 = 3qM^4 - pe^4$$

$$\begin{aligned}
\mathcal{T}_3: &\quad N^2 = pM^4 - 3qe^4.\\
\mathcal{T}_4: &\quad N^2 = pqM^4 - 3e^4\\
\mathcal{T}_5: &\quad N^2 = 3M^4 - pqe^4\\
\mathcal{T}_6: &\quad N^2 = 3pM^4 - qe^4.\\
\mathcal{T}_7: &\quad N^2 = qM^4 - 3pe^4.
\end{aligned}$$

Lemma 2.1. *There are no integer solutions for the torsor* $\mathcal{T}_1: \ N^2 = 3pqM^4 - e^4$.

Proof. Reducing $\mathcal{T}_1$ modulo 3, we get $N^2 \equiv -e^4 \pmod 3$. This implies

$$1 = \left(\frac{-e^4}{3}\right) = \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

which is a contradiction. Thus, $\mathcal{T}_1$ has no solutions in $\mathbb{Z}$. □

Lemma 2.2. *There are no integer solutions for the torsor* $\mathcal{T}_2: \ N^2 = 3qM^4 - pe^4$.

Proof. First note that the assumption implies $p \equiv q \equiv 1 \pmod 4$. Reducing $\mathcal{T}_2$ modulo 4, we get $N^2 \equiv 3M^4 - e^4 \pmod 4$. By the divisibility criteria, we have the various scenarios:

1. N even, M odd and e odd. In this case, we end up with a false argument: $0 \equiv 3 - 1 \equiv 2 \pmod 4$.
2. N odd, M even and e odd. In this case, we end up with another contradiction: $1 \equiv 0 - 1 \equiv 3 \pmod 4$.
3. N odd, M odd and e even. In this case, we have $1 \equiv 3 - 0 \equiv 3 \pmod 4$, which is a contradiction.

In any case, we get a contradiction. Thus, $\mathcal{T}_2$ has no solutions in $\mathbb{Z}$. □

Lemma 2.3. *There are no solutions for the torsor* $\mathcal{T}_3: \ N^2 = pM^4 - 3qe^4$.

Proof. Reducing $\mathcal{T}_3$ modulo 3, we get $N^2 \equiv pM^4 \pmod 3$. This implies

$$1 = \left(\frac{pM^4}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

since $p \equiv 2 \pmod 3$. This is a contradiction. Thus, $\mathcal{T}_3$ has no solutions in $\mathbb{Z}$. □

Lemma 2.4. *There are no integer solutions for the torsor* $\mathcal{T}_4: \ N^2 = pqM^4 - 3e^4$.

Proof. Reducing $\mathcal{T}_4$ modulo p, we get $N^2 \equiv -3e^4 \pmod p$. This implies

$$1 = \left(\frac{-3e^4}{p}\right) = \left(\frac{-3}{p}\right).$$

Since

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{12} \\ -1 & \text{if } p \equiv 5 \text{ or } 11 \pmod{12} \end{cases},$$

we get $p \equiv 1 \pmod{12}$ or $p \equiv 7 \pmod{12}$. This means that $p \equiv 1 \pmod 3$. This is a contradiction to the assumption that $p \equiv 5 \pmod{24}$ (i.e. $p \equiv 2 \pmod 3$). Thus, $\mathcal{T}_4$ has no solutions in $\mathbb{Z}$. □

Lemma 2.5. *There are no integer solutions for the torsor* $\mathcal{T}_5: \ N^2 = 3M^4 - pqe^4$.

Proof. Reducing $\mathcal{T}_5$ modulo 3, we get $N^2 \equiv -pqe^4 \pmod 3$. Since $p \equiv q \equiv 2 \pmod 3$ by assumption, we get $N^2 \equiv -e^4 \pmod 3$. This implies

$$1 = \left(\frac{-e^4}{3}\right) = \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

which is a contradiction. Thus, $\mathcal{T}_5$ has no solutions in $\mathbb{Z}$. □

Lemma 2.6. *There are no integer solutions for the torsor* $\mathcal{T}_6: \ N^2 = 3pM^4 - qe^4$.

Proof. By applying the assumptions, we get $p \equiv q \equiv 1 \pmod 4$. Reducing $\mathcal{T}_6$ modulo 4, we get $N^2 \equiv 3M^4 - e^4 \pmod 4$. By the divisibility criteria, we can consider the following scenarios:

1. N even, M odd and e odd. In this case, we arrive at a contradictory statement: $0 \equiv 3 - 1 \equiv 2 \pmod 4$.
2. N odd, M even and e odd. In this case, we have $1 \equiv 0 - 1 \equiv 3 \pmod 4$, which is false.
3. N odd, M odd and e even. In this case, we have $1 \equiv 3 - 0 \equiv 3 \pmod 4$, which is a contradiction.

In any case, we get a contradiction. Thus, $\mathcal{T}_6$ has no solutions in $\mathbb{Z}$. □

Lemma 2.7. *There are no integer solutions for the torsor* $\mathcal{T}_7: \quad N^2 = qM^4 - 3pe^4$.

Proof. Reducing $\mathcal{T}_7$ modulo 3, we get $N^2 \equiv qM^4 \pmod 3$. This implies

$$1 = \left(\frac{qM^4}{3}\right) = \left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

since $q \equiv 2 \pmod 3$. This is a contradiction. Thus, $\mathcal{T}_7$ has no solutions in $\mathbb{Z}$. □

We have presented that $\alpha(\Gamma) = \{1, -3pq\}$ and so $|\alpha(\Gamma)| = 2$. We then determine $|\overline{\alpha}(\overline{\Gamma})|$. Recall that $\overline{E}: y^2 = x^3 + 12pqx$ and we already have $1, 12pq \in \overline{\alpha}(\overline{\Gamma})$. We also have all the possible divisors b_1 of $12pq$ modulo $\mathbb{Q}^{\times 2}$ in the following set

$$\{2, 3, 4, 6, 12, q, 2q, 3q, 4q, 6q, 12q, p, 2p, 3p, 4p, 6p, 12p, pq, 2pq, 3pq, 4pq, 6pq\}.$$

We removed the negative values of b_1 since the corresponding torsors $N^2 = b_1M^4 + b_2e^4$ will have no solutions if b_1 and b_2 are both negative. Hence, we consider the solvability of the following torsors over the set of integers.

$$\begin{aligned}
\mathcal{T}_1^{'}: &\quad N^2 = 2M^4 + 6pqe^4 \\
\mathcal{T}_2^{'}: &\quad N^2 = 3M^4 + 4pqe^4 \\
\mathcal{T}_3^{'}: &\quad N^2 = 4M^4 + 3pqe^4. \\
\mathcal{T}_4^{'}: &\quad N^2 = 6M^4 + 2pqe^4
\end{aligned}$$

$$\begin{aligned}
\mathcal{T}_5^{'}: &\quad N^2 = 12M^4 + pqe^4. \\
\mathcal{T}_6^{'}: &\quad N^2 = qM^4 + 12pe^4 \\
\mathcal{T}_7^{'}: &\quad N^2 = 2qM^4 + 6pe^4. \\
\mathcal{T}_8^{'}: &\quad N^2 = 3qM^4 + 4pe^4 \\
\mathcal{T}_9^{'}: &\quad N^2 = 4qM^4 + 3pe^4 \\
\mathcal{T}_{10}^{'}: &\quad N^2 = 6qM^4 + 2pe^4. \\
\mathcal{T}_{11}^{'}: &\quad N^2 = 12qM^4 + pe^4
\end{aligned}$$

Lemma 2.8. *There are no integer solutions for the torsor* $\mathcal{T}_1^{'}: \ N^2 = 2M^4 + 6pqe^4$.

Proof. Reducing $\mathcal{T}_1^{'}$ modulo 3, we get $N^2 \equiv 2M^4 \pmod 3$. This implies

$$1 = \left(\frac{2M^4}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

which is a contradiction. Thus, $\mathcal{T}_1^{'}$ has no solutions in $\mathbb{Z}$. □

Lemma 2.9. *There are no integer solutions for the torsor* $\mathcal{T}_2^{'}: \ N^2 = 3M^4 + 4pqe^4$.

Proof. By the divisibility criteria, since $4pq$ is even, we have M odd and consequently, N odd. Thus, $N^2 \equiv M^4 \equiv 1 \pmod 4$. Reducing $\mathcal{T}_2^{'}$ modulo 4, we get $1 \equiv 3(1) \pmod 4$. We get a contradiction. Thus, $\mathcal{T}_2^{'}$ has no solutions in $\mathbb{Z}$. □

Lemma 2.10. *There are no integer solutions for the torsor* $\mathcal{T}_3^{'}: \ N^2 = 4M^4 + 3pqe^4$.

Proof. By the divisibility criteria, since 4 is even, we have e odd and consequently, N odd. Thus, $N^2 \equiv e^4 \equiv 1 \pmod 4$. Also, $p \equiv q \equiv 1 \pmod 4$ by assumption. Reducing $\mathcal{T}_3^{'}$ modulo 4, we get $1 \equiv 3 \pmod 4$, which is a contradiction. Thus, $\mathcal{T}_3^{'}$ has no solutions in $\mathbb{Z}$. □

Lemma 2.11. *There are no integer solutions for the torsor* $\mathcal{T}_4^{'}: \ N^2 = 6M^4 + 2pqe^4$.

Proof. By the divisibility criteria, we have $3 \nmid e$ and consequently, $3 \nmid N$. Thus, $N^2 \equiv e^4 \equiv 1 \pmod 3$. Also, $p \equiv q \equiv 2 \pmod 3$. Reducing $\mathcal{T}_4^{'}$ modulo 3, we get $1 \equiv 2(2)(2) \equiv 2 \pmod 3$, which is a contradiction. Thus, $\mathcal{T}_4^{'}$ has no solutions in $\mathbb{Z}$. □

Lemma 2.12. *There are no integer solutions for the torsor* $\mathcal{T}_5^{'}: \ N^2 = 12M^4 + pqe^4$.

Proof. Reducing $\mathcal{T}_5^{'}$ modulo p, we get $N^2 \equiv 12M^4 \pmod p$. This implies

$$1 = \left(\frac{12M^4}{p}\right) = \left(\frac{3}{p}\right).$$

Since

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12} \end{cases},$$

we obtain $p \equiv 1$ or $11 \pmod{12}$. This is a contradiction to the assumption that $p \equiv 5 \pmod{12}$. Thus, $\mathcal{T}_5^{'}$ has no solutions in $\mathbb{Z}$. □

Lemma 2.13. *There are no integer solutions for the torsor* $\mathcal{T}_6'$: $N^2 = qM^4 + 12pe^4$.

Proof. Reducing $\mathcal{T}_6'$ modulo 3, we get $N^2 \equiv qM^4 \pmod 3$. This implies

$$1 = \left(\frac{qM^4}{3}\right) = \left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

since $q \equiv 2 \pmod 3$. This is a contradiction. Thus, $\mathcal{T}_6'$ has no solutions in $\mathbb{Z}$. □

Lemma 2.14. *There are no integer solutions for the torsor* $\mathcal{T}_7'$: $N^2 = 2qM^4 + 6pe^4$.

Proof. By the divisibility criteria, we know that both M and e are odd. Note also that there exists an integer N_1 such that $2N_1^2 = qM^4 + 3pe^4$. Reducing the equation modulo 8, we get $2N_1^2 \equiv q + 3p \pmod 8$. Note that $p \equiv q \equiv 5 \pmod 8$ by assumption. So we get $2N_1^2 \equiv 5 + 3(5) \equiv 4 \pmod 8$. Dividing both sides by 2, we obtain $N_1^2 \equiv 2 \pmod 4$, which is a contradiction. Thus, $\mathcal{T}_7'$ has no solutions in $\mathbb{Z}$. □

Lemma 2.15. *There are no integer solutions for the torsor* $\mathcal{T}_8'$: $N^2 = 3qM^4 + 4pe^4$.

Proof. By the divisibility criteria, we have $3 \nmid e$ and consequently, $3 \nmid N$. Thus, $N^2 \equiv e^4 \equiv 1 \pmod 3$. Also, $p \equiv q \equiv 2 \pmod 3$ by assumption. Reducing $\mathcal{T}_8'$ modulo 3, we get $1 \equiv 2 \pmod 3$, which is a contradiction. Thus, $\mathcal{T}_8'$ has no solutions in $\mathbb{Z}$. □

Lemma 2.16. *There are no integer solutions for the torsor* $\mathcal{T}_9'$: $N^2 = 4qM^4 + 3pe^4$.

Proof. By divisibility criteria, since $4q$ is even, we have e odd. Reducing $\mathcal{T}_9'$ modulo 4, we get $N^2 \equiv 3pe^4 \equiv 3p \pmod 4$. Since $p \equiv 1 \pmod 4$, we obtain $N^2 \equiv 3 \pmod 4$, which is a contradiction. Thus, $\mathcal{T}_9'$ has no solutions in $\mathbb{Z}$. □

Lemma 2.17. *There are no integer solutions for the torsor* $\mathcal{T}_{10}'$: $N^2 = 6qM^4 + 2pe^4$.

Proof. By the divisibility criteria, we know that both M and e are odd. Note also that there exists an integer N_1 such that $2N_1^2 = 3qM^4 + pe^4$. Reducing the equation modulo 8, we get $2N_1^2 \equiv 3q + p \pmod 8$. Note that $p \equiv q \equiv 5 \pmod 8$ by assumption. So we get $2N_1^2 \equiv 3(5) + 5 \equiv 4 \pmod 8$. Dividing both sides by 2, we obtain $N_1^2 \equiv 2 \pmod 4$, which is a contradiction. Thus, $\mathcal{T}_{10}'$ has no solutions in $\mathbb{Z}$. □

Lemma 2.18. *There are no integer solutions for the torsor* $\mathcal{T}_{11}'$: $N^2 = 12qM^4 + pe^4$.

Proof. Reducing $\mathcal{T}_{11}'$ modulo 3, we get $N^2 \equiv pe^4 \pmod 3$. This implies

$$1 = \left(\frac{pe^4}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

since $p \equiv 2 \pmod 3$. This is a contradiction. Thus, $\mathcal{T}_{11}'$ has no solutions in $\mathbb{Z}$. □

Thus, we have shown that $\overline{\alpha}(\overline{\Gamma}) = \{1, 12pq\}$ and so $|\overline{\alpha}(\overline{\Gamma})| = 2$. Using the formula for the rank, we have

$$2^r = \frac{1}{4}(|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|) = \frac{(2)(2)}{4} = 1,$$

for which we get that $r = 0$. This proves the main result. □

By imposing less stricter assumptions on p and q, the following corollaries are obtained:

Corollary 2.1. *Under the same assumptions of Theorem 2.1, if the congruence* $p \equiv 5 \pmod{24}$ *is replaced by* $p \equiv 5 \pmod{12}$*, then the elliptic curve* E *has rank at most one.*

Proof. The removed restriction from this case is that p need not satisfy $p \equiv 5 \pmod{8}$. In that case, we see from the proof of Theorem 2.1 that all but two torsors $\mathcal{T}_7'$ and $\mathcal{T}_{10}'$, did not use the assumption $p \equiv 5 \pmod{8}$. This implies that the torsors $\mathcal{T}_7'$ and $\mathcal{T}_{10}'$ may have solutions. So it is possible that $2q, 6p, 2p, 6q \in \overline{\alpha}(\overline{\Gamma})$ making $|\overline{\alpha}(\overline{\Gamma})| \leq 6$. As a consequence, we obtain $0 \leq r \leq 1$. □

The same holds if we replace the assumption $q \equiv 5 \pmod{24}$ by $q \equiv 5 \pmod{12}$ in Theorem 2.1. From this corollary, we obtain specific values of p and q such that the rank of E is exactly one.

Theorem 2.2. *Let* $p = 24k + 17$ *and* $q = 24\ell + 5$ *for some* $k, \ell \in \mathbb{N}_0$*. If* $9k + 3\ell + 7$ *is a perfect square, then* E *has rank equal to one.*

Proof. If $p = 24k + 17$ and $q = 24\ell + 5$, then it satisfies the assumptions of Corollary 2.1, so, the only torsors that may have a solution are $\mathcal{T}_7'$ and $\mathcal{T}_{10}'$. Also,

$$\mathcal{T}_7' : \quad N^2 = 2(24\ell + 5)M^4 + 6(24k + 17)e^4$$

has a solution $(N, M, e) = (4\sqrt{9k + 3\ell + 7}, 1, 1)$. Hence, $2q, 6p \in \overline{\alpha}(\overline{\Gamma})$. Moreover, $\mathcal{T}_{10}'$ cannot have a solution, otherwise, $2p, 6q \in \overline{\alpha}(\overline{\Gamma})$ would imply that

$$|\overline{\alpha}(\overline{\Gamma})| = 6.$$

Applying the rank's formula, we obtain

$$2^r = \frac{1}{4}(|\alpha(\Gamma)|)|\overline{\alpha}(\overline{\Gamma})| = \frac{(2)(6)}{4} = 3,$$

which is not possible. Hence, $|\overline{\alpha}(\overline{\Gamma})| = 4$. As a consequence, we obtain $r = 1$. □

To confirm our result in Theorem 2.1, we list down in Table 1 some pairs of primes p and $q > p$ that satisfy the said conditions, and the rank of the corresponding elliptic curves. All computations are done in SAGE [11].

Also, to confirm our results in Theorem 2.2, we list down in Table 2 some prime pairs p and $q > p$ that satisfy the said conditions, the corresponding rank of E and a generator of the free part of the Mordell-Weil group.

Table 1: Values of primes p and q that satisfy conditions in Theorem 2.1.

p	q	$\text{rank}(E)$
5	29	0
29	53	0
53	149	0
101	197	0
149	173	0
173	197	0
173	269	0
269	389	0

Table 2: Values of primes p and q that satisfy conditions in Theorem 2.2.

k	ℓ	p	q	$\text{rank}(E)$	generator
0	6	17	149	1	$(100, 490)$
0	19	17	461	1	$(256, 3280)$
1	11	41	269	1	$(196, 1022)$
3	29	89	701	1	$(484, 4774)$
4	7	113	173	1	$(256, 1328)$
4	19	113	461	1	$(400, 1220)$
5	16	137	389	1	$(400, 220)$
5	23	137	557	1	$(484, 1606)$

Acknowledgement The authors would like to thank University of the Philippines Baguio and DOST-ASTHRDP for the support given in the conduct of the study. They also would like to thank the referees for devoting their time and effort in reviewing the manuscript, and achieving a quality output.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] H. Daghigh & S. Didari (2014). On the elliptic curves of the form $y^2 = x^3 - 3px$. *Bulletin of the Iranian Mathematical Society*, *40*(5), 1119–1133.

[2] H. Daghigh & S. Didari (2015). On the elliptic curves of the form $y^2 = x^3 - pqx$. *Iranian Journal of Mathematical Sciences and Informatics*, *10*(2), 77–86. https://doi.org/10.7508/ijmsi.2015.02.008.

[3] Y. Fujita & N. Terai (2011). Integer points and independent points on the elliptic curves $y^2 = x^3 - p^k x$. *Tokyo Journal of Mathematics*, *34*(2), 365–381.

[4] A. Hollier, B. Spearman & Q. Yang (2010). Elliptic curves $y^2 = x^3 + pqx$ with maximal rank. *International Mathematical Forum*, *5*(21-24), 1105–1110.

[5] N. Ismail & M. Misro (2022). Bezier coefficients matrix for elgamal elliptic curve cryptosystem. *Malaysian Journal of Mathematical Sciences*, *16*(3), 483–499. https://doi.org/10.47836/mjms.16.3.06.

[6] S. W. Kim (2015). Ranks of elliptic curves $y^2 = x^3 \pm 4px$. *International Journal of Algebra*, *9*(5), 205–211. https://doi.org/10.12988/ija.2015.5421.

[7] N. F. H. A. Saffar & M. R. M. Said (2015). Speeding up the elliptic curve scalar multiplication using the window-w non adjacent form. *Malaysian Journal of Mathematical Sciences*, *9*(1), 91–110.

[8] J. H. Silverman & J. Tate (1985). *Rational points on elliptic curves*. Springer, New York.

[9] B. Spearman (2007). Elliptic curves $y^2 = x^3 - px$ of rank two. *Mathematical Journal of Okayama University*, *49*, 183–184.

[10] B. Spearman (2007). On the group structure of elliptic curves $y^2 = x^3 - 2px$. *International Journal of Algebra*, *1*(5-8), 247–250. http://dx.doi.org/10.12988/ija.2007.07026.

[11] W. A. Stein (2020). Sage mathematics software (version 9.2). *The Sage Development Team*, (USA). http://www.sagemath.org.