# RANK OF THE ELLIPTIC CURVE $y^2 = x^3 - 2pqx$

**Renz Jimwel Mina**
*Department of Mathematics and Computer Science, University of the Philippines Baguio, Baguio City, Philippines*
rsmina1@up.edu.ph

**Jerico Bacani**
*Department of Mathematics and Computer Science, University of the Philippines Baguio, Baguio City, Philippines*
jbbacani@up.edu.ph

*Received: 8/29/25, Accepted: 3/25/26, Published: 5/1/26*

**Abstract**

This paper aims to determine the rank of the elliptic curve $E_{2pq} : y^2 = x^3 - 2pqx$ defined over the field of rational numbers. The associated Selmer groups with respect to a 2-isogeny are completely determined to provide upper bounds for its rank for each pair of distinct odd primes $p$ and $q$, and the parity conjecture is used to refine the results. Finally, an infinite number of elliptic curves $E_{2pq}$ with rank three is provided, assuming that a conjecture of Schinzel and Sierpinski holds.

## 1. Introduction

For an elliptic curve $E$ defined over the field of rational numbers $\mathbb{Q}$, it is known that the set $E(\mathbb{Q})$ of rational points together with the point at infinity $\mathcal{O}$ forms an abelian group (called the *Mordell-Weil group*) that is isomorphic to $T \times \mathbb{Z}^{\text{rank}(E(\mathbb{Q}))}$, where $T$ is a finite abelian group, and $\text{rank}(E(\mathbb{Q}))$ is a nonnegative number called the *Mordell-Weil rank* or simply the *rank* of $E(\mathbb{Q})$. One of the interesting problems in the study of elliptic curves is the determination of ranks. Recently, there have been studies that aimed to classify elliptic curves

$$E_n : y^2 = x^3 - nx,$$

where $n$ is a product of primes, in terms of their ranks. Specifically, Spearman [9, 10] considered the cases where $n$ is prime or twice a prime number. He provided conditions on $n$ so that $E_n$ has rank exactly two and three, respectively. In 2010, Hollier, Spearman, and Yang [5] studied the case where $n = -pq$, with $p$ and $q$

DOI: 10.5281/zenodo.19949477

representing distinct primes. They were successful in providing conditions on $p$ and $q$ so that $E_n$ has rank exactly four. In 2011, Fujita and Terai [4] gave a necessary and sufficient condition so that $E_n$ for $n = p^k$, where $p$ is prime and $k \in \{1, 2, 3\}$, has rank one or two. In 2015, Daghigh and Didari [2] classified the Selmer groups of $E_n$, where $n = 3p$, $p \neq 3$ a prime, which in turn gave bounds for the rank of $E_n$. A similar study was done by the same authors for the case where $n = pq$, where $p$ and $q$ are distinct primes [3]. In 2023, Mina and Bacani [6] considered $E_n$, where $n = 3pq$ and $p, q \neq 3$ are distinct odd primes. They provided some conditions on $p$ and $q$ so that the rank of $E_n$ is zero or one.

Motivated by the works mentioned above, the present study deals with the elliptic curve $E_n$ where $n = 2pq$ and $p$ and $q$ are distinct odd primes. Here, the Selmer groups of $E_{2pq}$, whose cardinalities give an upper bound for the rank of $E_{2pq}$, are completely classified and an upper bound for the rank for each possible case is obtained. Moreover, the well-known parity conjecture is used to refine the results obtained. The main results are stated in the following theorem.

**Theorem 1.** *Let $p$ and $q$ be distinct odd primes and consider the elliptic curve*

$$E_{2pq} : y^2 = x^3 - 2pqx.$$

*Assuming the validity of the parity conjecture for $E_{2pq}$, the following statements hold.*

*i. If one of the following is satisfied,*

   *a.* $(p, q) \equiv (3, 3), (3, 5), (3, 7), (5, 5),$ *or* $(5, 7) \pmod 8$,
   *b.* $(p, q) \equiv (1, 3), (1, 5),$ *or* $(1, 7) \pmod 8$, *and* $\left(\frac{p}{q}\right) = -1$,

   *then* $\operatorname{rank}(E_{2pq}(\mathbb{Q})) = 1$.

*ii. If one of the following is satisfied,*

   *a.* $(p, q) \equiv (1, 1) \pmod 8$ *and* $\left(\frac{p}{q}\right) = -1$,
   *b.* $(p, q) \equiv (7, 7) \pmod 8$,
   *c.* $(p, q) \equiv (1, 3), (1, 5),$ *or* $(1, 7) \pmod 8$, *and* $\left(\frac{p}{q}\right) = 1$,

   *then* $\operatorname{rank}(E_{2pq}(\mathbb{Q})) = 1$ *or* $3$.

*iii. If* $(p, q) \equiv (1, 1) \pmod 8$ *and* $\left(\frac{p}{q}\right) = 1$, *then* $\operatorname{rank}(E_{2pq}(\mathbb{Q})) = 1, 3,$ *or* $5$.

*The above statements also hold if $p$ and $q$ are interchanged.*

Here, there are no additional conditions that set apart the primes $p$ and $q$. This means that if the case $(p, q) \equiv (3, 5) \pmod 8$ yields $E_{2pq}$ having rank one, then the case $(p, q) \equiv (5, 3) \pmod 8$ also yields $E_{2pq}$ having rank one.

One of the numerical observations obtained using PARI/GP [11] is that for each prime pair $(p, q) \pmod 8$ in part iii., the rank of $E_{2pq}$ is either one or three for $p, q < 1000$. Thus, it is conjectured that the rank is at most three for each prime pair in part iii. of Theorem 1.

The next theorem gives an infinite family of elliptic curves $E_{2pq}$ having rank equal to three provided that a conjecture of Schinzel and Sierpinski holds. This conjecture will be presented in Section 2.

**Theorem 2.** *If* $p = 272r^2+120r+9$ *and* $q = 2p+9 = 544r^2+240r+27$ *are primes for some positive integer* $r$*, then* $\operatorname{rank}(E_{2pq}(\mathbb{Q})) = 3$ *assuming that the parity conjecture holds for* $E_{2pq}$*. Moreover, assuming that the conjecture of Schinzel and Sierpinski holds, then there exist infinitely many elliptic curves* $E_{2pq}$ *with rank equal to* 3*.*

Table 1 shows primes $p$ and $q$ that yield a rank-three elliptic curve $E_{2pq}$. These results are verified numerically using PARI/GP.

| $r$ | $p$ | $q$ | $r$ | $p$ | $q$ |
|---|---|---|---|---|---|
| 1 | 401 | 811 | 50 | 686009 | 1372027 |
| 10 | 28409 | 56827 | 73 | 1458257 | 2916523 |
| 17 | 80657 | 161323 | 85 | 1975409 | 3950827 |
| 40 | 440009 | 880027 | 94 | 2414681 | 4829371 |
| 43 | 508097 | 1016203 | 109 | 3244721 | 6489451 |

Table 1: Some values of primes $p$ and $q$ such that $E_{2pq}$ has rank three.

## 2. Preliminaries

In this section, the necessary tools for the main results will be discussed.

An *isogeny* from one elliptic curve to another is a homomorphism that is given by rational functions. If such a mapping exists, then the two elliptic curves are said to be *isogenous*. For the elliptic curve

$$E_n/\mathbb{Q} : y^2 = x^3 - nx,$$

there is an isogeny of degree two given by $\phi : E_n \to E'_n$, $(x, y) \mapsto (y^2/x^2, -y(n + x^2)/x^2)$, where

$$E'_n/\mathbb{Q} : y^2 = x^3 + 4nx.$$

Moreover, $\widehat{\phi} : E'_n \to E_n$ given by $(x, y) \mapsto (y^2/4x^2, y(4n - x^2)/8x^2)$ is also an isogeny, called the *dual isogeny* to $\phi$. Define the following sets

$$S := \{\text{primes } p \text{ such that } p \mid \Delta_{E_n} = 2^6 \cdot n^3\} \cup \{\infty\}$$

and

$$\mathbb{Q}(S,2) := \{d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \mathrm{ord}_p(d) \equiv 0 \pmod 2 \text{ for all } p \notin S\},$$

where $\mathrm{ord}_p$ is the $p$-adic valuation on $\mathbb{Q}$. For each $d \in \mathbb{Q}(S,2)$, define the *homogeneous spaces* $C_d/\mathbb{Q} : dw^2 = d^2 + 4nz^4$ and $C'_d/\mathbb{Q} : dw^2 = d^2 - nz^4$. The *$\phi$-Selmer group* and *$\widehat{\phi}$-Selmer group* are defined as

$$S^{(\phi)}(E_n/\mathbb{Q}) := \{d \in \mathbb{Q}(S,2) : C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in S\},$$
$$S^{(\widehat{\phi})}(E'_n/\mathbb{Q}) := \{d \in \mathbb{Q}(S,2) : C'_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in S\},$$

respectively. Define the map $\delta : E'_n(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by

$$\begin{aligned}\delta(\mathcal{O}) &= 1 \pmod{(\mathbb{Q}^*)^2},\\ \delta(0,0) &= 4n \equiv n \pmod{(\mathbb{Q}^*)^2},\\ \delta(x,y) &= x \pmod{(\mathbb{Q}^*)^2},\ (x,y) \neq (0,0), \mathcal{O}.\end{aligned}$$

Similarly, define $\delta' : E_n(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by

$$\begin{aligned}\delta'(\mathcal{O}) &= 1 \pmod{(\mathbb{Q}^*)^2},\\ \delta'(0,0) &= -n \pmod{(\mathbb{Q}^*)^2},\\ \delta'(x,y) &= x \pmod{(\mathbb{Q}^*)^2},\ (x,y) \neq (0,0), \mathcal{O}.\end{aligned}$$

The images $\mathrm{Im}(\delta)$ and $\mathrm{Im}(\delta')$ of the maps $\delta$ and $\delta'$ are subgroups of the $\phi$-Selmer group and the $\widehat{\phi}$-Selmer group, respectively. The corresponding quotient groups are called the *$\phi$-part and the $\widehat{\phi}$-part of the Shafarevich-Tate group*, denoted by $Ш(E_n/\mathbb{Q})[\phi]$ and $Ш(E'_n/\mathbb{Q})[\widehat{\phi}]$, respectively. The nontrivial elements of these quotient groups, if they exist, correspond to homogeneous spaces that are everywhere locally solvable but have no global solution. The following exact sequences summarizes the relation of the groups:

$$0 \longrightarrow \mathrm{Im}(\delta) \longrightarrow S^{(\phi)}(E_n/\mathbb{Q}) \longrightarrow Ш(E_n/\mathbb{Q})[\phi] \longrightarrow 0,$$
$$0 \longrightarrow \mathrm{Im}(\delta') \longrightarrow S^{(\widehat{\phi})}(E'_n/\mathbb{Q}) \longrightarrow Ш(E'_n/\mathbb{Q})[\widehat{\phi}] \longrightarrow 0.$$

A formula for the rank of $E_n$ is given by

$$\begin{aligned}\mathrm{rank}(E_n(\mathbb{Q})) = \dim_{\mathbb{F}_2} S^{(\phi)}(E_n/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\widehat{\phi})}(E'_n/\mathbb{Q}) -\\ \dim_{\mathbb{F}_2} Ш(E_n/\mathbb{Q})[\phi] - \dim_{\mathbb{F}_2} Ш(E'_n/\mathbb{Q})[\widehat{\phi}] - 2.\end{aligned}$$

Removing the two nonpositive terms on the right-hand side gives an upper bound

$$\dim_{\mathbb{F}_2} S^{(\phi)}(E_n/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\widehat{\phi})}(E'_n/\mathbb{Q}) - 2$$

for the rank, called the *Selmer rank*. The Hensel's lemma is used to determine the local solvability of homogeneous spaces needed in the computation of Selmer groups.

**Lemma 1** (Hensel's lemma, [8])**.** *Let* $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$. *Suppose*

$$\mathrm{ord}_p(f(a_1, \ldots, a_n)) > 2\,\mathrm{ord}_p\left(\frac{\partial f}{\partial x_i}(a_1, \ldots, a_n)\right)$$

*for some* $1 \leq i \leq n$ *and* $(a_1, \ldots, a_n) \in \mathbb{Z}_p^n$. *Then* $f(x_1, \ldots, x_n) = 0$ *has a solution in* $\mathbb{Z}_p^n$.

For an elliptic curve $E$ defined over $\mathbb{Q}$ and a prime number $p$, let $n_p$ be the number of points on the reduction of $E$ modulo $p$ and let $a_p = p + 1 - n_p$. The *local part of the L-series of* $E$ *at* $p$ is defined as

$$L_p(T) = \begin{cases} 1 - a_pT + pT^2 & \text{if } E \text{ has a good reduction at } p \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } p \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The *L-series of* $E$ is defined to be

$$L(E, s) = \prod_{\text{prime } p} \frac{1}{L_p(p^{-s})}.$$

This is known to have an analytic continuation to the entire complex plane, and it satisfies the functional equation

$$\Lambda(E, s) = \epsilon(E)\Lambda(E, 2 - s),$$

where

$$\Lambda(E, s) = (N_{E/\mathbb{Q}})^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s),$$

$N_{E/\mathbb{Q}}$ is the *conductor* of $E$, $\Gamma$ is the Gamma function, and $\epsilon(E) = \pm 1$ is the *root number* of $E$. The *parity conjecture* states that

$$\epsilon(E) = (-1)^{\mathrm{rank}(E(\mathbb{Q}))},$$

which is an implication of the Birch and Swinnerton-Dyer (BSD) conjecture.

For the elliptic curve $E_n/\mathbb{Q} : y^2 = x^3 - nx$, where $n$ is not divisible by 4 or any fourth power, Birch and Stephens [1] obtained an explicit form of the root number:

$$\epsilon(E_n) = \mathrm{sgn}(-n)w(n) \prod_{p^2||n} \left(\frac{-1}{p}\right)$$

with $p \geq 3$ a prime, and

$$w(n) = \begin{cases} -1 & \text{if } n \equiv 1, 3, 11, \text{ or } 13 \pmod{16}, \\ 1 & \text{if } n \equiv 2, 5, 6, 7, 9, 10, 14, \text{ or } 15 \pmod{16}. \end{cases}$$

For the case where $n = 2pq$, and $p$ and $q$ are distinct odd primes, the root number is $\epsilon(E_{2pq}) = -1$. Thus, $\text{rank}(E_{2pq}(\mathbb{Q}))$ is always odd.

Finally, the following conjecture by Schinzel and Sierpinski [7] is a generalization of Dirichlet's theorem on primes in arithmetic progression, and will be used to prove Theorem 2.

**Conjecture 1** ([7])**.** Let $f_1(x), f_2(x), \ldots, f_n(x) \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading coefficients. Assuming that there is no integer greater than 1 that divides $f_1(k), f_2(k), \ldots, f_n(k)$ for all $k \in \mathbb{Z}$, then there are infinitely many positive integers $l$ such that $f_1(l), f_2(l), \ldots, f_n(l)$ are all primes.

## 3. Proofs of Main Results

*Proof of Theorem 1.* The first goal is to classify the Selmer groups of $E_{2pq}$. Note that $E_{2pq}$ has discriminant $\Delta_{E_{2pq}} = 2^9p^3q^3$. The 2-isogenous curve to $E_{2pq}$ is given by $E'_{2pq} : y^2 = x^3 + 8pqx$. Then $S = \{\infty, 2, p, q\}$ and

$$\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\}.$$

For each $d \in \mathbb{Q}(S, 2)$, the corresponding homogeneous spaces are given by

$$C_d : dw^2 = d^2 + 8pqz^4 \tag{1}$$

and

$$C'_d : dw^2 = d^2 - 2pqz^4. \tag{2}$$

Note that the images of $\mathcal{O}$ and $(0, 0)$ under $\delta$ and $\delta'$ are

$$1, 2pq \in S^{(\phi)}(E_{2pq}/\mathbb{Q}) \quad \text{and} \quad 1, -2pq \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q}),$$

respectively. Consider the other values $d \in \mathbb{Q}(S, 2)$. Note that $d$ and $2pq/d$ both correspond to the homogeneous space $C_d$. To see that, replace $d$ by $2pq/d$, to obtain $dw^2 = 2pq + 4d^2z^4$. Replacing $(z, w)$ by $(1/2z, w/2z^2)$, gives $dw^2 = d^2 + 8pqz^4$, which is the original homogeneous space. Similarly, $d$ and $-2pq/d$ both correspond to the homogeneous space $C'_d$. Thus, each case comes in pairs. One may use the value that will make the computation less complicated. Let $f(w) = dw^2$ and $g(z) = d^2 + 8pqz^4$. We have the following cases.

`Case 1:` $d < 0$. Note that $C_d(\mathbb{Q}_\infty) = C_d(\mathbb{R}) = \emptyset$ since $f(w) \leq 0$, while $g(z) > 0$.

`Case 2:` $d = 2, pq$.

$\mathbb{Q}_2$. Let $(z, w) \in C_{pq}(\mathbb{Q}_2)$ and $v := \text{ord}_2(z)$. Note that $\text{ord}_2(f(w))$ is even. This implies that $\text{ord}_2(g(z)) = \min\{0, 3 + 4v\} = 0$, that is, $v \geq 0$. Consequently,

$\mathrm{ord}_2(f(w)) = 0$, so $\mathrm{ord}_2(w) = 0$. Thus, $z, w \in \mathbb{Z}_2$. Reducing Equation (1) modulo 8 yields $pq \equiv 1 \pmod 8$. Conversely, if $pq \equiv 1 \pmod 8$ then the solution $w = 1$ to the congruence $w^2 \equiv pq \pmod 8$ lifts to a point in $C_{pq}(\mathbb{Q}_2)$ by Hensel's lemma (Lemma 1). Thus, $pq \equiv 1 \pmod 8$ if and only if $C_{pq}(\mathbb{Q}_2) \neq \emptyset$.

$\mathbb{Q}_p$. Let $(z, w) \in C_2(\mathbb{Q}_p)$. Using similar arguments as above, one can show that $z, w \in \mathbb{Z}_p$. In addition, one gets $\left(\frac{2}{p}\right) = 1$ upon reducing Equation (1) modulo $p$. Conversely, if $\left(\frac{2}{p}\right) = 1$, then any solution to the congruence $w^2 \equiv 2 \pmod p$ extends to a point in $C_2(\mathbb{Q}_p)$. Hence, $p \equiv 1$ or $7 \pmod 8$ if and only if $C_2(\mathbb{Q}_p) \neq \emptyset$.

$\mathbb{Q}_q$. Similarly, $q \equiv 1$ or $7 \pmod 8$ if and only if $C_2(\mathbb{Q}_q) \neq \emptyset$.

Thus, $2, pq \in S^{(\phi)}(E_{2pq}/\mathbb{Q})$ if and only if $p \equiv q \equiv 1$ or $7 \pmod 8$.

`Case 3:` $d = p, q, 2q, 2p$.

$\mathbb{Q}_2$. Let $(z, w) \in C_p(\mathbb{Q}_2)$. Following similar arguments as in prior cases, it follows that $z, w \in \mathbb{Z}_2$. Upon reducing Equation (1) modulo 8, it emerges that $p \equiv 1 \pmod 8$. Conversely, if $p \equiv 1 \pmod 8$, then the solution $w = 1$ to $w^2 \equiv p \pmod 8$ translates to a point in $C_p(\mathbb{Q}_2)$. Hence, $p \equiv 1 \pmod 8$ if and only if $C_p(\mathbb{Q}_2) \neq \emptyset$. Likewise, $q \equiv 1 \pmod 8$ if and only if $C_q(\mathbb{Q}_2) \neq \emptyset$.

$\mathbb{Q}_p$. Let $(z, w) \in C_{2q}(\mathbb{Q}_p)$. Analogous to preceding instances, it follows that $z, w \in \mathbb{Z}_p$. Upon reducing Equation (1) modulo $p$, we deduce $\left(\frac{2q}{p}\right) = 1$. Conversely, if $\left(\frac{2q}{p}\right) = 1$ then any solution to $w^2 \equiv 2q \pmod p$ projects to a point in $C_{2q}(\mathbb{Q}_p)$. Thus, $\left(\frac{2q}{p}\right) = 1$ if and only if $C_{2q}(\mathbb{Q}_p) \neq \emptyset$. Analogously, we have $\left(\frac{2p}{q}\right) = 1$ if and only if $C_{2p}(\mathbb{Q}_q) \neq \emptyset$.

$\mathbb{Q}_q$. Let $(z, w) \in C_p(\mathbb{Q}_q)$. Similar to previous cases, $z, w \in \mathbb{Z}_q$. Reducing Equation (1) modulo $q$ yields $\left(\frac{p}{q}\right) = 1$. Conversely, if $\left(\frac{p}{q}\right) = 1$ then any solution to $w^2 \equiv p \pmod q$ lifts to a point in $C_p(\mathbb{Q}_q)$. Thus, $\left(\frac{p}{q}\right) = 1$ if and only if $C_p(\mathbb{Q}_q) \neq \emptyset$. Similarly, $\left(\frac{q}{p}\right) = 1$ if and only if $C_q(\mathbb{Q}_p) \neq \emptyset$.

Let $(z, w) \in C_p(\mathbb{Q}_q)$. Analogous to previous cases, we have $z, w \in \mathbb{Z}_q$. Reducing Equation (1) modulo $q$ yields $\left(\frac{p}{q}\right) = 1$. Conversely, if $\left(\frac{p}{q}\right) = 1$ then any solution to $w^2 \equiv p \pmod q$ lifts to a point in $C_p(\mathbb{Q}_q)$. Hence, $\left(\frac{p}{q}\right) = 1$ if and only if $C_p(\mathbb{Q}_q) \neq \emptyset$. Moreover, $\left(\frac{q}{p}\right) = 1$ if and only if $C_q(\mathbb{Q}_p) \neq \emptyset$.

Therefore, $p, 2q \in S^{(\phi)}(E_{2pq}/\mathbb{Q})$ if and only if $p \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = 1$. Also, $q, 2p \in S^{(\phi)}(E_{2pq}/\mathbb{Q})$ if and only if $q \equiv 1 \pmod 8$ and $\left(\frac{p}{q}\right) = 1$.

Table 2 shows the summary of the classification of the $\phi$-Selmer groups of $E_{2pq}$.

| $(p,q) \pmod 8$ | $S^{(\phi)}(E_{2pq}/\mathbb{Q})$ |
|---|---|
| $(3,3),(3,5),(3,7),(5,3),$ $(5,5),(5,7),(7,3),(7,5)$ or $(1,3),(1,5),(1,7),(3,1),(5,1),$ or $(7,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,2pq\}$ |
| $(7,7)$ or $(1,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,2pq,2,pq\}$ |
| $(1,3),(1,5)$ or $(1,7)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,2pq,p,2q\}$ |
| $(3,1),(5,1)$ or $(7,1)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,2pq,q,2p\}$ |
| $(1,1)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,2pq,2,pq,p,2q,q,2p\}$ |

Table 2: Classification of the $\phi$-Selmer groups of $E_{2pq}$.

The next goal is to determine $S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$. Let $f(w)=dw^2$ and $g(z)=d^2-2pqz^4$. We have the following cases.

`Case 1:` $d=-1,2pq$.

$\mathbb{Q}_2$. Let $(z,w)\in C'_{-1}(\mathbb{Q}_2)$. Similar to previous cases, $z,w\in\mathbb{Z}_2$. Reducing Equation (2) modulo 8 yields $pq\equiv 1 \pmod 4$. Conversely, if $pq\equiv 1 \pmod 4$ then the solution $(z,w)=(1,1)$ to $w^2\equiv -1+2pqz^4 \pmod 8$ lifts to a point in $C'_{-1}(\mathbb{Q}_2)$. Thus, $pq\equiv 1 \pmod 4$ if and only if $C'_{-1}(\mathbb{Q}_2)\neq\emptyset$.

$\mathbb{Q}_p$. Let $(z,w)\in C'_{-1}(\mathbb{Q}_p)$. As in preceding instances, it follows that $z,w\in\mathbb{Z}_p$. Reducing Equation (2) modulo $p$ yields $p\equiv 1 \pmod 4$. Conversely, if $p\equiv 1 \pmod 4$, then any solution to $w^2\equiv -1 \pmod p$, lifts to a point in $C'_{-1}(\mathbb{Q}_p)$. Thus, $p\equiv 1 \pmod 4$ if and only if $C'_{-1}(\mathbb{Q}_p)\neq\emptyset$.

$\mathbb{Q}_q$. Similarly, $q\equiv 1 \pmod 4$ if and only if $C'_{-1}(\mathbb{Q}_q)\neq\emptyset$.

Thus, $-1,2pq\in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $p\equiv q\equiv 1 \pmod 4$.

`Case 2:` $d=2,-pq$.

$\mathbb{Q}_2$. Let $(z,w)\in C'_{-pq}(\mathbb{Q}_2)$. As in previous cases, one can show that $z,w\in\mathbb{Z}_2$. Furthermore, $pq\equiv 1$ or $7 \pmod 8$ is obtained by reducing Equation (2) modulo 8. Conversely, if $pq\equiv 1 \pmod 8$, then the solution $(z,w)=(1,1)$ to $w^2\equiv -pq+2z^4 \pmod 8$ extends to a point in $C'_{-pq}(\mathbb{Q}_2)$. Thus, $pq\equiv 1$ or $7 \pmod 8$ if and only if $C'_{-pq}(\mathbb{Q}_2)\neq\emptyset$.

$\mathbb{Q}_p$. Let $(z,w)\in C'_2(\mathbb{Q}_p)$. Consequently, we have $z,w\in\mathbb{Z}_p$. Reducing Equation (2) modulo $p$, we obtain $\left(\frac{2}{p}\right)=1$. Conversely, if $\left(\frac{2}{p}\right)=1$ then any solution to $w^2\equiv 2 \pmod p$ extends to a point in $C'_2(\mathbb{Q}_p)$. Thus, $p\equiv 1$ or $7 \pmod 8$ if and only if $C'_2(\mathbb{Q}_p)\neq\emptyset$.

$\mathbb{Q}_q$. Similarly, $q \equiv 1$ or $7 \pmod 8$ if and only if $C_2'(\mathbb{Q}_q) \neq \emptyset$.

Therefore, $2, -pq \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $p$ and $q \equiv 1$ or $7 \pmod 8$.

Case 3: $d = -2, pq$.

$\mathbb{Q}_2$. Let $(z, w) \in C'_{pq}(\mathbb{Q}_2)$. Similar to what previously observed, we have $z, w \in \mathbb{Z}_2$. Reducing Equation (2) modulo 8 yields $pq \equiv 1$ or $3 \pmod 8$. Conversely, if $pq \equiv 1 \pmod 8$ then the solution $(z, w) = (0, 1)$ to $w^2 \equiv pq - 2z^4 \pmod 8$ lifts to a point in $C'_{pq}(\mathbb{Q}_2)$, and if $pq \equiv 3 \pmod 8$ then the solution $(z, w) = (1, 1)$ lifts to a point in $C'_{pq}(\mathbb{Q}_2)$. Thus, $pq \equiv 1$ or $3 \pmod 8$ if and only if $C'_{pq}(\mathbb{Q}_2) \neq \emptyset$.

$\mathbb{Q}_p$. Let $(z, w) \in C'_{-2}(\mathbb{Q}_p)$. Analogous to prior cases, $z, w \in \mathbb{Z}_p$. Reducing Equation (2) modulo $p$ yields $\left(\frac{-2}{p}\right) = 1$. Conversely, if $\left(\frac{-2}{p}\right) = 1$ then any solution to $w^2 \equiv -2 \pmod p$ extends to a point in $C'_{-2}(\mathbb{Q}_p)$. Thus, $p \equiv 1$ or $3 \pmod 8$ if and only if $C'_{-2}(\mathbb{Q}_p) \neq \emptyset$.

$\mathbb{Q}_q$. Similarly, $q \equiv 1$ or $3 \pmod 8$ if and only if $C'_{-2}(\mathbb{Q}_q) \neq \emptyset$.

Therefore, $-2, pq \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $p$ and $q \equiv 1$ or $3 \pmod 8$.

Case 4: $d = p, q, -2q, -2p$.

$\mathbb{Q}_2$. Let $(z, w) \in C'_p(\mathbb{Q}_2)$. Using similar arguments as before, we observed that $z, w \in \mathbb{Z}_2$. Simplifying Equation (2) modulo 8 leads to $p \equiv 1 \pmod 8$; or $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 7 \pmod 8$ and $q \equiv 3 \pmod 4$. Conversely, if $p \equiv 1 \pmod 8$ then the solution $(z, w) = (0, 1)$ to $w^2 \equiv p - 2qz^4 \pmod 8$ lifts to a point in $C'_p(\mathbb{Q}_2)$, and if $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 4$ or if $p \equiv 7 \pmod 8$ and $q \equiv 3 \pmod 4$, then the solution $(z, w) = (1, 1)$ lifts to a point in $C'_p(\mathbb{Q}_2)$. Thus, $p \equiv 1 \pmod 8$; or $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 7 \pmod 8$ and $q \equiv 3 \pmod 4$ if and only if $C'_p(\mathbb{Q}_2) \neq \emptyset$. Similarly, $q \equiv 1 \pmod 8$; or $q \equiv 3 \pmod 8$ and $p \equiv 1 \pmod 4$; or $q \equiv 7 \pmod 8$ and $p \equiv 3 \pmod 4$ if and only if $C'_q(\mathbb{Q}_2) \neq \emptyset$.

$\mathbb{Q}_p$. Let $(z, w) \in C'_{-2q}(\mathbb{Q}_p)$. Then, $z, w \in \mathbb{Z}_p$. Reducing Equation (2) modulo $p$ yields $\left(\frac{-2q}{p}\right) = 1$. Conversely, if $\left(\frac{-2q}{p}\right) = 1$ then any solution to $w^2 \equiv -2q \pmod p$ translates to a point in $C'_{-2q}(\mathbb{Q}_p)$. Thus, $\left(\frac{-2q}{p}\right) = 1$ if and only if $C'_{-2q}(\mathbb{Q}_p) \neq \emptyset$. Similarly, $\left(\frac{-2p}{q}\right) = 1$ if and only if $C'_{-2p}(\mathbb{Q}_q) \neq \emptyset$.

$\mathbb{Q}_q$. Let $(z, w) \in C'_p(\mathbb{Q}_q)$. As previously seen, $z, w \in \mathbb{Z}_q$. Reducing Equation (2) modulo $q$ yields $\left(\frac{p}{q}\right) = 1$. Conversely, if $\left(\frac{p}{q}\right) = 1$ then any solution to $w^2 \equiv p \pmod q$ projects to a point in $C'_p(\mathbb{Q}_q)$. Hence, $\left(\frac{p}{q}\right) = 1$ if and only if $C'_p(\mathbb{Q}_q) \neq \emptyset$. Analogously, $\left(\frac{q}{p}\right) = 1$ if and only if $C'_q(\mathbb{Q}_p) \neq \emptyset$.

Therefore, $p, -2q \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $p \equiv 1 \pmod 8$; or $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 7 \pmod 8$ and $q \equiv 3 \pmod 4$, and $\left(\frac{-2q}{p}\right) = \left(\frac{p}{q}\right) = 1$. Furthermore, $q, -2p \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $q \equiv 1 \pmod 8$; or $q \equiv 3 \pmod 8$ and $p \equiv 1 \pmod 4$; or $q \equiv 7 \pmod 8$ and $p \equiv 3 \pmod 4$, and $\left(\frac{-2p}{q}\right) = \left(\frac{q}{p}\right) = 1$.

`Case 5:` $d = -p, -q, 2q, 2p$.

$\mathbb{Q}_2$. Let $(z, w) \in C'_{-p}(\mathbb{Q}_2)$. We then observed that $z, w \in \mathbb{Z}_2$. Reducing Equation (2) modulo 8 yields $p \equiv 7 \pmod 8$; or $p \equiv 1 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$. Conversely, if $p \equiv 7 \pmod 8$ then the solution $(z, w) = (0, 1)$ to $w^2 \equiv -p + 2qz^4 \pmod 8$ lifts to a point in $C'_{-p}(\mathbb{Q}_2)$, and if $p \equiv 1 \pmod 8$ and $q \equiv 1 \pmod 4$ or if $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$, then the solution $(z, w) = (1, 1)$ extends to a point in $C'_{-p}(\mathbb{Q}_2)$. Thus, $p \equiv 7 \pmod 8$; or $p \equiv 1 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$ if and only if $C'_{-p}(\mathbb{Q}_2) \neq \emptyset$. Also, $q \equiv 7 \pmod 8$; or $q \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 4$; or $q \equiv 5 \pmod 8$ and $p \equiv 3 \pmod 4$ if and only if $C'_{-q}(\mathbb{Q}_2) \neq \emptyset$.

$\mathbb{Q}_p$. Let $(z, w) \in C'_{2q}(\mathbb{Q}_p)$. Similar to previous cases, $z, w \in \mathbb{Z}_p$. Reducing Equation (2) modulo $p$ one arrives at $\left(\frac{2q}{p}\right) = 1$. Conversely, if $\left(\frac{2q}{p}\right) = 1$ then any solution to $w^2 \equiv 2q \pmod p$ lifts to a point in $C'_{2q}(\mathbb{Q}_p)$. Thus, $\left(\frac{2q}{p}\right) = 1$ if and only if $C'_{2q}(\mathbb{Q}_p) \neq \emptyset$. Similarly, $\left(\frac{2p}{q}\right) = 1$ if and only if $C'_{2p}(\mathbb{Q}_q) \neq \emptyset$.

$\mathbb{Q}_q$. Let $(z, w) \in C'_{-p}(\mathbb{Q}_q)$. It follows that $z, w \in \mathbb{Z}_q$. Reducing Equation (2) modulo $q$ yields $\left(\frac{-p}{q}\right) = 1$. Conversely, if $\left(\frac{-p}{q}\right) = 1$ then any solution to $w^2 \equiv -p \pmod q$ lifts to a point in $C'_{-p}(\mathbb{Q}_q)$. Hence, $\left(\frac{-p}{q}\right) = 1$ if and only if $C'_{-p}(\mathbb{Q}_q) \neq \emptyset$. Analogously, $\left(\frac{-q}{p}\right) = 1$ if and only if $C'_{-q}(\mathbb{Q}_p) \neq \emptyset$.

Thus, $-p, 2q \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $p \equiv 7 \pmod 8$; or $p \equiv 1 \pmod 8$ and $q \equiv 1 \pmod 4$; or $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$, and $\left(\frac{2q}{p}\right) = \left(\frac{-p}{q}\right) = 1$. Moreover, $-q, 2p \in S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ if and only if $q \equiv 7 \pmod 8$; or $q \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 4$; or $q \equiv 5 \pmod 8$ and $p \equiv 3 \pmod 4$, and $\left(\frac{2p}{q}\right) = \left(\frac{-q}{p}\right) = 1$.

Table 3 shows the classification of the $\widehat{\phi}$-Selmer groups of $E_{2pq}$.

Using Tables 2 and 3, an upper bound for the rank, which is the Selmer rank, is obtained for each case. Since the rank is always odd assuming that the parity conjecture holds true for $E_{2pq}$, then the results of Theorem 1 is obtained. □

The proof of Theorem 2 is given as follows.

*Proof of Theorem 2.* Note that $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$ and

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{2p+9}{p}\right) = \left(\frac{9}{p}\right) = 1.$$

| $(p,q) \pmod 8$ | $S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q})$ |
|---|---|
| $(5,5)$<br>$(1,5)$ or $(5,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,-2pq,-1,2pq\}$ |
| $(1,7)$ or $(7,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,-2pq,2,-pq\}$ |
| $(3,3)$<br>$(1,3)$ or $(3,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,-2pq,-2,pq\}$ |
| $(3,5)$ or $(7,3)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,p,-2q\}$ |
| $(3,7)$ with $\left(\frac{p}{q}\right)=-1$<br>$(5,3)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,q,-2p\}$ |
| $(5,3),(5,7)$ or $(7,3)$, with $\left(\frac{p}{q}\right)=-1$<br>$(7,5)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,-p,2q\}$ |
| $(3,5)$ or $(7,5)$ with $\left(\frac{p}{q}\right)=-1$<br>$(3,7)$ or $(5,7)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,-q,2p\}$ |
| $(1,1)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,-2pq,-1,2pq,2,-pq,-2,pq\}$ |
| $(1,5)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,-1,2pq,p,-2q,-p,2q\}$ |
| $(5,1)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,-1,2pq,q,-2p,-q,2p\}$ |
| $(1,7)$ or $(7,7)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,2,-pq,p,-2q,-q,2p\}$ |
| $(7,1)$ with $\left(\frac{p}{q}\right)=1$<br>$(7,7)$ with $\left(\frac{p}{q}\right)=-1$ | $\{1,-2pq,2,-pq,q,-2p,-p,2q\}$ |
| $(1,3)$ or $(3,1)$ with $\left(\frac{p}{q}\right)=1$ | $\{1,-2pq,-2,pq,p,-2q,q,-2p\}$ |
| $(1,1)$ with $\left(\frac{p}{q}\right)=1$ | $\mathbb{Q}(S,2)$ |

Table 3: Classification of the $\widehat{\phi}$-Selmer groups of $E_{2pq}$.

By Theorem 1, $\operatorname{rank}(E_{2pq}) \leq 3$, and

$$S^{(\phi)}(E_{2pq}/\mathbb{Q}) = \{1, 2pq, p, 2q\},$$

and

$$S^{(\widehat{\phi})}(E'_{2pq}/\mathbb{Q}) = \{1,-2pq,-2,pq,p,-2q,q,-2p\}.$$

Now, the homogeneous space $C_p : w^2 = p+8qz^4$ has a solution $(w,z) = (68r+15,1)$. Consequently, $C_{2q}$ also has a solution. Also, the homogeneous space $C'_q : w^2 = q - 2pz^4$ has a solution $(w,z) = (3,1)$. Consequently, $C'_{-2p}$ also has a solution. Thus, $\dim_{\mathbb{F}_2} Ш(E_{2pq}/\mathbb{Q})[\phi] = 0$ and $\dim_{\mathbb{F}_2} Ш(E'_{2pq}/\mathbb{Q})[\widehat{\phi}] \leq 1$. As a consequence,

$$\begin{aligned}\operatorname{rank}(E_n(\mathbb{Q})) &= \dim_{\mathbb{F}_2} S^{(\phi)}(E_n/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\widehat{\phi})}(E'_n/\mathbb{Q}) - \\ &\qquad \dim_{\mathbb{F}_2} Ш(E_n/\mathbb{Q})[\phi] - \dim_{\mathbb{F}_2} Ш(E'_n/\mathbb{Q})[\widehat{\phi}] - 2 \\ &\geq 2+3-0-1-2 = 2.\end{aligned}$$

Since $2 \leq \operatorname{rank}(E_{2pq}(\mathbb{Q})) \leq 3$ and the parity conjecture guarantees that the rank is odd, it follows that $\operatorname{rank}(E_{2pq}(\mathbb{Q})) = 3$. Moreover, by Conjecture 1, there are

infinitely many primes $p = 272r^2 + 120r + 9$ and $q = 544r^2 + 240r + 27$, which means that there are infinitely many elliptic curves $E_{2pq}$ with rank equal to three. □

**Acknowledgements.** The authors would like to thank the University of the Philippines Baguio and the DOST-ASTHRDP for the support given in the conduct of the study.

## References

[1] B.J. Birch and N.M. Stephens, The parity of the rank of the Mordell-Weil group, *Topology*, **5** (1966), 295-299.

[2] H. Daghigh and S. Didari, S., On the elliptic curves of the form $y^2 = x^3 - 3px$, *Bull. Iran. Math. Soc.*, **40** (2014), 1119-1133.

[3] H. Daghigh and S. Didari, On the elliptic curves of the form $y^2 = x^3 - pqx$, *Iran. J. Math. Sci. Inform.*, **10** (2015), 77-86.

[4] Y. Fujita and N. Terai, Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$, *Tokyo J. Math.*, **34** (2011), 367-381.

[5] A.J. Hollier, B.K. Spearman and Q. Yang, Elliptic curves $y^2 = x^3 + pqx$ with maximal rank, *Int. Math. Forum*, **5** (2010) 1105-1110.

[6] R.J. Mina and J. Bacani, Elliptic curves of type $y^2 = x^3 - 3pqx$ having ranks zero and one, *Malaysian J. Math. Sci.*, **17**(1) (2023), 67-76.

[7] A. Schinzel and W. Sierpinski, Sur Certaines Hypotheses Concernant les Nombres Premiers, *Acta Arith.*, **4** (1958), 185-208.

[8] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 2009.

[9] B.K. Spearman, Elliptic curves $y^2 = x^3 - px$ of rank two, *Math. J. Okayama Univ.*, **49** (2007), 183-184.

[10] B.K. Spearman, On the group structure of elliptic curves $y^2 = x^3 - 2px$, *Int. J. Algebra*, **1** (2007), 247-250.

[11] The PARI Group, *PARI/GP Version 2.15.2*, Univ. Bordeaux, 2022.