EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 8, No. 1, 2015, 126-134
ISSN 1307-5543 – www.ejpam.com

On the Group of the Elliptic Curve $y^2 = x^3 + 4px$

Naser Zamani[1,*], Arman Shams[2]

[1] *Faculty of Mathematical Science, University of Mohaghegh Ardabili, Ardabil, Iran*
[2] *Department of mathematics, Shahid Madani University, Tabriz, Iran*

Abstract. In this paper we study the group structure of the elliptic curves $E : y^2 = x^3 + 4px$, where p is 3, 5 or a prime of the form $u^4 + v^4$ for positive integers u, v.

2010 Mathematics Subject Classifications: 11G05
Key Words and Phrases: Elliptic curves, Rank, Isogenous, Selmer group

---

1. Introduction

Let E denote an elliptic curve over $\mathbb{Q}$ and $\Gamma = E(\mathbb{Q})$ be the set of all rational points on E. A seminal Theorem of Mordell-Weil asserts that Γ is a finitely generated Abelian group in a natural way with zero element $\mathscr{O}$. We put $\Gamma = \mathscr{T} \oplus \mathscr{F}$ where $\mathscr{T}$ and $\mathscr{F}$ are the torsion and maximal free subgroups of Γ respectively. By the rank of E, rank(E), we mean the rank of $\mathscr{F}$. Hence the rank of E is positive if and only if E possesses an infinity of rational points. Computational works show that a typical elliptic curve has more small rank [1, 9].

Let p be a prime number and consider the curve $E = E_{4p} : y^2 = x^3 + 4px$. We study the group Γ and show that $\mathscr{T} = \mathbb{Z}_2$. By combining some facts of [4], a result on the Selmer group of Γ and that of its isogenous $\tilde{\Gamma}$ will be given. Next, when $p = 3, 5, u^4 + v^4$ for positive integers u, v, some results on the rank of E are presented. Although, it can be find some similar results concerning the 2-isogenous of E in the literatures ([5, 8]), which imply some of our results, our method of study completely differs from those.

2. Preliminaries

We begin with the following proposition which shows some properties of Γ.

Proposition 1. *Let $Q = (x', y'), P = (x, y)$ be two points of E such that $x' \in \mathbb{Z}$ and $Q = 2P$. Then $x \in \mathbb{Z}$ is even.*

---

*Corresponding author.

Email addresses: `zamanin@uma.ac.ir`, `naserzaka@yahoo.com` (N. Zamani), `shzarghar.arman@gmail.com` (A. Shams)

Proof. Let $x = a/b$, $\gcd(a,b) = 1$ and $x \notin \mathbb{Z}$. According to the group law of Γ, one can see that

$$x' = \frac{(a^2 - 4pb^2)^2}{4ab(a^2 + 4pb^2)}.$$

Hence, $(a^2-4pb^2)^2-4ab(a^2+4pb^2)x' = 0$ which gives that $a^4 \equiv 0 \pmod 4$ and so a is even. Also, we have $b \mid (a^2 - 4pb^2)^2$. Thus b is either even or $b = \pm 1$. The first case contradicts $\gcd(a,b) = 1$. Thus we must have $b = \pm 1$ and $x \in \mathbb{Z}$ is even. □

Lemma 1. *For any prime p, the point* $\mathbf{0} = (0,0)$ *is the only element of order* 2 *in* Γ.

Proof. Suppose the contrary, $\mathbf{0} \neq P = (x,y) \in \Gamma$ is of order 2. Thus $2P = \mathcal{O}$ and hence $(x,y) = (x,-y)$. Then $x \neq 0$, $y = 0$ and $x^3 + 4px = 0$. Setting $x = a/b$ and $\gcd(a,b) = 1$, we get $a^3 + 4pab^2 = 0$. Hence $b^2 \mid a^3$. Since a, b are coprime, so $b = \pm 1$, i.e. $x \in \mathbb{Z}$. But, we have $p = x^3/(-4x) = x^2/(-4) < 0$, a contradiction. □

Proposition 2. *For any prime p, there is no point of order* 3 *in* Γ.

Proof. On the contrary, we suppose $P = (x,y) \in \Gamma$ is of order 3, i.e. $2P = -P$. Let $P = (x,y)$, $2P = (x',y')$. Hence $(x',y') = -(x,y) = (x,-y)$, so $x' = x$. On the other hand, from duplication formula, we have

$$x = x' = \frac{(x^2 - 4p)^2}{4(x^3 + 4px)}.$$

Thus, $16p^2 - 24x^2p - 3x^4 = 0$ is a quadratic polynomial in variable p. Therefore,

$$p = \frac{12x^2 \pm \sqrt{\Delta'}}{16} \quad \text{with} \quad \Delta' = 192x^4.$$

Since Δ' is not square, then $p \notin \mathbb{N}$, a contradiction. □

The following is one of our main results.

Theorem 1. *For any prime p,* $\mathcal{T} \cong \mathbb{Z}_2$.

Proof. By Lemma 1, $\{\mathcal{O}, 0\} \subseteq \mathcal{T}$. Let $P := (x,y) \in \mathcal{T} \setminus \{\mathcal{O}, 0\}$. By Lutz-Nagell theorem, x and y are integers such that y^2 divides the discriminant $\Delta = 2^8p^3$ of the curve E. Thus

$$y^2 = 1, 2^2, 2^4, 2^6, 2^8, p^2, 2^2p^2, 2^4p^2, 2^6p^2, 2^8p^2.$$

We list the computations done with $2P = (x_2, y_2)$ where

$$x_2 = \frac{(3x^2 + 4p)^2}{4y^2} - 2x = \frac{(x^2 - 4p)^2}{4(x^3 + 4px)}$$

in the following table:

Table 1: Computations with $2P=(x_2,y_2)$

y^2	x	$(x,y^2;p)$	x_2
1	±1	–	–
4	$\pm1,\pm2,\pm4$	–	–
16	$\pm1,\pm2,\pm4,\pm8,\pm16$	–	–
64	$\pm1,\pm2,\pm4,\pm8,\pm16,\pm32,\pm64$	(2, 64; 7)	$\frac{9}{4}$
256	$\pm1,\pm2,\pm4,\pm8,\pm16,\pm32,\pm64,$ $\pm128,\pm256$	$(2,256;31)$	$\frac{225}{16}$
p^2	$\pm1,\pm p,\pm p^2$	–	–
$4p^2$	$\pm1,\pm2,\pm4,\pm p,\pm2p,\pm4p,\pm p^2,$ $\pm2p^2,\pm4p^2$	–	–
$16p^2$	$\pm1,\pm2,\pm4,\pm8,\pm16,\pm p,\pm2p,$ $\pm4p,\pm8p,\pm16p$	–	–
$64p^2$	$\pm1,\pm2,\pm4,\pm8,\pm16,\pm32,\pm64,$ $\pm p,\pm2p,\pm4p,\pm8p,\pm16p,\pm32p$ $\pm64p,\pm p^2,\pm2p^2,\pm4p^2,\pm8p^2,$ $\pm16p^2,\pm32p^2,\pm64p^2,\pm64p^2$	(14, 3136; 7)	$\frac{9}{4}$
$256p^2$	$\pm1,\pm2,\pm4,\pm8,\pm16,\pm32,\pm64,$ $\pm128,\pm256,\pm p,\pm2p,\pm4p,\pm8p,$ $\pm16p,\pm32p,\pm64p,\pm128p,\pm256$ $\pm p^2,\pm2p^2,\pm4p^2,\pm8p^2,\pm16p^2$ $\pm32p^2,\pm64p^2,\pm128p^2,\pm256p^2$	(62, 246016; 31)	$\frac{225}{16}$

The symbol '–' in Table 1 means that the equation $y^2 = x^3 + 4px$ has no integer solution $(x, y; p)$ and hence no solution for x_2. We see that x_2 is never zero and so $2P$ can not be of finite order. This contradicts the fact that $2P \in \mathscr{T}$. □

3. A Result on Selmer Group of E

In this section, we want to evaluate the Selmer group of E. For ease in access, we recall some basic facts on the Selmer groups of the elliptic curves [4, 7]. Let E, E' be elliptic curves defined over $\mathbb{Q}$ and assume that there exists an isogeny $\varphi : E \longrightarrow E'$ over $\mathbb{Q}$ with $\varphi' : E' \to E$ its dual. Let $\mathbb{K}$ be a field containing $\mathbb{Q}$ with $\overline{\mathbb{Q}}$ its integral closure in $\mathbb{K}$. Then there is an exact sequence

$$0 \longrightarrow E[\varphi] \longrightarrow E \xrightarrow{\varphi} E' \longrightarrow 0,$$

of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$-modules where $E[\varphi] = \ker(\varphi)$. Taking Galois cohomology, we obtain the exact sequence

$$0 \longrightarrow E'(\mathbb{K})/\varphi(E(\mathbb{K})) \xrightarrow{\delta_{\mathbb{K}}} H^1(\mathbb{K}, E[\varphi]) \xrightarrow{\varphi^*} H^1(\mathbb{K}, E)[\varphi] \longrightarrow 0,$$

where $H^1(\mathbb{K},E)[\varphi]$ is the kernel of φ^* and $\delta_{\mathbb{K}}$ is the connecting homomorphism. Consider the following commutative diagram ($\delta_q := \delta_{\mathbb{Q}_q}$):

$$\begin{array}{ccccccc}
0 \longrightarrow & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) & \xrightarrow{\delta_{\mathbb{Q}}} & H^1(\mathbb{Q},E[\varphi]) & \longrightarrow & H^1(\mathbb{Q},E)[\varphi] & \longrightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \longrightarrow & \Pi E'(\mathbb{Q}_q)/\varphi(E(\mathbb{Q}_q)) & \xrightarrow{\Pi\delta_q} & \Pi H^1(\mathbb{Q}_q,E[\varphi]) & \longrightarrow & \Pi H^1(\mathbb{Q}_q,E)[\varphi] & \longrightarrow 0
\end{array}$$

where the symbol Π means the direct product over $P_\infty = \{primes\} \cup \{\infty\}$ and $q \in P_\infty$. Then, the *φ-Selmer group* $S^{(\varphi)}(E/\mathbb{Q})$ and the *Shafarevich-Tate group* $Ш(E/\mathbb{Q})$ are defined by

$$S^{(\varphi)}(E/\mathbb{Q}) = \ker\{H^1(\mathbb{Q},E[\varphi]) \longrightarrow \Pi H^1(\mathbb{Q}_q,E)[\varphi]\}$$

and

$$Ш(E/\mathbb{Q}) = \ker\{H^1(\mathbb{Q},E) \longrightarrow \Pi H^1(\mathbb{Q}_q,E)\}$$

respectively. We note that there is another method of calculating the Selmer group. From the above commutative diagram and the definition of the Selmer group, we have the equivalent definition

$$\begin{aligned} S^{(\varphi)}(E/\mathbb{Q}) =& \{x \in H^1(\mathbb{Q},E[\varphi]) \mid \mathrm{res}_q(x) \in \mathrm{Im}(\delta_q), \forall q \in P_\infty\} \\ =& \bigcap_{q \in P_\infty} \mathrm{Im}(\delta_{\mathrm{q}}) \end{aligned} \tag{1}$$

where for each $q \in P_\infty$, $\mathrm{Im}(\delta_q)$ is regarded as the subgroup of the group $H^1(\mathbb{Q},E[\varphi])$ and $\mathrm{res}_q(x)$ is the residue of x at q.

In the following using some nice results of [4], we are able to calculate the Selmer group of E.

Theorem 2. *Assume that $q \in P_\infty$ and let $(\ ,\ )_q$ be the Hilbert symbol. For a subgroup $V \subset \mathbb{Q}_q^\times/\mathbb{Q}_q^{\times^2}$ we define*

$$V^\perp = \left\{x \in \mathbb{Q}_q^\times/\mathbb{Q}_q^{\times^2} \mid (x,y)_q = 1,\ \forall y \in V\right\}.$$

Then we have

(1) $\mathrm{Im}(\delta_q) = \mathrm{Im}(\delta_2) = \mathrm{Im}(\delta_2')^\perp = (-4q)$

(2) $\mathrm{Im}(\delta_q') = (q)$.

Proof. It follows [4, Theorem 2.1, Propositions 4.1, 4.2]. □

Corollary 1. *Let $\tilde{E}$ be the simultaneous curve of E. Then, we have $S^{(\varphi)}(E/\mathbb{Q}) = (-4p)$ and $S^{(\tilde{\varphi})}(\tilde{E}/\mathbb{Q}) = (16p)$.*

Proof. It follows from (1) and the previous theorem that

$$\begin{aligned} S^{(\varphi)}(E/\mathbb{Q}) =& \mathrm{Im}(\delta_\infty) \cap \mathrm{Im}(\delta_2) \cap \mathrm{Im}(\delta_p) \\ =& (\mathbb{R}^\times/\mathbb{R}^{\times^2}) \cap (-4p) \cap (-4p) \\ =& (-4p) \end{aligned}$$

and

$$\begin{aligned} S^{(\varphi')}(\tilde{E}/\mathbb{Q}) =& S^{(\varphi')}(\tilde{E}/\mathbb{Q}) \\ =& \mathrm{Im}(\delta'_\infty) \cap \mathrm{Im}(\delta'_2) \cap \mathrm{Im}(\delta'_p) \\ =& \{1\} \cap (4p) \cap (16p) \\ =& (16p). \end{aligned}$$

□

4. Computation of the Rank of E

In this section we assume that $p = u^4 + v^4$ is a prime number with $u, v \in \mathbb{N}$. We note that

$$(2(u^4+v^4)(u+v)^2, 4(u^2+uv+v^2)(u^4+v^4)/(u+v)^3)$$

is a point of E. Let $\tilde{E}$ be the simultaneous curve of E and $\tilde{\Gamma}$ be its corresponding group. We consider α and $\tilde{\alpha}$ be the group homomorphism

$$\alpha : \Gamma \longrightarrow \mathbf{Q}^\times/\mathbf{Q}^{\times 2} \tilde{\alpha} : \tilde{\Gamma} \longrightarrow \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$$

$$\alpha(P) = \begin{cases} 1 & \text{for } P = \mathcal{O} \\ \beta(p) & \text{for } P = 0 \\ \beta(x) & \text{for } x \neq 0 \end{cases} \quad \tilde{\alpha}(P) = \begin{cases} 1 & \text{for } P = \mathcal{O} \\ \beta(-p) & \text{for } P = 0 \\ \beta(x) & \text{for } x \neq 0 \end{cases}$$

where $P = (x, y)$ and β is a natural group homomorphism $\mathbf{Q}^\times \longmapsto \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. To compute the rank of E we use the well-known formula (see for example [2, 6])

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\tilde{\alpha}(\tilde{\Gamma})}{4}, \qquad r = \mathrm{rank}(E). \tag{2}$$

Here, $\alpha(\Gamma)$ and $\tilde{\alpha}(\tilde{\Gamma})$ are given as

$$\begin{aligned} 1, \beta(p) \in \alpha(\Gamma) = \left\{\beta(d) : C_d \text{ has at } \textit{least} \text{ an integral solution for } d|4p\right\}, \\ 1, \beta(-p) \in \tilde{\alpha}(\tilde{\Gamma}) = \left\{\beta(\tilde{d}) : C_{\tilde{d}} \text{ has at } \textit{least} \text{ an integral solution for } \tilde{d}| - 16p\right\} \end{aligned}$$

where C_d and $C_{\tilde{d}}$ are *Super-Fermat equations* [3]:

$$C_d : dt^4 + \frac{4p}{d} z^4 = w^2, \ t \geq 1, \ z \geq 1, \ \gcd\left(t, 4p/d\right) = 1$$

$$C_{\tilde{d}} : \tilde{d}t^4 - \frac{16p}{\tilde{d}}z^4 = w^2,\ t \geq 1,\ z \geq 1,\ \gcd(t, 16p/\tilde{d}) = 1,$$

with integer solutions (t, z, w). Hence,

$$d = \pm 1, \pm 2, \pm 4, \pm p, \pm 2p, \pm 4p$$
$$\tilde{d} = \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm p, \pm 2p, \pm 4p, \pm 8p, \pm 16p,$$

and so,

$$\alpha(\Gamma) \subseteq \left\{\beta(-1), \beta(\pm 2), \beta(\pm p), \beta(\pm 2p), \beta(-4p)\right\},$$
$$\tilde{\alpha}(\tilde{\Gamma}) \subseteq \left\{\beta(-1), \beta(\pm 2), \beta(\pm 4), \beta(\pm 8), \beta(\pm 16), \beta(\pm p), \beta(\pm 2p), \beta(\pm 4p), \beta(16p)\right\},$$

together with $1, \beta(p) \in \alpha(\Gamma)$ and $1, \beta(-16p) \in \tilde{\alpha}(\tilde{\Gamma})$. Now, we define

$$S_d = \left\{(t, z, w) | C_d \text{ has integer solutions for } d \neq 1, 4p\right\},$$
$$S_{\tilde{d}} = \left\{(t, z, w) | C_{\tilde{d}} \text{ has integer solutions for } d \neq 1, -16p\right\}.$$

According to [2]

$$\exists s, \exists \tilde{s} \in \mathbb{N} \text{ such that } \sum_{d|4p} \#S_d = 2^s - 2, \quad \sum_{\tilde{d}|16p} \#S_{\tilde{d}} = 2^{\tilde{s}} - 2,$$

where d and $\tilde{d}$ are square free, $\#S_d = 0$ if $S_d = \emptyset$ and $\#S_d = 1$ if $S_d \neq \emptyset$. Similarly for $S_{\tilde{d}}$. By (2) we conclude that $r = s + \tilde{s} - 2$. By the closed property of $\alpha(\Gamma)$ and having a note to the Table 2, we conclude that

$$\alpha(\Gamma) = \{1, \beta(2), \beta(p), \beta(2p)\}.$$

Also, using Tables 3 and 4, we have

$$\tilde{\alpha}(\tilde{\Gamma}) = \{1, \beta(-1), \beta(p), \beta(-p)\}.$$

Now, using these two equalities together with (2) gives that $r = 2$.

Table 2: Elements of S_d

d	C_d	integer solutions
2	$2t^4 + 2pz^4 = w^2$	$(u \pm v, 1, 2u^2 \pm 2uv + 2v^2)$
$2p$	$2pt^4 + 2z^4 = w^2$	$(1, u \pm v, 2u^2 \pm 2uv + 2v^2)$

Table 3: Elements of $S_{\tilde{d}}$ for $\tilde{d} > 0$

d	$C_{\tilde{d}}$	integer solutions
2	$2t^4 - 8pz^4 = w^2$	–
$2p$	$2pt^4 - 8z^4 = w^2$	–

Table 4: Elements of $S_{\tilde{d}}$ for $\tilde{d} < 0$

d	$C_{\tilde{d}}$	integer solutions
-1	$-t^4 + 16pz^4 = w^2$	–
-2	$-2t^4 + 8pz^4 = w^2$	–
$-2p$	$-2pt^4 + 8z^4 = w^2$	–

In Tables 3 and 4, the symbol '–' shows that the corresponding equation dose not have any integer solution (t,z,w). One can check this straightforward. For example, concerning $C_{\tilde{2}}$ in the Table 3, if there is any solution, then we conclude that $2t^4 \equiv 0 \pmod 4$, a contradiction with $\gcd(t,-8p) = 1$. Also, concerning $C_{\tilde{2p}}$ in the Table 3, if there is any solution (t,z,w), then we conclude that $2|t$ which contradicts $\gcd(t,-8) = 1$. Similar arguments can be done for other cases. The following theorem, thus, has been proved.

Theorem 3. *For the elliptic curve $E : y^2 = x^3 + 4px$ $(p = u^4 + v^4)$, the Mordell-Weil theorem holds as following:*

$$\Gamma \cong \mathbb{Z}_2 \oplus \mathbb{Z}^2.$$

As other observations about the rank of $E : y^2 = x^3 + 4px$, we also examined rank(E) in the cases $p = 3, 5$. The resulting illustrations done with MWRANK† have been collected in Tables 5-7.

Table 5: $p = 3$

$C_d, C_{\tilde{d}}$	Legendre value	integer solutions
$w^2 = 2t^4 + 6z^4$	$\left(\frac{2}{6}\right) = -1$	Not
$w^2 = 3t^4 + 4z^4$	$\left(\frac{3}{4}\right) = -1$	Not
$w^2 = 6t^4 + 2z^4$	$\left(\frac{6}{2}\right) = -1$	Not
$w^2 = 2t^4 - 24z^4$	$\left(\frac{-2}{24}\right) = -1$	Not
$w^2 = 3t^4 - 16z^4$	$\left(\frac{-3}{16}\right) = -1$	Not
$w^2 = 6t^4 - 8z^4$	$\left(\frac{-6}{8}\right) = -1$	Not
$w^2 = -t^4 + 48z^4$	$\left(\frac{-1}{48}\right) = -1$	Not
$w^2 = -2t^4 + 24z^4$	$\left(\frac{-2}{24}\right) = -1$	Not
$w^2 = -3t^4 + 16z^4$	$\left(\frac{-3}{16}\right) = -1$	Not
$w^2 = -4t^4 + 12z^4$	$\left(\frac{-4}{12}\right) = -1$	Not
$w^2 = -6t^4 + 8z^4$	$\left(\frac{-6}{8}\right) = -1$	Not

†`http://homepages.warwick.ac.uk/~masgaj/mwrank/`

Table 6: Rank

p	rank of E	$\#Ш(E/\mathbf{Q})[2]$
2	1	1
3	0	1
5	1	1
$17 \leq p \leq 10^6$	2	1

Table 7: $p = 5$

$C_d, C_{\tilde{d}}$	Legendre value	integer solutions
$w^2 = 2t^4 + 10z^4$	$\left(\frac{2}{10}\right) = -1$	Not
$w^2 = 4t^4 + 5z^4$	$\left(\frac{4}{5}\right) = 1$	$(1, 1, 3)$
$w^2 = 5t^4 + 4z^4$	$\left(\frac{5}{4}\right) = 1$	$(1, 1, 3)$
$w^2 = 10t^4 + 2z^4$	$\left(\frac{2}{10}\right) = -1$	Not
$w^2 = 2t^4 - 40z^4$	$\left(\frac{-2}{40}\right) = -1$	Not
$w^2 = 5t^4 - 16z^4$	$\left(\frac{-5}{16}\right) = -1$	Not
$w^2 = 10t^4 - 8z^4$	$\left(\frac{-8}{10}\right) = -1$	Not
$w^2 = -t^4 + 80z^4$	$\left(\frac{-1}{80}\right) = -1$	Not
$w^2 = -2t^4 + 40z^4$	$\left(\frac{-4}{20}\right) = -1$	Not
$w^2 = -4t^4 + 20z^4$	$\left(\frac{-4}{20}\right) = -1$	Not
$w^2 = -5t^4 + 16z^4$	$\left(\frac{-5}{16}\right) = -1$	Not
$w^2 = -10t^4 + 8z^4$	$\left(\frac{10}{-8}\right) = -1$	Not

References

[1] A. Brumer and O Mc. Guinness. *The behaviour of the Mordell-Weil group of elliptic curves*, Bulletin of American Mathematical Society, 23, 375-382, 1990.

[2] J. S. Chahal. *Topics in number theory*, Kluwer Academic/Plenum Publisher, 1988.

[3] H. Cohen. *Number theory: Tools and Diophantine equations*, Springer, Vol. I, 2007.

[4] T. Goto. *A study on the Selmer groups of elliptic curves with a rational 2-torsion*, Kyushu University, PhD thesis 2002.

[5] T. Kudo and K. Motose. *On group structures of some special elliptic curves*, Mathematical Journal of Okayama University, 47, 81-84, 2005.

[6] J. H. Silverman and J. Tate. *Rational points on elliptic curves*, Springer, 1992.

[7] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 2009.

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

[9] D. Zagier and G. Kramarz. *Numerical investigations related to the L-series of certain elliptic curves*, Journal of Indian Mathematical Society, 52, 51-69, 1987.