Theory of Approximation and Applications

Vol. 10, No.2, (2016), 13-22

On the rank of certain parametrized elliptic curves

A. Hadavand [a,*]

[a] *Department of mathematics, Arak Branch, Islamic Azad university, Arak, Iran.*

Received 14 August 2015; accepted 25 March 2016

Abstract

In this paper the family of elliptic curves over $\mathbb{Q}$ given by the equation $E_p : Y^2 = (X-p)^3 + X^3 + (X+p)^3$ where p is a prime number, is studied. It is shown that the maximal rank of the elliptic curves is at most 3 and some conditions under which we have $\text{rank}(E_p(\mathbb{Q})) = 0$ or $\text{rank}(E_p(\mathbb{Q})) = 1$ or $\text{rank}(E_p(\mathbb{Q})) \geq 2$ are given.

Key words: Elliptic Curve, Selmer Group.

2010 AMS Mathematics Subject Classification : 11G05.

* Corresponding author's E-mail: hadavand@iau-arak.ac.ir

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and $E(\mathbb{Q})$ be the Mordell-Weil group of E over $\mathbb{Q}$ which is a finitely generated abelian group. The rank of $E(\mathbb{Q})$ as a $\mathbb{Z}$-module is called the rank of E over $\mathbb{Q}$. There is no algorithm which can compute the rank of any given elliptic curve so far. So it seems necessary to consider certain families of elliptic curves and to investigate their ranks (see [3,5,8,9]).

In this paper we consider the family of elliptic curves over $\mathbb{Q}$ given by the equation

$$E_p:\ Y^2 = (X-p)^3 + X^3 + (X+p)^3,$$

where p is a prime number, and show that the maximal rank of the elliptic curves is at most 3. Moreover some conditions under which we have $\mathrm{rank}(E_p(\mathbb{Q})) = 0$ or $\mathrm{rank}(E_p(\mathbb{Q})) = 1$ or $\mathrm{rank}(E_p(\mathbb{Q})) \geq 2$ are given.

2 Conclusions and Suggestions

In this section the following theorem and propositions will be proved.

Theorem 1 *We have*

(1) If $p = 2, 3$ or $p \equiv 7 \pmod{24}$, then $\mathrm{rank}(E_p(\mathbb{Q})) = 0$.
(2) If $p \equiv 5, 13, 17 \pmod{24}$, then $\mathrm{rank}(E_p(\mathbb{Q})) \leq 1$.
(3) If $p \equiv 1 \pmod{24}$ & $(\frac{2}{p})_4 = 1$, then $\mathrm{rank}(E_p(\mathbb{Q})) \leq 3$.
(4) In the other cases, $\mathrm{rank}(E_p(\mathbb{Q})) \leq 2$.

Proposition 2 *Let $p \equiv 17 \pmod{24}$ and $(\frac{2}{p})_4 = 1$. If there are integers a, b such that $3p = a^4 + 2b^4$, then $\mathrm{rank}(E_p(\mathbb{Q})) = 1$.*

Proposition 3 *Let $p \equiv 1 \pmod{24}$ and $(\frac{2}{p})_4 = 1$. If there are integers a, b, c, and d such that $p = a^4 + 18b^4$ and $3p = c^4 + 2d^4$, then $\mathrm{rank}(E_p(\mathbb{Q})) \geq 2$.*

Some primes which satisfy the conditions in Proposition 2 and Proposition 3 will be given and It will be shown that in the family there are elliptic curves with rank 0,1,2 and 3.

For proving the theorem we have to deal with the Selmer groups of E_p corresponding to certain 2-isogenies. Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ with a torsion point of order 2. We use 2-descent via 2-isogeny method to compute the rank of E over $\mathbb{Q}$ which is based on computing of the Selmer groups corresponding to certain 2-isogeny of E (see [2,6,7]).

Let

$$E : y^2 = x^3 + ax^2 + bx \qquad , a, b \in \mathbb{Z},$$

be an elliptic curve and

$$\overline{E} : Y^2 = X^3 + \overline{a}X^2 + \overline{b}X,$$

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$, be its 2-isogeny curve. Let

$$\begin{aligned} \Psi : E &\to \overline{E} \\ (x, y) &\longmapsto (\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}) \end{aligned}$$

be 2-isogeny of degree 2 and

$$\begin{aligned} \overline{\Psi} : \overline{E} &\to E \\ (X, Y) &\longmapsto (\frac{Y^2}{4X^2}, \frac{Y(b - X^2)}{8X^2}) \end{aligned}$$

be dual isogeny of Ψ. Let

$$C_{b_1} : b_1 w^2 = b_1^2 + b_1 \overline{a} z^2 + b z^4,$$

and

$$C_{\overline{b}_1} : \overline{b}_1 w^2 = \overline{b}_1^2 - 2\overline{b}_1 \overline{a} z^2 + \overline{b} z^4,$$

where $b_1 | b$ and $\overline{b}_1 | \overline{b}$, be the homogeneous spaces for $E/\mathbb{Q}$ and $\overline{E}/\mathbb{Q}$, respectively. The Selmer groups corresponding to the 2-isogneies $\overline{\Psi}$ and Ψ

of these curves are

$$S[\overline{\Psi}] = \{1.\mathbb{Q}^{*2}, b.\mathbb{Q}^{*2}\} \cup \{b_1.\mathbb{Q}^{*2} : \ b_1|b \text{ and } C_{b_1}(\mathbb{Q}_p) \neq \phi \text{ for all } p \in S\},$$

where $S := \{\infty\} \cup \{p : \ p \text{ is a prime and } p|2b\bar{b}\}$.
And

$$S[\Psi] = \{1.\mathbb{Q}^{*2}, \bar{b}.\mathbb{Q}^{*2}\} \cup \{\bar{b}_1.\mathbb{Q}^{*2} : \ \bar{b}_1|\bar{b} \text{ and } C_{\bar{b}_1}(\mathbb{Q}_p) \neq \phi \text{ for all } p \in S\}.$$

Now consider the elliptic curve E_p. With the change of variables $x = 3X$ and $y = 3Y$ the equation of E_p becomes

$$E_p : y^2 = x^3 + 18p^2x,$$

and the following propositions give us the structure of the Selmer groups.

Proposition 4 *Using the notations introduced above, we have*

(1) If $p \equiv 11, 19 \ (mod\ 24)$ *or* $[p \equiv 1 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = 1]$, *then* $S_p[\overline{\Psi}] \cong (\frac{\mathbb{Z}}{2\mathbb{Z}})^3$.
(2) If $p = 2, 3$ *or* $p \equiv 7 \ (mod\ 24)$, *then* $S_p[\overline{\Psi}] \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.
(3) In the other cases, $S_p[\overline{\Psi}] \cong (\frac{\mathbb{Z}}{2\mathbb{Z}})^2$.

Proposition 5 *We have*

(1) If $p \equiv 23 \ (mod\ 24)$ *or* $[p \equiv 1 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = 1]$, *then* $S_p[\Psi] \cong (\frac{\mathbb{Z}}{2\mathbb{Z}})^2$.
(2) In the other cases, $S_p[\Psi] \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.

We prove Proposition 4 and one can prove Proposition 5 by the same method.

By the definition it is clear that

$$\{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}\} \subseteq S_p[\overline{\Psi}].$$

So it is sufficient to check solvability of the equations

$$C_{b_1} : w^2 = b_1 + \frac{18p^2}{b_1} z^4,$$

for $b_1 = -1, \pm 3, \pm p, \pm 3p$ over $\mathbb{Q}_l$ where $l \in \{\infty, 2, 3, p\}$. If $b_1 < 0$ it is clear that $C_{b_1}(\mathbb{Q}_\infty) = \phi$ and then $b_1.\mathbb{Q}^{*2} \notin S_p[\overline{\Psi}]$. For any $b_1 > 0$ we have $C_{b_1}(\mathbb{Q}_\infty) \neq \phi$. Let $p \neq 2, 3$, we consider the equation

$$w^2 = 3 + 6p^2 z^4, \tag{2.1}$$

corresponding to $b_1 = 3$. The solution $(z, w) = (1, 1)$ for the congruence $w^2 \equiv 3 + 6p^2 z^4 \pmod 8$ can be lifted to a solution for the equation (2.1) in $\mathbb{Q}_2$ by using Hensel's lemma, and then $C_3(\mathbb{Q}_2) \neq \phi$. By considering the equation (2.1) modulo 3 we have $w^2 \equiv 0 \pmod 3$, say $w = 3W$, so it can be written as $3W^2 = 1 + 2p^2 z^4$, and again the solution $(z, W) = (1, 1)$ for the congruence $3W^2 \equiv 1 + 2p^2 z^4 \pmod 3$ lifts to a solution for the equation $3W^2 = 1 + 2p^2 z^4$ in $\mathbb{Q}_3$ which implies $C_3(\mathbb{Q}_3) \neq \phi$. Now consider the equation (2.1) over $\mathbb{Q}_p$.

(1) Let $(\frac{3}{p}) = 1$, then there is $w_0 \in \mathbb{Z}$ such that $w_0^2 \equiv 3 \pmod p$. The solution $(z, w) = (1, w_0)$ for the congruence $w^2 \equiv 3 + 6p^2 z^4 \pmod{\text{p}}$ lifts to a solution for the equation (2.1) in $\mathbb{Q}_p$.

(2) Let $(\frac{3}{p}) = -1$ & $(\frac{2}{p}) = -1$, then $(\frac{6}{p}) = 1$ and there is $w_0 \in \mathbb{Z}$ such that $w_0^2 \equiv 6 \pmod p$. Let j be a positive integer number, then the solution $(z, w) = (1, w_0)$ for the congruence $w^2 \equiv 3p^{2+4j} + 6z^4 \pmod{\text{p}}$ lifts to a solution such as $(z, w) = (\alpha, \beta)$ for the equation $w^2 = 3p^{2+4j} + 6z^4$ in $\mathbb{Q}_p$. So $(z, w) = (p^{-(1+j)}\alpha, p^{-(1+2j)}\beta)$ is a solution for the equation (2.1) in $\mathbb{Q}_p$.

(3) Let $(\frac{3}{p}) = -1$ & $(\frac{2}{p}) = 1$, in this case one can show that there is no solution for the equation (2.1) in $\mathbb{Q}_p$ since 3 and 6 are non-square mod p.

Therefore

$$p \equiv 7, 17 \ (mod\ 24) \Leftrightarrow 3.\mathbb{Q}^{*2} \notin S_p[\overline{\Psi}].$$

Now we deal with the case $b_1 = p$. The corresponding equation is

$$w^2 = p + 18pz^4. \tag{2.2}$$

Suppose that $C_p(\mathbb{Q}_2) \neq \phi$. Since $v_2(w^2)$ is even and $v_2(18pz^4)$ is odd, then necessarily $z,\ w \in \mathbb{Z}_2$, and therefore we deduce $p \equiv 1, 3 \pmod 8$. Conversely, let $p \equiv 1, 3 \pmod 8$. In the case $p \equiv 1 \pmod 8$ the solution $(z, w) = (2, 1)$ and in the case $p \equiv 3 \pmod 8$ the solution $(z, w) = (1, 1)$ for the congruence $w^2 \equiv p+2pz^4 \pmod 8$ lift to solutions for the equation (2.2) in $\mathbb{Q}_2$, respectively.

When $p \equiv 1 \pmod 3$ the solution $(z, w) = (1, 1)$ for the equation (2.2) mod 3 lifts to a solution for it in $\mathbb{Q}_3$. Now let $p \equiv 2 \pmod 3$ and j be a positive integer number, the solution $(z, w) = (1, 1)$ for the congruence $w^2 \equiv 3^{2+4j}p + 2pz^4 \pmod 3$ lifts to a solution such as $(z, w) = (\alpha, \beta)$ for the equation $w^2 = 3^{2+4j}p + 2pz^4$ in $\mathbb{Q}_3$. So $(z, w) = (3^{-(1+j)}\alpha, 3^{-(1+2j)}\beta)$ is a solution for the equation (2.2) in $\mathbb{Q}_3$, therefore $C_p(\mathbb{Q}_3) \neq \phi$.

Let $p \equiv 3 \pmod 8$, then there is $z_0 \in \mathbb{Z}$ such that $1 + 18z_0^4 \equiv 0 \pmod p$ since for any integer x, one of x and $-x$ is a quadratic residue and the other one is a non-residue. So the solution $(z, W) = (z_0, 1)$ for the congruence $pW^2 \equiv 1 + 18z^4 \pmod p$ lifts to a solution for the equation $pW^2 = 1 + 18z^4$ in $\mathbb{Q}_p$ and then $C_p(\mathbb{Q}_p) \neq \phi$. Now let $p \equiv 1 \pmod 8$ and $C_p(\mathbb{Q}_p) \neq \phi$. Suppose that (z, w) is a solution for the equation (2.2) in $\mathbb{Q}_p$. Let $v_p(w) = k$ and $v_p(z) = j$, it is clear that j must be zero and $k > 0$. So considering equation (2.2) mod p implies that $(\frac{-18}{p})_4 = 1$ where $(\frac{-}{p})_4$ is the rational quartic residue symbol mod p. Conversely, if $(\frac{-18}{p})_4 = 1$ then $C_p(\mathbb{Q}_p) \neq \phi$. Therefore $p.\mathbb{Q}^{*2} \in S_p[\overline{\Psi}]$ if and only if

$$[p \equiv 11, 19 \pmod{24}]$$

or

$$[p \equiv 1 \pmod{24}\ \&\ (\frac{2}{p})_4 = 1]\ \textit{or}\ [p \equiv 17 \pmod{24}\ \&\ (\frac{2}{p})_4 = -1].$$

In the case $b_1 = 3p$, the corresponding equation is

$$w^2 = 3p + 6pz^4. \tag{2.3}$$

By the same methods as in the case $b_1 = p$ one can show that

$$[p \equiv 11, 19 \pmod{24}] \text{ or } [p \equiv 1, 17 \pmod{24} \ \& \ (\frac{2}{p})_4 = 1] \Leftrightarrow 3p.\mathbb{Q}^{*2} \in S_p[\overline{\Psi}].$$

Finally for $p = 2, 3$ we have

$$S_2[\overline{\Psi}] = S_3[\overline{\Psi}] = \{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}\},$$

which completes the proof of Proposition 4. □

Corollary 6 *We have*

(1) If $p \equiv 11, 19 \ (mod\ 24)$ *or* $[p \equiv 1 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = 1]$, *then* $S_p[\overline{\Psi}] = \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, 2, 3, 6, p, 2p, 3p, 6p\}$.
(2) If $[p \equiv 5, 13, 23 \ (mod\ 24)]$ *or* $[p \equiv 1 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = -1]$, *then* $S_p[\overline{\Psi}] = \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, 2, 3, 6\}$.
(3) If $p \equiv 17 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = 1$, *then* $S_p[\overline{\Psi}] = \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, 2, 3p, 6p\}$.
(4) If $p \equiv 17 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = -1$, *then* $S_p[\overline{\Psi}] = \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, 2, p, 2p\}$.
(5) In the other cases, $S_p[\overline{\Psi}] = \{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}\}$.

And

$$S_p[\Psi] = \begin{cases} \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, -2, p, -2p\} & , p \equiv 1 \ (mod\ 24) \ \& \ (\frac{2}{p})_4 = 1; \\ \{b_1.\mathbb{Q}^{*2} : \ b_1 = 1, -2, -p, 2p\} & , p \equiv 23 \ (mod\ 24); \\ \{1.\mathbb{Q}^{*2}, -2.\mathbb{Q}^{*2}\}, & otherwise. \end{cases}$$

Note that the first result in Corollary 6 is clear because of the proof of Proposition 4, and one can obtain the second part with the same method.

Now we have the structures of the Selmer groups and we can prove Theorem 1. Consider the following map

$$\begin{aligned}\alpha_p :\ E_p(\mathbb{Q}) &\to S_p[\overline{\Psi}]\\ \mathcal{O} &\longmapsto 1.\mathbb{Q}^{*2}\\ (0,0) &\mapsto 2.\mathbb{Q}^{*2}\\ (x,y) &\mapsto x.\mathbb{Q}^{*2} \quad for\ x \neq 0.\end{aligned}$$

The following sequence is exact

$$0 \to E_p(\mathbb{Q})/\overline{\Psi}(\overline{E}_p(\mathbb{Q})) \to S_p[\overline{\Psi}] \to Ш_p[\overline{\Psi}] \to 0$$

where $Ш_p[\overline{\Psi}]$ is the cokernel of the left hand side injection which is called Tate-Shafarevich group of E_p. For the rank of E_p and $\overline{E}_p$ one obtains the following formula

$$\text{rank}(E_p(\mathbb{Q})) = dim_{\mathbb{F}_2}(S_p[\overline{\Psi}]) + dim_{\mathbb{F}_2}(S_p[\Psi]) - dim_{\mathbb{F}_2}(Ш_p[\overline{\Psi}]) - dim_{\mathbb{F}_2}(Ш_p[\Psi]) - 2.$$

Now one can easily complete the proof of Theorem 1. □

For proving Proposition 2 and Proposition 3 we use the same method as in [4], for more details see [1] or [7].

Proof of Proposition 2. Since $p \equiv 17 \pmod{24}$ and $(\frac{2}{p})_4 = 1$ by Corollary 6 we have $S_p[\overline{\Psi}] = \{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}, 3p.\mathbb{Q}^{*2}, 6p.\mathbb{Q}^{*2}\}$ and $S_p[\Psi] = \{1.\mathbb{Q}^{*2}, -2.\mathbb{Q}^{*2}\}$. Consider the equation $3pS^4 + 6pT^4 = U^2$, $(S,T,U) = (a,b,3p)$ is a solution for it such that $a,\ b \geq 1$ and $gcd(a,6p) = 1$. Because a is odd and if $gcd(a,6p) = d$, then d will be odd. Now note that $6p = 2a^4 + 4b^4$ so $d|4b^4$ and then $d|b^4$ therefore we deduce $d|p$. Suppose $d = p$, this implies that $d|a$ and $d|b$, i.e., there are integers a_1 and b_1 such that $a = pa_1$ and $b = pb_1$, so we have $3p = p^4(a_1^4 + 2b_1^4)$ which is a contradiction. Thus $d = 1$ and then $3p.\mathbb{Q}^{*2} \in Im\alpha_p$. Therefore $Im\alpha_p = \{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}, 3p.\mathbb{Q}^{*2}, 6p.\mathbb{Q}^{*2}\}$ and $Im\overline{\alpha}_p = \{1.\mathbb{Q}^{*2}, -2.\mathbb{Q}^{*2}\}$, and then $rank(E_p(\mathbb{Q})) = 1$. □

Note that $p = 1217,\ 1601,\ 5297,\ 9521$ are some primes which satisfy the conditions in Proposition 2.

Proof of Proposition 3. By Corollary 6 we have

$$S_p[\overline{\Psi}] = \{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}, 3.\mathbb{Q}^{*2}, 6.\mathbb{Q}^{*2}, p.\mathbb{Q}^{*2}, 2p.\mathbb{Q}^{*2}, 3p.\mathbb{Q}^{*2}, 6p.\mathbb{Q}^{*2}\}$$

and $S_p[\Psi] = \{1.\mathbb{Q}^{*2}, -2.\mathbb{Q}^{*2}, p.\mathbb{Q}^{*2}, -2p.\mathbb{Q}^{*2}\}$, and Proposition 2 implies that $\{1.\mathbb{Q}^{*2}, 2.\mathbb{Q}^{*2}, 3p.\mathbb{Q}^{*2}, 6p.\mathbb{Q}^{*2}\} \subseteq Im\alpha_p$. On the other hand $(S, T, U) = (a, b, p)$ is a solution for the equation $pS^4 + 18pT^4 = U^2$ which implies that $p.\mathbb{Q}^{*2} \in Im\alpha_p$, so $\#Im\alpha_p = \#S_p[\overline{\Psi}] = 8$ and then $rank(E_p(\mathbb{Q})) \geq 2$. Note that $gcd(a, 18p) = 1$, since if $gcd(a, 18p) = d_1$, then $d_1|p$ because a is odd and $3 \nmid a$. Suppose $d_1 = p$, this concludes that $d_1|a$ and $d_1|b$ which give us a contradiction. □

$p = 19249$ is a prime which satisfies the conditions in Proposition 3. By using the results one can see that $rank(E_7(\mathbb{Q})) = 0$, $rank(E_5(\mathbb{Q})) = 1$, $rank(E_{11}(\mathbb{Q})) = 2$ and $rank(E_{19249}(\mathbb{Q})) = 3$.

References

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

[2] J. E. Cremona, *Algorithms of modular elliptic curves*, Cambridge University Press, 1997.

[3] A.J. Hollier, B. K. Spearman and Q. Yang, On the rank and integral points of Elliptic Curves $y^2 = x^3 - px$, *Int. J. Algebra*, *3* (2009), no. 8, 401-406.

[4] T. Kudo and K. Motose, On Group structures of some special elliptic curves,*Math. J. Okayama Univ. 47* (2005), 81-84.

[5] S. Schmitt, Computing of the Selmer groups of certain parametrized elliptic curves, *Acta Arithmetica. LXXVIII* (1997) 241–254.

[6] J. H. Silverman, *The Arithmetic of Elliptic curves*, GTM 106. Springer-Verlage, New York, 1986.

[7] J. H. Silverman and J. Tate, *Rational Points on Elliptic curves*, Springer-Verlage, New York, 1994.

[8] R. J. Stroeker and J. Top, On the equation $y^2 = (X + p)(X^2 + p^2)$, *Rocky Mountain J. Math. 27* (1994), 1135–1161.

[9] P. G. Walsh, Maximal Ranks and Integer Points on a Family of Elliptic Curves,*Glasnik Matematički. 44* (2009), 83-87.