Bull. Iranian Math. Soc.
Vol. 40 (2014), No. 5, pp. 1119–1133
Online ISSN: 1735-8515

ON THE ELLIPTIC CURVES OF THE FORM $y^2 = x^3 - 3px$

H. DAGHIGH* AND S. DIDARI

(Communicated by Rahim Zaare-Nahandi)

Abstract. By the Mordell-Weil theorem, the group of rational points on an elliptic curve over a number field is a finitely generated abelian group. There is no known algorithm for finding the rank of this group. This paper computes the rank of the family $E_p : y^2 = x^3 - 3px$ of elliptic curves, where p is a prime.
Keywords: Elliptic Curves, Mordell-Weil group, Selmer Group, Birch and Swinnerton-Dyer conjecture, parity conjecture.
MSC(2010): Primary: 11G05; Secondary: 14H52, 14G05.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and $E(\mathbb{Q})$ be its Mordell-Weil group over $\mathbb{Q}$ which is a finitely generated abelian group. The rank of the free part of $E(\mathbb{Q})$ as a $\mathbb{Z}$-module is called the rank of E over $\mathbb{Q}$. There does not exist an algorithm which would be able to compute the rank of a given elliptic curve. Many authors [3–7, 11, 19] have considered different families of elliptic curves and compute their rank and integral points. Elliptic curves of the form $y^2 = x^3 - pqx$ are considered by many authors. For example Maenishi [13] constructed some elliptic curves of this form with rank exactly four. Spearman [17] gives a condition on p, such that the elliptic curve $y^2 = x^3 - 2px$ has rank three. Later Walsh [19] provided a sufficient condition for elliptic curves of the form $y^2 = x^3 - 2px$, to have rank three.

Article electronically published on October 27, 2014.
Received: 29 April 2013, Accepted: 25 August 2013.
*Corresponding author.

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

$$E_p : \; y^2 = x^3 - 3px,$$

where p is a prime$\neq 2, 3$. First using Selmer groups we find an upper bound for the rank of this family. Then using Parity conjecture, we refine our result and we find infinite families of elliptic curves which conjecturally have rank two. Finally we find integral points on curves in the family, and provide a sufficient condition on p, such that the elliptic curve $y^2 = x^3 - 3px$ has rank two. We also show that conjecturally, there exist infinitely many of such primes. Our main result is the following theorem:

Main Theorem. *Let p be a prime number and E_p be the elliptic curve $y^2 = x^3 - 3px$ and E'_p be the elliptic curve $y^2 = x^3 + 12px$. We have*

- (a1) $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ *for* $p \equiv 1, 7, 19, 23, 25, 35, 47 \ (mod\ 48)$*;*
- (a2) $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *for* $p \equiv 5, 11, 13, 17, 29, 31, 37, 41, 43 \ (mod\ 48)$*;*
- (a3) $S^{(\varphi)}(E_p/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ *for* $p \equiv 1, 5, 13, 25, 29, 37, 47 \ (mod\ 48)$*;*
- (a4) $S^{(\varphi)}(E_p/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *for* $p \equiv 7, 11, 17, 19, 23, 31, 35, 41, 43 \ (mod\ 48)$*,*

where $\varphi : E_p \longrightarrow E'_p$ is a 2-isogeny defined in Section 2. And we have the:

- (b1) *If* $p \equiv 1, 25, 47 \ (mod\ 48)$*, then* $rank(E_p(\mathbb{Q})) \leq 2$*;*
- (b2) *If* $p \equiv 5, 7, 13, 19, 23, 29, 35, 37 \ (mod\ 48)$ *, then* $rank(E_p(\mathbb{Q})) \leq 1$*;*
- (b3) *In all other cases,* $rank(E_p(\mathbb{Q})) = 0$*.*

Furthermore there exists an infinite family of primes p with $rank(E_p) = 2$.

2. Computing the Selmer group

In this section, first we recall some basic facts on the Selmer groups of elliptic curves with at least one 2-torsion rational point and then obtain an upper bound on the rank of elliptic curves in the family. Let E and E' be elliptic curves defined over $\mathbb{Q}$, and $\varphi : E \longrightarrow E'$ be a non zero $2-$isogeny. Then we have the exact sequence of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-modules

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

where $E[\varphi] = ker\ \varphi$. Taking Galois cohomology, for each place v of $\mathbb{Q}$ we obtain the short exact sequence

$$0 \longrightarrow E'(\mathbb{Q}_v)/\varphi(E(\mathbb{Q}_v)) \xrightarrow{\delta} H^1(\mathbb{Q}_v, E[\varphi]) \longrightarrow H^1(\mathbb{Q}_v, E)[\varphi] \longrightarrow 0,$$

where $H^1(\mathbb{Q}_v, -)$ denotes $H^1(Gal(\overline{\mathbb{Q}_v}/\mathbb{Q}_v), -)$ and δ is the connecting homomorphism. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) & \xrightarrow{\delta} & H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}, E[\varphi]) & \longrightarrow & H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}, E)[\varphi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E'(\mathbb{Q}_v)/\varphi(E(\mathbb{Q}_v)) & \xrightarrow{\delta} & \prod_v H^1(\mathbb{Q}_v, E[\varphi]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E)[\varphi] & \longrightarrow & 0. \end{array}$$

Then φ- Selmer group is defined as

$$S^{(\varphi)}(E/\mathbb{Q}) = Ker\{H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), E[\varphi]) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E)\},$$

and the Shafarevich-Tate group $Ш(E/\mathbb{Q})$ is

$$Ш(E/\mathbb{Q}) = Ker\{H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), E) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E)\}.$$

From the above commutative diagram and the definition of the Selmer and Shafarevich-Tate groups, we immediately obtain the exact sequence

$$(2.1) \quad 0 \longrightarrow E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \longrightarrow S^{(\varphi)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[\varphi] \longrightarrow 0.$$

Let $\hat{\varphi} : E' \longrightarrow E$ be the dual isogeny of φ. Interchanging the role of E and E', we obtain another exact sequence

$$(2.2) \quad 0 \longrightarrow E(\mathbb{Q})/\hat{\varphi}(E'(\mathbb{Q})) \longrightarrow S^{(\hat{\varphi})}(E'/\mathbb{Q}) \longrightarrow Ш(E'/\mathbb{Q})[\hat{\varphi}] \longrightarrow 0.$$

And there is the exact sequence

$$(2.3) \quad 0 \longrightarrow \frac{E'(\mathbb{Q})[\hat{\varphi}]}{\varphi(E(\mathbb{Q}[2]))} \longrightarrow \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{2(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{\hat{\varphi}(E'(\mathbb{Q}))} \longrightarrow 0.$$

Hence, from above exact sequence we have

$$(2.4) \quad dim_{\mathbb{F}_2}\frac{E(\mathbb{Q})}{2(E(\mathbb{Q}))} = dim_{\mathbb{F}_2}\frac{E(\mathbb{Q})}{\hat{\varphi}(E'(\mathbb{Q}))} + dim_{\mathbb{F}_2}\frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} - dim_{\mathbb{F}_2}\frac{E'(\mathbb{Q})[\hat{\varphi}]}{\varphi(E(\mathbb{Q})[2])}.$$

On the other hand,

$$(2.5) \quad E(\mathbb{Q}) \cong \mathbb{Z}^r + E(\mathbb{Q})_{tors}.$$

Hence

$$(2.6) \quad E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r + E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors},$$

and therefore

$$rank\ E(\mathbb{Q}) = dim_{\mathbb{F}_2}E(\mathbb{Q})/2(E(\mathbb{Q})) - dim_{\mathbb{F}_2}E(\mathbb{Q})_{tors}/2E(\mathbb{Q})_{tors}.$$

From the above formulas we can see that, if φ is a 2-isogeny and $E(\mathbb{Q})_{tors}$ $= E[2]$, then the rank of the elliptic curve is given by

$$(2.7) \quad rankE(\mathbb{Q}) = dim_{\mathbb{F}_2}E(\mathbb{Q})/\hat{\varphi}(E'(\mathbb{Q})) + dim_{\mathbb{F}_2}E(\mathbb{Q})/\varphi(E(\mathbb{Q})) - 2.$$

On the other hand from (2.1) and (2.2) we have

(2.8) $dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) = dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) - dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi]$

and

(2.9) $dim_{\mathbb{F}_2} E(\mathbb{Q})/\hat{\varphi}(E'(\mathbb{Q})) = dim_{\mathbb{F}_2} S^{(\hat{\varphi})}(E'/\mathbb{Q}) - dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\hat{\varphi}]$.

Finally (2.7), (2.8) and (2.9) imply that

$$\begin{aligned} rank E(\mathbb{Q}) &= dim_{\mathbb{F}_2} S^{(\hat{\varphi})}(E'/\mathbb{Q}) - dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\hat{\varphi}] + \\ &\quad dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) - dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi] - 2. \end{aligned} \tag{2.10}$$

In our case, we use $E'_p : y^2 = x^3 + 12px$ and the 2-isogeny $\varphi : E_p \longrightarrow E'_p$ defined by

$$\varphi(x, y) = (y^2/x^2, -y(3p + x^2)/x^2).$$

To compute Selmer groups, we use proposition X.4.9 in [16]. Thus letting $S = \{\infty, 2, 3, p\} \subseteq M_{\mathbb{Q}}$,

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2;\ ord_v(b) \equiv 0 (mod\ 2)\ for\ all\ v \notin S\},$$

and

$$C_d : dy^2 = d^2 + 12px^4,$$
$$C'_d : dy^2 = d^2 - 3px^4,$$

we have the following identifications:

$$S^{(\varphi)}(E_p/\mathbb{Q}) \simeq \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{Q}_l) \neq \phi\ for\ all\ l \in S\},$$
$$S^{(\hat{\varphi})}(E_p/\mathbb{Q}) \simeq \{d \in \mathbb{Q}(S, 2) : C'_d(\mathbb{Q}_l) \neq \phi\ for\ all\ l \in S\}.$$

Note that $\{\pm 1, \pm 2, \pm 3, \pm p, \pm 6, \pm 2p, \pm 3p, \pm 6p\}$ is a complete set of representatives for $\mathbb{Q}(S, 2)$. We identify this set with $\mathbb{Q}(S, 2)$.

Proposition 2.1. *We have*

(1) $S^{(\varphi)}(E_p/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ *for* $p \equiv 1, 5, 13, 25, 29, 37, 47\ (mod\ 48)$*;*
(2) $S^{(\varphi)}(E_p/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *in all other cases.*

Proof. Using the above identification we have $\{1, 3p\} \subseteq S^{(\varphi)}(E_p/\mathbb{Q})$. On the other hand $C_d(\mathbb{R}) = \phi$ for $d < 0$, and $C_d(\mathbb{R}) \neq \phi$ for $d > 0$.
For $d = 2$, $C_2(\mathbb{Q}_3) = \phi$, so $2 \notin S^{(\varphi)}(E_p/\mathbb{Q})$. For $d = p$,we have:

$$C_p(\mathbb{Q}_2) \neq \phi \Longleftrightarrow p \equiv 1 (mod\ 4),$$

$$C_p(\mathbb{Q}_3) \neq \phi \Longleftrightarrow p \equiv 1 (mod\ 3),$$

$$C_p(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{3}{p}) = 1.$$

Therefore, $3 \in S^{(\varphi)}(E_p/\mathbb{Q})$ if and only if $p \equiv 1(mod\ 12)$.
For $d = 6$, we have:

$$C_6(\mathbb{Q}_2) \neq \phi \Longleftrightarrow p \equiv 5, 13, 15(mod\ 16),$$

$$C_6(\mathbb{Q}_3) \neq \phi \Longleftrightarrow (\tfrac{2p}{3}) = 1 \Longleftrightarrow p \equiv 2(mod\ 3),$$

$$C_6(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{6}{p}) = 1.$$

Thus $6 \in S^{(\varphi)}(E_p/\mathbb{Q})$ if and only if $p \equiv 5, 29, 47(mod\ 48)$.
Since $3p \in S^{(\varphi)}(E_p/\mathbb{Q})$ we conclude that

$$\begin{gathered} 3 \in S^{(\varphi)}(E_p/\mathbb{Q}) \Longleftrightarrow p \in S^{(\varphi)}(E_p/\mathbb{Q}) \Longleftrightarrow p \equiv 1(mod\ 12), \\ 6p \in S^{(\varphi)}(E_p/\mathbb{Q}) \Longleftrightarrow 2 \in S^{(\varphi)}(E_p/\mathbb{Q}), \text{ which is impossible}, \\ 2p \in S^{(\varphi)}(E_p/\mathbb{Q}) \Longleftrightarrow 6 \in S^{(\varphi)}(E_p/\mathbb{Q}) \Longleftrightarrow p \equiv 5, 29, 47(mod\ 48). \end{gathered}$$

Finally we have:

If $p \equiv 1, 13, 25, 37$ (mod 48), then $S^{(\varphi)}(E_p/\mathbb{Q}) = \{1, 3, p, 3p\}$.
If $p \equiv 5, 29, 47$ (mod 48), then $S^{(\varphi)}(E_p/\mathbb{Q}) = \{1, 6, 2p, 3p\}$.
In all other cases, $S^{(\varphi)}(E_p/\mathbb{Q}) = \{1, 3p\}$.

This completes the proof. □

Proposition 2.2. *We have*

(1) $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ *for* $p \equiv 1, 7, 19, 23, 25, 35, 47$ $(mod\ 48)$*;*
(2) $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *in all other cases.*

Proof. It is clear from the definition that $\{1, -3p\} \subseteq S^{(\hat{\varphi})}(E'_p/\mathbb{Q})$. Suppose that d=2k with $k = \pm 1, \pm 3, \pm p$ and $C'_{2k}(\mathbb{Q}_2) \neq \phi$. Taking the valuation v_2 at 2 of both sides, we obtain a contradiction.
For $d = -1$, we have $C'_{-1}(\mathbb{Q}_3) = \phi$, so $-1 \notin S^{(\hat{\varphi})}(E'_p/\mathbb{Q})$.
For $d = 3$ we have:

$$C'_3(\mathbb{Q}_2) \neq \phi \Longleftrightarrow p \equiv 3, 7, 15(mod\ 16),$$

$$C'_3(\mathbb{Q}_3) \neq \phi \Longleftrightarrow p \equiv 2(mod\ 3),$$

$$C'_3(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{3}{p}) = 1 \Longleftrightarrow p \equiv 1, 11(mod\ 12).$$

For $d = -3$, we have

$$C'_{-3}(\mathbb{Q}_2) \neq \phi \Longleftrightarrow p \equiv 1, 3, 7, 9 (mod\ 16),$$

$$C'_{-3}(\mathbb{Q}_3) \neq \phi \Longleftrightarrow (\tfrac{p}{3}) = 1 \Longleftrightarrow p \equiv 1 (mod\ 3),$$

$$C'_{-3}(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{-3}{p}) = 1 \Longleftrightarrow p \equiv 1, 7 (mod\ 12).$$

So

$$\pm 2, \pm 2p, \pm 6 \notin S^{(\hat{\varphi})}(E'_p/\mathbb{Q}),$$

$$3 \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow p \equiv 23, 35, 47 (mod\ 48),$$

$$-3 \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow\ p \equiv 1, 7, 19, 25 (mod\ 48).$$

Since $-3p \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q})$ we conclude that

$$p \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow -3 \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow\ p \equiv 1, 7, 19, 25 (mod\ 48),$$

$$-p \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow 3 \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow p \equiv 23, 35, 47 (mod\ 48),$$

$$3p \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) \Longleftrightarrow -1 \in S^{(\hat{\varphi})}(E'_p/\mathbb{Q}),\ \textit{which is impossible.}$$

Finally we have:

If $p \equiv 1, 7, 19, 25$ (mod 12), then $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) = \{1, -3, p, -3p\}$,
If $p \equiv 23, 35, 47$ (mod 12), then $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) = \{1, 3, -p, -3p\}$,
In the other cases, then $S^{(\hat{\varphi})}(E'_p/\mathbb{Q}) = \{1, -3p\}$.

This completes the proof. □

Theorem 2.3. *Following statements hold:*
If $p \equiv 1, 25, 47$ $(mod\ 48)$*, then* $rank(E_p(\mathbb{Q})) \leq 2$;
If $p \equiv 5, 7, 13, 19, 23, 29, 35, 37$ $(mod\ 48)$ *, then* $rank(E_p(\mathbb{Q})) \leq 1$;
In all other cases, $rank(E_p(\mathbb{Q})) = 0$.

Proof. This follows from propositions 2.1, 2.2 and (2.10). □

3. **Calculation of the root number**

In this section, first we recall the concept of the root number and then using Parity conjecture refine our results in the previous section. Let E be an elliptic curve over $\mathbb{Q}$ and n_p be the number of points in the reduction of curve modulo p. Also let $a_p = p+1-n_p$. Local part of the L-series of E at p is defined as

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

Definition 3.1. *The L-series of E is defined to be*

$$L(E,s) = \prod_p \frac{1}{L_p(p^{-s})},$$

where the product is over all primes.

Theorem 3.2. *The L-series $L(E,s)$ has 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 and Γ is the Gamma function. Here $\epsilon(E) = \pm 1$ is called the global root number of E.

The Parity conjecture states that

$$\epsilon(E) = (-1)^{r_E}, \tag{3.1}$$

where r_E denotes the rank of Mordell-Weil group of E. On the other hand, $\epsilon(E)$ can be expressed as a product $\prod_l \epsilon_l(E)$ taken over all places of $\mathbb{Q}$, each local root number $\epsilon_l(E)$ being defined in terms of representations of Weil-Deligne group of $\mathbb{Q}_l$. We recall some facts from [14].

Proposition 3.3. *Let l be a prime. Then*

1. *If E is any elliptic curve over $\mathbb{R}$, then $\epsilon_\infty(E) = -1$.*
2. *If $E/\mathbb{Q}_l$ has good reduction, then $\epsilon_l(E) = 1$.*
3. *If $E/\mathbb{Q}_l$ has multiplicative reduction, $\epsilon_l(E) = -1$ if and only if the reduction is split.*
4. *If $E/\mathbb{Q}_l$ has additive, potentially multiplicative reduction then for $l > 2$, $\epsilon_l(E) = (-1/l)$ and for $l = 2$, $\epsilon_2(E) \equiv -c_6/2^{v_2(c_6)}$ mod 4.*
5. *If $E/\mathbb{Q}_l$ has additive, potentially good reduction with $l > 3$ and $e = 12/gcd(v_l(\Delta), 12)$. then*

$$\epsilon_l(E) = \begin{cases} (-1/l) & \text{if } e = 2 \text{ or } 6 \\ (-3/l) & \text{if } e = 3 \\ (-2/l) & \text{if } e = 4 \end{cases}$$

(6) *If $E/\mathbb{Q}_l$ has additive, potentially good reduction with $l = 3$ (respectively l=2) and E is given in minimal form, then $\epsilon_l(E)$ depends only on the l-adic expansion of c_4, c_6 and Δ; if E is given in minimal Weirestrass form, $\epsilon_l(E)$ can be read from table II of [9].*

Proposition 3.4. *For any prime l, if $E/\mathbb{Q}_l$ is in minimal Weierstrass form, then its reduction is: good if and only if $v_l(\Delta) = 0$, multiplicative if and only if $v_l(\Delta) > 0$ and $v_l(c_4) = 0$, additive if and only if $v_l(\Delta) > 0$ and $v_l(c_4) > 0$. In the last case, the reduction is potentially multiplicative if and only if $v_l(\Delta) > 3v_l(c_4)$.*

For the elliptic curve E in the family, we have $\Delta_E = 2^6 \times 3^3 \times p^3$. In particular, $y^2 = x^3 - 3px$ is in global minimal Weierstrass form. In this case the reduction of E_p is additive, potentially good at 2,3 and p, and good at all other primes.

Proposition 3.5. *For elliptic curve $E : y^2 = x^3 - 3px$, we have*

$$\epsilon(E_p) = \begin{cases} +1 & \text{if } p \equiv 1, 9, 11, 15 \ (mod\ 16) \\ -1 & \text{if } p \equiv 3, 5, 7, 13 \ (mod\ 16). \end{cases}$$

Proof. Let $\epsilon_l(E_p)$ denote the local root number at l. From proposition 3.3 and above discussion, we have

$$\epsilon_2(E_p) = \begin{cases} +1 & \text{if } p \equiv 3, 15 \ (mod\ 16) \\ -1 & \text{if } p \equiv 1, 5, 7, 9, 11, 13 \ (mod\ 16), \end{cases}$$

and

$$\epsilon_3(E_p) = 1,$$

and, finally

$$\epsilon_p(E_p) = (\tfrac{-2}{p}) = \begin{cases} +1 & \text{if } p \equiv 1, 3 \ (mod\ 8) \\ -1 & \text{if } p \equiv 5, 7 \ (mod\ 8). \end{cases}$$

The assertion follows. □

Corollary 3.6. *Assume the Parity conjecture holds for the family E_p. Then*

(1) *if* $p \equiv 5, 7, 13, 19, 23, 29, 35, 37$ $(mod\ 48)$*, then* $r_p = 1$;
(2) *if* $p \equiv 11, 17, 31, 41, 43$ $(mod\ 48)$*, then* $r_p = 0$;
(3) *if* $p \equiv 1, 25, 47$ $(mod\ 48)$*, the Parity conjecture implies* $r_p = 0$ *or* 2*.*

Remark 3.7. *Recall that Kolyvagin's work [10] proves that if E is a modular elliptic curve over* $\mathbb{Q}$ *and if analytic rank of E is 0 or 1, then the analytic rank equals the algebraic rank. Thanks to Wiles we can remove modularity hypothesis from these results. Actually, in (3) both cases appear:* $r_{191} = r_{197} = r_{313} = 0$ *and* $r_{47} = r_{337} = r_{3529} = 2$*.*

4. Integer points and independent points

In this section, first we find integral points on the elliptic curve, and using Weil-Châtelet group we give a condition on p, such that $y^2 = x^3 - 3px$ has maximal rank.
If (x, y) is an integer point on E_p, then the equation $y^2 = x(x^2 - 3p)$ implies that $x = du^2$ and $x^2 - 3p = dv^2$ for some squarefree integer d and positive integers u,v. Combining these two equations yields $d^2u^4 - 3p = dv^2$; hence, d is a divisor of $3p$, and

$$du^4 - (3p/d) = v^2. \tag{4.1}$$

We examine each cases separately.

(1) ***d=1.***In this case (4.1) can be rewritten as $3p = u^4 - v^2$, therefore $p = 2u^2 - 3$, and $(u^2, u(p-3)/2)$ is on the curve.
(2) ***d=-1.*** In this case (4.1) can be rewritten as $3p = u^4 + v^2$, which is impossible modulo 3.
(3) ***d=3.*** In this case (4.1) can be rewritten as $p = 3u^4 - v^2$, and $(3u^2, 3uv)$ is on the curve.
(4) ***d=-3.*** In this case (4.1) can be rewritten as $p = 3u^4 + v^2$, and $(-3u^2, -3uv)$ is on the curve.
(5) ***d=p.*** In this case (4.1) can be rewritten as $pu^4 = v^2 + 3$ and (pu^2, puv) is on the curve.
(6) ***d=-p.*** In this case (4.1) can be rewritten as $-pu^4 = v^2 - 3$, which is impossible, since $p \neq 2, 3$.
(7) ***d=3p.*** In this case (4.1) can be rewritten as $3pu^4 = v^2 + 1$, which is impossible modulo 3.
(8) ***d=-3p.*** In this case (4.1) can be rewritten as $-3pu^4 = v^2 - 1$, which is impossible.

Remark 4.1. *From above discussion, if p satisfies any two cases of (1),(3),(4),(5) above, then we can find two integer points on the elliptic curve. For example,* $47 = 2\times5^2-3$ *and* $47 = 3\times2^4-1$*, then* $P = (25, 110)$ *and* $Q = (12, 6)$ *are on* $E_{47} : y^2 = x^3 - 141x$*. On the other hand, we have*

$$\langle P, P\rangle = 3.05926,$$
$$\langle P, Q\rangle = -1.38191,$$
$$\langle Q, Q\rangle = 2.27932.$$

Where as [21]

$$\langle R_1, R_2\rangle = \hat{h}(R_1 + R_2) - \hat{h}(R_1) - \hat{h}(R_2),$$

is the height pairing. Therefore

$$det \begin{bmatrix} \langle P, P\rangle & \langle P, Q\rangle \\ \langle P, Q\rangle & \langle Q, Q\rangle \end{bmatrix} = det \begin{bmatrix} 3.05926 & -1.38191 \\ -1.38191 & 2.27932 \end{bmatrix} = 5.0633 \neq 0.$$

Hence, P *and* Q *are independent points on* $E_{47} : y^2 = x^3 - 141x$*.*

Now, following [12, 22] we try to find elliptic curves with maximal rank in the family. Using the homomorphism

$$\alpha : E_p(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

which is defined by

$$\alpha(P) = \begin{cases} \mathbb{Q}^{\times 2} & \text{if } P = \mathcal{O} \\ -3p\mathbb{Q}^{\times 2} & \text{if } P = (0, 0) \\ x\mathbb{Q}^{\times 2} & \text{if } P = (x, y) \neq (0, 0), P \neq \mathcal{O}. \end{cases}$$

We have the following exact sequence

$$0 \longrightarrow \hat{\varphi}(E_p'(\mathbb{Q})) \longrightarrow E_p(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

as well as the corresponding result for the dual isogeny:

$$0 \longrightarrow \varphi(E_p(\mathbb{Q})) \longrightarrow E_p'(\mathbb{Q}) \xrightarrow{\beta} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

So $im\alpha \simeq \dfrac{E_p(\mathbb{Q})}{\hat{\varphi}(E_p'(\mathbb{Q}))}$ and $im\beta \simeq \dfrac{E_p'(\mathbb{Q})}{\varphi(E_p(\mathbb{Q}))}$. As mentioned in [12], The images of α and β can be described as follows: $WC(E_p'/\mathbb{Q}) := im\alpha$ consists of all classes $b_1\mathbb{Q}^{\times 2}$, where b_1 is a squarefree integer such that

$$N^2 = b_1M^4 + b_2e^4, \quad b_1b_2 = -3p \tag{4.2}$$

has a nontrivial solution $N, M, e \in \mathbb{N}$ with $(M, e) = (N, e) = 1$. The equation (4.2) is called a torsor of $E/\mathbb{Q}$ and is denoted by $\mathcal{T}^{(\hat{\varphi})}(b_1)$.

Similarly, $WC(E_p/\mathbb{Q}) := im\beta$ consists of all classes $b_1\mathbb{Q}^{\times 2}$, where b_1 is a squarefree integer such that

$$(4.3) \qquad \mathcal{T}^{(\varphi)}(b_1) : N^2 = b_1 M^4 + b_2 e^4, \quad b_1 b_2 = 12p$$

has a nontrivial solution in integer $N, M, e \in \mathbb{N}$. It is easy to see that every rational point $P \neq \mathcal{O}$ on E_p has the form $P = (m/e^2, n/e^3)$ for integers $n, m, e \in \mathbb{Z}$ such that $(m, e) = (n, e) = 1$, and by definition we have $\alpha(P) = m\mathbb{Q}^{\times 2}$. Moreover, it can be shown that the corresponding torsor $\mathcal{T}^{(\hat{\varphi})}(m)$ is solvable. Conversely, if (N, M, e) is a nontrivial primitive solution of $\mathcal{T}^{(\hat{\varphi})}(b_1)$, then $(b_1 M^2/e^2, b_1 MN/e^3)$ is a rational point on E. Finally from (2.1) and (2.2) we have the following exact sequences

$$(4.4) \quad 0 \to WC(E_p/\mathbb{Q}) \to S^{(\varphi)}(E_p/\mathbb{Q}) \to Ш(E_p/\mathbb{Q})[\varphi] \to 0,$$

$$(4.5) \quad 0 \to WC(E_p'/\mathbb{Q}) \to S^{(\hat{\varphi})}(E_p'/\mathbb{Q}) \to Ш(E_p'/\mathbb{Q})[\hat{\varphi}] \to 0.$$

Proposition 4.2. *If the parity conjecture holds for the family E_p, then*

(1) *if $p = 48a^4 + n^2$, and $n^2 \equiv 1, 25, 47$ $(mod\ 48)$ then $r_p = 2$.*
(2) *if $p = 48a^4 - n^2$ and $n^2 \equiv 1, 23, 47$ $(mod\ 48)$, then $r_p = 2$.*

Proof. If $p = 48a^4 + n^2$ then $(2a, n, 1)$ is a nontrivial solution of $-3M^4 + pe^4 = N^2$, then $\mathcal{T}^{(\hat{\varphi})}(-3) \neq \phi$ and so $\{1, -3p, -3, p\} \subseteq WC(E_p'/\mathbb{Q})$. Thus (4.5) and proposition 2.2 imply that $dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\hat{\varphi}] = 0$. On the other hand, $\{1, 3p\} \subseteq WC(E_p/\mathbb{Q})$, and therefore (4.4) and proposition 2.1 imply $dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi] \leq 1$. Now (2.10) implies $r_p \geq 1$. Thus from parity conjecture we conclude that $r_p = 2$. Proof of part (2) is similar. □

Corollary 4.3. *If $p = 48a^4 + (4a^4 + m^4 - 3)^2$ or $p = 48a^4 + (12a^4 + 3m^4 - 1)^2$, then $r_p = 2$.*

Proof. As we see in the proof of last proposition, in these cases $dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\hat{\varphi}] = 0$. If $p = 48a^4 + (4a^4 + m^4 - 3)^2$, then $p = (4a^4 + m^4 + 3)^2 - 12m^4$ and therefore $(M, N, e) = (m, 4a^4 + m^4 + 3, 1)$ is a solution of $\mathcal{T}^{(\varphi)}(12)$. So $12 \in WC(E_p/\mathbb{Q})$, and thus $\{1, 3p, 3, p\} \subseteq WC(E_p/\mathbb{Q})$. Therefore, (4.4) and proposition 2.1 imply $dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi] = 0$. Now, (2.10) implies $r_p \geq 2$, and we conclude that $r_p = 2$. For $p = 48a^4 + (12a^4 + 3m^4 - 1)^2$ we have a similar argument. □

The following conjecture due to Schinzel and Sierpinski [15] implies that there exist infinitely many such primes.

Conjecture 4.4. *Let $f_1(x), f_2(x), \ldots, f_m(x) \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading coefficients. Assume that there exists no integer $n > 1$ dividing $f_1(k), f_2(k), \ldots, f_m(k)$ for all integers k. Then there exist infinitely many positive integers l such that each of the numbers $f_1(l), f_2(l), \ldots, f_m(l)$ is prime.*

We can see that $f(x) = 48x^4 + (4x^4 + 13)^2$ and $g(x) = 48x^4 + (12x^4 + 47)^2$ satisfy the assumption of the conjecture with $m = 1$. So there exist infinitely many positive integers l_1 and l_2, such that $f(l_1)$ and $g(l_2)$ are prime numbers. So there exist infinitely many elliptic curves $y^2 = x^3 - 3px$ with rank two. Some examples of such primes are: 337, 1087657, 27071017, 3529, 243391009, 832957129, 61941751969.

5. Numerical calculations related to the rank

As we see in corollary 3.6, if $p \equiv 1, 25, 47$ $(mod\ 48)$, then parity conjecture implies $r_p = 0$ *or* 2. Now, using Magma [1], we have some examples in table 1.

TABLE 1.

$p \equiv 1$ $(mod\ 48)$	r_p	$p \equiv 25$ $(mod\ 48)$	r_p	$p \equiv 47$ $(mod\ 48)$	r_p
1249	0	4969	0	4943	0
3889	2	5449	0	5711	0
4177	2	5737	2	15647	0
4657	0	5881	2	16223	0
5281	0	39241	0	17903	2
5521	0	39769	0	17903	2
6529	0	42841	0	34319	2
28513	2	44617	2	47087	2
33409	2	47017	2	47903	0
34897	2	47977	0	47951	0

Let $N_k(x, r)$ denote the number of elliptic curves E_p with $p = 48i + k$ and $i \leq x$, such that $r_p = r$, and set $n_k(x, 0) := \frac{N_k(x,0)}{N_k(x,0)+N_k(x,2)}$ and $n_k(x, 2) := \frac{N_k(x,2)}{N_k(x,0)+N_k(x,2)}$. Tables 2, 3, 4 suggest that the elliptic curves E_p, with rank 2 thin out. Therefore considering corollary 3.6 and the Dirichlet theorem on arithmetic progressions, it seems that half of the curves in the family have rank1 and the other half have rank 0.

Table 2.

x	$N_1(x,2)$	$N_1(x,0)$	$n_1(x,2)$	$n_1(x,0)$
10000	577	1905	0.2325	0.7675
20000	945	3725	0.2024	0.7976
30000	1293	5513	0.19	0.81
40000	1596	7317	0.1791	0.8901
50000	2151	8830	0.1959	0.8041
60000	2400	10613	0.1844	0.8156
70000	2646	12376	0.1761	0.8239
80000	2855	14137	0.168	0.832
90000	3060	15894	0.1614	0.8386
100000	3239	17676	0.1549	0.8451

Table 3.

x	$N_{25}(x,2)$	$N_{25}(x,0)$	$n_{25}(x,2)$	$n_{25}(x,0)$
10000	627	1845	0.2617	0.7383
20000	1000	3697	0.2129	0.7871
30000	1318	5513	0.1929	0.8071
40000	1605	7282	0.1806	0.8194
50000	1855	9089	0.1695	0.8305
60000	2116	10855	0.1631	0.8369
70000	2340	12652	0.1561	0.8439
80000	2549	14420	0.1502	0.8498
90000	2755	16192	0.1454	0.8546
100000	2961	17939	0.1417	0.8583

6. Acknowledgement

We would like to thank Professor Henri Darmon for reading the initial version of this paper and for his interest in our work and useful advices. This research was in part supported by University of Kashan under grant number 159037/1.

References

[1] J. Cannon, MAGMA Computational Algebra System, http://magma.maths.usyd.edu.au/magma/handbook/.

Table 4.

x	$N_{47}(x,2)$	$N_{47}(x,0)$	$n_{47}(x,2)$	$n_{47}(x,0)$
10000	895	1639	0.3532	0.6468
20000	1495	3248	0.3152	0.6848
30000	1990	4886	0.2894	0.7106
40000	2455	6481	0.2747	0.7253
50000	2860	8140	0.26	0.74
60000	3260	9779	0.25	0.75
70000	3643	11381	0.2425	0.7575
80000	3958	13019	0.2331	0.7669
90000	4310	14640	0.2274	0.7726
100000	4646	16290	0.2219	0.7781

[2] D. Andrzej and M. Wieczorek, On the equation $y^2 = x(x-2^m)(x+q-2^m)$. *J. Number Theory* **124(2)** (2007) 364–379.
[3] K. A. Draziotis and D. Poulakis, Practical solution of the Diophantine equation $y^2 = x(x+2^ap^b)(x-2^ap^b)$, *Math. Comp.* **75** (2006), no. 255, 1585–1593.
[4] K. A. Draziotis, Integer points on the curve $Y^2 = X^3 \pm p^kX$, *Math. Comp.* **75** (2006), no. 255, 1493–1505.
[5] K. Feng and M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero, *J. Number Theory* **109** (2004), no. 1, 1–26.
[6] Y. Fujita and N. Terai, Integer Points and Independent points on the elliptic curve $y^2 = x^3 - p^kx$. *Tokyo J. Math.* **34** (2011), no. 2, 367–381.
[7] Y. Fujita and T. Nara, On the MordellWeil group of the elliptic curve, *J. Number Theory* **132** (2012), no. 3, 448–466.
[8] T. Goto, A study on the Selmer groups of the elliptic curves with a rational 2-torsion, Ph.D Thesis, Kyushu Univ., (2002).
[9] E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3, *C. R. Acad. Sci. Paris Ser. I Math* **326** (1998), no. 9, 1047–1052.
[10] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Sha(E,\mathbb{Q})$ for a subclass of Weil curves, *Izv. Akad. Nauk SSSR Ser. Mat.* **52** (1998), no. 3, 522–540, translation in: *Math. USSR-Izv* **32** (1989), no. 3, 523–541.
[11] F. Lemmermeyer and R. Mollin, On Tate-Shafarevich groups of $y^2 = x(x^2-k^2)$, *Acta Math. Univ. Comenian. (N.S.)* **72** (2003), no. 1, 73–80.
[12] F. Lemmermeyer, On Tate-Shafarevich Groups of Some Elliptic Curves, Algebraic Number Theory and Diophantine Analysis, (1998), 277–291, de Gruyter, Berlin, 2000.
[13] M. Maenishi, On the rank of elliptic curves $y^2 = x^3 - pqx$, *Kumamoto J. Math.* **15** (2002) 1–5.
[14] O. G. Rizzo, Average root numbers for a nonconstant family of elliptic curves, *Compositio Math.* **136** (2003), no. 1, 1–23.

[15] A. Schinzel and W. Sierpinski, Sur certaines hypotheses concernant les nombres premiers, *Acta Arith.* **4** (1958) 185–208.
[16] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.
[17] B. K. Spearman, On the group structure of elliptic curves $y^2 = x^3 - 2px$, *Int. J. Algebra.* **1** (2007), no. 5-8, 247–250.
[18] P. Walsh, Maximal ranks and integer points on a family of elliptic curves II, *Rocky Mountain J. Math.* **41** (2011), no. 1, 311–317.
[19] P. Walsh, Maximal ranks and integer points on a family of elliptic curves, *Glas. Mat. Ser. III* **44(64)** (2009), no. 1, 83–87.
[20] P. Walsh, Integer solutions to the equation $y^2 = x(x^2 \pm p^k)$, *Rocky Mountain J. Math.* **38** (2008), no. 4, 1285–1302.
[21] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall, Boca Raton, 2008.
[22] A. Weil, Sur un theoreme de mordell, *Bull. Sci. Math.* **54** (1930), no. 2, 182–191.

(Hassan Daghigh) Department of Mathematics, University of Kashan, P.O. Box 87317-51167, Kashan, Iran
E-mail address: hassan@kashanu.ac.ir

(Somayeh Didari) Department of Mathematics, University of Kashan, P.O. Box 87317-51167, Kashan, Iran
E-mail address: s.didari@grad.kashanu.ac.ir