Iranian Journal of Mathematical Sciences and Informatics
Vol. 10, No. 2 (2015), pp 77-86
DOI: 10.7508/ijmsi.2015.02.008

On the Elliptic Curves of the Form $\mathbf{y^2 = x^3 - pqx}$

Hassan Daghigh*, Somayeh Didari

Department of Mathematics, University of Kashan, Kashan, Iran.

E-mail: hassan@kashanu.ac.ir
E-mail: somayeh.didari@gmail.com

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. This paper studies the rank of the family $E_{pq} : y^2 = x^3 - pqx$ of elliptic curves, where p and q are distinct primes. We give infinite families of elliptic curves of the form $y^2 = x^3 - pqx$ with rank two, three and four, assuming a conjecture of Schinzel and Sierpinski is true.

Keywords: Diophantine equation, Elliptic curves, Mordell weil group, Selmer group, Birch and Swinnerton- dyer conjecture, Parity conjecture.

2010 Mathematics subject classification: 11G05, 14H52.

1. Introduction

Finding integral solutions of Diophantine equations has a long history [1, 2, 3, 11]. Elliptic curves over rational numbers are special types of these equations. 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 $\mathbb{Q}$.

In our previous paper[4], we considered the family of elliptic curves of the form $E_p : y^2 = x^3 - 3px$ over $\mathbb{Q}$, where p is a prime number. In this paper we consider the family of elliptic curves over $\mathbb{Q}$ given by the equation

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

*Corresponding Author

Received 29 April 2014; Accepted 02 July 2014

where p and q are distinct primes $\neq 2, 3$. Using Selmer groups we first find an upper bound for the rank of this family. Then using the Parity conjecture, we refine our result and find infinite families of elliptic curves which conjecturally have rank zero. Finally we provide sufficient conditions on p and q, for the elliptic curves $y^2 = x^3 - pqx$ to have rank two, three and four. We also show that conjecturally, there exist infinitely many such primes.

2. Computing Selmer Groups and Proof of the Main Result

Let E and E' be elliptic curves defined over $\mathbb{Q}$, and $\varphi : E \longrightarrow E'$ a non zero $2-$isogeny. Then we have the following commutative diagram:

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

where $H^1(\mathbb{Q}_v, -)$ denotes $H^1(Gal(\mathbb{Q}_v/\mathbb{Q}), -)$ and δ is the connecting homomorphism. φ- Selmer group is then 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 $\text{Ш}(E/\mathbb{Q})$ is

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

Using the dual isogeny $\hat{\varphi} : E' \longrightarrow E$, $S^{(\hat{\varphi})}(E'/\mathbb{Q})$ and $\text{Ш}(E'/\mathbb{Q})[\hat{\varphi}]$ are similarly defined. We have the following relation

$$\begin{aligned} rankE(\mathbb{Q}) \quad = \quad & dim_{\mathbb{F}_2} S^{(\hat{\varphi})}(E'/\mathbb{Q}) - dim_{\mathbb{F}_2} \text{Ш}(E'/\mathbb{Q})[\hat{\varphi}] + \\ & dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) - dim_{\mathbb{F}_2} \text{Ш}(E/\mathbb{Q})[\varphi] - 2. \end{aligned} \tag{2.1}$$

In our case, we use $E'_{pq} : y^2 = x^3 + 4pqx$ and the 2-isogeny $\varphi : E_{pq} \longrightarrow E'_{pq}$ defined by

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

For computing Selmer groups, we use proposition X.4.9 in [14]. Thus letting $S = \{\infty, 2, p, q\} \subseteq M_{\mathbb{Q}}$,

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

and for

$$C_d : dy^2 = d^2 + 4pqx^4,$$
$$C'_d : dy^2 = d^2 - pqx^4,$$

we have the following identifications:

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

Note that $\{\pm 1, \pm 2, \pm q, \pm p, \pm 2q, \pm 2p, \pm qp, \pm 2pq\}$ 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) $\{1, pq\} \subseteq S^{(\varphi)}(E_{pq}/\mathbb{Q})$;
(2) *if* $d < 0$ *then* $d \notin S^{(\varphi)}(E_{pq}/\mathbb{Q})$;
(3) $2 \in S^{(\varphi)}(E_{pq}/\mathbb{Q})$ *iff* $(\frac{2}{p}) = (\frac{2}{q}) = 1$ *and* $pq \equiv 1, 7, 15 (mod\ 16)$;
(4) $p \in S^{(\varphi)}(E_{pq}/\mathbb{Q})$ *iff* $(\frac{q}{p}) = 1$ *and* $[p \equiv 1 (mod\ 4)$ *or* $q \equiv 1 (mod\ 4)]$;
(5) $2p \in S^{(\varphi)}(E_{pq}/\mathbb{Q})$ *iff* $(\frac{2p}{q}) = (\frac{2q}{p}) = 1$ *and* $p + q \equiv 0, 2, 8 (mod\ 16)$;

Proof. Using the identification in lemma we have $\{1, pq\} \subseteq S^{(\varphi)}(E/\mathbb{Q})$. On the other hand $C_d(\mathbb{R}) = \phi$ for $d < 0$, and $C_d(\mathbb{R}) \neq \phi$ for $d > 0$.
For $d = 2$,we have:

$$C_2(\mathbb{Q}_2) \neq \phi \Longleftrightarrow pq \equiv 1, 7, 15 (mod\ 16),$$

$$C_2(\mathbb{Q}_q) \neq \phi \Longleftrightarrow (\tfrac{2}{q}) = 1 \Longleftrightarrow q \equiv 1, 7 (mod\ 8),$$

$$C_2(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{2}{p}) = 1 \Longleftrightarrow p \equiv 1, 7 (mod\ 8),$$

For $d = p$,we have:

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

$$C_p(\mathbb{Q}_q) \neq \phi \Longleftrightarrow (\tfrac{p}{q}) = 1,$$

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

For $d = 2p$,we have:

$$C_{2p}(\mathbb{Q}_2) \neq \phi \Longleftrightarrow p + q \equiv 0, 2, 8 (mod\ 16).$$

$$C_{2p}(\mathbb{Q}_q) \neq \phi \Longleftrightarrow (\tfrac{2p}{q}) = 1 \Longleftrightarrow p \equiv 2 (mod\ 3).$$

$$C_{2p}(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{2q}{p}) = 1.$$

Since $pq \in S^{(\varphi)}(E_{pq}/\mathbb{Q})$ we conclude that

$$q \in S^{(\varphi)}(E_{pq}/\mathbb{Q}) \Longleftrightarrow p \in S^{(\varphi)}(E_{pq}/\mathbb{Q}),$$

$$2pq \in S^{(\varphi)}(E_{pq}/\mathbb{Q}) \Longleftrightarrow 2 \in S^{(\varphi)}(E_{pq}/\mathbb{Q}),$$

$$2p \in S^{(\varphi)}(E_{pq}/\mathbb{Q}) \Longleftrightarrow 2q \in S^{(\varphi)}(E_{pq}/\mathbb{Q}).$$

This completes the proof. □

Proposition 2.2. *We have*

(1) $\{1, -pq\} \subseteq S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$;

(2) $-1 \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$ *iff* $p \equiv q \equiv 1(mod\ 4)$ *and* $pq \equiv 1, 5, 9(mod\ 16)$;
(3) $\pm 2 \notin S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$;
(4) $p \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$ *iff* $(\frac{-q}{p}) = (\frac{p}{q}) = 1$ *and one of the following conditions hold:*
- $p \equiv 1(mod\ 8)$
- $q \equiv 7(mod\ 8)$
- $p - q \equiv 0, 4(mod\ 16)$

(5) $q \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$ *iff* $(\frac{-p}{q}) = (\frac{q}{p}) = 1$ *and one of the following conditions hold:*
- $q \equiv 1(mod\ 8)$
- $p \equiv 7(mod\ 8)$
- $q - p \equiv 0, 4(mod\ 16)$

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

Proof. It is clear from definition that $\{1, -pq\} \subseteq S^{(\hat{\varphi})}(E'/\mathbb{Q})$. Suppose next that d=2k with $k = \pm 1, \pm q, \pm p$ 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

$$C'_{-1}(\mathbb{Q}_2) \neq \phi \Longleftrightarrow pq \equiv 1, 5, 9(mod\ 16)$$

$$C'_{-1}(\mathbb{Q}_p) \neq \phi \Longleftrightarrow p \equiv 1(mod\ 4).$$

$$C'_{-1}(\mathbb{Q}_q) \neq \phi \Longleftrightarrow q \equiv 1(mod\ 4).$$

For $d = p$ we have:

$$C'_p(\mathbb{Q}_2) \neq \phi \Longleftrightarrow [p - q \equiv 0, 4(mod\ 16)\ or\ p \equiv 1(mod\ 8)\ or\ q \equiv 7(mod\ 8)]$$

$$C'_p(\mathbb{Q}_q) \neq \phi \Longleftrightarrow (\tfrac{p}{q}) = 1,$$

$$C'_p(\mathbb{Q}_p) \neq \phi \Longleftrightarrow (\tfrac{-q}{p}) = 1.$$

For $d = q$, similar to case $d = p$ we get the desired result.
Since $-pq \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$ we conclude that

$$p \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}) \Longleftrightarrow -q \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}),$$

$$-p \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}) \Longleftrightarrow q \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q})$$

$$pq \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}) \Longleftrightarrow -1 \in S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}).$$

This completes the proof. □

Theorem 2.3. *We have the following facts about the rank of $E_{pq}(\mathbb{Q})$:*
(i) $rank(E_{pq}(\mathbb{Q})) \leq 4$.
(ii) *If* $(p, q) \equiv (3, 11), (3, 15) \ (mod\ 16)$ *and* $(\frac{q}{p}) = 1$, *then* $rank(E_{pq}(\mathbb{Q})) = 0$.
(iii) *If* $(p, q) \equiv (1, 3), (1, 11), (3, 9), (3, 11), (5, 7), (5, 9), (5, 15), (7, 13), (9, 11), (13, 15)$ $(mod\ 48)$ *and* $(\frac{q}{p}) = -1$, *then* $rank(E_{pq}(\mathbb{Q})) = 0$.

3. Calculation of the Root Number

In this section, we first recall the concept of the root number and then use Parity conjecture to refine our result 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 $a_p = p + 1 - n_p$. The local part of the L-series of E at p is defined as

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

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

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

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[12]

Proposition 3.3. *Let l be any prime of $\mathbb{Q}$. 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 $l = 3$ (resp.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 Weierestrass form, $\epsilon_l(E)$ can be read from table II of* [6].

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_{pq} in the family, we have $\Delta_{E_{pq}} = 2^6 \times p^3 \times q^3$. In particular, $y^2 = x^3 - pqx$ is in global minimal Weierstrass form. In this case the reduction of E_{pq} is additive, potentially good at 2,p and q, and good at all other primes.

Proposition 3.5. *For elliptic curve $E_{pq} : y^2 = x^3 - pqx$, we have*

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

Proof. Let $\epsilon_l(E_{pq})$ denote the local root number at l. Therefore from proposition 3.3 and above discussion, we have

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

and

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

and, finally

$$\epsilon_q(E_{pq}) = (\tfrac{-2}{q}) = \begin{cases} +1 & \text{if } q \equiv 1, 3 \ (mod\ 8) \\ -1 & \text{if } q \equiv 5, 7 \ (mod\ 8) \end{cases}$$

The assertion now follows. □

Remark 3.6. If the parity conjecture holds true in the family, then

(1) If $(p,q) \equiv (5,7),(5,15),(7,11),(13,15) \pmod{16}$ and $(\frac{q}{p}) = 1$, then $\mathrm{rank}(E_{pq}(\mathbb{Q})) = 0$.
(2) If $(p,q) \equiv (1,13),(7,11),(15,15) \pmod{16}$ and $(\frac{q}{p}) = -1$, then $\mathrm{rank}(E_{pq}(\mathbb{Q})) = 0$.
(3) If $pq \equiv 5,7,9,15$ $(mod\ 16)$, then $rank(E_{pq}(\mathbb{Q})) > 0$.

4. Infinite Family with Non-zero Rank

Now, following [9, 15] we try to find elliptic curves with maximal rank in the family. Using the homomorphism

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

which is defined by

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

we have the following exact sequence

$$0 \longrightarrow \hat{\varphi}(E'_{pq}(\mathbb{Q})) \longrightarrow E_{pq}(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$$

as well as the corresponding result for the dual isogeny:

$$0 \longrightarrow \varphi(E_{pq}(\mathbb{Q})) \longrightarrow E'_{pq}(\mathbb{Q}) \xrightarrow{\beta} \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}.$$

So $im\alpha \simeq \dfrac{E_{pq}(\mathbb{Q})}{\hat{\varphi}(E'_{pq}(\mathbb{Q}))}$ and $im\beta \simeq \dfrac{E'_{pq}(\mathbb{Q})}{\varphi(E_{pq}(\mathbb{Q}))}$. As mentioned in [9], The images of α and β can be described as follows: $WC(E'_{pq}/\mathbb{Q}) := im\alpha$ consists of all classes $b_1\mathbb{Q}^{\times 2}$, where b_1 is a squarefree integer such that

$$N^2 = b_1M^4 + b_2e^4, \qquad b_1b_2 = -pq \tag{4.1}$$

has a nontrivial solution $N, M, e \in \mathbb{N}$ with $(M,e) = (N,e) = 1$. The equation (4.1) is called a torsor of $E/\mathbb{Q}$ and is denoted by $\mathcal{T}^{(\hat{\varphi})}(b_1)$. Similarly, $WC(E_{pq}/\mathbb{Q}) := im\beta$ consists of all classes $b_1\mathbb{Q}^{\times 2}$, where b_1 is a squarefree integer such that

$$\mathcal{T}^{(\varphi)}(b_1) : N^2 = b_1M^4 + b_2e^4, \qquad b_1b_2 = 4pq \tag{4.2}$$

has a nontrivial solution in integers $N, M, e \in \mathbb{N}$. It is easy to see that every rational point $P \neq \mathcal{O}$ on E_{pq} 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 $(b_1M^2/e^2, b_1MN/e^3)$ is a rational point on E. Finally we have the following exact sequences

$$0 \to WC(E_{pq}/\mathbb{Q}) \to S^{(\varphi)}(E_{pq}/\mathbb{Q}) \to Ш(E_{pq}/\mathbb{Q})[\varphi] \to 0, \tag{4.3}$$

$$0 \to WC(E'_{pq}/\mathbb{Q}) \to S^{(\hat{\varphi})}(E'_{pq}/\mathbb{Q}) \to Ш(E'_{pq}/\mathbb{Q})[\hat{\varphi}] \to 0. \tag{4.4}$$

Proposition 4.1. *If* $p = 1 + 4x_1^2 + b^4 - 2b^2$ *and* $q = p + 4b^2$, *then* $rank(E_{pq}(\mathbb{Q})) \geq 2$.

Proof. First we see that $q - p = 4b^2$, thus $(M, N, e) = (1, 1, 2b)$ is a solution of $\mathcal{T}^{(\hat{\varphi})}(q)$so $q \in WC(E'_{pq}/\mathbb{Q})$, thus $\{1, -pq, q, -p\} \subseteq WC(E'_{pq}/\mathbb{Q})$. On the other hand $pq-(2x_1b)^4 = (1+4x_1^4-b^4)^2$, which implies that $pq \in WC(E'_{pq}/\mathbb{Q})$. From these we get $WC(E'_{pq}/\mathbb{Q}) = \{1, -pq, q, -p, pq, -1, -q, p\}$. Now our assertion follows from 2.1 and (4.4). □

Corollary 4.2. *If* $p = (5 + b^4) - 2b^2$ *and* $q = p + 4b^2$, *then* $r_{p,q} = 3$.

Proof. The last proposition with $x_1 = 1$ implies that

$$WC(E'_{pq}/\mathbb{Q}) = \{1, -pq, q, -p, pq, -1, -q, p\}.$$

Now if we let $x = b + 1$, then $4p + qx^4 = (p + 2bx^2)^2$. Therefore $(M, N, e) = (1, x, p + 2bx^2)$ is a solution of $\mathcal{T}^{(\varphi)}(4p)$ so $4p \in WC(E_{pq}/\mathbb{Q})$, thus $\{1, pq, p, q\} \subseteq WC(E_{pq}/\mathbb{Q})$. □

Corollary 4.3. *Under the assumption of proposition 4.1, if* $1 + 4x_1^2 + b^4$ *is a square, then* $r_{p,q} \geq 3$.

Proof. From the proposition, we know that

$$WC(E'_{pq}/\mathbb{Q}) = \{1, -pq, q, -p, pq, -1, -q, p\}.$$

Now if there exists y such that $1 + 4x_1^2 + b^4 = y^2$, then $p + q = 2y^2$ therefore $(M, N, e) = (1, 1, 2y)$ is a solution of $\mathcal{T}^{(\varphi)}(p)$ so $p \in WC(E_{pq}/\mathbb{Q})$, thus $\{1, pq, 2p, 2q\} \subseteq WC(E_{pq}/\mathbb{Q})$. □

Corollary 4.4. *If* $p = (1 + 8b_1^4)^2 - 8b_1^2$ *and* $q = p + 16b_1^2$, *then* $r_{p,q} = 4$.

Proof. By letting $x_1 = 2b_1^2$ and $b = 2b_1$ in corollary 4.3, we get $WC(E'_{pq}/\mathbb{Q}) = \{1, -pq, q, -p, pq, -1, -q, p\}$ and $\{1, pq, 2p, 2q\} \subseteq WC(E_{pq}/\mathbb{Q})$. On the other hand, we have $4p(2b_1^2)^4 + q(1 + 2b_1)^4 = (2(2b_1^2)^4 + \frac{(1+2b_1)^4+p}{2})^2$, therefore $(M, N, e) = (2b_1^2, 1 + 2b_1, 2(2b_1^2)^4 + \frac{(1+2b_1)^4+p}{2})$ is a solution of $\mathcal{T}^{(\varphi)}(4p)$ so $p \in WC(E_{pq}/\mathbb{Q})$, thus $\{1, pq, 2p, 2q, p, 2, q, 2pq\} \subseteq WC(E_{pq}/\mathbb{Q})$, and the rank is maximal. □

The following conjecture due to Schinzel and Sierpinski [13] implies that there exist infinitely many such primes.

Conjecture 4.5. *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 $f(x) = 64x^8+16x^4-8x^2+1$ and $g(x) = 64x^8+16x^4+8x^2+1$ satisfy the assumption of the conjecture with $m = 2$. So there exist infinitely many positive integers l, such that $f(l)$ and $g(l)$ are prime numbers. So there exist infinitely many elliptic curves $y^2 = x^3-pqx$ with rank four. The following table gives some values for b_1 with $p = (1+8b_1^4)^2 - 8b_1^2$ and $q = (1+8b_1^4)^2+8b_1^2$ prime, which results in E_{pq} of rank exactly four.

Table 1

b_1	p	q
1	73	89
16	274878953473	274878957569
82	130825015677259489	130825015677367073
89	251941684568745673	251941684568872409
137	7942267523567796169	7942267523568096473
292	3382538789388030027649	3382538789388031391873
337	10646802084655597975369	10646802084655599792473
374	24499250121921170415073	24499250121921172653089
409	50114850374836220150473	50114850374836222826969
649	2014362131305403061936073	2014362131305403068675289
718	4520386069891056038654689	4520386069891056046903073
748	6271808031136689174004609	6271808031136689182956673
761	7198752264425208374121673	7198752264425208383387609
853	17937925803933572266971529	17937925803933572278613273

Acknowledgments

The authors would like to thank the anonymous referees for their useful comments and suggestions.

References

1. S. Abraham, S. Sanyal, M. Sanglikar, Finding numerical solutions of diophantine equations using ant colony optimization, *Applied Mathematics and Computation*, **219**(24), (2013), 11376-11387.
2. M. Bahramian, H. Daghgigh, A Generalized Fibonacci Sequence and the Diophantine Equations $x^2 \pm kxy - y^2 \pm x = 0$, *Iranian Journal of Mathematical Sciences and Informatics*, **8**(2), (2013), 111-121.
3. J. W. S. Cassels, The rational solutions of the diophantine equation, *Acta Mathematica*, **82**(1), (1950), 243-273.

4. H. Daghigh, S. Didari, On the elliptic curves of the form $y^2 = x^3 - 3px$, *Bull. Iranian Math. Soc.*, **40**(5), (2014), 1119- 1133.
5. T. Goto, *A study on the Selmer Groups of the Elliptic Curves with a Rational 2-Torsion*, Doctoral Thesis, Kyushu Univ., 2002.
6. E. Halberstadt, Signes Locaux des Courbes Elliptiques en 2 et 3, *C.R. Acad. Sci. Paris, Ser. I Math*, **326**, (1998), 1047-1052.
7. V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Sha(E, \mathbb{Q})$ for a Subclass of Weil Curves, *Izv. Ackad. Nauk SSSR ser. Mat.*, **52**(3), (1998), 522-540. (English translation: *Math. USSR, Izvestiya*, **32**, (1989).)
8. F. Lemmermeyer, R. Mollin, On Tate-Shafarevich Groups of $y^2 = x(x^2 - k^2)$, *Acta Math*, **72**, (2003), 73-80.
9. F. Lemmermeyer, On Tate-Shafarevich Groups of Some Elliptic Curves, *Algebraic Number Theory and Diophantine Analysis.*, (Graz, 1998), (2000), 277-291.
10. M. Maenishi , On the Rank of Elliptic Curves $y^2 = x^3 - pqx$, *Kumamoto Journal of Mathematics*, **15**, (2002), 1-5.
11. T. Nagell, On a special class of diophantine equations of the second degree, *Arkiv för Matematik.*, **3**(1), (1954), 51-65.
12. O. G. Rizzo, Average Root Numbers for a Nonconstant Family of Elliptic Curves, *Compositio Mathematica.*, **136**(1), (2003), 1-23.
13. A. Schinzel, W. Sierpinski, Sur Certaines Hypotheses Concernant les Nombres Premiers, *Acta Arith.*, **4**, (1958), 185-208.
14. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009.
15. A. Weil, Sur Un Theoreme de Mordell, *Bull. Sci.Math.*, **54**(2), (1930), 182-191.