ISSN: 1017-060X (Print)

ISSN: 1735-8515 (Online)

Bulletin of the Iranian Mathematical Society

Vol. 42 (2016), No. 3, pp. 585–594

Title:

Complete characterization of the Mordell-Weil group of some families of elliptic curves

Author(s):

H. Daghigh and S. Didari

Published by Iranian Mathematical Society
http://bims.ims.ir

Bull. Iranian Math. Soc.
Vol. 42 (2016), No. 3, pp. 585–594
Online ISSN: 1735-8515

COMPLETE CHARACTERIZATION OF THE MORDELL-WEIL GROUP OF SOME FAMILIES OF ELLIPTIC CURVES

H. DAGHIGH* AND S. DIDARI

(Communicated by Rahim Zaare-Nahandi)

Abstract. The Mordell-Weil theorem states that the group of rational points on an elliptic curve over the rational numbers is a finitely generated abelian group. In our previous paper, H. Daghigh, and S. Didari, On the elliptic curves of the form $y^2 = x^3 - 3px$, *Bull. Iranian Math. Soc.* 40 (2014), no. 5, 1119–1133., using Selmer groups, we have shown that for a prime p the rank of elliptic curve $y^2 = x^3 - 3px$ is at most two. In this paper we go further, and using height function, we will determine the Mordell-Weil group of a family of elliptic curves of the form $y^2 = x^3 - 3nx$, and give a set of its generators under certain conditions. We will introduce an infinite family of elliptic curves with rank at least two. The full Mordell-Weil group and the generators of a family (which is expected to be infinite under the assumption of a standard conjecture) of elliptic curves with exact rank two will be described.
Keywords: Elliptic curve, Mordell-Weil group, generators, height function.
MSC(2010): Primary: 11G05; Secondary: 14H52.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and let $E(\mathbb{Q})$ be the group of rational points on E. By the Mordell-Weil theorem $E(\mathbb{Q})$ is a finitely generated abelian group, and so it can be written as

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

where $E(\mathbb{Q})_{tors}$ denotes the torsion subgroup of $E(\mathbb{Q})$. The number r is called the (algebraic) rank of E over $\mathbb{Q}$. Recently Duquesne [5] and Fujita and Terai [6, 8], found the generators of some specific families of elliptic curves. In this paper, we will prove the following result.

Article electronically published on June 29, 2016.
Received: 10 February 2014, Accepted: 7 March 2015.
*Corresponding author.

Theorem 1.1. Let n be a positive fourth-power-free odd integer. Suppose that there exist positive integers $m_1,\ n_1, m_2, n_2$ with m_1 odd and m_2 even such that

$$n = 3m_1^4 - n_1^2, \qquad n = 3m_2^4 - n_2^2. \tag{1.1}$$

Let E_{3n} be the elliptic curve $y^2 = x^3 - 3nx$. Then the following statements hold.

(1) The points $Q_1 = (3m_1^2, 3m_1n_1)$ and $Q_2 = (3m_2^2, 3m_2n_2)$ are independent points in $E_{3n}(\mathbb{Q})$ and hence $\mathrm{rank}(\mathrm{E_{3n}}(\mathbb{Q})) \geq 2$.

(2) Let $m = \max\{\mathrm{m_1, m_2}\}$. If $m^4 \leq 27n$, $3|m_1$, and $3 \nmid m_2n_2$, then $\{Q_1, Q_2\}$ is part of a system of generators for the free part of $E_{3n}(\mathbb{Q})$.

(3) For every fourth-power-free d of the form $d = 2592r^4+6048r^3+5112r^2+1848r+239$, we have that the points $Q_1 = (108r^2+108r+27, 648r^3+756r^2+252r+18)$ and $Q_2 = (108r^2+144r+48, 648r^3+1512r^2+1134r+276)$ are part of a system of generators of the free part of $E_{3d}(\mathbb{Q})$ and so $\mathrm{rank}(\mathrm{E_{3d}}(\mathbb{Q})) \geq 2$.

(4) If d in the previous part is prime, then $\mathrm{rank}(\mathrm{E_{3d}}(\mathbb{Q})) = 2$ and the given points generate the free part of $E_{3d}(\mathbb{Q})$.

Part (1) of the theorem is proved by considering the properties of the elements of $2E(\mathbb{Q})$. We define the lattice index of $\{Q_1, Q_2\}$ in section 4, and find upper bounds for the canonical heights of Q_1 and Q_2. Using these bounds and Theorem 4.1, which is one the main ingredients of the proof, we show that v, the lattice index of $\{Q_1, Q_2\}$, is less than 5. Finally using the properties of the points in $2E_{3n}(\mathbb{Q})$ and $3E_{3n}(\mathbb{Q})$ we show that the lattice index is indeed 1, which proves (2).

We note that under the assumption of a standard conjecture on prime values of polynomials (Conjecture 4.1), Theorem 1.1 produces an infinite family of elliptic curves of rank 2.

Notation 1.1. Throughout the paper the number n will be of the form $n = 3m_1^4 - n_1^2 = 3m_2^4 - n_2^2$, $Q_1 = (3m_1^2, 3m_1n_1)$, $Q_2 = (3m_2^2, 3m_2n_2)$, and $m = \max\{\mathrm{m_1, m_2}\}$.

For computing $E_{tors}(\mathbb{Q})$ in our family, we use the following fact from [14, p. 347].

Lemma 1.2. Let D be a fourth-power free integer, and E_D be the elliptic curve

$$E_D : y^2 = x^3 + Dx.$$

Then

$$E_{tors}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } D{=}4 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } {-D} \text{ is a perfect square} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

2. Estimating the canonical height

Let $E: y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve with integer coefficients, and let $P \in E(\mathbb{Q})$. By [15, P. 68], $P = (x, y) = (\frac{a}{d^2}, \frac{b}{d^3})$, where a, b and d are integers and $\gcd(\mathrm{a}, \mathrm{d}) = \gcd(\mathrm{b}, \mathrm{d}) = 1$. We define the naive height of P by $h(P) = \max\{\log|\mathrm{a}|, \log|\mathrm{d}^2|\}$ and the canonical height of P by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}.$$

As mentioned in [16, Chapter VI], the value $\hat{h}(P)$ can be expressed as

$$\hat{h}(P) = \sum_{p\ prime} \hat{\lambda}_p(P) + \hat{\lambda}_\infty(P),$$

where $\hat{\lambda}_p(P)$ is the local height at prime p and $\hat{\lambda}_\infty(P)$ is the local height at infinity. Let

$$\hat{h}_{fin}(P) = \textstyle\sum_{p\ prime} \hat{\lambda}_p(P).$$

To estimate the canonical height of desired points, we need the following lemmas.

Lemma 2.1. ([7, lemma 3.2]) Let n be a positive fourth-power-free integer and E_n be the elliptic curve given by $y^2 = x^3 - nx$. For every $P = (a/d^2, b/d^3)$, $\hat{h}_{fin}(P)$ can be computed as

$$\hat{h}_{fin}(P) = 2\log d - \frac{1}{2}\log(\prod_{p|(a,n), p\neq 2} p^{e_p}) + \hat{h}_2(P),$$

where $p^{e_p}||n$ and $\hat{h}_2(P)$ is a real number satisfying $-(7\log 2)/4 \le \hat{h}_2(P) \le 0$.

Remark 2.2. To compute the exact value of $\hat{h}_2(P)$, one can use Lemma 2.3 in [7].

Lemma 2.3. For any point $P \in E_n(\mathbb{Q})$, $\widehat{\lambda}_\infty(P)$ is computed using the Tate series

$$\hat{\lambda}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{k=0}^{\infty} \frac{c_k}{4^k},$$

where $c_k = \log|z(2^kP)|$ and $z(Q) = (1 + n/x(Q)^2)^2$ for $Q \in E_n(\mathbb{Q}) \setminus \{(0, 0)\}$.

Proof. This follows from Cohen's formula [2, Algorithm 7.5.7]. □

Remark 2.4. For any non-torsion point $P \in E_n(\mathbb{Q})$, we have $2^kP \in E_n^0(\mathbb{R})$, where $E_n^0(\mathbb{R})$ denotes the identity component of $E_n(\mathbb{R})$, and $x(2^kP) \ge \sqrt{n}$ for all positive integers k. Therefore the series in Lemma 2.3 converges.

Next lemma determines a lower bound on the canonical height of points in $E_{3n}(\mathbb{Q})$.

Lemma 2.5. ([7, Proposition 3.3]) Let n be a positive fourth-power-free integer and E_n be the elliptic curve $y^2 = x^3 - nx$. If $n \not\equiv 12 \pmod{16}$, then $\hat{h}(P) > 0.125 \log n + 0.3917$ for any non-torsion point $P \in E_n(\mathbb{Q})$.

Next lemma will be used to bound the lattice index of $\{Q_1, Q_2\}$.

Lemma 2.6. For $i = 1, 2$, we have

$$\hat{h}(Q_i) \leq 0.45 + 2 \log m_i.$$

Proof. By Lemma 2.3, we have

$$\hat{\lambda}_\infty(Q_i) = \log 3m_i^2 + \tfrac{1}{4} \textstyle\sum_{k=0}^{\infty} \frac{c_k}{4^k}.$$

On the other hand by Remark 2.4, we have $c_k \leq \log 4$. Therefore

$$\hat{\lambda}_\infty(Q_i) \leq \log 3m_i^2 + \frac{1}{4} \sum_{k=0}^{\infty} \frac{\log 4}{4^k}.$$

Hence

$$\hat{\lambda}_\infty(Q_i) \leq \log 3m_i^2 + \frac{2}{3} \log 2.$$

On the other hand

$$\hat{h}_{fin}(Q_i) = \frac{-1}{2} \log 3 + \hat{h}_2(Q_i),$$

where

$$\frac{-7 \log 2}{4} \leq \hat{h}_2(Q_i) \leq 0.$$

Therefore

$$\hat{h}(Q_i) \leq \frac{1}{2} \log 3 + \frac{2}{3} \log 2 + 2 \log m_i < 0.45 + 2 \log m_i.$$

□

3. Independence of the points

In this section we prove the independence of the points Q_1 and Q_2. We then prove that none of the point $Q_1, Q_2, Q_1 + Q_2, Q_1 - Q_2$ is in $3E_{3n}(\mathbb{Q})$. These results will be used in the next section to prove that Q_1 and Q_2 are in fact part of a set of generators of the free part of $E(\mathbb{Q})$.

Lemma 3.1. ([11, p. 85]) Let E_{3n} be the elliptic curve $y^2 = x^3 - 3nx$. If $P \in 2E_{3n}(\mathbb{Q})$ then $x(P)$ is a rational square and $x(P) + \sqrt{3n}$ is a square in $\mathbb{Q}(\sqrt{3n})$.

Lemma 3.2. If $P = (u^2/s^2, v/s^3) \in E_{3n}(\mathbb{Q})$ and $2 \nmid s$. Then $P \notin 2E_{3n}(\mathbb{Q})$.

Proof. Suppose that $P \in 2E_{3n}(\mathbb{Q})$. Then from the previous lemma, $(u^2/s^2) + \sqrt{3n}$ is a square in $\mathbb{Q}(\sqrt{3n})$. So there exist $A, B \in \mathbb{Q}$ such that

$$u^2 + s^2\sqrt{3n} = (A^2 + 3nB^2) + 2AB\sqrt{3n}.$$

From this equation we can see that A, B are integers. Now s^2 must be even, which contradicts the assumption. Hence $P \notin 2E_{3n}(\mathbb{Q})$. □

Lemma 3.3. Q_1 and Q_2 are independent modulo $E_{3n}(\mathbb{Q})_{tors}$.

Proof. By Lemma 1.2, $E_{3n}(\mathbb{Q})_{tors} = \{\mathcal{O}, T\}$, where $T = (0, 0)$. From the previous lemma we have $Q_1, Q_2 \notin 2E(\mathbb{Q})$. On the other hand

$$x(Q_1 + Q_2) = (m_1n_2 - m_2n_2)^2/(m_2^2 - m_1^2)^2.$$

If m_2 is even and m_1 is odd then

$$2 \nmid (m_2^2 - m_1^2)^2.$$

Therefore from the previous lemma we have $Q_1 + Q_2 \notin 2E_{3n}(\mathbb{Q})$. On the other hand $Q_1 + T$, $Q_2 + T$, and $Q_1 + Q_2 + T \in E^0_{3n}(\mathbb{Q})$, so $Q_1 + T$, $Q_2 + T$, and $Q_1 + Q_2 + T \notin 2E_{3n}(\mathbb{Q})$. Hence Q_1 and Q_2 are independent modulo $E_{3n}(\mathbb{Q})_{tors}$. □

Lemma 3.4. If $\log m_1^2 < 1.125 \log 3n + 3.0753$, then $Q_1 \notin 3E_{3n}(\mathbb{Q})$.

Proof. Suppose that there exists $R \in E_{3n}(\mathbb{Q})$ such that $Q_1 = 3R$. Then using Lemma 2.6 we have

$$9\hat{h}(R) = \hat{h}(3R) = \hat{h}(Q_1) \leq 0.45 + 2 \log m_1.$$

On the other hand Lemma 2.5 implies that

$$9\hat{h}(R) \geq 9(0.125 \log 3n + 0.3917).$$

Hence

$$9(0.125 \log 3n + 0.3917) \leq 0.45 + 2 \log m_1 < 0.45 + 1.125 \log 3n + 3.0753,$$

which is a contradiction. □

Lemma 3.5. Suppose that $P = (u/s^2, v/s^3) \in 3E_{3n}(\mathbb{Q})$. We have

(1) If $3|u$ then $\mathrm{ord}_3(\mathrm{u}) \geq 3$.
(2) If $3 \nmid u$ then $\mathrm{ord}_3(\mathrm{s}) \geq 1$.

Proof. (1) Let $R = (w/t^2, z/t^3) \in E_{3n}(\mathbb{Q})$ and $P = 3R$. Then

$$\begin{aligned} u/s^2 =& (-236196t^{24}w^9n^9 + 472392t^{20}w^{11}n^8 - 393660t^{16}w^{13}n^7 + 174960t^{12}w^{15}n^6 \\ &- 43740t^8w^{17}n^5 + (5832t^4w^{19} + 729t^{16}w)n^4 + (-324w^{21} - 648t^{12}w^3)n^3 \\ &+ 270t^8w^5n^2 + 36t^4w^7n + w^9)/(3tw^4 - 18t^5w^2n - 9t^9n^2)^2. \end{aligned}$$

Hence

$$\begin{aligned} u(3tw^4 - 18t^5w^2n - 9t^9n^2)^2 =& s^2(-236196t^{24}w^9n^9 + 472392t^{20}w^{11}n^8 - 393660t^{16}w^{13}n^7 \\ &+ 174960t^{12}w^{15}n^6 - 43740t^8w^{17}n^5 + (5832t^4w^{19} + 729t^{16}w)n^4 \\ &+ (-324w^{21} - 648t^{12}w^3)n^3 + 270t^8w^5n^2 + 36t^4w^7n + w^9). \end{aligned}$$

Since $3|u$, $3 \nmid s$, considering the above equation modulo 3, we have $3|w$, and hence $3 \nmid t$. Therefore
$\mathrm{ord_3(u)+4 \geq ord_3(-3^4 \times 2^3 w^3 t^{12} n^3 + 3^6 t^{16} wn^4 + 3^3 \times 5 \times 2t^8 w^5 n^2 + 3^2 \times 2^2 w^7 n + w^9)}$.
Let $w = 3w_1$, we have

$$\mathrm{ord_3(u) + 4 \geq 7 + ord_3(w_1)},$$

and therefore $\mathrm{ord_3(u) \geq 3}$.

(2) Suppose that there exists $R \in E_{3n}(\mathbb{Q})$ such that $P = 3R$. Then $P+T = 3(R+T)$, and so $P+T \in 3E_{3n}(\mathbb{Q})$. On the other hand $x(P+T) = -3ns^2/u$. Now using the previous part we have $\mathrm{ord_3(-3ns^2) \geq 3}$, and therefore $\mathrm{ord_3(s) \geq 1}$.

□

Lemma 3.6. None of the points Q_2, Q_1+Q_2, Q_1-Q_2 is in $3E_{3n}(\mathbb{Q})$.

Proof. This follows from Lemma 3.5 □

4. Proof of the main theorem

Let E be an elliptic curve of rank $r(\geq 2)$ defined over a number field K. Let $Q_1, Q_2, \ldots, Q_s$ $(s \leq r)$ be independent points in $E(K)$. By [13, Theorem 3.1], there exist generators $G_1, G_2, \ldots, G_s$ of the free part of $E(K)$ such that $Q_1, Q_2, \ldots, Q_s \in \mathbb{Z}G_1 + \mathbb{Z}G_2 + \ldots + \mathbb{Z}G_s$. The index of the subgroup $\mathbb{Z}Q_1 + \mathbb{Z}Q_2 + \ldots + \mathbb{Z}Q_s$ in $\mathbb{Z}G_1 + \mathbb{Z}G_2 + \ldots + \mathbb{Z}G_s$ is called the lattice index of $\{Q_1, Q_2, \ldots, Q_s\}$.

For every points P and Q in $E(\mathbb{Q})$,

$$\langle P, Q\rangle = \tfrac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$$

denotes the scalar product associated to $\hat{h}$. If $P_1, P_2, \ldots, P_t$ are t points in the free part of $E(\mathbb{Q})$, then the elliptic regulator of $P_1, P_2, \ldots, P_t$ is defined as

$$R(P_1, P_2, \ldots, P_t) = \mathrm{det(\langle P_i, P_j\rangle)_{1\leq i,j\leq t}}.$$

The following theorem gives an upper bound for the lattice index.

Theorem 4.1. ([13, Theorem 3.1]) Let E be an elliptic curve of rank $(r \geq 2)$ defined over a number field K. Let $Q_1, Q_2, \ldots, Q_s$ $(s \leq r)$ be independent points in $E(K)$ and v be the lattice index of $\{Q_1, Q_2, \ldots, Q_s\}$. Suppose that $\lambda > 0$ is a constant such that any point $P \in E(K)$ of infinite order satisfies $\hat{h}(P) > \lambda$. Then

$$v \leq R(Q_1, Q_2, \ldots, Q_s)^{1/2}(\gamma_s/\lambda)^{s/2},$$

where γ_is are the *Hermite constants* [10, p. 372], and the exact value of γ_n is known only for $1 \leq n \leq 8$ and for $n = 24$:

$$\gamma_1 = 1,\ \gamma_2^2 = \tfrac{4}{3},\ \gamma_3^3 = 2,\ \gamma_4^4 = 4,\ \gamma_5^5 = 8,\ \gamma_6^6 = \tfrac{64}{3},\ \gamma_7^7 = 64,\ \gamma_8^8 = 256,$$

and $\gamma_{24} = 4$.

As we saw in Lemma 3.3, the points Q_1 and Q_2 are independent. Let v be the lattice index of $\{Q_1, Q_2\}$. To prove that the set $\{Q_1, Q_2\}$ is a set of generators for $E_{3n}(\mathbb{Q})$, it suffices to show that $v = 1$. In the next lemma we will find an upper bound for v.

Lemma 4.2. Let $3n$ be a positive fourth-power-free integer. If $n \not\equiv 4 \pmod{16}$ and $4\log m \leq \log 3n + 2.49$ then $v < 5$.

Proof. Since

$$R(Q_1, Q_2) = \hat{h}(Q_1)\hat{h}(Q_2) - \tfrac{1}{4}\{\hat{h}(Q_1 + Q_2) - \hat{h}(Q_1) - \hat{Q_2}\}^2,$$

by Theorem 4.1 and Lemma 2.5 we have

$$v^2 \leq \frac{4R(Q_1, Q_2)}{3(0.125\log 3n + 0.3917)^2} \leq \frac{4\hat{h}(Q_1)\hat{h}(Q_2)}{3(0.125\log 3n + 0.3917)^2}. \tag{4.1}$$

Now by Lemma 2.6,

$$v^2 \leq \frac{4\hat{h}(Q_1)\hat{h}(Q_2)}{3(0.125\log 3n + 0.3917)^2} \leq \frac{4(0.45 + 2\log m_1)(0.45 + 2\log m_2)}{3(0.125\log 3n + 0.3917)^2}. \tag{4.2}$$

Let $m = \max\{\mathrm{m_1}, \mathrm{m_2}\}$. If $4\log m \leq \log 3n + 2.23$, then

$$2\log m + 0.45 \leq 4(0.125\log 3n + 0.3917). \tag{4.3}$$

Therefore (4.2) implies that

$$v^2 \leq \frac{4 \times 16(0.125\log 3n + 0.3917)^2}{3(0.125\log 3n + 0.3917)^2} < 25. \tag{4.4}$$

□

Now we can prove our main theorem.

Proof of Theorem1.1.

Proof. (1) This follow from Lemma 3.3.

(2) Let $\{G_1, G_2\}$ be part of a set of generators for E, with $Q_1, Q_2 \in \mathbb{Z}G_1 + \mathbb{Z}G_2$ then there exists a matrix $M \in M_{2\times 2}(\mathbb{Z})$ such that

$$\begin{bmatrix} Q_1 \\ Q_2 \end{bmatrix} = M \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}.$$

Note that the lattice index of $\{Q_1, Q_2\}$ is $|\mathrm{det(M)}|$. For any rational prime p, we have

$$\begin{bmatrix} Q_1 \\ Q_2 \end{bmatrix} \equiv \overline{M} \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \pmod{\mathrm{pE_{3n}}(\mathbb{Q})},$$

where $\overline{M}$ is the image of M in $M_2(\mathbb{Z}/p\mathbb{Z})$. If $p|\mathrm{det(M)}$ then there exists a matrix $A \in M_{2\times 2}(\mathbb{Z}/p\mathbb{Z})$ such that $A\overline{M}$ has a zero row. So if $p|v$ then there exist $k_1, k_2 \in \mathbb{Z}/p\mathbb{Z}$ such that $k_1Q_1 + k_2Q_2 \in pE_{3n}(\mathbb{Q})$. From Propositions 3.3, 3.4 and 3.6, we know in the case $p = 2$ or $p = 3$

there is no such k_1 and k_2. Hence $2 \nmid v$ and $3 \nmid v$. On the other hand $v < 5$ and therefore $v = 1$.

(3) For every $r_1, r_2 \in \mathbb{Z}$ we have

$$3(3r_1)^4 - (18r_1^2 - r_2^2)^2 = 3r_2^4 - (2r_2^2 - 9r_1^2)^2.$$

Let r be a nonzero integer and $r_1 = 2r + 1$, $r_2 = 3r_1 + 1$ and $n = 3(3r_1)^4 - (18r_1^2 - r_2^2)^2 = 2592r^4 + 6048r^3 + 5112r^2 + 1848r + 239$. Then r_1 is odd, r_2 is even, and we can easily check that for every $r \in \mathbb{N} \cup \{0\}$,

$$27(2592r^4 + 6048r^3 + 5112r^2 + 1848r + 239) - (3(2r + 1) + 1)^4 > 0.$$

Therefore every fourth-power-free n of the form $2592r^4 + 6048r^3 + 5112r^2 + 1848r + 239$ satisfies the conditions, in (2). This proves (3).

(4) This follows from (3) and the next theorem.

□

In our previous paper [4], we have proved the following theorem.

Theorem 4.3. Let p be a prime number such that there exist $m_1, n_1 \in \mathbb{Z}$ such that $p = 3m_1^4 - n_1^2$. Let E_{3p} be the elliptic curve $y^2 = x^3 - 3px$. Then $\mathrm{rank}(\mathrm{E_{3p}}(\mathbb{Q})) \leq 2$.

Indeed, we have a more precise statement:

Corollary 4.1. Let p be a prime number. Suppose that there exist positive integers m_1, n_1, m_2, n_2 with m_1 odd and m_2 even such that

$$p = 3m_1^4 - n_1^2, \qquad p = 3m_2^4 - n_2^2.$$

Let E_{3p} be the elliptic curve $y^2 = x^3 - 3px$. Then $\mathrm{rank}(\mathrm{E_{3p}}(\mathbb{Q})) = 2$ and points $Q_1 = (3m_1^2, 3m_1n_1)$ and $Q_2 = (3m_2^2, 3m_2n_2)$ are independent points. Moreover if $m^4 \leq 27p$, $3|m_1$ and $3 \nmid m_2n_2$ then $\{Q_1, Q_2\}$ is a system of generators for $E_{3p}(\mathbb{Q})$.

Proof. This follows from part (1) in Theorem 1.1 and Theorem 4.3. □

Remark 4.4. In 1922 Nagell [12] proved that for a natural number k, every irreducible polynomial f of degree $d \leq k$ assumes infinitely many kth-power-free values. Thus $f(x) = 2592x^4 + 6048x^3 + 5112x^2 + 1848x + 239$ assumes infinitely many fourth-power-free values. Hence there exist infinitely many n which satisfies part (3) of Theorem 1.1.

Example 4.1. Let $n = 15839 = 3 \times 9^4 - 62^2 = 3 \times 10^4 - 119^2$, and $E : y^2 = x^3 - 3nx$. The points $Q_1 = (300, 3570)$ and $Q_2 = (243, 1674)$ are independent points on E. Using online package of Magma [3], we can see that rank(E) = 4.

To show that in part (4) of Theorem 1.1 there exist infinitely many prime value of d, we use the following conjecture.

Conjecture 4.1. ([1]) A necessary and sufficient condition for a polynomial $f(x) \in \mathbb{Z}[x]$ to be irreducible is that there exist infinitely many integers m such that $f(m)/N_f$ is prime, where $N_f = \mathrm{GCD}\{\mathrm{f(n)}, 1 \leq \mathrm{n} \leq \mathrm{g+1}\}$ and $g = deg\ f$.

We have

$$\begin{aligned} f(x) &= 2592x^4 + 6048x^3 + 5112x^2 + 1848x + 239 \\ &= 3(3(2x+1))^4 - (18(2x+1)^2 - (3(2x+1)+1)^2)^2 \\ &= 3(3(2x+1)+1)^4 - (2(3(2x+1)+1)^2 - 9(2x+1)^2)^2. \end{aligned}$$

The polynomial $f(x)$ is irreducible. To see this, we first note that the equality $3y^4 - z^2 = 0$ is impossible modulo 4, and hence $f(x)$ has no integer roots. On the other hand, if

$$f(x) = (ax^2 + bx \pm 1)(dx^2 + ex \pm 239), \tag{4.5}$$

we will have

$$\begin{cases} \pm 239b \pm e = 1848 \\ \pm 239a \pm d + be = 5112 \\ ae + bd = 6048 \\ ad = 2592. \end{cases}$$

Considering this system of equations modulo powers of 2, we can see that the system has no integer solutions. Therefore the factorization(4.5) is impossible. Hence $f(x)$ is irreducible. Thus the above conjecture predicts the existence of infinitely many positive integers r, such that $f(r)$ is a prime number. Some examples of such primes are 239, 425039, 4860959,.... Table 1 gives a list of primes p in the desired form and the generators of the elliptic curve $y^2 = x^3 - 3px$

Table 1.

r	$p = f(r)$	Q_1	Q_2
0	239	[27, 18]	[48, 276]
3	425039	[1323, 25074]	[1452, 34782]
6	4860959	[4563, 168714]	[4800, 201480]
9	21846047	[9747, 535914]	[10092, 605346]
11	46638479	[14283, 956754]	[14700, 1058190]
14	117198047	[22707, 1929834]	[23232, 2090616]
15	152810159	[25947, 2360898]	[26508, 2544486]
621	386929964541119	[41716323, 155476724634]	[41738700, 155768817210]
623	391933978780079	[41985243, 156982812354]	[42007692, 157276787622]
632	415055242121519	[43206075, 163880631090]	[43228848, 164183153316]
644	447456903156047	[44861067, 173388012354]	[44884272, 173702121036]
655	478791623202479	[46405467, 182419878978]	[46429068, 182744799846]
663	502593430360559	[47545083, 189181873314]	[47568972, 189514772502]
664	505629858048047	[47688507, 190038688434]	[47712432, 190372591716]
669	521018890986047	[48408867, 194361588954]	[48432972, 194700535386]
9209	18646396922899206047	[9160008147, 506136249996714]	[9160339692, 506200371214146]
9230	18817052067570298079	[9201830067, 509606550774378]	[9202162368, 509670964747896]
9235	18857856307302144719	[9211801707, 510435144220338]	[9212134188, 510499627995966]
9237	18874196570501260799	[9215791875, 510766832921850]	[9216124428, 510831344628906]
9243	18923281079193672719	[9227767563, 511762761110034]	[9228100332, 511827356647662]
9244	18931471129046076047	[9229764267, 511928874902754]	[9230097072, 511993484417436]
9250	18980667270912594239	[9241749027, 512926312581018]	[9242082048, 512991005989776]
9264	19095831117581448047	[9269743707, 515258703786834]	[9270077232, 515323593160116]

Acknowledgments

We would like to thank Professor Henri Darmon for reading an initial version of this paper and for his interest in our work and useful advices. We are also indebted to the referee whose careful reading and valuable comments helped us to make the paper more readable. This research was in part supported by the University of Kashan under grant number 159037/1.

References

[1] V. Bouniakowski, Sur les diviseurs numeriques invariables des functions rationelles entieres, *Mem. Acad. Sci. St. Petersburg* **6** (1857) 305–309.

[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.

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

[4] H. Daghigh, and S. Didari, On the elliptic curves of the form $y^2 = x^3 - 3px$, *Bull. Iranian Math. Soc.* **40** (2014), no. 5, 1119–1133.

[5] S. Duquesne, Elliptic curves associated with simplest quartic fields, *J. Théor. Nombres Bordeaux* **19** (2007), no. 1, 81–100.

[6] Y. Fujita and T. Nara, On the Mordell-Weil group of the elliptic curve $y^2 = x^3 + n$, *J. Number Theory* **132** (2012), no. 3, 448–466.

[7] Y. Fujita, N. Terai, Generators for the elliptic curve $y^2 = x^3 - nx$, *J. Théor. Nombres Bordeaux* **23** (2011), no. 2, 403–416.

[8] Y. Fujita, Generators for the elliptic curve $y^2 = x^3 - nx$ of rank at least three, *J. Number Theory* **133** (2013), no. 5, 1645–1662.

[9] C. Hooley, On the power-free values of polynomials in two variables, Analytic number theory, 235–266, Cambridge University Press, Cambridge, 2009.

[10] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics), Springer, New York, 2008.

[11] A. W. Knapp, Elliptic Curves, Princeton University Press, Princeton, 1992.

[12] T. Nagell, Zur Arithmetik der polynome, *Abhandl. Math. Sem. Hamburg* **1** (1922) 179–194.

[13] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), no. 4, 1501–1538.

[14] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[15] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[16] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, 151, Springer-Verlag, New York, 1994.

[17] J.H. Silverman, Computing heights on elliptic curves, *Math. Comp.* **51** (1988), no. 183, 339–358.

[18] L. C. Washington, Elliptic curves: Number Theory and Cryptography, Chapman & Hall/CRC, Boca Raton, 2008.

(Hassan Daghigh) Faculty of Mathematical Sciences, University of Kashan, P.O. Box 8731751167, Kashan, Iran.

E-mail address: hassan@kashanu.ac.ir

(Somayeh Didari) Faculty of Mathematical Sciences, University of Kashan, P.O. Box 8731751167, Kashan, Iran.

E-mail address: didari@kashanu.ac.ir