ON THE MORDELL–WEIL GROUP OF THE ELLIPTIC CURVE $y^2 = x^3 + n$

YASUTSUGU FUJITA AND TADAHISA NARA

Abstract. We study an infinite family of Mordell curves (i.e. the elliptic curves in the form $y^2 = x^3 + n$, $n \in \mathbb{Z}$) over $\mathbb{Q}$ with three explicit integral points. We show that the points are independent in certain cases. We describe how to compute bounds of the canonical heights of the points. Using the result we show that any pair in the three points can always be a part of a basis of the free part of the Mordell–Weil group.

1. Introduction

Let E be an elliptic curve over a number field K. It is known that the set of rational points $E(K)$ is a finitely generated abelian group by the Mordell–Weil theorem. If the absolute value of the discriminant of E is not large, we can practically use Cremona's program 'mwrank'. However there is no known algorithm which determines the structure of $E(K)$ even if $K = \mathbb{Q}$. The difficulties come from the free part of the group. We are interested in the families of elliptic curves of which we can at least partially determine the structure of the Mordell–Weil group, that is, the families which have explicit points which can be in a system of generators of the Mordell–Weil group. In the paper [6], Duquesne considered an infinite family of elliptic curves in the form $y^2 = x^3 - nx$. He showed that the curves in the family have two explicit integral points which can always be in a system of generators. Recently, the first author and Terai ([7]) generalized Duquesne's theorem on generators and showed that the same is true for infinitely many binary forms $n = n(k, l)$ in $\mathbb{Z}[k, l]$. In this paper we consider an infinite family of elliptic curves in the form of $y^2 = x^3 + n$ with three explicit integral points.

Let a, b be integers and

$$E_{a,b} : y^2 = x^3 + a^6 + 16b^6 \tag{1.1}$$

the elliptic curve over $\mathbb{Q}$. We put

$$P_1 = (-a^2, 4b^3),\ P_2 = (2ab, a^3 + 4b^3),\ P_3 = (-2ab, a^3 - 4b^3). \tag{1.2}$$

Then it is easy to see that they are in $E_{a,b}(\mathbb{Q})$. In this paper we prove the following theorem.

Theorem 1.3. *Assume that a, b are relatively prime integers with $a, b \geq 3$ such that $a^6 + 16b^6$ is square-free, ab is odd and b is divisible by 3 but not by 9. Then the rank of the Mordell–Weil group $E_{a,b}(\mathbb{Q})$ is at least 3 and any pair of two points $\{P_i, P_j\}$ $(i = 1, 2, 3,\ i \neq j)$ can always be in a system of generators of $E_{a,b}(\mathbb{Q})$.*

Key words and phrases. elliptic curve, Mordell–Weil group, canonical height, Mordell curve.

Remark 1.4. If n is square-free and not equal to 1, the elliptic curve $y^2 = x^3 + n$ has no rational torsion points by [11, Theorem 5.3]. Therefore P_1, P_2, P_3 are non-torsion in the situation of Theorem 1.3.

Remark 1.5. Kihara ([9], [10]) constructed elliptic curves of higher ranks using the elliptic curve $y^2 = x^3 + k$, where

$$k = \frac{1}{4}\left(a^6 + b^6 + c^6 - 2a^3b^3 - 2b^3c^3 - 2c^3a^3\right)$$

with a, b, c variables. Our family is given by substituting $2b$ for b and $-a$ for c in this curve.

We prove Theorem 1.3 along similar lines to Duquesne's ([6]). The goal of the proof is to show that the lattice indices of $\{P_i, P_j\}$ $(i, j = 1, 2, 3,\ i \neq j)$ equal 1 (for the definition of the lattice index see Section 5). To estimate the lattice indices, we use Siksek's theorem, which comes from the theory of quadratic forms. To apply the theorem, we need upper bounds of the canonical heights of P_i's $(i = 1, 2, 3)$ and a uniform lower bound of the canonical heights independent of points. The computations of canonical heights are done through the decomposition into the sum of local heights. Whereas the non-archimedean parts of canonical heights are computed by using Siverman's algorithm, the archimedean parts are computed in two ways: using Tate's series and using Cohen's algorithm. We use the former to compute bounds of the canonical heights of P_i's $(i = 1, 2, 3)$ and the latter to compute the uniform lower bound. With the bounds given we can show that the lattice indices are less than 5. An argument of the descent shows that the lattice indices are divisible by neither 2 nor 3. This completes the proof.

There are two difficulties in our case, which are not encountered in [6] or [7]. One is that the lattice indices of $\{P_i, P_j\}$ with $i \neq j$ can be only shown to be less than 5, not 3 as in [6] and [7], even for sufficiently large a, b (note that the canonical heights of two independent points in [6] and [7] are very small, so are the lattice indices; see Section 1 in [7]). Thus, we need not only 2-descent but also 3-descent. The other is that Tate's series

$$\log|x(P)| + \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n} \log|z(2^n P)|,$$

where $z(P)$ is a polynomial over $\mathbb{Q}$ in $t = 1/x(P)$, converges away from the y-axis. In order to apply Tate's series, we thus have to shift the elliptic curve in the direction of the x-axis. Moreover, we find in our case $z(P)$ above is bounded independently of a, b and P. Thanks to this, we obtain an upper bound and a lower bound whose difference is a constant.

The organization of this paper is as follows. In Section 2 we review basic notations of elliptic curves. We also review the canonical height and the local height function. In Section 3 we compute bounds of the canonical heights of P_1, P_2, P_3. In Section 4 we compute a uniform lower bound of the canonical height. In Section 5 we estimate the lattice indices by applying Siksek's theorem to the results of Sections 3 and 4. In Section 6 we prove that the lattice indices do not vanish modulo 2 or 3 by an argument of the descent. Then we complete the proof of Theorem 1.3. Further we prove that the family of the elliptic curves satisfying the condition of Theorem 1.3

is an infinite family. Finally in Section 7 we compute the bounds of $z(P)$, which are used in Section 3.

2. Preliminaries

The standard symbols $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}$ will denote respectively the set of rational, real and complex numbers and the rational integers. We denote the discrete valuation on $\mathbb{Z}$ at the prime p by $v_p(\cdot)$. We denote the set of all places of a number field K by M_K.

Throughout this paper, we assume that $a, b \in \mathbb{Z}$, $a, b \geq 3$, $\gcd(a, b) = 1$ and $m = a^6 + 16b^6$.

As usual we write the Weierstrass equation for elliptic curves E over a number field K as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ (a_1, a_2, a_3, a_4, a_6 \in K). \tag{2.1}$$

Since the characteristic of K is not equal to 2, by completing the square of the left-hand side we have

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.2}$$

where

$$\begin{aligned} &b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\ &b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned} \tag{2.3}$$

Further, we put

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^2b_8 + 36b_2b_4 - 216b_6$$

as usual. We also define the discriminant of E as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{2.4}$$

Using the form (2.3), we can write

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} \tag{2.5}$$

for $P = (x, y) \in E$.

Next we define the canonical height, which is a powerful tool to consider the arithmetic of elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$ and $P = (x, y) \in E(\mathbb{Q})$. If $x = n/d$ and $\gcd(n, d) = 1$, we define the naïve height of P by $h(P) = \max\{\log|n|, \log|d|\}$ and the canonical height of P by

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

([6, p. 86]).

Remark 2.6. In our definition the value of $\hat{h}$ is twice of those in [14], [4] and [13].

The canonical height has the following properties.

- $\hat{h}(P) = 0$ if and only if P is a torsion point.
- $\hat{h}(kP) = k^2\hat{h}(P)$ for all $P \in E(\mathbb{Q})$ and all $k \in \mathbb{Z}$.
- $\hat{h}$ is a quadratic form on E.

For details see also [14, Chapter VIII Section 9].

Our computations of the canonical height is done by using the local height. We recall the existence of the local height function as follows.

Theorem 2.7. (*Néron, Tate,* [13, p. 341]) *Let K be a number field, v a place and K_v its completion with respect to an absolute value $|\cdot|_v$. Let E be the elliptic curve over K given by* (2.1)*. Then there exists a unique function $\hat{\lambda}_v : E(K_v) \setminus O \to \mathbb{R}$ which has the following three properties.*

(1) *For all $P \in E(K_v)$ with $2P \neq O$,*

$$\hat{\lambda}_v(2P) = 4\hat{\lambda}_v(P) - 2\log|2y(P) + a_1x(P) + a_3|_v.$$

(2) *The limit $\lim_{\substack{P \to O \\ v\text{-}adic}}(\hat{\lambda}_v(P) - \log|x(P)|_v)$ exists.*

(3) *$\hat{\lambda}_v$ is bounded on any v-adic open subset of $E(K_v)$ disjoint from O.*

The function $\hat{\lambda}_v$ above is called the *local height function*. If we have to specify the elliptic curve, we may use the notation such as $\hat{\lambda}_{E,v}$. The canonical height can be decomposed as the sum of local heights. The sum of the local heights for all archimedean (resp. non-archimedean) places is called the archimedean (resp. non-archimedean) part of the canonical height and denoted by $\hat{h}_f(P)$ (resp. $\hat{h}_\infty(P)$). We only consider the case $K = \mathbb{Q}$ and in this situation,

$$\hat{h}(P) = \hat{h}_f(P) + \hat{h}_\infty(P) = \sum_{p:\text{prime}} \hat{\lambda}_p(P) + \hat{\lambda}_\infty(P). \tag{2.8}$$

Let $d \in K$ and

$$E' : (y')^2 + a_1{}'x'y' + a_3{}'y' = (x')^3 + a_2{}'(x')^2 + a_4{}'x' + a_6{}'$$

the elliptic curve obtained by making the substitution

$$x' = x + d,\ y' = y \tag{2.9}$$

in (2.1). Then

$$\begin{aligned} &a_1{}' = a_1,\ a_2{}' = a_2 - 3d,\ a_3{}' = a_3 - da_1, \\ &a_4{}' = a_4 - 2da_2 + 3d^2,\ a_6{}' = a_6 - da_4 + d^2a_2 - d^3. \end{aligned} \tag{2.10}$$

Now let $P \in E(K_v)$ and $P' = (x(P) + d, y(P)) \in E'(K_v)$. It is clear that the map $E(K_v) \ni P \mapsto P' \in E'(K_v)$ is a group isomorphism.

Lemma 2.11. *In the situation above, we have $\hat{\lambda}_{E,v}(P) = \hat{\lambda}_{E',v}(P')$.*

Proof. To see this, it is sufficient to show that the function $f : E'(K_v) \to \mathbb{R}$ defined by $f(P') = \hat{\lambda}_{E,v}(P)$ satisfies the three properties of $\hat{\lambda}_v$ in Theorem 2.7.

The property (1) follows from the equality

$$2y' + a_1{}'x' + a_3{}' = 2y + a_1(x + d) + a_3 - da_1 = 2y + a_1x + a_3.$$

For the property (2), we have

$$\begin{aligned}\lim_{\substack{P'\to O'\\ v\text{-adic}}}\{f(P')-\log|x'(P')|_v\} &= \lim_{\substack{P\to O\\ v\text{-adic}}}\{\hat\lambda_{E,v}(P)-\log|x(P)+d|_v\}\\ &= \lim_{\substack{P\to O\\ v\text{-adic}}}\left\{\hat\lambda_{E,v}(P)-\log|x(P)|_v-\log\left|\frac{x(P)+d}{x(P)}\right|_v\right\}\\ &= \lim_{\substack{P\to O\\ v\text{-adic}}}\left\{\hat\lambda_{E,v}(P)-\log|x(P)|_v-\log\left|1+\frac{d}{x(P)}\right|_v\right\}\\ &= \lim_{\substack{P\to O\\ v\text{-adic}}}\{\hat\lambda_{E,v}(P)-\log|x(P)|_v\}.\end{aligned}$$

The property (3) is clearly satisfied. □

3. Computing the canonical height

Let $E_{a,b}$ be the elliptic curve (1.1) and P_1, P_2, P_3 the rational points on $E_{a,b}$ defined in (1.2).

Proposition 3.1. *If ab is odd, $v_3(b) = 1$ and m is square-free, then the canonical heights of the points P_1, P_2, P_3 on $E_{a,b}$ have the following bounds*

$$\begin{aligned}\frac{1}{3}\log m - 0.7441 < \hat h(P_1) < \frac{1}{3}\log m + 0.5409,\\ \frac{1}{3}\log m - 0.7579 < \hat h(P_2) < \frac{1}{3}\log m + 1.0515,\\ \frac{1}{3}\log m - 0.5113 < \hat h(P_3) < \frac{1}{3}\log m + 0.5665.\end{aligned}$$

Proof of Proposition 3.1. We use the decomposition (2.8) to estimate the canonical height. We first estimate the archimedean part $\hat h_\infty(P_i)(=\hat\lambda_\infty(P_i))$ $(i = 1, 2, 3)$ by using Tate's series with Silverman's shifting trick ([13]).

Let E be the elliptic curve defined by (2.1). For $P \in E(\mathbb{R})$, we put

$$\begin{aligned}t = t(P) &:= 1/x(P),\\ z = z(P) &:= 1 - b_4t^2 - 2b_6t^3 - b_8t^4,\\ w = w(P) &:= 4t + b_2t^2 + 2b_4t^3 + b_6t^4,\end{aligned}\tag{3.2}$$

where b_2, b_4, b_6, b_8 are as in (2.3). Note that we have $x(2P) = z(P)/w(P)$. By the property of the local height (Theorem 2.7 (1)) we have

$$\hat\lambda_\infty(2P) = 4\hat\lambda_\infty(P) - 2\log|2y(P) + a_1x(P) + a_3|.$$

Then using (2.2), we have

$$\begin{aligned}\hat\lambda_\infty(2P) - \log|x(2P)| &= 4\hat\lambda_\infty(P) - 2\log|2y(P) + a_1x(P) + a_3| - \log|x(2P)|\\ &= 4\hat\lambda_\infty(P) - \log|4x(P)^3 + b_2x(P)^2 + 2b_4x(P) + b_6|\\ &\quad - \log|z(P)/w(P)|\\ &= 4\{\hat\lambda_\infty(P) - \log|x(P)|\} - \log|z(P)|.\end{aligned}$$

Putting $\mu(P) := \hat{\lambda}_\infty(P) - \log|x(P)|$,

$$\mu(2P) = 4\mu(P) - \log|z(P)|.$$

So if we ignore the convergence, we have

$$\mu(P) = \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n}\log|z(2^nP)|.$$

In fact, by Tate's theorem ([13, Theorem 1.2]), if there is $\epsilon > 0$ such that $|x(P)| > \epsilon$ for all $P \in E(\mathbb{R})$, then for any $P \in E(\mathbb{R})$, $\log|z(2^nP)|$ is bounded independently of n and therefore

$$\hat{\lambda}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n}\log|z(2^nP)|.$$

For $d \in \mathbb{Q}$ and $P \in E(\mathbb{R})$, the point $P' = (x(P)+d, y(P))$ is on the curve

$$E' : (y')^2 + {a_1}'x'y' + {a_3}'y' = (x')^3 + {a_2}'(x')^2 + {a_4}'x' + {a_6}', \tag{3.3}$$

where

$${a_1}' = a_1,\ {a_2}' = a_2 - 3d,\ {a_3}' = a_3 - da_1,$$
$${a_4}' = a_4 - 2da_2 + 3d^2,\ {a_6}' = a_6 - da_4 + d^2a_2 - d^3$$

as we saw in (2.10). We similarly put

$$\begin{aligned} t' = t'(P') &:= 1/x'(P'),\\ z' = z'(P') &:= 1 - b_4'(t')^2 - 2b_6'(t')^3 - b_8'(t')^4,\\ w' = w'(P') &:= 4t' + b_2'(t')^2 + 2b_4'(t')^3 + b_6'(t')^4, \end{aligned} \tag{3.4}$$

where b_2', b_4', b_6', b_8' are the values obtained by replacing $a_1, \dots, a_6$ by $a_1', \dots, a_6'$ in (2.3).

The reason why we make this substitution is that we obtain the Weierstrass model to which we can apply Tate's theorem above. We call this the *shifting trick* following Silverman.

Now we consider the elliptic curve $E_{a,b}$. We keep using the above notation. If $P \in E_{a,b}(\mathbb{R})$, then $x(P) \geq -m^{1/3}$. So if we take d such that $d > m^{1/3}$, then $x'(P') = x(P) + d \geq -m^{1/3} + d > 0$. Therefore the assumption of Tate's theorem is satisfied and we have the convergent series

$$\hat{\lambda}_{E'_{a,b},\infty}(P') = \log|x'(P')| + \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n}\log|z'(2^nP')|.$$

This equals $\hat{\lambda}_{E_{a,b},\infty}(P)$ by Lemma 2.11.

Let us compute $\hat{\lambda}_\infty(P_2)$ $(=\hat{\lambda}_{E_{a,b},\infty}(P_2))$ by this formula, taking $d = 2a^2 + 4b^2$. Then the condition $d > m^{1/3}$ is clearly satisfied. Now we compute the serires

$$\hat{\lambda}_\infty(P_2) = \log|x'(P_2')| + \frac{1}{4}\sum_{n=0}^{\infty} 4^{-n}\log|z'(2^nP_2')|. \tag{3.5}$$

Following the definition (3.4) with the notation $X := a/b$, we see that $x'(P_2')$, $z'(P_2')$, $z'(2P_2')$, $z'(4P_2')$ are as follows.

- $x'(P_2') = 2ab + 2a^2 + 4b^2$ (see (1.2) for the coordinate of P_2)

- $z'(P_2') = (X^8 - 2X^7 + 2X^6 + 8X^5 + 2X^4 + 16X^3 + 16X^2 - 32X + 32)/(2X^8 + 8X^7 + 28X^6 + 56X^5 + 98X^4 + 112X^3 + 112X^2 + 64X + 32)$
- $z'(2P_2') = (X^{32} + 4X^{31} + 2X^{30} - 32X^{29} + \cdots + 2097152)/(2X^{32} - 16X^{31} + 64X^{30} - 96X^{29} + \cdots + 2097152)$
- $z'(4P_2') = (X^{128} - 8X^{127} + 2X^{126} + 384X^{125} + \cdots + 38685626227668133590597632)/(2X^{128} + 32X^{127} + 208X^{126} + 448X^{125} + \cdots + 38685626227668133590597632)$

In this computation, the functions about elliptic curves in the software PARI/GP ([3]) are useful to compute b_4', b_6', b_8'.

Since $x'(P_2')^3/m$, $z'(P_2')$, $z'(2P_2')$, $z'(4P_2')$ are functions of X, by elementary calculus we can compute their maximum and minimum. So we can find the following bounds.

$$\begin{aligned} &\frac{1}{3}\log(4m) < \log x'(P_2') < \frac{1}{3}\log(57.2218701m), \\ &-0.6637015 < 4^{-1}\log z'(P_2') < 0, \\ &-0.0433217 < 4^{-2}\log z'(2P_2') < 0.1396289, \\ &-0.0363430 < 4^{-3}\log z'(4P_2') \le 0. \end{aligned} \tag{3.6}$$

For example, we compute the bounds of $\log x'(P_2')$ as follows. Note that it suffices to show

$$4 < \frac{x'(P_2')^3}{m} \left(= \frac{(2X^2 + 2X + 4)^3}{X^6 + 16}\right) < 57.2218701.$$

By numerical computation we see that the only positive root of the numerator of $((2X^2 + 2X + 4)^3/(X^6 + 16))'$ is $X = 1.6484223\cdots$ and that it gives $x'(P_2')^3/m = 57.22187008\cdots$. Since $\lim_{X\to 0}(2X^2 + 2X + 4)^3/(X^6 + 16) = 4$ and $\lim_{X\to\infty}(2X^2 + 2X + 4)^3/(X^6 + 16) = 8$, we have the bounds for $\log x'(P_2')$ as above.

We can estimate $z'(P_2')$, $z'(2P_2')$, $z'(4P_2')$ similarly. Note that if a, b are real numbers, $d = 2a^2 + 4b^2 > m^{1/3}$ is satisfied. Then $\log|z'(2^nP_2')|$ has a finite value by Tate's theorem. So the denominators of $z'(P_2')$, $z'(2P_2')$, $z'(4P_2')$ do not have real roots.

For the estimate of the remaining terms $z'(2^nP_2')$ $(n \ge 3)$, we use the following two lemmas, which we shall prove in Section 7.

Lemma 3.7. *Let $d = 2a^2 + 4b^2$ or $d = 3a^2 + 4b^2$. Then $z'(P') < 120.531634$ for any $P \in E_{a,b}(\mathbb{R})$.*

Lemma 3.8. (1) *If $d = 2a^2 + 4b^2$, then $0.062326 < z'(P')$ for any $P \in E_{a,b}(\mathbb{R})$.*

(2) *If $d = 3a^2 + 4b^2$, then $0.038068 < z'(P')$ for any $P \in E_{a,b}(\mathbb{R})$.*

Remark 3.9. In general there is Silverman's bound of $z'(P')$ ([13, Lemma 4.1]), which gives a bound dependent on a, b. In our case we find that there is a bound of $z'(P')$ independent of a, b.

We continue the proof of Proposition 3.1. Since $(1/4)\sum_{n=3}^{\infty} 4^{-n} = 1/192$, we have

$$\frac{1}{192}\log(0.062326) < \frac{1}{4}\sum_{n=3}^{\infty} 4^{-n}\log z'(2^nP_2') < \frac{1}{192}\log(120.531634). \tag{3.10}$$

By (3.5), (3.6) and (3.10), we have

$$\frac{1}{3}\log m - 0.295724 < \hat{\lambda}_\infty(P_2) < \frac{1}{3}\log m + 1.513566.$$

To compute the non-archimedean part $\hat{h}_f(P_2)$, we use Lemma 3.18, which is proved in the next subsection. Recall $P_2 = (2ab, a^3 + 4b^3)$. So α, β, δ in Lemma 3.18 correspond to $2ab, a^3 + 4b^3, 1$ respectively. Therefore

$$\hat{h}_f(P_2) = -\frac{2}{3}\log 2.$$

Since $\hat{h}(P_2) = \hat{\lambda}_\infty(P_2) + \hat{h}_f(P_2)$, we have

$$\frac{1}{3}\log m - 0.7579 < \hat{h}(P_2) < \frac{1}{3}\log m + 1.0515.$$

We can estimate $\hat{h}(P_1)$, $\hat{h}(P_3)$ similarly by taking $d = 3a^2 + 4b^2, 2a^2 + 4b^2$ respectively. □

Remark 3.11. The shifting width d is not necessary to be $3a^2 + 4b^2, 2a^2 + 4b^2$. We choose the width which give good enough bounds. We do not have an idea to determine the width which give the best bound.

3.1. **Non-archimedean part.** In this subsection we compute the non-archimedean part of the canonical height, which was required in the proof of Proposition 3.1. To do this, we use [13, THEOREM 5.2]. The Weierstrass equation of the elliptic curve to which we apply this theorem needs to be minimal at p to compute $\hat{\lambda}_p$. Let $n \in \mathbb{Z}$ be sixth power free and E the elliptic curve $y^2 = x^3 + n$. Then the Weierstrass equation of E is global minimal if and only if $n \not\equiv 16 \pmod{64}$ ([5, Corollary 5.6.4]). Therefore if n is square-free, E is global minimal.

Lemma 3.12. *Let n be square-free integer and E the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$. Let $P = (\alpha/\delta^2, \beta/\delta^3)$ $(\alpha, \beta, \delta \in \mathbb{Z},\ \delta > 0,\ \gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1)$ be a rational point on E. If $v_2(\alpha) = 0$, then $\hat{\lambda}_2(P) = 2v_2(\delta)\log 2$. If $v_2(\alpha) \neq 0$, then $\hat{\lambda}_2(P) = -\frac{2}{3}\log 2$.*

Proof. Since n is square-free, $y^2 = x^3 + n$ is global minimal. So we compute $\hat{\lambda}_2(P)$ following the algorithm ([13, p.354, SUBROUTINE in THEOREM 5.2]).

For the general Weierstrass equation (2.1) and a point P on it, we put $x := x(P),\ y := y(P)$. Further we define A, B, C, Λ for P as follows.

$$\begin{aligned} &A := v_p(3x^2 + 2a_2x + a_4 - a_1y),\ B := v_p(2y + a_1x + a_3),\\ &C := v_p(3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8),\\ &\Lambda := \hat{\lambda}_p(P)/\log p. \end{aligned} \tag{3.13}$$

This is the same definition as in [13] but the value of Λ is twice of that in the algorithm. Recall that in our definition the value of the canonical height is twice of that in [13].

For our elliptic curve, since $a_1 = a_2 = a_3 = a_4 = 0$, $b_2 = b_4 = b_8 = 0$ and $b_6 = 4n$, we have

$$A = v_p\left(\frac{3\alpha^2}{\delta^4}\right),\ B = v_p\left(\frac{2\beta}{\delta^3}\right),\ C = v_p\left(\frac{3\alpha(\alpha^3 + 4n\delta^6)}{\delta^8}\right). \tag{3.14}$$

Note that $c_4 = 0$ (i.e. $v_p(c_4) \neq 0$). This condition has an effect in the algorithm.

On this condition, by the algorithm we have

$$\Lambda = \begin{cases} 2\max\left\{0, -\frac{1}{2}v_p(\alpha/\delta^2)\right\} & \text{if } A \le 0 \text{ or } B \le 0 \\ -\frac{2B}{3} & \text{if } A,\ B > 0,\ C \ge 3B \\ -\frac{C}{4} & \text{if } A,\ B > 0,\ C < 3B \end{cases} . \tag{3.15}$$

Now we consider the case of $p = 2$. If $v_2(\alpha) = 0$, then $A \le 0$ and by (3.15)

$$\hat{\lambda}_2(P) = \Lambda \log 2 = 2\max\left\{0, -\frac{1}{2}v_2(\alpha/\delta^2)\right\} \cdot \log 2 = 2v_2(\delta)\log 2.$$

We assume that $v_2(\alpha) \neq 0$. Then $v_2(\delta) = 0$, since $\gcd(\alpha, \delta) = 1$. So $A,\ B > 0$. Since P is on E, we have the equation $n\delta^6 = \beta^2 - \alpha^3$. Since n is square-free, $v_2(n) = 0$ or 1. So only the case of $v_2(n) = 0$ and $v_2(\beta) = 0$ is possible. So $B = v_2(2\beta) = 1$ and $C = v_2(\alpha) + v_2(\alpha^3 + 4n\delta^6) \ge 1 + 2 = 3$. So $C \ge 3B$, and by (3.15)

$$\hat{\lambda}_2(P) = \Lambda \log 2 = -\frac{2B}{3}\log 2 = -\frac{2}{3}\log 2.$$

□

Lemma 3.16. *We consider the situation of Lemma 3.12. If $v_3(\beta) = 0$, then $\hat{\lambda}_3(P) = 2v_3(\delta)\log 3$. If $v_3(\beta) \neq 0$, then $\hat{\lambda}_3(P) = -\frac{1}{2}\log 3$.*

Proof. We compute $\hat{\lambda}_3(P)$ following (3.14), (3.15) for $p = 3$.

If $v_3(\beta) = 0$, then $B \le 0$ and by (3.15)

$$\hat{\lambda}_3(P) = \Lambda \log 3 = 2\max\left\{0, -\frac{1}{2}v_3(\alpha/\delta^2)\right\} \cdot \log 3 = 2v_3(\delta)\log 3.$$

The last equality is as follows. If $v_3(\delta) = 0$, then $\max\left\{0, -\frac{1}{2}v_3(\alpha/\delta^2)\right\} = 0$. So $\max\left\{0, -\frac{1}{2}v_3(\alpha/\delta^2)\right\} = v_3(\delta)$. If $v_3(\delta) \neq 0$, then since $\gcd(\alpha, \delta) = 1, v_3(\alpha) = 0$. So $\max\left\{0, -\frac{1}{2}v_3(\alpha/\delta^2)\right\} = v_3(\delta)$.

We assume that $v_3(\beta) \neq 0$. Then $v_3(\delta) = 0$, since $\gcd(\beta, \delta) = 1$. So $B = v_3(2\beta/\delta^3) = v_3(\beta) > 0$ and $A = v_3(3\alpha^2/\delta^4) = v_3(3\alpha^2) > 0$. Since P is on E, $n\delta^6 = \beta^2 - \alpha^3$. Since $v_3(n) = 0$ or 1, only the case of $v_3(n) = 0$ and $v_3(\alpha) = 0$ is possible. Using the equality $\alpha^3 + 4n\delta^6 = \beta^2 + 3n\delta^6$,

$$C = v_3(3\alpha) + v_3(\alpha^3 + 4n\delta^6) = v_3(3\alpha) + v_3(\beta^2 + 3n\delta^6) = 1 + 1 = 2.$$

So we have $3B > C$. By (3.15)

$$\hat{\lambda}_3(P) = \Lambda \log 3 = -\frac{C}{4}\log 3 = -\frac{1}{2}\log 3.$$

□

Lemma 3.17. *Let $n \in \mathbb{Z}$ be square-free and E the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$. Let $P = (\alpha/\delta^2, \beta/\delta^3)$ $(\alpha, \beta, \delta \in \mathbb{Z},\ \delta > 0,\ \gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1)$ be a rational point on E. We assume that $p \neq 2, 3$. Then $\hat{\lambda}_p(P) = 2v_p(\delta)\log p$.*

Proof. We compute $\hat{\lambda}_p(P)$ following (3.14), (3.15). At first if $v_p(\alpha) = 0$ or $v_p(\beta) = 0$, then since δ is an integer, $A \leq 0$ or $B \leq 0$. So

$$\hat{\lambda}_p(P) = \Lambda \log p = 2 \max \left\{ 0, -\frac{1}{2} v_p(\alpha/\delta^2) \right\} \cdot \log p = 2 v_p(\delta) \log p.$$

The last equality follows from the same reason as that in the proof of Lemma 3.16.

Next we assume that $v_p(\alpha) > 0$ and $v_p(\beta) > 0$. Then $v_p(\delta) = 0$ because $\gcd(\alpha, \delta) = 1$. Since $v_p(\beta^2 - \alpha^3) > 1$ and $n\delta^6 = \beta^2 - \alpha^3$, we have $v_p(n\delta^6) > 1$. But n is square-free, $v_p(n) = 0$ or 1. So this case does not happen.

□

By the previous four lemmas, we have the following lemma.

Lemma 3.18. *Let $n \in \mathbb{Z}$ be square-free and E the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$. Let $P = (\alpha/\delta^2, \beta/\delta^3)$ $(\alpha, \beta, \delta \in \mathbb{Z},\ \delta > 0,\ \gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1)$ be a rational point on E. Then the non-archimedean part of the canonical height of P is as follows:*

$$\hat{h}_f(P) = 2 \log \delta + \lambda_2'(P) + \lambda_3'(P),$$

where

$$\lambda_2'(P) = \begin{cases} 0 & (v_2(\alpha) = 0), \\ -\dfrac{2}{3} \log 2 & (v_2(\alpha) \neq 0), \end{cases}$$

$$\lambda_3'(P) = \begin{cases} 0 & (v_3(\beta) = 0), \\ -\dfrac{1}{2} \log 3 & (v_3(\beta) \neq 0). \end{cases}$$

Proof.

$$\begin{aligned} \hat{h}_f(P) &= \hat{\lambda}_2(P) + \hat{\lambda}_3(P) + \sum_{p \neq 2,3} \hat{\lambda}_p(P) \\ &= \hat{\lambda}_2(P) + \hat{\lambda}_3(P) + \sum_{p \neq 2,3} 2 v_p(\delta) \log p \\ &= \hat{\lambda}_2(P) - 2 v_2(\delta) \log 2 + \hat{\lambda}_3(P) - 2 v_3(\delta) \log 3 + 2 \log \prod_p p^{v_p(\delta)} \\ &= \hat{\lambda}_2(P) - 2 v_2(\delta) \log 2 + \hat{\lambda}_3(P) - 2 v_3(\delta) \log 3 + 2 \log \delta. \end{aligned}$$

Here by Lemmas 3.12 and 3.16 we see that $\hat{\lambda}_2(P) - 2 v_2(\delta) \log 2$ and $\hat{\lambda}_3(P) - 2 v_3(\delta) \log 3$ are nothing but $\lambda_2'(P)$ and $\lambda_3'(P)$ respectively.

□

4. Uniform lower bound

In this section we compute a uniform lower bound of the canonical height (Proposition 4.3), that is a lower bound of the canonical height independent of $P \in E(\mathbb{Q})$.

Proposition 4.1. *Let $n \in \mathbb{Z}$ and let E be the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$. Let $P = (\alpha/\delta^2, \beta/\delta^3)$ $(\alpha, \beta, \delta \in \mathbb{Z},\ \delta > 0,\ \gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1)$ be a rational point on E. We assume that $n > 0$. Then we have*

$$\hat{\lambda}_\infty(P) > \frac{1}{12}\log n + \frac{1}{2}\log\left|\frac{\beta}{\delta^3}\right| + 0.31494685.$$

Proof. Recall that in our definition the value of the canonical height is twice of that in [4]. By Algorithm 7.5.7 [4] and (2.2)

$$\hat{\lambda}_\infty(P) = \frac{1}{16}\log\left|\frac{\Delta}{q}\right| + \frac{1}{4}\log\left(\frac{\omega_1 y(P)^2}{2\pi}\right) - \frac{1}{2}\log|\theta|\,, \tag{4.2}$$

where $q = \exp(2\pi i\omega_2/\omega_1)$, $\theta = \sum_{n=0}^{\infty}(-1)^n q^{\frac{n(n+1)}{2}}\sin\{2\pi(2n+1)\mathrm{Re}(z_P)/\omega_1\}$, Δ is the discriminant of E, ω_1 and ω_2 are periods of E such that $\omega_1 > 0$, $\mathrm{Im}(\omega_2) > 0$ and $\mathrm{Re}(\omega_2/\omega_1) = -1/2$ and z_P is the elliptic logarithm of P. Recall that z_P is the complex number in $\{t_1\omega_1 + t_2\omega_2 : 0 \le t_1, t_2 \le 1\}$ such that $\wp(z_P) = x(P)$ and $\wp'(z_P) = 2y(P)$, where $\wp$ is the Weierstrass $\wp$-function.

Note that q is a real number since

$$\begin{aligned} q = \exp\left(2\pi i\frac{\omega_2}{\omega_1}\right) &= \exp\left(2\pi i\left(-\frac{1}{2} + i\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)\right)\right) \\ &= \exp\left(-\pi i - 2\pi\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)\right) = -\exp\left(-2\pi\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)\right). \end{aligned}$$

By Definition 7.4.6 and Algorithm 7.4.7 in [4]

$$\omega_1 = \frac{2\pi}{\mathrm{AGM}(2\sqrt[4]{3}n^{\frac{1}{6}}, \sqrt{2\sqrt{3}-3}n^{\frac{1}{6}})} = n^{-\frac{1}{6}}\cdot\frac{2\pi}{\mathrm{AGM}(2\sqrt[4]{3}, \sqrt{2\sqrt{3}-3})},$$

where $\mathrm{AGM}(\cdot,\cdot)$ is the arithmetic geometric mean. So if we let ω_1', ω_2' be the periods of the elliptic $y^2 = x^3 + 1$, then we have $\omega_1 = n^{-\frac{1}{6}}\times\ \omega_1'$. It turns out that $\omega_1' = 4.206546315\cdots$. This can be done by PARI/GP (Version 2.3.4) ([3]) as follows.

```
E1=ellinit([0,0,0,0,1]);
E1.omega
```

Similarly by [4, Algorithm 7.4.7], we have

$$\begin{aligned} \omega_2/\omega_1 &= -\frac{1}{2} + \frac{i}{2}\frac{\mathrm{AGM}(2\sqrt[4]{3}n^{\frac{1}{6}}, \sqrt{2\sqrt{3}+3}n^{\frac{1}{6}})}{\mathrm{AGM}(2\sqrt[4]{3}n^{\frac{1}{6}}, \sqrt{2\sqrt{3}-3}n^{\frac{1}{6}})} \\ &= -\frac{1}{2} + \frac{i}{2}\frac{\mathrm{AGM}(2\sqrt[4]{3}, \sqrt{2\sqrt{3}+3})}{\mathrm{AGM}(2\sqrt[4]{3}, \sqrt{2\sqrt{3}-3})} = \omega_2'/\omega_1' \end{aligned}$$

and so it turns out that $q = -0.163033534\cdots$ by PARI/GP as follows(the above commands are needed).

```
-exp(-2*Pi*imag(E1.omega[2]/E1.omega[1]))
```

Substituting these values and $\Delta = -432n^2$ in (4.2), we have

$$\begin{aligned}\hat{\lambda}_\infty(P) &= \frac{1}{16}\log\left|\frac{432n^2}{q}\right| + \frac{1}{4}\log\left(\frac{n^{-\frac{1}{6}}\omega_1'\beta^2}{2\pi\delta^6}\right) - \frac{1}{2}\log|\theta| \\ &> \frac{1}{16}\log\left|\frac{432n^2}{0.163033535}\right| + \frac{1}{4}\log\left(\frac{4.206546315n^{-\frac{1}{6}}\beta^2}{2\pi\delta^6}\right) - \frac{1}{2}\log|1.167385748| \\ &= \frac{1}{12}\log n + \frac{1}{2}\log\left|\frac{\beta}{\delta^3}\right| + 0.3149468597\cdots\end{aligned}$$

by the trivial bound $|\theta| < 1 + |q| + |q|^3 + |q|^6 + |q|^{10} + |q|^{15} + |q|^{21} + \cdots < 1 + |q| + |q|^3 + |q|^6 + \frac{|q|^{10}}{1-|q|^5}$=1.16738574713$\cdots$.

□

Proposition 4.3. *Let n be a positive, square-free integer and E the elliptic curve $y^2 = x^3 + n$. If P is a rational, non-torsion point on E, then*

$$\hat{h}(P) > \frac{1}{12}\log n - 0.147152. \tag{4.4}$$

Proof. By Lemmas 3.12, 3.16, 3.18 and Proposition 4.1, we have

$$\begin{aligned}\hat{h}(P) &= \hat{h}_f(P) + \hat{\lambda}_\infty(P) \\ &> 2\log\delta + \lambda_2'(P) + \lambda_3'(P) + \frac{1}{12}\log n + \frac{1}{2}\log\left|\frac{\beta}{\delta^3}\right| + 0.31494685 \\ &= \frac{1}{2}\log\delta + \lambda_2'(P) + \left\{\lambda_3'(P) + \frac{1}{2}\log|\beta|\right\} + \frac{1}{12}\log n + 0.31494685 \\ &\geq \frac{1}{12}\log n - \frac{2}{3}\log 2 + 0.31494685 = \frac{1}{12}\log n - 0.1471512\cdots,\end{aligned}$$

since $\delta \in \mathbb{Z}$ and $\lambda_3'(P) + \frac{1}{2}\log|\beta| \geq 0$. □

5. Estimate of the lattice index

Let E be an elliptic curve of rank $r(\geq 2)$ defined over a number filed K. Let $Q_1, Q_2, ..., Q_s$ $(s \leq r)$ be independent points in $E(K)$. Then there exist generators $G_1, G_2, ..., G_r$ of the free part of $E(K)$ such that $Q_1, Q_2, ..., Q_s \in \mathbb{Z}G_1 + \mathbb{Z}G_2 + \cdots + \mathbb{Z}G_s$ by the elementary divisor theory. The index of the subgroup $\mathbb{Z}Q_1 + \mathbb{Z}Q_2 + \cdots + \mathbb{Z}Q_s$ in $\mathbb{Z}G_1 + \mathbb{Z}G_2 + \cdots + \mathbb{Z}G_s$ is called the *lattice index* of $\{Q_1, Q_2, ..., Q_s\}$. We put

$$\begin{aligned}\langle Q_i, Q_j\rangle &= \frac{1}{2}\left(\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)\right), \\ R(Q_1, Q_2, ..., Q_s) &= \det\left(\langle Q_i, Q_j\rangle\right)_{1\leq i,j\leq s}.\end{aligned}$$

It is known that the canonical height $\hat{h}$ is a positive definite quadratic form on $E(K)/E(K)_{\mathrm{tors}}$. When we identify $E(K)/E(K)_{\mathrm{tors}} \simeq \mathbb{Z}G_1 + \mathbb{Z}G_2 + \cdots + \mathbb{Z}G_r$ as $\mathbb{Z}$-modules, $\hat{h}$ is the quadratic form defined by the symmetric matrix $(\langle G_i, G_j\rangle)_{1\leq i,j\leq r}$.

Let $f(\mathbf{x}) = \sum_{i,j=1}^n f_{i,j}x_ix_j$ be a positive definite symmetric quadratic form. Then it is known that there exists a constant γ_n called the *Hermite constant* such that

$$\inf_{\mathbf{m}\in\mathbb{Z}^r\setminus\{\mathbf{0}\}} f(\mathbf{m}) \leq \gamma_n \det(f_{i,j}).$$

For example,

$$\gamma_1^1 = 1,\ \gamma_2^2 = 4/3,\ \gamma_3^3 = 2,\ \gamma_4^4 = 4,\ \dots$$

In this section we estimate the lattice index. For this we use the following theorem of Siksek.

Theorem 5.1. ([12, Theorem 3.1]) *Let E be an elliptic curve of rank r (≥ 2) defined over a number field K. Let $Q_1, Q_2, ..., Q_s$ ($s \leq r$) be independent points in $E(K)$ and ν the lattice index of $\{Q_1, Q_2, ..., Q_s\}$. Suppose that $\lambda > 0$ is a constant such that any point $P \in E(K)$ of infinite order satisfies $\hat{h}(P) > \lambda$. Then*

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

Proposition 5.2. *Assume that $m = a^6 + 16b^6$ is square-free, ab is odd and the discrete valuation $v_3(b)$ equals 1. If $m > 6.38 \times 10^{22}$ (this is true for either $a > 6321$ or $b > 3982$), the lattice indices of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ are less than 5. If $m > 19088$ (this is always true), the lattice indices of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ are less than 7.*

Proof. In this situation P_1, P_2, P_3 are independent by Proposition 6.7 in the next section. Let $\lambda = \frac{1}{12}\log m - 0.147152$. Then $\hat{h}(P) > \lambda$ for any non-torsion point $P \in E_{a,b}(\mathbb{Q})$. Now by Theorem 5.1, it suffices to show that $R(P_i, P_j)^{1/2}(\gamma_2/\lambda)^{2/2}$ is less than 5 or 7, when $m > 6.38 \times 10^{22}$ or $m > 19088$ respectively for $i \neq j$ $(i, j = 1, 2, 3)$. Since

$$R(P_2, P_3) = \hat{h}(P_2)\hat{h}(P_3) - \frac{1}{4}\left\{\hat{h}(P_2 + P_3) - \hat{h}(P_2) - \hat{h}(P_3)\right\}^2,$$

we have

$$\begin{aligned}\left\{R(P_2, P_3)^{1/2}(\gamma_2/\lambda)^{2/2}\right\}^2 &= \frac{4}{3}\frac{\hat{h}(P_2)\hat{h}(P_3) - \frac{1}{4}\left\{\hat{h}(P_2 + P_3) - \hat{h}(P_2) - \hat{h}(P_3)\right\}^2}{\lambda^2} \\ &< \frac{4}{3}\frac{\hat{h}(P_2)\hat{h}(P_3)}{\lambda^2} \\ &< \frac{4}{3}\frac{(\frac{1}{3}\log m + 1.0515)(\frac{1}{3}\log m + 0.5665)}{(\frac{1}{12}\log m - 0.147152)^2}.\end{aligned}$$

The last inequality follows from Propositions 3.1 and 4.3. By elementary calculus we see that the last bound is less than 25 if $m > 6.38 \times 10^{22}$, less than 49 if $m > 19088$ and decreasing if $m > e^2$.

Since the upper bound of $\hat{h}(P_1)$ given in Proposition 3.1 is less than those of $\hat{h}(P_2)$ and $\hat{h}(P_3)$, the cases of $\{P_1, P_2\}$, $\{P_3, P_1\}$ are clear. □

6. Independence of P_1, P_2, P_3

In this section we show that in the situation of Proposition 5.2, P_1, P_2, P_3 are independent and the lattice index of $\{P_i, P_j\}$ $(i \neq j)$ is not divisible by $2, 3$.

Lemma 6.1. *Let $n \in \mathbb{Z}$ and let E be the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$ and $Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$. We write $x(Q) = u/s^2$ with $\gcd(u, s) = 1$. Then $Q \notin 2E(\mathbb{Q})$ in either of the following cases:*

(1) n is odd, $u \not\equiv 0 \pmod 8$ and s is odd,
(2) $n \equiv 1 \pmod 9$, $u \equiv 2 \pmod 3$ and $s \not\equiv 0 \pmod 3$.

Proof. We assume that there exists $R = (w/t^2, z/t^3) \in E(\mathbb{Q})$ with $\gcd(w,t) = 1$ such that $Q = 2R$ and deduce a contradiction. By (2.5) or the following PARI/GP commands,

```
En=ellinit([0,0,0,0,n]);
ellpow(En,[w/t^2,z/t^3],2)[1]
```

we have $x(2R) = (9w^4 - 8wz^2)/(4z^2t^2)$ and so $u/s^2 = (9w^4 - 8wz^2)/(4z^2t^2)$. On the other hand $(z/t^3)^2 = (w/t^2)^3 + n$ since R is on E. Eliminating z,

$$s^2w(w^3 - 8nt^6) = 4ut^2(w^3 + nt^6). \tag{6.2}$$

(1) If n and s are odd, then w is even by (6.2). Further t is odd since $\gcd(w,t) = 1$. Then $v_2(w(w^3 - 8nt^6)) \geq 5$ (note that if $v_2(w) = 1$, $w^3 - 8nt^6 = 8\times$ even). So $v_2(4ut^2(w^3 + nt^6)) \geq 5$ and therefore $v_2(u) \geq 3$. This is a contradiction since $u \not\equiv 0 \pmod 8$.

(2) Assume that $n \equiv 1 \pmod 9$, $u \equiv 2 \pmod 3$ and $s \not\equiv 0 \pmod 3$. Note that if $x \not\equiv 0 \pmod 3$, then $x^2 \equiv 1 \pmod 9$ (so modulo 3 also).

Assume $w \equiv 0 \pmod 3$. Then $t \not\equiv 0 \pmod 3$ since $\gcd(w,t) = 1$. So the left hand side of (6.2) $\equiv 0 \pmod 3$ and the right hand side of (6.2) $\not\equiv 0 \pmod 3$. This is a contradiction.

Assume $w \equiv 1 \pmod 3$. If $t \equiv 0 \pmod 3$, then the left hand side of (6.2) $\equiv 1 \pmod 3$ and the right hand side of (6.2) $\equiv 0 \pmod 3$. This is a contradiction.

If $t \not\equiv 0 \pmod 3$, then the left hand side of (6.2) $\equiv 2 \pmod 3$ and the right hand side of (6.2) $\equiv 1 \pmod 3$. This is a contradiction.

Assume $w \equiv -1 \pmod 3$. If $t \equiv 0 \pmod 3$, then the left hand side of (6.2) $\not\equiv 0 \pmod 3$ and the right hand side of (6.2) $\equiv 0 \pmod 3$. This is a contradiction.

Note that $w^3 \equiv -1 \pmod 9$.

If $t \not\equiv 0 \pmod 3$, then $w^3 - 8nt^6 \equiv 0 \pmod 9$ and $w^3 + nt^6 \equiv 0 \pmod 9$. So we can write $w^3 - 8nt^6 = 9W_1$, $w^3 + nt^6 = 9W_2$. Then by (6.2) we have $s^2w \cdot 9W_1 \equiv 4ut^2 \cdot 9W_2 \pmod{27}$. So $s^2wW_1 \equiv 4ut^2W_2 \pmod 3$. Therefore $-W_1 \equiv -W_2 \pmod 3$. On the other hand $9W_2 - 9W_1 = 9nt^6$ and so $W_2 - W_1 = nt^6 \not\equiv 0 \pmod 3$. This is a contradiction. □

Remark 6.3. Assume that we can write $x(Q) = u/s^2 = u'/s'^2$ ($u', s' \in \mathbb{Z}$ and not necessarily $\gcd(u', s') = 1$). So $u|u'$ and $s|s'$. Then if $u' \not\equiv 0 \pmod 8$, $u \not\equiv 0 \pmod 8$. If s' is odd, s is odd. If $s' \not\equiv 0 \pmod 3$, $s \not\equiv 0 \pmod 3$. If $u' \equiv 2 \pmod 3$, $u \equiv 2 \pmod 3$ since $u' = (s'/s)^2 u$ and $s'/s \not\equiv 0 \pmod 3$.

So it is not necessary to assume $\gcd(u, s) = 1$ in Lemma 6.1.

Lemma 6.4. *Let $n \in \mathbb{Z}$ and let E be the elliptic curve $y^2 = x^3 + n$ over $\mathbb{Q}$ and $Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$. We write $x(Q) = u/s^2$ with $\gcd(u, s) = 1$. Then $Q \notin 3E(\mathbb{Q})$ in either of the following cases:*

(1) *n is odd and u is even,*
(2) *$n \equiv 1 \pmod 9$, $u \equiv 1 \pmod 3$ and $v_3(s) = 1$.*

Proof. We assume that there exists $R = (w/t^2, z/t^3) \in E(\mathbb{Q})$ with $\gcd(w,t) = 1$ such that $Q = 3R$ and deduce a contradiction. By the following PARI/GP commands

```
En=ellinit([0,0,0,0,n]);
ellpow(En,[w/t^2,z/t^3],3)[1]
```

we have $x(3R) = (64z^6 - 144w^3z^4 + 81w^9)/9t^2w^2(4z^2 - 3w^3)^2$ and so $u/s^2 = (64z^6 - 144w^3z^4 + 81w^9)/9t^2w^2(4z^2 - 3w^3)^2$. On the other hand $(z/t^3)^2 = (w/t^2)^3 + n$ since R is on E. Eliminating z,

$$s^2\left\{(w^3 + 4nt^6)^3 - 2^2 3^3 nw^6t^6\right\} = 3^2uw^2t^2(w^3 + 4nt^6)^2. \tag{6.5}$$

(1) If u is even, then s is odd since $\gcd(u, s) = 1$. Then since $(w^3 + 4nt^6)^3 - 2^2 3^3 nw^6t^6$ is even, w must be even. So t is odd since $\gcd(w, t) = 1$. Since n is odd, $v_2(w^3 + 4nt^6) = 2$ and therefore v_2(the left hand side of (6.5)) $= 6$. On the other hand v_2(the right hand side of (6.5)) ≥ 7.

(2) If $v_3(s) = 1$, we can write $s = 3s'$ ($s' \not\equiv 0 \pmod 3$). So we have

$$s'^2\left\{(w^3 + 4nt^6)^3 - 2^2 3^3 nw^6t^6\right\} = uw^2t^2(w^3 + 4nt^6)^2. \tag{6.6}$$

Now we show $wt \not\equiv 0 \pmod 3$. Assume that $wt \equiv 0 \pmod 3$. Then since the each side of (6.6) $\equiv 0 \pmod 3$, we have $(w^3 + 4nt^6)^3 - 2^2 3^3 nw^6t^6 \equiv 0 \pmod 3$. So $w^3 + 4nt^6 \equiv 0 \pmod 3$. But this does not happen since $\gcd(w, t) = 1$ and $n \equiv 1 \pmod 9$. So we see $wt \not\equiv 0 \pmod 3$.

Now if we assume that $w \equiv -1 \pmod 3$, then $w^3 + 4nt^6 \equiv -1 + 4t^6 \equiv 3 \pmod 9$. So $v_3(w^3 + 4nt^6) = 1$. Then v_3(the left hand side of (6.6)) ≥ 3
and v_3(the right hand side of (6.6)) $= 2$. This is a contradiction.

If we assume that $w \equiv 1 \pmod 3$, then $w^3 + 4nt^6 \equiv -1 \pmod 3$. Then seeing (6.6) modulo 3, we have $u \equiv -1 \pmod 3$. This is a contradiction.

□

Proposition 6.7. *We assume that $m = a^6 + 16b^6$ is square-free, ab is odd and the discrete valuation $v_3(b)$ equals 1. Then P_1, P_2, P_3, $P_1 + P_2$, $P_2 + P_3$, $P_1 + P_3$, $P_1 + P_2 + P_3 \notin 2E_{a,b}(\mathbb{Q})$ and P_1, P_2, P_3, $P_1 \pm P_2$, $P_2 \pm P_3$, $P_1 \pm P_3$, $P_1 + P_2 \pm P_3$, $P_1 - P_2 \pm P_3 \notin 3E_{a,b}(\mathbb{Q})$. In particular, P_1, P_2, P_3 are independent and the lattice indices of $\{P_1, P_2, P_3\}$, $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ are not divisible by 2 nor 3.*

Proof. To ease the notation, we put $E = E_{a,b}$. We have

$$x(P_1) = -a^2,\ x(P_2) = 2ab,\ x(P_3) = -2ab,$$

$$x(P_1 + P_2) = \frac{2a(a^3 + a^2b - 2ab^2 - 4b^3)}{(a + 2b)^2},$$

$$x(P_1 - P_2) = \frac{2(a^4 - 3a^3b + 6a^2b^2 - 8ab^2 + 8b^4)}{a^2},$$

$$x(P_1 + P_3) = \frac{2(a^4 + 3a^3b + 6a^2b^2 + 8ab^3 + 8b^4)}{a^2},$$

$$x(P_1 - P_3) = \frac{2a(a^3 - a^2b - 2ab^2 + 4b^3)}{(a - 2b)^2},$$

$$x(P_2 + P_3) = \frac{4b^4}{a^2},\ x(P_2 - P_3) = \frac{a^4}{(2b)^2},$$

$$x(P_1 + P_2 + P_3) = \frac{2a(a^5 + 4a^4b + 8a^3b^2 + 12a^2b^3 + 14ab^4 + 8b^5)}{(a^2 + 2ab + 2b^2)^2},$$

$$x(P_1 - P_2 - P_3) = \frac{2a(a^5 - 4a^4b + 8a^3b^2 - 12a^2b^3 + 14ab^4 - 8b^5)}{(a^2 - 2ab + 2b^2)^2}.$$

Note that $m = a^6 + 16b^6 \equiv 1 \pmod 9$ since $v_3(b) = 1$ and $\gcd(a, b) = 1$. As we saw in Remark 6.3, we can use Lemma 6.1 without the assumption that the x-coordinate is an irreducible fraction. Note that m in this proposition corresponds to n in Lemma 6.1.

We see that $P_1 + P_2 \notin 2E(\mathbb{Q})$ by Lemma 6.1(2) since $2a(a^3 + a^2b - 2ab^2 - 4b^3) \equiv 2a^4 \equiv 2 \pmod 3$ and $a + 2b \equiv a \not\equiv 0 \pmod 3$. Similarly $P_1 + P_3 \notin 2E(\mathbb{Q})$ by Lemma 6.1(2). It is clear that P_1, P_2, P_3, $P_2 + P_3$, $P_1 + P_2 + P_3 \notin 2E(\mathbb{Q})$ by Lemma 6.1(1).

If there is a rational point R such that $P_1 = 3R$, then $\hat{h}(P_1) = 9\hat{h}(R)$. But by Proposition 4.4 we have $9\hat{h}(R) > 9(\frac{1}{12}\log m - 0.147152) > \frac{1}{3}\log m + 0.5409 > \hat{h}(P_1)$ for $m \geq 88$, which is a contradiction. So $P_1 \notin 3E(\mathbb{Q})$.

Since $a^4/(2b)^2$ is an irreducible fraction, by Lemma 6.4(2) $P_2 - P_3 \notin 3E(\mathbb{Q})$. By computations we have

$$\begin{aligned}&x(2P_1 - 2P_2 - P_3)\\ &= a(-6144b^{17} + 34816ab^{16} - 101376a^2b^{15} + 204544a^3b^{14} - 320128a^4b^{13} + 409472a^5b^{12} - \\ &439840a^6b^{11} + 403168a^7b^{10} - 318248a^8b^9 + 217216a^9b^8 - 128160a^{10}b^7 + 65072a^{11}b^6 - \\ &28152a^{12}b^5 + 10200a^{13}b^4 - 3006a^{14}b^3 + 684a^{15}b^2 - 108a^{16}b + 9a^{17})/b^2(2b - a)^2(16b^6 - \\ &40ab^5 + 56a^2b^4 - 46a^3b^3 + 28a^4b^2 - 12a^5b + 3a^6)^2.\end{aligned}$$

We denote the numerator by U' and the denominator by S'^2. Further we write $U'/S'^2 = U/S^2$ as an irreducible fraction since it is an x-coordinate of an elliptic curve. Since $v_3(9a^{17}) = 2$ and the orders of other terms of U' is greater than 2, $v_3(U') = 2$. In S', $v_3(b^2) = 2, v_3(3a^6) = 1$ and other factors are not divisible by 3. So $v_3(S'^2) = 4$. Therefore, $v_3(S) = 1$ and $U'' := U'/9$, $S'' := S'/9$ are integers. Clearly $U''/S''^2 = U/S^2$. Since $U'' \equiv a^{18} \equiv 1 \pmod 3$, $U \equiv 1$ by the same argument as in Remark 6.3. So $2P_1 - 2P_2 - P_3 \notin 3E(\mathbb{Q})$ by Lemma 6.4(2). Therefore $P_1 - P_2 + P_3 = -(2P_1 - 2P_2 - P_3) + 3(P_1 - P_2) \notin 3E(\mathbb{Q})$. We have

$$\begin{aligned}&x(2P_1 + 2P_2 + P_3)\\ &= (4096b^{18} + 24576ab^{17} + 71680a^2b^{16} + 135680a^3b^{15} + 188160a^4b^{14} + 204800a^5b^{13} + \\ &181632a^6b^{12} + 133536a^7b^{11} + 83488a^8b^{10} + 48472a^9b^9 + 30720a^{10}b^8 + 22464a^{11}b^7 + \\ &16496a^{12}b^6 + 10584a^{13}b^5 + 5496a^{14}b^4 + 2178a^{15}b^3 + 612a^{16}b^2 + 108a^{17}b + 9a^{18})/a^2b^2(48b^6 + \\ &128ab^5 + 156a^2b^4 + 114a^3b^3 + 56a^4b^2 + 18a^5b + 3a^6)^2\end{aligned}$$

and by the same argument as above, we have $2P_1 + 2P_2 + P_3 \notin 3E(\mathbb{Q})$ by Lemma 6.4(2). Therefore $P_1 + P_2 - P_3 = -(2P_1 + 2P_2 + P_3) + 3(P_1 + P_2) \notin 3E(\mathbb{Q})$. We see that P_2, P_3, $P_1 \pm P_2$, $P_2 + P_3$, $P_1 \pm P_3$, $P_1 + P_2 + P_3$, $P_1 - P_2 - P_3 \notin 3E(\mathbb{Q})$ by Lemma 6.4(1), since the denominators of the x-coordinates of them are all odd.

Next we prove the latter assertion of the proposition. By the elementary divisor theory there are generators $G_1, \ldots, G_r \in E(\mathbb{Q})$ and $M \in M_3(\mathbb{Z})$ such that

$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} = M \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix}. \tag{6.8}$$

Note that the lattice index of $\{P_1, P_2, P_3\}$ equals $|\det M|$. Let p be a rational prime. We have

$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \equiv \bar{M} \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix} \pmod{pE(\mathbb{Q})}, \tag{6.9}$$

where $\bar{M}$ is the image of M in $M_3(\mathbb{Z}/p\mathbb{Z})$. We assume that there exists $A \in \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ such that $A\bar{M}$ has the row $[\bar{0}\ \bar{0}\ \bar{0}]$ and deduce a contradiction. Since we may assume that the first row is $[\bar{0}\ \bar{0}\ \bar{0}]$, by the left multiplication of A on (6.9) we have

$$\begin{bmatrix} k_1P_1 + k_2P_2 + k_3P_3 \\ * \\ * \end{bmatrix} \equiv \begin{bmatrix} \bar{0} & \bar{0} & \bar{0} \\ * & * & * \\ * & * & * \end{bmatrix} \begin{bmatrix} G_1 \\ G_2 \\ G_3 \end{bmatrix} \pmod{pE(\mathbb{Q})}, \tag{6.10}$$

where $[k_1\ k_2\ k_3]$ is the first row of A. But the former assertion of this proposition implies that $k_1P_1 + k_2P_2 + k_3P_3 \notin pE(\mathbb{Q})$ $(p = 2, 3)$ for any $(k_1, k_2, k_3) \in (\mathbb{Z}/p\mathbb{Z})^3 \setminus (\bar{0}, \bar{0}, \bar{0})$. This is a contradiction. Therefore $\det M$ is not congruent to 0 modulo 2 or modulo 3.

By the same argument as above, the cases of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ follow. □

Remark 6.11. By the same reason as above, if we verify that P_1, P_2, P_3, $P_1 \pm P_2$, $P_2 \pm P_3$, $P_3 \pm P_1$, $P_1 \pm 2P_2$, $P_2 \pm 2P_3$, $P_3 \pm 2P_1 \notin 5E_{a,b}(\mathbb{Q})$, we can prove that the lattice indices of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ are not divisible by 5. Note that $P \notin 5E(\mathbb{Q})$ amounts to $kP \notin 5E(\mathbb{Q})$ $(k = \pm 1, \pm 2)$. For $3 \leq a \leq 6321$, $3 \leq b \leq 3982$ we can verify this by the function `DivisionPoints` of the software Magma ([1]).

Now we can finish the proof of our main theorem.

Proof of Theorem 1.3. For $a > 6321, b > 3982$ by Propositions 5.2, 6.7 the lattice indices of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ equal 1. For $5 \leq a \leq 6321, 3 \leq b \leq 3982$ by Propositions 5.2, 6.7 and Remark 6.11 the lattice indices of $\{P_1, P_2\}$, $\{P_2, P_3\}$, $\{P_3, P_1\}$ equal 1. This completes the proof of Theorem 1.3.

□

We prove that there are infinitely many (a, b)'s which satisfy the condition of Theorem 1.3.

Lemma 6.12. *The set*

$$S := \left\{ m = a^6 + 16b^6 \in \mathbb{Z} \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z}_{>2},\ m : \text{square-free} \\ v_2(ab) = 0,\ v_3(b) = 1 \end{array} \right\}$$

is an infinite set.

Proof. We put

$$S_0 := \left\{ m = (2k + 3l)^6 + 16(6k - 9l)^6 \in \mathbb{Z} \;\middle|\; k, l \in \mathbb{Z}_{>0},\ m : \text{square-free} \right\}.$$

For $(2k + 3l)^6 + 16(6k - 9l)^6$ being square-free it is necessary that $v_3(k) = v_2(l) = 0$. Hence S_0 is a subset of S. From Greaves' theorem ([8, THEOREM]) we see that S_0 is an infinite set, since $(2x + 3y)^6 + 16(6x - 9y)^6 = 8503785y^6 - 34009308xy^5 +$

$56691900x^2y^4-50384160x^3y^3+25196400x^4y^2-6717888x^5y+746560x^6$ is an irreducible polynomial over $\mathbb{Z}$. This is verified by the function `factor` of the software Maple ([2]). Therefore S is an infinite set.

□

7. Uniform bounds of $z'(P')$

We use the notation of (3.3), (3.4). In this section we prove Lemmas 3.7 and 3.8, which were used in Proposition 3.1 to give bounds of $z'(P')$ which is independent of $P \in E_{a,b}(\mathbb{Q})$.

In the proof below, we used Maple for all computations including numerical evaluations.

Proof of Lemma 3.7. Since the Weierstrass equation of $E'_{a,b}$ is $y^2 = (x-d)^3 + m$, the correspondent values to (3.3) are as follows. $a'_1 = a'_3 = 0$, $a'_2 = -3d$, $a'_4 = 3d^2$, $a'_6 = m - d^3$, $b'_4 = 6d^2$, $b'_6 = 4m - 4d^3$, $b'_8 = 3d^4 - 12dm$. Putting $x = x(P)$ for $P \in E_{a,b}(\mathbb{Q})$ with (3.4), we have

$$z'(P') = 1 - \frac{6d^2}{(x+d)^2} - 2\frac{4m-4d^3}{(x+d)^3} - \frac{3d^4-12dm}{(x+d)^4} = \frac{x^4+4dx^3-8mx+4dm}{(x+d)^4}.$$

Since $x^3 + m = y^2 \geq 0$, $x \geq -m^{1/3}$. Clearly $d > m^{1/3}$, since $(3a^2+4b^2)^3 > (2a^2+4b^2)^3 > (a^6+16b^6)$.

If $x \geq 0$

$$\begin{aligned}\frac{x^4+4dx^3-8mx+4dm}{(x+d)^4} &\leq \frac{x^4}{(x+d)^4} + \frac{4dx^3}{(x+d)^4} + \frac{4dm}{(x+d)^4} \\ &< 1+4+4 = 9.\end{aligned}$$

If $x < 0$

$$\begin{aligned}\frac{x^4+4dx^3-8mx+4dm}{(x+d)^4} &= \frac{x^3(x+4d)}{(x+d)^4} + \frac{-8mx+4dm}{(x+d)^4} \\ &< \frac{-8mx+4dm}{(x+d)^4} < \frac{8m^{\frac{4}{3}}+4dm}{(-m^{\frac{1}{3}}+d)^4}.\end{aligned}$$

Assume $d = 2a^2+4b^2$. Putting $Y = (a/b)^2$ yields

$$\frac{8m^{\frac{4}{3}}+4dm}{(-m^{\frac{1}{3}}+d)^4} = \frac{8\,(Y^3+16)\,\left((Y^3+16)^{\frac{1}{3}}+Y+2\right)}{\left((Y^3+16)^{\frac{1}{3}}-2\,Y-4\right)^4}.$$

We denote the right hand side by $g_{2,4}(Y)$. Then

$$\frac{d}{dY}g_{2,4}(Y) = -\frac{48\,(Y^2-8)\,\left(2\,Y\,(Y^3+16)^{\frac{2}{3}}+4\,(Y^3+16)^{\frac{2}{3}}+3\,Y^3+48\right)}{(Y^3+16)^{\frac{2}{3}}\,\left((Y^3+16)^{\frac{1}{3}}-2\,Y-4\right)^5}.$$

Since $(Y^3+16)^{\frac{1}{3}} - 2\,Y - 4 < 0$, $g_{2,4}(Y)$ has a minimum at $Y = \sqrt{8}$ and a maximum at $Y = -\sqrt{8}$. But $Y > 0$ and therefore

$$g_{2,4}(Y) \leq \max\left\{\lim_{Y\to 0} g_{2,4}(Y), \lim_{Y\to\infty} g_{2,4}(Y)\right\}.$$

Since $g_{2,4}(0) = 120.53163357\cdots$ and $\lim_{Y\to\infty} g_{2,4}(Y) = 16$, we have $z'(P') = g_{2,4}(Y) < 120.531634$.

The case $d = 3a^2 + 4b^2$ is similar and we have $z'(P') < 120.531634$. □

Proof of Lemma 3.8. We use the notation at the beginning of the proof of Lemma 3.7. We put $x = x(P)$, $u = u(P) := x/d$ and $u_0 = -m^{1/3}/d$. Then $u \geq u_0 > -1$, since $x \geq -m^{1/3} > -d$. Putting $Y = (a/b)^2$ with substitution $d = 2a^2 + 4b^2$ yields

$$z'(P') = \frac{x^4 + 4dx^3 - 8mx + 4dm}{(x+d)^4} = \frac{d^4u^4 + 4d^4u^3 - 8dmu + 4dm}{(du+d)^4}$$
$$= \frac{2u^4(Y^3+6Y^2+12Y+8) + 8u^3(Y^3+6Y^2+12Y+8) - 2u(Y^3+16) + Y^3 + 16}{2(u+1)^4(Y+2)^3}.$$

We denote the last function by $f(u, Y)$. Computing the derivatives, we have

$$\frac{\partial f}{\partial Y} = -\frac{3(2u-1)(Y^2-8)}{(u+1)^4(Y+2)^4},$$
$$\frac{\partial f}{\partial u} = 3\frac{(4u^2Y^3 + uY^3 - Y^3 + 24u^2Y^2 + 48u^2Y + 32u^2 + 16u - 16)}{(u+1)^5(Y+2)^3}$$
$$= 12(Y^3+6Y^2+12Y+8)\frac{(u-u_1)(u-u_2)}{(u+1)^5(Y+2)^3},$$

where

$$u_1 = -\frac{\sqrt{17Y^6 + 96Y^5 + 192Y^4 + 416Y^3 + 1536Y^2 + 3072Y + 2304} + Y^3 + 16}{8Y^3 + 48Y^2 + 96Y + 64},$$
$$u_2 = \frac{\sqrt{17Y^6 + 96Y^5 + 192Y^4 + 416Y^3 + 1536Y^2 + 3072Y + 2304} - Y^3 - 16}{8Y^3 + 48Y^2 + 96Y + 64}.$$

It is easy to see $u_1 < 0 < u_2$ for any $Y(> 0)$. Considering the increase or decrease of $f(u, Y)$, we have $f(u, Y) \geq \min\{f(u_0, Y), f(u_2, Y)\}$.

At first we consider $f(u_0, Y)$. Since $d = 2a^2 + 4b^2$,

$$f(u_0, Y) = f(-m^{\frac{1}{3}}/d, Y) = \left.\frac{x^4 + 4dx^3 - 8mx + 4dm}{(x+d)^4}\right|_{x=-m^{\frac{1}{3}}}$$
$$= \frac{9m^{\frac{4}{3}}}{(d - m^{\frac{1}{3}})^4} = \frac{9(Y^3+16)^{\frac{4}{3}}}{(2Y + 4 - (Y^3+16)^{\frac{1}{3}})^4} \geq 0.75725080\cdots.$$

The last inequality follows from elementary calculus.

Next we consider $f(u_2, Y)$.

$$\frac{df(u_2, Y)}{dY} = \left.\frac{\partial f}{\partial u}\right|_{u=u_2} \cdot \frac{du_2}{dY} + \left.\frac{\partial f}{\partial Y}\right|_{u=u_2} \cdot \frac{dY}{dY}$$
$$= \left.\frac{\partial f}{\partial Y}\right|_{u=u_2}$$
$$= -\frac{3(2u_2-1)(Y^2-8)}{(u_2+1)^4(Y+2)^4}.$$

Here we see $2u_2 - 1 < 0$ by simple calculation. So $f(u_2, Y) \geq f\left(u_2(\sqrt{8}), \sqrt{8}\right) = 0.06232685\cdots$. Therefore $z'(P') = f(u, Y) > 0.062326$.

The case $d = 3a^2 + 4b^2$ is similar and we have $z'(P') > 0.03806854\cdots$. □

Acknowledgements

The second author thanks his adviser Prof. Akihiko Yukie for careful reading and giving corrections. The authors are grateful to the referee for valuable suggestions.

References

[1] *Magma*. Computational Algebra Group, School of Mathematics and Statistics, University of Sydney, http://magma.maths.usyd.edu.au/magma/.
[2] *Maple*. http://www.maplesoft.com/products/maple/.
[3] *PARI/GP*. http://pari.math.u-bordeaux.fr/.
[4] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.
[5] I. Connell. *Elliptic Curve Handbook*. http://www.ucm.es/BUCM/mat/doc8354.pdf or http://www.math.mcgill.ca/connell/, 1999.
[6] S. Duquesne. Elliptic curves associated with simplest quartic fields. *J. Theor. Nombres Bordeaux*, Vol. 19, pp. 81–100, 2007.
[7] Y. Fujita and N. Terai. Generators for the elliptic curve $y^2 = x^3 - nx$. *to appear in J. Theor. Nombres Bordeaux*.
[8] G. Greaves. Power-free values of binary forms. *Quart. J. Math. Oxford (2)*, Vol. 43, pp. 45–65, 1992.
[9] S. Kihara. On the rank of the elliptic curve $y^2 = x^3 + k$. *Proc. Japan Acad. Ser. A Math. Sci.*, Vol. 63, pp. 76–78, 1987.
[10] S. Kihara. On the rank of the elliptic curve $y^2 = x^3 + k$. II. *Proc. Japan Acad. Ser. A Math. Sci.*, Vol. 72, pp. 228–229, 1996.
[11] A. Knapp. *Elliptic Curves*. Princeton Univ. Press, 1992.
[12] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, Vol. 25, pp. 1501–1538, 1995.
[13] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, Vol. 51, pp. 339–358, 1988.
[14] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

(Y. Fujita) Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba 275–8576, Japan

(T. Nara) Mathematical Institute, Tohoku University, Sendai 980-8578, Japan