JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Yasutsugu FUJITA et Nobuhiro TERAI

Generators for the elliptic curve $y^2 = x^3 - nx$

Tome 23, nº 2 (2011), p. 403-416.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_403_0>

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 403-416

Generators for the elliptic curve $y^2 = x^3 - nx$

par Yasutsugu FUJITA et Nobuhiro TERAI

Résumé. Soit E la courbe elliptique définie par $y^2 = x^3 - nx$ où n est un entier strictement positif. En 2007, Duquesne a démontré que, pour k entier, si $n = (2k^2 - 2k + 1)(18k^2 + 30k + 17)$ est sans facteur carré, alors deux points rationnels spécifiques peuvent toujours se compléter en un système de générateurs du groupe de Mordell-Weil associé à E. Dans ce papier, nous généralisons ce résultat en le montrant pour des entiers $n = n(k, l)$ pour une infinité de formes binaires $n(k, l) \in \mathbb{Z}[k, l]$.

Abstract. Let E be an elliptic curve given by $y^2 = x^3 - nx$ with a positive integer n. Duquesne in 2007 showed that if $n = (2k^2 - 2k + 1)(18k^2 + 30k + 17)$ is square-free with an integer k, then certain two rational points of infinite order can always be in a system of generators for the Mordell-Weil group of E. In this paper, we generalize this result and show that the same is true for infinitely many binary forms $n = n(k, l)$ in $\mathbb{Z}[k, l]$.

1. Introduction

Let E be an elliptic curve over the rationals $\mathbb{Q}$ defined by

$$E : y^2 = x^3 - nx$$

with a positive integer n. Mordell's theorem asserts that the group $E(\mathbb{Q})$ of rational points on E is finitely generated. It is easy to check that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of $E(\mathbb{Q})$ is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$ depending on whether n is square or not, respectively (cf. [9]). On the contrary, it is not so easy to determine the structure of the free part of $E(\mathbb{Q})$.

In [6] we investigated ranks of $E(\mathbb{Q})$ and integer points on E for $n = p^k$ with p prime and $k \in \{1, 2, 3\}$. While in some cases of rank one we determined the generators for $E(\mathbb{Q})$ (e.g., in case $k = 1$ and $p = (2t)^2 + 1$ with odd t, $E(\mathbb{Q}) = \langle(0, 0), (-1, 2t)\rangle$), we were not able to do that in rank two cases (e.g., in case $k = 1$ and $p = a^4 + b^4 > 17$, the independence of the points $(-b^2, a^2b)$ and $(-a^2, ab^2)$ was only found). Duquesne ([5, Theorem 12.3]) remarkably showed that if $n = (2k^2-2k+1)(18k^2+30k+17)$ is square-free with an integer k, then the points $G_1 = (-(2k^2-2k+1), 4(k+1)(2k^2-$

Manuscrit reçu le 11 mai 2010.

$2k+1))$ and $G_2 = (9(2k^2-2k+1), 12(3k-2)(2k^2-2k+1))$ can always be in a system of generators for $E(\mathbb{Q})$ (where G_1 and G_2 above correspond to G_2 and G_1+G_2 in [5], respectively. Note that he also determined the integer points on a quartic form of E assuming $\mathrm{rank}E(\mathbb{Q})=2$). His main strategy is to bound the canonical height $\hat{h}$ on $E(\mathbb{Q})$ in two ways. More precisely, he gave a uniform lower bound for the Archimedean part $\hat{\lambda}_\infty$ of $\hat{h}$ using Cohen's algorithm ([4, Algorithm 7.5.7]), and gave upper bounds for $\hat{\lambda}_\infty(G_1)$ and $\hat{\lambda}_\infty(G_2)$ using Tate's series (cf. [13]). By combining them with bounds for the non-Archimedean part $\hat{h}_{\mathrm{fin}}$ of $\hat{h}$, he checked that in case $\mathrm{rank}E(\mathbb{Q})=2$ Siksek's theorem ([11, Theorem 3.1]) implies $\nu<3$, where ν denotes the lattice index of the span of G_1 and G_2 in $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. Since one easily see that $\nu \neq 2$, this shows the result.

The major reasons Duquesne's family worked well are that the x-coordinate $x(G_i)$ of G_i $(i \in \{1,2\})$ more or less divides n, which makes $\hat{h}_{\mathrm{fin}}(G_i)$ less than about $-(\log|x(G_i)|)/2$, and that $x(G_i)$ is similar in size to $\sqrt{n}$, which keeps $\hat{\lambda}_\infty(G_i)$ no larger than about $(\log n)/2$, and hence, $\hat{h}(G_i) = \hat{h}_{\mathrm{fin}}(G_i) + \hat{\lambda}_\infty(G_i)$ is less than about $(\log n)/4$ (see Lemma 3.2, Proposition 3.4 and its proof in Section 3). Moreover, putting $s = 2k^2-2k+1$ and $t = 18k^2+30k+17$ (then $n = st$), we found that G_1 comes from the relation $t-s=\Box$ and G_2 comes from the relation $81s-t=\Box$. These considerations lead us to the following.

Theorem 1.1. *Let n be a positive, non-square, fourth-power-free integer such that $n = st$ with positive, non-square integers s and t. Suppose that there exist positive integers α, β and m such that*

$$t-s=\alpha^2 \quad \text{and} \quad m^4 s - t = \beta^2. \tag{1.1}$$

Let E be the elliptic curve defined by

$$E : y^2 = x^3 - nx.$$

Then, the points $G_1 = (-s, s\alpha)$ and $G_2 = (m^2 s, ms\beta)$ can always be in a system of generators for $E(\mathbb{Q})$ if $m = 2$ or 3. In case $m \geq 4$, the same is true for $n \geq m^{26}$.

This paper is organized as follows. In Section 2, using the 2-descent lemma we show that the points G_1 and G_2 are independent. In Section 3, following Duquesne's strategy we estimate the canonical heights on E. In Section 4, applying Siksek's theorem to the height estimates we complete the proof of Theorem 1.1. Finally in Section 5, we show that for each integer $m \geq 2$ there exist infinitely many binary forms $n = n(k,l)$ in $\mathbb{Z}[k,l]$ each of which represents infinitely many integers satisfying the assumptions in Theorem 1.1 (cf. Proposition 5.1 and the subsequent Remarks (1)), and give several examples (cf. Example just after the proof of Proposition 5.1) of infinite families $n = n(k, l)$, one of which contains Duquesne's family (cf. Remark at the end of Section 5).

We now fix the notation. Let E be an elliptic curve defined by $y^2 = x^3 - nx$ with a positive integer n. For this model of E, $x(P)$ denotes the x-coordinate of a point P on E. For $P = (x, y)$ in $E(\mathbb{Q})$ with $x = b/a$ and $\gcd(a, b) = 1$, the naïve height $h : E(\mathbb{Q}) \to \mathbb{R}$ is defined by $h(P) = \log \max\{|a|, |b|\}$. The canonical height $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is defined by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

(note that this value is double the definitions in [12, 13, 4]). The canonical height has a decomposition into local heights:

$$\hat{h}(P) = \sum_{p:\text{prime or } \infty} \hat{\lambda}_p(P) \qquad \text{for } P \in E(\mathbb{Q}) \setminus \{O\}.$$

We normalize the symbols $\hat{\lambda}_p$ following Duquesne's paper (which are double the definitions in [4], and satisfy $\hat{\lambda}_p = 2(\hat{\lambda}'_p + \log|\Delta|_p/12)$, where $\hat{\lambda}'_p$ denote the local heights defined in [13, 14]). Finally, for a prime number p denote by v_p the valuation on $\mathbb{Q}$ normalized by $v_p(p) = 1$.

2. Independence of the points G_1 and G_2

Let $n, s, t, m, \alpha, \beta$ be integers as in Theorem 1.1. Then, $E(\mathbb{Q})_{\text{tors}} = \langle T \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, where $T = (0, 0)$ (cf. [9]). In addition, E has the following $\mathbb{Q}$-rational points

$$G_1 = (-s, s\alpha), \quad G_2 = (m^2 s, ms\beta).$$

Lemma 2.1. *Let denote by n' the square-free part of n. On the assumptions in Theorem* 1.1*, any prime divisor p of n' does not divide $m^2 s - t$.*

Proof. Suppose that a prime divisor p of n' divides $m^2 s - t$. Since p is a divisor of $n = st$, it divides both ms and t. Then, $m^4 s - t = \beta^2 \equiv 0 \pmod{p^2}$. Since n is fourth-power-free, we have either

$$v_p(m^4 s) = v_p(t) = 1$$

or

$$v_p(m^4 s) \geq 2 \text{ and } v_p(t) = 2.$$

Since p divides n', the latter holds and $v_p(s) = 1$, $v_p(t) = 2$. This implies that $v_p(\alpha^2) = v_p(t - s) = 1$, which is a contradiction. □

Proposition 2.2. *On the assumptions in Theorem* 1.1*, $G_1, G_2, G_1 + T, G_2 + T, G_1 + G_2, G_1 + G_2 + T \notin 2E(\mathbb{Q})$. Thus, G_1 and G_2 are independent modulo $E(\mathbb{Q})_{\text{tors}}$.*

Proof. By the 2-descent lemma (cf. [9, Theorem 4.2]), if a point $P = (x, y)$ on E is in $2E(\mathbb{Q})$, then $x, x + \sqrt{n}, x - \sqrt{n}$ must be squares in $\mathbb{Q}(\sqrt{n})$. We now have

$$G_1 + T = (t, t\alpha), \qquad G_2 + T = \left(-\frac{t}{m^2}, \frac{t\beta}{m^3}\right),$$

$$x(G_1 + G_2) = -\left(\frac{m\alpha + \beta}{m^2 + 1}\right)^2, \qquad x(G_1 + G_2 + T) = n\left(\frac{m\alpha - \beta}{m^2 s - t}\right)^2$$

(note that $s(m^4 - 1) = \alpha^2 + \beta^2$ and $(m^2 s + t)(m^2 - 1) = m^2\alpha^2 + \beta^2$ by assumption (1.1)). Hence, it is clear that $G_1, G_2 + T, G_1 + G_2 \notin 2E(\mathbb{Q})$. Moreover, since s, t and $n = st$ are non-square, the square-free part of n equals that of neither s nor t. Thus, $s, t \notin \mathbb{Q}(\sqrt{n})^2$, that is, $G_2, G_1 + T \notin 2E(\mathbb{Q})$.

Suppose that $G_1 + G_2 + T \in 2E(\mathbb{Q})$. Let $n = n_0^2 n'$ with square-free integers n_0, n'. Then, $x(G_1 + G_2 + T) + \sqrt{n} \in \mathbb{Q}(\sqrt{n'})^2$ implies that

$$(m\alpha - \beta)^2 n + (m^2 s - t)^2 \sqrt{n} = (A + B\sqrt{n'})^2$$

for some A, B with $A, B \in \mathbb{Z}$ or $A, B \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$. This means that

$$(m\alpha - \beta)^2 n = A^2 + B^2 n', \tag{2.1}$$

$$(m^2 s - t)^2 n_0 = 2AB. \tag{2.2}$$

Clearly $A, B \in \mathbb{Z}$. By (2.1) n' divides A, and by (2.2) and Lemma 2.1 n' divides n_0. Hence by (2.1) n' divides B, which contradicts (2.2) and Lemma 2.1. Therefore, $G_1 + G_2 + T \notin 2E(\mathbb{Q})$. □

Remarks. (1) Modifying the second equation of (1.1) a little, one can obtain an analogous result to the above proposition. More precisely, let $n = st$ and E be as in the proposition. Suppose that there exist positive integers α, β and m with m even such that

$$t - s = \alpha^2 \quad \text{and} \quad t - m^4 s = \beta^2.$$

Let $G_1 = (-s, s\alpha)$ and $G_2 = (-m^2 s, ms\beta)$. Then, G_1 and G_2 are independent modulo $E(\mathbb{Q})_{\text{tors}}$. The reason this family did not work well is that $x(G_1)$, $x(G_2)$ are not necessarily similar in size to $\sqrt{n}$. One can easily see that the same is true for the family of a negative $n = -st$ satisfying

$$t + s = \alpha^2 \quad \text{and} \quad t + m^4 s = \beta^2$$

by replacing s with $-s$ in the above argument.

(2) In the case where n is square, G_1 and G_2 are not necessarily independent modulo $E(\mathbb{Q})_{\text{tors}}$. Indeed, let $s = m^2 - 1$ and $t = m^2(m^2 - 1)$ with a positive integer m. Then, $t - s = (m^2 - 1)^2$, $m^4 s - t = m^2(m^2 - 1)^2$, and both s and t are non-square. On the other hand, since $G_1 = (1 - m^2, (m^2 - 1)^2)$ and $G_2 = (m^2(m^2 - 1), m^2(m^2 - 1)^2)$, we obtain $G_1 + T = G_2$. Note that $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for a square n.

3. Computation of the canonical heights on E

We begin by a brief summary of arithmetical properties of E. The discriminant of E is $64n^3$. Let p be a prime dividing n. By Tate's algorithm ([15]), the reduction of E at p is of Kodaira type III, I_M^* or III^* if respectively $v_p(n) = 1$, 2 or 3, where $M = 0$ for odd p. The exponent of the conductor of E at p is 2 or $8 - M$ if respectively p is odd or $p = 2$, where if $v_p(n) = 2$, then M corresponds to the subscript of I_M^*; otherwise $M = 0$. If n is fourth-power-free and $n \not\equiv 0 \pmod 4$, then the sign $\omega(E)$ of the functional equation of the Hasse-Weil L-function $L(E, s)$ is given by

$$\omega(E) = -\epsilon(n) \cdot \prod_{p^2 || n} \left(\frac{-1}{p}\right), \tag{3.1}$$

where the product runs over odd primes, and

$$\epsilon(n) = \begin{cases} -1 & \text{if } n \equiv 1, 3, 11, 13 \pmod{16}, \\ 1 & \text{otherwise} \end{cases}$$

(see [1]). Periods of E can be expressed as follows.

Lemma 3.1. *Let ω_1, ω_2 be periods of E such that $\omega_1 > 0$ and $i\omega_2 < 0$. Then, $\omega_2 = i\omega_1$ and $\omega_1 \geq \pi/(\sqrt{2}n^{\frac{1}{4}})$.*

Proof. This lemma can be shown in the same way as Lemma 8.2 in [5]. □

Hereinafter, we give an uniform lower bound for the canonical height on E and lower bounds for the canonical heights of the points G_1 and G_2. The computation method follows Duquesne's paper. The non-Archimedean part $\hat{h}_{\text{fin}}(P)$ of $\hat{h}(P)$ can be computed by using Silverman's algorithm ([13, Theorem 5.2]). The computation of the Archimedean part $\hat{\lambda}_\infty(P)$ is crucial. We compute $\hat{\lambda}_\infty(P)$ for any point $P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\text{tors}}$ using the following formula due to Cohen ([4, Algorithm 7.5.7]):

$$\hat{\lambda}_\infty(P) = \frac{1}{16} \log \left| \frac{64n^3}{q} \right| + \frac{1}{4} \log \left(\frac{\omega_1}{2\pi} y(P)^2 \right) - \frac{1}{2} \log |\theta|, \tag{3.2}$$

where

$$q = e^{2\pi i \frac{\omega_2}{\omega_1}},\ \omega_1 > 0,\ \operatorname{Im}(\omega_2) > 0,\ \operatorname{Re}(\omega_2) = 0,$$

either $\operatorname{Im}(z) = 0,\ 0 \leq z < \omega_1$ or $\operatorname{Im}(z) = \operatorname{Im}(\omega_2/2),\ 0 \leq z - \omega_2/2 < \omega_1$, and

$$\theta = \sum_{k=0}^{\infty} (-1)^k q^{k(k+1)/2} \sin\left((2k+1) \frac{2\pi}{\omega_1} \operatorname{Re}(z) \right)$$

with the elliptic logarithm $z = z(P)$ of P. Note that θ has a trivial bound $|\theta| < 1/(1 - |q|)$.

On the other hand, we compute $\hat{\lambda}_\infty(G_1)$ and $\hat{\lambda}_\infty(G_2)$ using Tate's series (cf. [13]):

$$\hat{\lambda}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{k=0}^{N-1}\frac{c_k}{4^k} + R(N), \tag{3.3}$$

where

$$c_k = \log|Z(2^kP)|,\ \ Z(Q) = \left(1 + \frac{n}{x(Q)^2}\right)^2 \ \text{ for } Q \in E(\mathbb{Q}) \setminus \{(0,0)\},$$

$$\frac{1}{3\cdot 4^N}\log\left(\frac{(64n^3)^2}{2^{60}H^8}\right) \le R(N) \le \frac{1}{3\cdot 4^N}\log\left(2^{11}H\right), \tag{3.4}$$

with $H = \max\{4n, n^2\}$.

We first compute the finite part $\hat{h}_{\mathrm{fin}}(P)$.

Lemma 3.2. *For any point $P = (a/d^2, b/d^3)$ in $E(\mathbb{Q})$ with $a, b, d \in \mathbb{Z}$, $\gcd(a,d) = \gcd(b,d) = 1$ and $d > 0$, we have*

$$\hat{h}_{\mathrm{fin}}(P) = 2\log d - \frac{1}{2}\log\left(\prod_{p_i|\gcd(a,b,n),\, p_i\ne 2} p_i^{e_i}\right) + \hat{h}_2(P), \tag{3.5}$$

where $p_i^{e_i}\|n$ with $e_i \in \{1,2,3\}$, and $\hat{h}_2(P)$ is given by the following:

- *If d is even, then $\hat{h}_2(P) = 0$.*
- *If d is odd, then the following holds.*

n	a	b	$\hat{h}_2(P)$
even	*odd*	*odd*	0
odd	*even*	*even*	0
odd	*odd*	*even*	$-\frac{1}{2}\log 2$
$v_2(n) = 1$	*even*	*even*	$-\frac{1}{2}\log 2$
$v_2(n) = 2$ *and* $n/4 \equiv 1 \pmod 4$	$v_2(a) = 1$	$v_2(b) \ge 3$	$-\frac{3}{2}\log 2$
$v_2(n) = 2$ *and* $n/4 \equiv 3 \pmod 4$	$v_2(a) = 1$	$v_2(b) = 2$	$-\frac{7}{4}\log 2$
$v_2(n) = 2$	$v_2(a) \ge 2$	$v_2(b) \ge 2$	$-\log 2$
$v_2(n) = 3$	$v_2(a) \ge 3$	$v_2(b) \ge 3$	$-\frac{3}{2}\log 2$

Proof. Since n is fourth-power-free, the equation $y^2 = x^3 - nx$ is global minimal for E, and we may use Silverman's algorithm in [13]. As mentioned at the beginning of this section, the reduction type of E at an odd prime p is III, I_0^* or III^* if respectively $v_p(n) = 1$, 2 or 3. Hence

$$\hat{\lambda}_p(P) = -\frac{1}{4}v_p(\psi_3)\log p,$$

where $\psi_3 = 3a^2(a^2 - 2nd^4) - n^2d^8$. Noting that $b^2 = a(a^2 - nd^4)$, one can see that if p divides a, then $v_p(\psi_3)/4 = v_p(n)/2$, and $\hat{\lambda}_p(P) = -(v_p(P)\log p)/2$. The case $p = 2$ follows also from the algorithm through a case-by-case argument. □

We now bound $\hat{h}(P)$ below for any point P.

Proposition 3.3. *Let n be a positive, fourth-power-free integer and E the elliptic curve given by $y^2 = x^3 - nx$. If $n \not\equiv 12 \pmod{16}$, then*

$$\hat{h}(P) > 0.125 \log n + 0.3917$$

for any non-torsion point P in $E(\mathbb{Q})$.

Proof. Let $P = (a/d^2, b/d^3)$ with $a, b, d \in \mathbb{Z}$, $\gcd(a,d) = \gcd(b,d) = 1$ and $d > 0$. By formula (3.2) and Lemma 3.1,

$$\begin{aligned}\hat{\lambda}_\infty(P) &\geq \frac{1}{16}\log\left(\frac{64n^3}{e^{-2\pi}}\right) + \frac{1}{4}\log\left(\frac{\omega_1 b^2}{2\pi d^6}\right) - \frac{1}{2}\log\frac{1}{1-e^{-2\pi}} \\ &\geq \frac{\pi}{8} - \frac{1}{2}\log\frac{1}{1-e^{-2\pi}} + \frac{1}{8}\log n + \frac{1}{2}\log\left|\frac{b}{d^3}\right| \\ &> 0.3917 + \frac{1}{8}\log n + \frac{1}{2}\log\left|\frac{b}{d^3}\right|.\end{aligned}$$

Combining this inequality with Lemma 3.2, we have

$$\begin{aligned}\hat{h}(P) &> 2\log d - \frac{1}{2}\log\left(\prod_{p_i \mid \gcd(a,b,n),\, p_i \neq 2} p_i^{e_i}\right) + \hat{h}_2(P) \\ &\qquad\qquad + 0.3917 + \frac{1}{8}\log n + \frac{1}{2}\log\left|\frac{b}{d^3}\right| \\ &= 0.125\log n + 0.3917 + \frac{1}{2}\log\frac{|bd|}{\displaystyle\prod_{p_i \mid \gcd(a,b,n),\, p_i \neq 2} p_i^{e_i}} + \hat{h}_2(P).\end{aligned}$$

Here, $b^2 = a(a^2 - nd^4)$ ensures that if $p_i \mid a$ and $p_i^{e_i} \mid n$, then $p_i^{e_i} \mid b$, and the table in Lemma 3.2 implies that if $n \not\equiv 12 \pmod{16}$, then $v_2(b)\log 2 + 2\hat{h}_2(P) \geq 0$. Therefore we have

$$\frac{1}{2}\log\frac{|bd|}{\displaystyle\prod_{p_i \mid \gcd(a,b,n),\, p_i \neq 2} p_i^{e_i}} + \hat{h}_2(P) > 0,$$

and obtain the desired inequality. □

Remarks. (1) Assumption (1.1) immediately implies that $n = st \not\equiv 12 \pmod{16}$. Thus, we can use Proposition 3.3 in the proof of Theorem 1.1.

(2) Finding lower bounds for the canonical height of elliptic curves has been an active area of research. As for our curve E (with n not necessarily positive), Krir showed for any non-torsion point P in $E(\mathbb{Q})$ that $\hat{h}(P) > (\log|n|)/64$ if n is fourth-power-free ([10, Proposition 4.1]), and that $\hat{h}(P) > (\log|n|)/16$ if n is square-free ([10, Remarque 4.2]). Although we are assuming $n > 0$ and $n \not\equiv 12 \pmod{16}$, Proposition 3.3 gives a better bound than Krir's ones.

We use Tate's series to bound $\hat{\lambda}_\infty(G_1)$ and $\hat{\lambda}_\infty(G_2)$ above.

Proposition 3.4. *On the assumptions in Theorem* 1.1*,*

$$\begin{aligned}\hat{h}(G_1) &< \frac{24577}{98304}\log n + \log m + \frac{131081}{196608}\log 2,\\ \hat{h}(G_2) &< \frac{24577}{98304}\log n + \frac{1}{2}\log\left(m^2\left(m^4+1\right)\right) + \frac{32777}{196608}\log 2.\end{aligned}$$

Proof. Since the discriminant $64n^3$ is positive, we have $x(Q) \geq \sqrt{n}$ for $Q \in E^0(\mathbb{R})$, the identity component of $E(\mathbb{R})$. Hence, $1 \leq Z(2^kP) \leq 4$ for $P \in E(\mathbb{Q})$ and a positive integer k. It follows from (3.3) and (3.4) that for $n \geq 4$,

$$\hat{\lambda}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{k=0}^{7}\frac{c_k}{4^k} + R(8),$$

where $c_0 = 2\log(x(P)^2+n) - 4\log|x(P)|$, $0 \leq c_i \leq \log 4$ $(1 \leq i \leq 7)$ and $R(8) \leq (11\log 2 + 2\log n)/(3\cdot 4^8)$. Since $G_1 = (-s, s\alpha)$, $G_2 = (m^2s, ms\beta)$ and $s^2 + n < 2n$, $m^4s^2 + n < (m^4+1)n$, we have

$$\begin{aligned}\hat{\lambda}_\infty(G_1) &< \frac{49153}{98304}\log n + \frac{131081}{196608}\log 2,\\ \hat{\lambda}_\infty(G_2) &< \frac{49153}{98304}\log n + \frac{1}{2}\log\left(m^4+1\right) + \frac{32777}{196608}\log 2.\end{aligned}$$

On the other hand, Lemma 3.2 together with $\sqrt{n} < m^2s$ implies that

$$\hat{h}_{\mathrm{fin}}(G_i) \leq -\frac{1}{2}\log s < -\frac{1}{4}\log n + \log m$$

for $i \in \{1, 2\}$. Therefore, we obtain the desired inequalities. □

4. Proof of Theorem 1.1

In order to prove Theorem 1.1, we need the following theorem of Siksek, based on the theory of quadratic forms (cf. [3]).

Theorem 4.1 (cf. [11, Theorem 3.1])**.** *Let E be an elliptic curve over $\mathbb{Q}$ of rank $r \geq 2$. Let G_1 and G_2 be independent points in $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{\mathrm{tors}}$. Choose a basis $\{P_1, P_2, \ldots, P_r\}$ for $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{\mathrm{tors}}$ such that $G_1, G_2 \in \langle P_1\rangle + \langle P_2\rangle$. Suppose that $E(\mathbb{Q})$ contains no point Q of infinite* *order with* $\hat{h}(Q) \leq \lambda$, *where* λ *is some positive real number. Then, the index* ν *of the span of* G_1 *and* G_2 *in* $\langle P_1 \rangle + \langle P_2 \rangle$ *satisfies*

$$\nu \leq \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{R(G_1, G_2)}}{\lambda},$$

where

$$R(G_1, G_2) = \hat{h}(G_1)\hat{h}(G_2) - \frac{1}{4}\left(\hat{h}(G_1 + G_2) - \hat{h}(G_1) - \hat{h}(G_2)\right)^2.$$

Proof of Theorem 1.1. In view of Proposition 2.2, in order to prove that G_1 and G_2 can be in a system of the generators for $E(\mathbb{Q})$, it suffices to show that the lattice index ν is less than 3. By Proposition 3.3 and the subsequent Remarks (1), we may take $\lambda = 0.125 \log n + 0.3917$. Since $R(G_1, G_2) < \hat{h}(G_1)\hat{h}(G_2)$, Proposition 3.4 and Theorem 4.1 together imply that $\nu < f(m, n)$, where

$$f(m, n) = \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{h_1 h_2}}{0.125 \log n + 0.3917}$$

with

$$\begin{aligned} h_1 &= \frac{24577}{98304} \log n + \log m + \frac{131081}{196608} \log 2, \\ h_2 &= \frac{24577}{98304} \log n + \frac{1}{2} \log(m^6 + m^2) + \frac{32777}{196608} \log 2. \end{aligned}$$

One can see that for a fixed m the function $f(m, n)$ is decreasing. In the case of $m = 2$, if $n \geq 4885$, then $\nu < f(2, n) < 3$. The pairs (s, t) satisfying $n \leq 4884$ and the conditions in Theorem 1.1 are

$$(s, t) = (3, 39),\ (6, 15),\ (6, 87),\ (15, 159),\ (30, 39),\ (51, 87).$$

In each case, it is easy to check (e.g., by Magma ([2])) that G_1 and G_2 can be in a system of generators for $E(\mathbb{Q})$. In fact, in the case of $(s, t) = (15, 159)$, $E(\mathbb{Q}) = \langle (0, 0), G_1, G_2, (-36, 198) \rangle$, and in all other cases, $E(\mathbb{Q}) = \langle (0, 0), G_1, G_2 \rangle$.

In the case of $m = 3$, if $n \geq 1.587 \cdot 10^8$, then $\nu < f(3, n) < 3$. The number of those pairs (s, t) satisfying $n < 1.587 \cdot 10^8$ and the assumptions in Theorem 1.1 is 2493. It is hard to check that G_1 and G_2 can be in a system of generators for $E(\mathbb{Q})$ directly. However, since $f(3, 10) < 5$, we have $f(3, n) < 5$ for all $n \geq 10$. Since $n \leq 9$ is not the case, it follows that $\nu < 5$. On the other hand, Proposition 2.2 implies that $\nu \neq 2, 4$. Hence, it suffices to show that $\nu \neq 3$ for the 2493 pairs (s, t). We confirmed it by checking that none of G_1, G_2, $G_1 + G_2$ and $G_1 - G_2$ has a three division point in $E(\mathbb{Q})$ for each (s, t) using the function "DivisionPoints$(*, 3)$" in Magma ([2]).

In the case of $m \geq 4$, consider the function $g(m) = f(m, m^{26})$. Since $g(m)$ is increasing and

$$\lim_{m\to\infty} g(m) = \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{\left(\frac{24577}{98304}\cdot 26+1\right)\left(\frac{24577}{98304}\cdot 26+3\right)}}{0.125\cdot 26} < 2.9992 < 3,$$

we have $\nu < 3$ for $n \geq m^{26}$. This completes the proof of Theorem 1.1. □

Remark. There is no reason why the assertion in Theorem 1.1 does not hold for $m \geq 4$ and $n < m^{26}$. For example, one can easily see that G_1 and G_2 can always be in a system of generators for $4 \leq m \leq 10$ and $s \leq 30$. Indeed, since $f(10, n) < 7$ for $n \geq 66$ and there is no n with $n \leq 65$ satisfying the assumptions in Theorem 1.1, it suffices to check that

$$G_1, G_2, G_1+G_2, G_1-G_2 \notin 3E(\mathbb{Q}),$$
$$G_1, G_2, G_1+G_2, G_1-G_2, G_1+2G_2, G_1-2G_2, 2G_1+G_2, 2G_1-G_2 \notin 5E(\mathbb{Q}),$$

which can be done by Magma ([2]).

5. Construction of infinite families

By eliminating t from assumption (1.1), we have $(m^4-1)s = \alpha^2+\beta^2$. Putting $\alpha = uk+vl$ and $\beta = ul-vk$ yields

$$s = \frac{\alpha^2+\beta^2}{m^4-1} = \frac{u^2+v^2}{m^4-1}(k^2+l^2) \quad \text{and} \quad t = s+(uk+vl)^2.$$

Hence, u and v satisfying $u^2+v^2 \equiv 0 \pmod{(m^4-1)}$ give a binary form $n = st$ in $\mathbb{Z}[k,l]$. This argument leads us to the following.

Proposition 5.1. *Fix an integer m greater than one and write $m^4-1 = m_0m_1m_2^2$, where m_0, m_1, m_2 are positive integers such that m_0m_1 is square-free and any prime divisor of m_0 (resp. m_1) is congruent to 3 (resp. 1 or 2) modulo 4. Let $p_1, \ldots, p_r$ be distinct primes congruent to 1 or 2 modulo 4 such that none of the odd p_i's divides m^4-1 (possibly $r = 0$. If $m_1 = 1$, assume $r \geq 1$; if $m_1 = p_1 = 2$, assume $r \geq 2$). Let u' and v' be positive integers satisfying*

$$(u')^2 + (v')^2 = m_1p_1\cdots p_r \tag{5.1}$$

and put $u = m_0m_2u'$ and $v = m_0m_2v'$. Then, the binary form $n = st$ with

$$s = \frac{u^2+v^2}{m^4-1}(k^2+l^2) \quad \textit{and} \quad t = s+(uk+vl)^2$$

represents infinitely many integers satisfying the assumptions in Theorem 1.1.

Remarks. (1) Since there exist infinitely many primes congruent to 1 modulo 4, Proposition 5.1 shows that for each integer $m \geq 2$ there exist infinitely many binary forms $n = n(k,l)$ in $\mathbb{Z}[k,l]$ each of which represents infinitely many integers satisfying the assumptions in Theorem 1.1.

(2) A theorem of Granville ([8, Theorem 1]) implies that if *ABC* conjecture is valid, then each expression of $n = st$ for each $m \geq 2$ in Proposition 5.1 satisfies the assumptions in Theorem 1.1 for infinitely many integers k and infinitely many integers l.

Proof. We prove this proposition by applying to n/m_0^2 or $n/(2m_0^2)$ a theorem of Gouvêa and Mazur ([7, Theorem 3]), which implies that if $f(k,l) \in \mathbb{Z}[k,l]$ is a binary form with nonzero discriminant, having no irreducible factor of degree exceeding three, and if the greatest common divisor of all values $f(k,l)$ is square-free, then $f(k,l)$ represents infinitely many square-free integers.

The direct computation shows that the discriminant of n is $16m^4(u^2 + v^2)^{12}/(m^4-1)^8$, which is nonzero. Moreover, since

$$s = m_0 p_1 \cdots p_r (k^2 + l^2), \quad t = s + (uk + vl)^2 \tag{5.2}$$

and $u \equiv v \equiv 0 \pmod{m_0}$, we always have $s/m_0, t/m_0 \in \mathbb{Z}[k,l]$, and if m is odd and $p_i = 2$ for some i, then both u and v must be even and $t/(2m_0) \in \mathbb{Z}[k,l]$. Thus, it suffices to show that if m is odd and $p_i = 2$ for some i, then $\gcd(n; k,l \in \mathbb{Z})$ divides $2m_0^2 p_1 \cdots p_r$; otherwise $\gcd(n; k,l \in \mathbb{Z})$ divides $m_0^2 p_1 \cdots p_r$.

Expressing n and t as $n(k,l)$ and $t(k,l)$, respectively, we see that $\gcd(n; k,l \in \mathbb{Z})$ divides

$$\gcd(n(1,0), n(0,1), n(1,1), n(1,-1)) = m_0 p_1 \cdots p_r t',$$

where $t' = \gcd(t(1,0), t(0,1), 2t(1,1), 2t(1,-1))$. If m is even, then $u^2 + v^2 = m_0(m^4-1)p_1 \cdots p_r$ implies that either u or v must be odd. Since

$$t = \frac{m^4u^2 + v^2}{m^4 - 1}k^2 + 2uvkl + \frac{u^2 + m^4v^2}{m^4 - 1}l^2,$$

either $t(1,0)$ or $t(0,1)$ must be odd. Hence, the 2-primary part $t'_{(2)}$ of t' equals 1. If m is odd, then both u and v must be even, and (5.2) implies that if $p_i = 2$ for some i, then $t'_{(2)} = 2$; otherwise $t'_{(2)} = 1$.

It remains to examine the odd part t'_{odd} of t'. By (5.2) t'_{odd} divides

$$\begin{aligned}\gcd(&m_0 p_1 \cdots p_r + u^2, m_0 p_1 \cdots p_r + v^2,\\ &2m_0 p_1 \cdots p_r + (u+v)^2, 2m_0 p_1 \cdots p_r + (u-v)^2)_{\mathrm{odd}},\end{aligned}$$

which divides

$$\begin{aligned}&\gcd(2m_0 p_1 \cdots p_r + u^2 + v^2, u^2 - v^2, uv)_{\mathrm{odd}}\\ &= \gcd(m_0 p_1 \cdots p_r (m_0 m_1 m_2^2 + 2), m_0^2 m_2^2((u')^2 - (v')^2), m_0^2 m_2^2 u'v')_{\mathrm{odd}},\end{aligned} \tag{5.3}$$

where $\gcd(*)_{\mathrm{odd}}$ denotes the odd part of $\gcd(*)$. By $\gcd(m_1, p_1 \cdots p_r)_{\mathrm{odd}} = 1$ and (5.1) we have $\gcd(u'v', m_1 p_1 \cdots p_r)_{\mathrm{odd}} = 1$, and by

$$\Big((u')^2 - (v')^2\Big)^2 = \Big((u')^2 + (v')^2\Big)^2 - 4(u')^2(v')^2 = m_1^2 p_1^2 \cdots p_r^2 - 4(u')^2(v')^2$$

we have $\gcd\left((u')^2 - (v')^2, u'v'\right)_{\mathrm{odd}} = 1$. Since $\gcd(m_0 m_2, p_1 \cdots p_r)_{\mathrm{odd}} = 1$, (5.3) divides

$$m_0 \gcd(m_0 m_1 m_2^2 + 2, m_0 m_2^2)_{\mathrm{odd}} = m_0,$$

from which it follows that t'_{odd} divides m_0. Since we have already seen that $\gcd(n; k, l \in \mathbb{Z})$ divides $m_0 p_1 \cdots p_r t'$, this completes the proof of Proposition 5.1. □

From Proposition 5.1 one can easily obtain several parameterizations of E in Theorem 1.1.

Example. Let k, l be nonzero integers. For each of the integers s, t expressed in terms of k, l as listed below, the points $G_1 = (-s, s\alpha)$ and $G_2 = (m^2 s, ms\beta)$ with $\alpha = \sqrt{t - s}$, $\beta = \sqrt{m^4 s - t}$ and $m = 2$ or 3 can always be in a system of generators for $E(\mathbb{Q})$ if $s, t, n = st$ are non-square and n is fourth-power-free.

(1) The $m = 2$ cases:
(a) $s = 3(k^2 + l^2)$, $t = 3(4k^2 + 12kl + 13l^2)$;
(b) $s = 6(k^2 + l^2)$, $t = 3(5k^2 + 18kl + 29l^2)$;
(c) $s = 15(k^2 + l^2)$, $t = 3(32k^2 + 72kl + 53l^2)$.

(2) The $m = 3$ cases:
(a) $s = k^2 + l^2$, $t = 17k^2 + 64kl + 65l^2$;
(b) $s = 2(k^2 + l^2)$, $t = 2(9k^2 + 48kl + 73l^2)$;
(c) $s = 5(k^2 + l^2)$, $t = 149k^2 + 384kl + 261l^2$.

Here, we took (u, v) in Proposition 5.1 as follows:

(1) (a) $(u, v) = (3, 6)$; (b) $(u, v) = (3, 9)$; (c) $(u, v) = (9, 12)$.
(2) (a) $(u, v) = (4, 8)$; (b) $(u, v) = (4, 12)$; (c) $(u, v) = (12, 16)$.

Remark. Duquesne's family with $s = 2k^2 - 2k + 1$, $t = 18k^2 + 30k + 17$ is contained in the family with (2) (a) in Example above, since $s = (1 - k)^2 + k^2$, $t = 17(1 - k)^2 + 64(1 - k)k + 65k^2$.

We conclude this paper with a consideration about the rank. Let r be the rank of $E(\mathbb{Q})$, and assume the parity conjecture. Then $(-1)^r = \omega(E)$ holds, where $\omega(E)$ is the sign of the functional equation of $L(E, s)$. If n is fourth-power-free and $n \not\equiv 0 \pmod 4$, then formula (3.1) implies that

$$(-1)^r = -\epsilon(n) \prod_{p^2 || n} \left(\frac{-1}{p}\right),$$

where if $n \equiv 1, 3, 11, 13 \pmod{16}$, $\epsilon(n) = -1$; otherwise, $\epsilon(n) = 1$. Consider the case (1) (a) in Example above. Noting $n \equiv 0 \pmod 9$ and $\left(\frac{-1}{3}\right) = -1$, one can see that if $k \equiv 2 \pmod 4$ and $n/9$ is square-free, then r is odd with $r \geq 3$. Similarly, in the case (2) (a), if $kl \equiv 2 \pmod 4$ and n is square-free, then r is odd with $r \geq 3$. We checked for $1 \leq k, l \leq 30$ by Magma ([2]) that (1) (a) with $k \equiv 2 \pmod 4$ and $n/9$ square-free has 70 cases, out of which 65 cases satisfy $r \geq 3$, and (2) (a) with $kl \equiv 2 \pmod 4$ and n square-free has 107 cases, out of which 81 cases satisfy $r \geq 3$. In either case, it seems difficult to find a third generic point without further parameterizing k, l by quadratic or quartic binary forms.

Acknowledgment. The authors express their sincere thanks to the referee for many valuable suggestions, which, in particular, made the lower bound for n in the case of $m \geq 4$ in Theorem 1.1 better.

References

[1] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group.* Topology **5** (1966), 296–299.

[2] W. Bosma and J. Cannon, *Handbook of magma functions.* Department of Mathematics, University of Sydney, available online at http://magma.maths.usyd.edu.au/magma/.

[3] J. W. S. Cassels, *Introduction to the geometry of numbers.* Springer-Verlag, 1959.

[4] H. Cohen, *A Course in computational algebraic number theory.* Springer-Verlag, 1993.

[5] S. Duquesne, *Elliptic curves associated with simplest quartic fields.* J. Theor. Nombres Bordeaux **19:1** (2007), 81–100.

[6] Y. Fujita and N. Terai, *Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$.* To appear in Tokyo J. Math.

[7] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves.* J. Amer. Math. Soc. **4:1** (1991), 1–23.

[8] A. Granville, *ABC allows us to count squarefrees.* Internat. Math. Res. Notices **19** (1998), 991–1009.

[9] A. W. Knapp, *Elliptic Curves.* Princeton, Princeton Univ. Press, 1992.

[10] M. Krir, *À propos de la conjecture de Lang sur la minoration de la hauteur de Néron-Tate pour les courbes elliptiques sur $\mathbb{Q}$.* Acta Arith. **100** (2001), 1–16.

[11] S. Siksek, *Infinite descent on elliptic curves.* Rocky Mountain J. Math. **25:4** (1995), 1501–1538.

[12] J. H. Silverman, *The arithmetic of elliptic curves.* Springer-Verlag, 1986.

[13] J. H. Silverman, *Computing heights on elliptic curves.* Math. Comp. **51** (1988), 339–358.

[14] J. H. Silverman, *The advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, 1994.

[15] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In Modular Functions of One Variable IV, Lecture Notes in Math. **476**, Springer-Verlag, 1975, 33–52.

Yasutsugu Fujita
College of Industrial Technology
Nihon University
2-11-1 Shin-ei, Narashino, Chiba 275–8576
Japan
E-mail: fujita.yasutsugu@nihon-u.ac.jp

Nobuhiro Terai
Division of General Education
Ashikaga Institute of Technology
268-1 Omae, Ashikaga, Tochigi 326–8558
Japan
E-mail: terai@ashitech.ac.jp