ACTA ARITHMETICA
160.4 (2013)

Generators and integer points on the elliptic curve $y^2 = x^3 - nx$

by

Yasutsugu Fujita (Narashino) and Nobuhiro Terai (Ashikaga)

1. Introduction. Let E be an elliptic curve over the rationals $\mathbb{Q}$. Mordell's theorem asserts that the group $E(\mathbb{Q})$ of rational points on E is finitely generated, and Siegel's theorem states that for a fixed Weierstrass equation defining E, the set of integer points on E is finite. We are interested in determining the generators for $E(\mathbb{Q})$ and the integer points on E for some families of E. More precisely, in this paper, we treat the elliptic curve

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

with a positive integer n, and examine the generators for the rank one or two part of $E(\mathbb{Q})$ and the integer points contained in the group generated by the generators and the torsion points.

First, we consider the case of rank at least one. Let N be a positive integer and E the elliptic curve defined by $y^2 = x^3 - N^2 x$. Then the torsion subgroup $E(\mathbb{Q})_{\rm tors}$ is $\{O, T_1, T_2, T_3\}$, where $T_1 = (-N, 0)$, $T_2 = (0, 0)$ and $T_3 = (N, 0)$. Using height functions and elliptic divisibility sequences, Ingram showed the following.

Theorem 1.1 ([14, Theorem 2]). *Let N be a square-free integer and E the elliptic curve defined by $y^2 = x^3 - N^2 x$. Let P be an integer point on E of infinite order. Then there exists at most one integer $m > 1$ such that mP is integral.*

We apply Theorem 1.1 to give a uniform upper bound for the number of integer points in the rank one case.

Theorem 1.2. *Let N be a square-free integer and E the elliptic curve defined by $y^2 = x^3 - N^2 x$. Let P be a non-torsion point in $E(\mathbb{Q})$ such that the x-coordinate of P is negative. Let Γ be the subgroup of $E(\mathbb{Q})$ generated*

2010 *Mathematics Subject Classification*: Primary 11D25, 11G05, 14G05; Secondary 11G50.
Key words and phrases: elliptic curves, generators, integer points, canonical heights.

DOI: 10.4064/aa160-4-3

by the points P, T_1 and T_2, and let Z be the set of integer points in Γ. Then there exist positive integers m_1, m_2, m_3 with m_1, m_2 odd and m_3 even such that

$$Z \subset \{T_1, T_2, T_3, \pm P, \pm P + T_1, \pm P + T_2, \pm P + T_3, \\ \pm m_1 P + T_1, \pm m_2 P + T_2, \pm m_3 P + T_3\}.$$

In particular, Z has at most 17 points.

Note that without loss of generality we may assume that "the x-coordinate of P is negative". If it is positive, then the x-coordinate of $P + T_2$ is negative and we can replace P by $P + T_2$.

We furthermore examine the congruent number elliptic curve with $N = st(s^2 + t^2)/2$, found by Serf [18].

Theorem 1.3. *Let s and t be positive integers, and assume that the integer $N = st(s^2 + t^2)/2$ is square-free and greater than one. Let E be the elliptic curve defined by $y^2 = x^3 - N^2 x$, and $P = (-s^2t^2, s^2t^2(s^2 - t^2)/2)$ the point in $E(\mathbb{Q})$.*

(1) *The point P can be in a system of generators for $E(\mathbb{Q})$.*
(2) *Let Γ be the subgroup of $E(\mathbb{Q})$ generated by the points P, T_1 and T_2, and let Z be the set of integer points in Γ. Then there exist positive integers m_1 and m_2 with m_1 odd and m_2 even such that*

$$Z \subset \{T_1, T_2, T_3, \pm P, \pm P + T_2, \pm m_1 P + T_2, \pm Q\},$$

where $Q \in \{P + T_1, m_2 P + T_3\}$. Moreover, if $|s - t| = 1$, then $Z = \{T_1, T_2, T_3, \pm P, \pm P + T_1\}$.

Theorem 1.3 implies the following.

Corollary 1.4. *Let s and t be positive integers, and N the square-free integer, greater than one, of the form either*

$$\text{(i) } N = \tfrac{1}{2}(s^4 + t^4) \quad \textit{or} \quad \text{(ii) } N = s^4 + 4t^4.$$

Let E be the elliptic curve defined by $y^2 = x^3 - N^2 x$, and P the point on E of the form either

$$\text{(i) } P = \left(-s^2t^2, \tfrac{1}{2}st(s^4 - t^4)\right) \quad \textit{or} \quad \text{(ii) } P = (-4s^2t^2, 2st(s^4 - 4t^4)),$$

respectively.

(1) *The point P can be in a system of generators for $E(\mathbb{Q})$.*
(2) *Let Γ be the subgroup of $E(\mathbb{Q})$ generated by the points P, T_1 and T_2, and let Z be the set of integer points in Γ. Then:*

- *If* (i) *$N = (s^4 + t^4)/2$, then $Z = \{T_1, T_2, T_3, \pm P\}$.*

- *If* (ii) $N = s^4 + 4t^4$, *then either* $Z = \{T_1, T_2, T_3, \pm P\}$ *or* $Z = \{T_1, T_2, T_3, \pm P, \pm P + T_1\}$; *the latter case occurs if and only if* $|s^2 - 2t^2| = 1$.

Secondly, consider the case of rank at least two. Let $n = s^4 + t^4$ with distinct positive integers s, t and let E be the elliptic curve defined by $y^2 = x^3 - nx$. Then the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is $\{O, T\}$, where $T = (0, 0)$. In the case where n is prime, Spearman [24] proved that the rank of $E(\mathbb{Q})$ is exactly two, and the authors [10] showed that the points $P_1 = (-t^2, s^2 t)$ and $P_2 = (-s^2, st^2)$ are independent modulo $E(\mathbb{Q})_{\mathrm{tors}}$, and that if $t = 1$, then the set of integer points on E is $\{T, \pm P_1, \pm P_2, \pm P_1 + T\}$. The third theorem in the present paper is a generalization of these results.

Theorem 1.5. *Let s and t be positive integers with $s > t$ and put $n = s^4 + t^4$. Let E be the elliptic curve defined by $y^2 = x^3 - nx$, and let $P_1 = (-t^2, s^2 t)$ and $P_2(-s^2, st^2)$ be the points in $E(\mathbb{Q})$.*

(1) *If n is fourth-power-free, then the points P_1 and P_2 can be in a system of generators for $E(\mathbb{Q})$.*

(2) *Assume that n is square-free. Let Γ be the subgroup of $E(\mathbb{Q})$ generated by the points T, P_1 and P_2, and let Z be the set of integer points in Γ. Then there exist coprime integers m_1 and m_2 with $m_1 \not\equiv m_2 \pmod 2$ such that*

$$Z \subset \{T, \pm P_1, \pm P_2, \pm(P_1 - P_2), \pm(m_1 P_1 + m_2 P_2) + T\}.$$

Moreover, if $n = s^4 + 1 > 17$, then $Z = \{T, \pm P_1, \pm P_2, \pm P_1 + T\}$.

Remark 1.6.

(1) For the curve E in Theorem 1.5(1), if n is a prime number, then the rank of $E(\mathbb{Q})$ is two by the theorem in [24]. Therefore, $E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})T + \mathbb{Z}P_1 + \mathbb{Z}P_2$ for n prime.

(2) In Theorem 1.5(2), $\pm(P_1 - P_2) \in Z$ if and only if $t = s - 1$, since $x(P_1 - P_2) = (s^2 - st + t^2)^2/(s - t)^2$.

(3) If $n = 2^4 + 1^4 = 17$ in Theorem 1.5, then the set Z has exactly nine elements:

$$\begin{aligned} Z &= \{T, \pm P_1, \pm P_2, \pm(P_1 - P_2), \pm P_1 + T\} \\ &= \{(0,0), (-1, \pm 4), (-4, \pm 2), (9, \pm 24), (17, \pm 68)\}. \end{aligned}$$

It is to be mentioned that Duquesne [8, 9] determined the generators and the integer points on some parameterized elliptic curves assuming rank $E(\mathbb{Q})$ $= 1$ or 2, where the main tool is "height functions". Our strategy common to the proofs concerning integer points is to combine "computing height functions" and "considering integer points modulo $2E(\mathbb{Q})$". As far as we know, the latter was used to examine integer points on elliptic curves first by Dujella and Pethő [7], who showed the following: Let $\{c_k\}$ be the recurrence sequence defined by $c_1 = 8$, $c_2 = 120$, $c_{k+2} = 14c_{k+1} - c_k + 8$ $(k \geq 1)$ and E the elliptic curve defined by $y^2 = (x+1)(3x+1)(c_k x+1)$. Assume that the rank of $E(\mathbb{Q})$ is two. Then the integer points on E are $(-1,0)$, $(0,\pm 1)$, $(c_{k-1}, \pm s_{k-1}t_{k-1}(2c_k - s_k t_k))$, $(c_{k+1}, \pm s_{k+1}t_{k+1}(2c_k + s_k t_k))$, where s_k and t_k are positive integers defined by $c_k + 1 = s_k^2$ and $3c_k + 1 = t_k^2$, respectively. Note that $\{1, 3, c_k\}$ is a *Diophantine triple*, which means that both $c_k + 1$ and $3c_k + 1$ are perfect squares.

In the rank one case, the following fact also plays an important role in examining integer points (see [20, Exercise 9.12]), which will be frequently used in Section 4:

FACT. *If a point Q in $E(\mathbb{Q})$ is not integral* (*with respect to a Weierstrass equation for E*), *then neither is mQ for any positive integer m.*

We now fix the notation. Let E be an elliptic curve defined by $y^2 = x^3 - nx$ with a positive integer n. In the case where $n = N^2$ for some positive integer N, let $T_1 = (-N, 0)$, $T_2 = (0,0)$ and $T_3 = (N, 0)$ be the 2-torsion points, and in the case where n is non-square, let $T = (0,0)$ be the 2-torsion point in $E(\mathbb{Q})$. Denote by $x(Q)$ the x-coordinate of a point Q on E. For Q in $E(\mathbb{Q})$ with $x(Q) = a/b$ and $\gcd(a,b) = 1$, the *naïve height* $h : E(\mathbb{Q}) \to \mathbb{R}$ is defined by $h(Q) = \log\max\{|a|, |b|\}$. The *canonical height* $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is defined by

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

(note that this value is the same as defined in [3, 9] and is double that of [20, 21, 5]). The canonical height has a decomposition into local heights:

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

We normalize the symbols $\hat{\lambda}_p$ following [9] (which are double the definitions in [5], and satisfy $\hat{\lambda}_p = 2(\hat{\lambda}'_p + \log|\Delta|_p/12)$, where $\hat{\lambda}'_p$ denote the local heights defined in [21, 22]). By $E(\mathbb{R})^0$ we denote the identity component of $E(\mathbb{R})$. Finally, $\square$ denotes the square of a rational number.

2. Preliminary results on Diophantine equations. In this section, we quote the results on Diophantine equations that are crucial to the proofs of our results.

LEMMA 2.1 (cf. [25, Theorems 1, 2]). *Let d be a positive integer. The system of simultaneous Pell equations*

$$X^2 - dY^2 = 1, \qquad Z^2 - 2dY^2 = 1$$

has at most one solution in positive integers. Moreover, if the system has a positive integer solution, then there exists a prime divisor p of d such that $p \equiv 3 \pmod 4$.

LEMMA 2.2 (cf. [6, Theorem]; see also [16]). *Let d be a positive integer. If $d \neq 1785$, then the Diophantine equation*

$$X^4 - dY^2 = 1$$

has at most one solution in positive integers. In the case where $d = 1785$, it has exactly two positive integer solutions $(X, Y) = (13, 4)$, $(239, 1352)$.

LEMMA 2.3 (cf. [4, Theorem D]). *Let d be an integer greater than two. Then the Diophantine equation*

$$X^2 - dY^4 = -1$$

has at most one solution in positive integers.

3. Proof of Theorem 1.2. By the following lemma, considering integer points P modulo $2E(\mathbb{Q})$ reduces to considering $x(P)$ modulo squares.

LEMMA 3.1 ([15, Proposition 4.6]). *Let $\{\delta_1, \delta_2, \delta_3\} = \{-N, 0, N\}$. Then the map $\varphi : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ defined by*

$$\varphi(X) = \begin{cases} (x+\delta_1)(\mathbb{Q}^\times)^2 & \text{if } X = (x, y) \neq O, (-\delta_1, 0), \\ (\delta_2 - \delta_1)(\delta_3 - \delta_1)(\mathbb{Q}^\times)^2 & \text{if } X = (-\delta_1, 0), \\ (\mathbb{Q}^\times)^2 & \text{if } X = O \end{cases}$$

is a group homomorphism.

Proof of Theorem 1.2. Let $X = (x, y)$ be an integer point in Γ. Then we have $X \equiv X_1 \pmod{2\Gamma}$, where

$$X_1 \in \{O, T_1, T_2, T_3, P, P+T_1, P+T_2, P+T_3\}.$$

Suppose that $X_1 = O$. Then we see from Lemma 3.1 that there exist positive integers x_0, A, B such that

$$x = x_0^2, \quad x + N = A^2, \quad x - N = B^2,$$

yielding $A^2 + B^2 = 2x_0^2$. The solutions of this Diophantine equation have the form

$$x_0 = k(\alpha^2 + \beta^2), \quad A = k(\alpha^2 - \beta^2 + 2\alpha\beta), \quad B = k(\alpha^2 - \beta^2 - 2\alpha\beta)$$

for some integers k, α, β. Hence,

$$N = A^2 - x_0^2 = k^2(\alpha^2 - \beta^2 + 2\alpha\beta)^2 - k^2(\alpha^2 + \beta^2)^2 = 4k^2\alpha\beta(\alpha^2 - \beta^2),$$

which contradicts the square-freeness of N. Therefore, we obtain $X_1 \neq O$.

If $X_1 = T_1$, then by Lemma 3.1 we have $x = -Nx_0^2$ and $x + N = 2\square$ for some positive integer x_0, which together with the square-freeness of N implies $-x_0^2 + 1 = 2N\square$. This shows that $x_0 = 1$ and $X = T_1$.

If $X_1 = T_2$, then we have $x = -x_0^2$ and $x + N = N\square$ for some non-negative integer x_0, which gives $-Nx_1^2 + 1 = \square$ for some non-negative integer x_1. Hence, $x_1 = x_0 = 0$ and $X = T_2$.

Suppose that $X_1 = T_3$. Then $x = Nx_0^2$, $x - N = 2\square$ and $x + N = 2N\square$ for some positive integer x_0, which implies that there exist non-negative integers α and β such that

$$x_0^2 - 2N\alpha^2 = 1, \quad \beta^2 - N\alpha^2 = 1. \tag{3.1}$$

By Lemma 2.1, there exists a positive integer m_3 such that $X = T_3$ or $X = \pm m_3 P + T_3$, where m_3 must be even, since $X \equiv T_3 \pmod{2\Gamma}$.

Suppose that $X_1 = P + T_i$ ($i \in \{1,2\}$). If $P + T_i$ is not integral, then neither is $mP + T_i$ for any odd integer m. Hence, $X_1 \neq P + T_i$. If $P + T_i$ is integral, then Theorem 1.1 implies that there exists at most one integer $m_i > 1$ such that $m_i P + T_i$ is integral. Hence, $X = \pm P + T_i$ or $X = \pm m_i P + T_i$, where m_i must be odd, since $X \equiv P + T_i \pmod{2\Gamma}$.

Finally, suppose that $X_1 = P$ or $X_1 = P + T_3$. Then since $X_1 \notin E(\mathbb{R})^0$ and hence $X \notin E(\mathbb{R})^0$, by Lemma 4.2 in [2] we know that if $X = mP + T$ for $m \in \mathbb{Z}$ and $T \in E(\mathbb{Q})_{\mathrm{tors}}$, then $|m| \leq 2$. Thus, we obtain $m = \pm 1$ and $X = \pm P$ or $X = \pm P + T_3$, respectively. This completes the proof of Theorem 1.2. ■

Remark 3.2. It is not difficult to give those examples where Z contains 13 points. Let a, b, c be a relatively prime Pythagorean triple with $a^2 + b^2 = c^2$ and put $N = ab/2$. Then the elliptic curve $E : y^2 = x^3 - N^2 x$ has the following integer points:

$$T_1,\ T_2,\ T_3,\ \pm P,\ \pm P + T_1,\ \pm P + T_2,\ \pm P + T_3,$$

where $P = (-a(c-a)/2, a^2(c-a)/2)$. Since the denominator of $x(2P + T_3)$ is $(a-b)^2$, we see that $2P + T_3 \in Z$ if and only if $|a - b| = 1$. In this case, $a^2 + (a \pm 1)^2 = c^2$ shows that

$$(2a \pm 1)^2 - 2c^2 = -1.$$

Hence, one can assert the following:

Let u, v be positive integers satisfying $u^2 - 2v^2 = -1$. Put $N = (u^2 - 1)/8$ and $P = (-a(c-a)/2, a^2(c-a)/2)$. Then

$$Z \supset \{T_1,\ T_2,\ T_3,\ \pm P,\ \pm P + T_1,\ \pm P + T_2,\ \pm P + T_3,\ \pm 2P + T_3\}.$$

For example, if $N = 6$ and $P = (-3, 9)$ with $u = 7$ and $v = 5$, then the rank of $E(\mathbb{Q})$ is one and Z is exactly the set of 13 points above.

On the other hand, we could not find any integer point of the form $m_1 P + T_1$ or $m_2 P + T_2$ with odd integers m_1, m_2 greater than one. We checked by Magma [1] that if $N < 10^{10}$ and $3 \leq m_i \leq 19$ ($i \in \{1,2\}$), then $m_i P + T_i$ cannot be integral, which leads us to conjecture that Z has at most 13 points.

4. Proof of Theorem 1.3. We consider the elliptic curve $E : y^2 = x^3 - nx$ for general n for the moment. Let $\overline{E}$ be the elliptic curve defined by

$y^2 = x^3 + 4nx$ and $\psi : \overline{E} \to E$ the isogeny defined by

$$(\bar{x}, \bar{y}) \mapsto \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{(\bar{x}^2 - 4n)\bar{y}}{8\bar{x}^2} \right).$$

The following lemma is an immediate consequence of (iii) in [23, p. 83] and its proof.

LEMMA 4.1. *Let $Q \neq O$ be a point in $E(\mathbb{Q})$.*

(1) *$Q \in \psi(\overline{E}(\mathbb{Q}))$ if and only if $x(Q)$ is a square. In this case, putting $Q = (x, y)$ with $x = x_0^2$, one can express $\overline{Q} \in \overline{E}(\mathbb{Q})$ with $\psi(\overline{Q}) = Q$ as*

$$\overline{Q} = \left(2\left(x_0^2 \pm \frac{y}{x_0} \right), \pm 2x_0 x(\overline{Q}) \right),$$

where the signs are taken simultaneously.

(2) *$Q \in 2E(\mathbb{Q})$ if and only if both $x(Q)$ and $x(\overline{Q})$ are squares for some $\overline{Q} \in \overline{E}(\mathbb{Q})$ with $\psi(\overline{Q}) = Q$.*

We here quote the results of [11] on the computation of the non-Archimedean part $\hat{h}_{\mathrm{fin}}$ of the canonical height $\hat{h}$ and a uniform lower bound for $\hat{h}$ of a non-torsion point.

LEMMA 4.2 ([11, Lemma 3.1]). *Assume that n is fourth-power-free. For any point $Q = (\alpha/\delta^2, \beta/\delta^3)$ in $E(\mathbb{Q})$ with $\alpha, \beta, \delta \in \mathbb{Z}$, $\gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1$ and $\delta > 0$, we have*

$$\hat{h}_{\mathrm{fin}}(Q) = 2 \log \delta - \frac{1}{2} \log\Big(\prod_{p_i \mid \alpha, \beta, n,\, p_i \neq 2} p_i^{e_i} \Big) + \hat{h}_2(Q), \tag{4.1}$$

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

- *If δ is even, then $\hat{h}_2(Q) = 0$.*
- *If δ is odd, then for v_2 denoting the valuation on $\mathbb{Q}$ normalized by $v_2(2) = 1$:*

n	α	β	$\hat{h}_2(Q)$
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* $n/4 \equiv 1 \pmod 4$	$v_2(\alpha) = 1$	$v_2(\beta) \geq 3$	$-\frac{3}{2}\log 2$
$v_2(n) = 2$ *and* $n/4 \equiv 3 \pmod 4$	$v_2(\alpha) = 1$	$v_2(\beta) = 2$	$-\frac{7}{4}\log 2$
$v_2(n) = 2$	$v_2(\alpha) \geq 2$	$v_2(\beta) \geq 2$	$-\log 2$
$v_2(n) = 3$	$v_2(\alpha) \geq 3$	$v_2(\beta) \geq 3$	$-\frac{3}{2}\log 2$

Lemma 4.3 ([11, Proposition 3.3]). *Assume that n is fourth-power-free. If $n \not\equiv 12 \pmod{16}$, then*

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

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

Remark 4.4.

(1) If n is fourth-power-free, then the equation $y^2 = x^3 - nx$ is globally minimal and we may apply Silverman's algorithm [21, Theorem 5.2] to compute $\hat{h}_{\mathrm{fin}}$. That is why we assume that n is fourth-power-free in Lemmas 4.2 and 4.3.

(2) If n has the form $n = N^2$ or $n = s^4 + t^4$ for some integers N, s, t, then $n \not\equiv 12 \pmod{16}$, and we have the inequality in Lemma 4.3.

We estimate the Archimedean part $\hat{\lambda}_\infty$ of the canonical height of a specific point using Tate's series (see [21]):

$$\hat{\lambda}_\infty(Q) = \log|x(Q)| + \frac{1}{4}\sum_{k=0}^{\infty} \frac{c_k(Q)}{4^k}, \tag{4.2}$$

where $c_k(Q) = \log(1 + n/x(2^kQ)^2)^2$ for $Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$. Note that the series converges for any $Q \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$, since $2^kQ \in E(\mathbb{R})^0$ and $x(2^kQ) \geq \sqrt{n}$ for all positive integers k.

We now restrict ourselves to the case $n = N^2$ and let $N = st(s^2 + t^2)/2 \geq 5$ be square-free with positive integers s and t. Then the elliptic curve $E : y^2 = x^3 - N^2x$ has the rational point $P = (-s^2t^2, s^2t^2(s^2 - t^2)/2)$ of infinite order, and we have

$$x(P + T_1) = \frac{N(s+t)^2}{(s-t)^2}, \quad x(P + T_2) = \frac{(s^2+t^2)^2}{4}, \quad x(P + T_3) = -\frac{N(s-t)^2}{(s+t)^2}.$$

Lemma 4.5. *$T_1, T_2, T_3, P, P + T_1, P + T_2, P + T_3 \notin 2E(\mathbb{Q})$.*

Proof. Since $E(\mathbb{Q})_{\mathrm{tors}} = \{O, T_1, T_2, T_3\}$, it is clear that $T_1, T_2, T_3 \notin 2E(\mathbb{Q})$. It is also clear that $P, P + T_3 \notin 2E(\mathbb{Q})$, since they are not in $E(\mathbb{R})^0$. From $x(P + T_1) = N\square$, the square-freeness of N and Lemma 3.1, we see that $P + T_1 \notin 2E(\mathbb{Q})$.

It remains to check the point $P + T_2$. Since $x(P + T_2) = \square$, Lemma 4.1(1) implies that $P + T_2$ is in the image of $\overline{E}(\mathbb{Q})$ under ψ, and that any point $\overline{P} \in \overline{E}(\mathbb{Q})$ with $\psi(\overline{P}) = P + T_2$ satisfies either $x(\overline{P}) = s^2(s^2 + t^2)$ or $x(\overline{P}) = t^2(s^2 + t^2)$. Since $N = st(s^2 + t^2)/2$ is square-free, $x(\overline{P})$ cannot be a square. It follows from Lemma 4.1(2) that $P + T_2 \notin 2E(\mathbb{Q})$. ∎

Lemma 4.6. *$\hat{h}(P) < 0.667 \log N + 0.463$.*

Proof. Since $\gcd(st, s^2 + t^2) = 1$ and $s^3t^3 > N$, Lemma 4.2 implies that

$$\hat{h}_{\mathrm{fin}}(P) = -\log(st) + \hat{h}_2(P) < -\tfrac{1}{3}\log N.$$

Moreover, by (4.2),

$$\begin{aligned}\hat{\lambda}_\infty &\le \tfrac{1}{2}\log(x(P)^2+N^2)+\tfrac{1}{4}\sum_{k=1}^{\infty}\frac{1}{4^k}\cdot 2\log\biggl(1+\frac{N^2}{x(2^kP)^2}\biggr)\\ &\le \tfrac{1}{2}\log(2N^2)+\tfrac{1}{6}\log 2=\log N+\tfrac{2}{3}\log 2.\end{aligned}$$

The assertion now follows immediately from the equality $\hat{h}(P)=\hat{h}_{\mathrm{fin}}(P)+\hat{\lambda}_\infty(P)$. ∎

Proof of Theorem 1.3. (1) Suppose that $P+T=mQ$ for some points $Q\in E(\mathbb{Q})$, $T\in E(\mathbb{Q})_{\mathrm{tors}}$ and some integer $m\ge 2$. By the basic property of the canonical height and Lemma 4.3,

$$\hat{h}(P)=\hat{h}(mQ)=m^2\hat{h}(Q)>0.25m^2\log N+0.3917,$$

which together with Lemma 4.6 implies that

$$(m^2-2.668)\log N<0.282.$$

Since $m\ge 3$ by Lemma 4.5, we obtain $N<e^{0.05}<1.1$, which contradicts $N\ge 5$. Therefore, $P+T$ does not have an m-division point in $E(\mathbb{Q})$ for any $T\in E(\mathbb{Q})_{\mathrm{tors}}$ and $m\ge 2$, which means that P can be in a system of generators for $E(\mathbb{Q})$.

(2) Let $X=(x,y)$ be a point in Z. We see from (1) that $X\equiv X_1 \pmod{2\Gamma}$, where

$$X_1\in\{O,T_1,T_2,T_3,P,P+T_1,P+T_2,P+T_3\}.$$

We have already seen in the proof of Theorem 1.2 that $X_1\ne O$, and that if $X_1\in\{T_1,T_2,P,P+T_3\}$, then $X=\pm X_1$. Suppose that $X_1=P+T_2$. If $P+T_2\notin Z$, then $mP+T_2\notin Z$ for any odd integer m. Hence, $X_1\ne P+T_2$. If $P+T_2\in Z$, then Theorem 1.1 implies that there exists at most one positive integer m_1 such that $X=\pm P+T_2$ or $X=\pm m_1P+T_2$. Note that $P+T_2\in Z$ if and only if both s and t are odd.

Suppose that $X_1=T_3$ or $X_1=P+T_1$. By Lemma 3.1 we have $x=Nx_0^2$ for some positive integer x_0. Since N is square-free, substituting this into $y^2=x^3-N^2x$, we obtain

$$x_0^4-Ny_0^2=1 \tag{4.3}$$

with some non-negative integer y_0. In the case where $N\ne 1785$, the Diophantine equation (4.3) has at most one positive solution by Lemma 2.2. If $P+T_1\notin Z$, then $mP+T_1\notin Z$ for any odd integer m. Hence, $X_1\ne P+T_1$ and thus there exists a positive even integer m_2 such that $X=T_3$ or $X=\pm m_2P+T_3$. If $P+T_1\in Z$, then $x_0=|(s+t)/(s-t)|$ is the solution of (4.3) and hence $X=T_3$ or $X=\pm P+T_1$, respectively. Note that $P+T_1\in Z$ if and only if $|s-t|\in\{1,2\}$. In the case where $N=1785$, we have $(s,t) = (6,7)$ or $(7,6)$, and $x_0 = 13$ or 239. The value $x_0 = 13$ corresponds to the point $P+T_1$, but $x_0 = 239$ does not give a point in Z, since by Lemma 3.1, $x_0^2+1 = 2(s^2+t^2)\square = 170\square$, which does not hold for $x_0 = 239$. Therefore, if $N = 1785$, then $X = T_3$ or $X = \pm P + T_1$, respectively.

In particular, in the case where $|s-t| = 1$, we have $P + T_2 \notin Z$ and $P + T_1 \in Z$, and thus the set Z is completely determined as in the second assertion of (2). ■

Remark 4.7. The proof of Theorem 1.3(2) implies that both $P + T_1$ and $P + T_2$ are integral if and only if $|s-t| = 2$ with s,t odd. In this case, we have

$$Z \supset \{T_1, T_2, T_3, \pm P, \pm P + T_1, \pm P + T_2\}.$$

For example, if $N = 15$ and $P = (-9, 36)$ with $s = 3$ and $t = 1$, then the rank of $E(\mathbb{Q})$ is one and Z is exactly the set of nine points above. We checked by Magma [1] that if $N < 10^{10}$ and $3 \le m_1 \le 19$, then $m_1 P + T_2$ cannot be integral, which leads us to conjecture that Z has at most nine points.

Proof of Corollary 1.4. (1) Substituting s and t in Theorem 1.3 for s^2 and (i) t^2 or (ii) $2t^2$, respectively, we have the isomorphism from E in Theorem 1.3 to E in Corollary 1.4 defined by

$$(x,y) \mapsto \left(\frac{x}{s^2t^2}, \frac{y}{s^3t^3}\right),$$

by means of which P in Theorem 1.3 corresponds to P in Corollary 1.4. The assertion follows immediately from Theorem 1.3.

(2) Let $X = (x,y) \in Z$. By (1) we have $X \equiv X_1 \pmod{2\varGamma}$, where $X_1 \in \{O, T_1, T_2, T_3, P, P+T_1, P+T_2, P+T_3\}$. All we have to do is to check the cases where $X_1 \in \{T_3, P+T_1, P+T_2\}$. Since

$$x(P+T_2) = \begin{cases} \dfrac{N^2}{s^2t^2} & \text{in (i)}, \\ \dfrac{N^2}{4s^2t^2} & \text{in (ii)}, \end{cases}$$

$P+T_2$ cannot be integral. Hence, $X_1 \ne P+T_2$. Moreover, in the case of (i), since $x(P+T_1) = N(s^2+t^2)^2/(s^2-t^2)^2$, $P+T_1$ cannot be integral, whence $X_1 \ne P+T_1$. In the case of (ii), since $x(P+T_1) = N(s^2+2t^2)^2/(s^2-2t^2)^2$, if $|s^2-2t^2| \ne 1$, then $X_1 \ne P+T_1$; if $|s^2-2t^2| = 1$, then we see from Theorem 1.3 that $X_1 = P+T_1$ means $X = P+T_1$.

Suppose that $X_1 = T_3$. As seen in the proof of Theorem 1.2, we have the simultaneous Pell equations (3.1). By Lemma 2.1, if (3.1) has a positive solution, then N has a prime divisor p_0 satisfying $p_0 \equiv 3 \pmod 4$. On the other hand, since $N = (s^4+t^4)/2$ or s^4+4t^4 and N is square-free, we see that any odd prime divisor p of N satisfies $p \equiv 1 \pmod 4$. This contradiction shows that $x_0 = 1$ and $X = T_3$. ∎

5. Proof of Theorem 1.5. Throughout this section, let s, t be positive integers with $s > t$, and let $n = s^4 + t^4$. We begin by proving the independence of the points $P_1 = (-t^2, s^2t)$ and $P_2 = (-s^2, st^2)$.

LEMMA 5.1. $P_1, P_2, P_1 + T, P_2 + T, P_1 + P_2, P_1 + P_2 + T \notin 2E(\mathbb{Q})$. *Thus P_1 and P_2 are independent modulo $E(\mathbb{Q})_{\mathrm{tors}}$.*

Proof. It is obvious that $T, P_1, P_2, P_1 + P_2 + T \notin 2E(\mathbb{Q})$, since they are not in $E(\mathbb{R})^0$. Moreover, since

$$P_1 + T = \left(\frac{n}{t^2}, \frac{ns^2}{t^3}\right), \qquad P_2 + T = \left(\frac{n}{s^2}, \frac{nt^2}{s^3}\right),$$

and $n = s^4 + t^4 \neq \square$, we also have $P_1 + T, P_2 + T \notin 2E(\mathbb{Q})$.

It remains to check the point $P_1 + P_2$. Since

$$P_1 + P_2 = \left(\frac{(s^2 + st + t^2)^2}{(s+t)^2}, -\frac{st(s^2 + st + t^2)(2s^2 + 3st + 2t^2)}{(s+t)^3}\right),$$

Lemma 4.1(1) implies that $P_1 + P_2$ is in the image of $\overline{E}(\mathbb{Q})$ under ψ, and that any point $\overline{P} \in \overline{E}(\mathbb{Q})$ with $\psi(\overline{P}) = P + T_2$ satisfies either $x(\overline{P}) = 2n/(s+t)^2$ or $x(\overline{P}) = 2(s+t)^2$. Since $n = s^4 + t^4 \neq 2\square$, it follows from Lemma 4.1(2) that $P_1 + P_2 \notin 2E(\mathbb{Q})$. ∎

The following theorem, due to Siksek, is a key to proving that the independent points P_1 and P_2 can be in a system of generators for $E(\mathbb{Q})$.

THEOREM 5.2 (cf. [19, Theorem 3.1]). *Let E be an elliptic curve over $\mathbb{Q}$ of rank $r \geq 2$. Let P_1 and P_2 be independent points in $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{\mathrm{tors}}$. Choose a basis $\{G_1, G_2, \ldots, G_r\}$ for $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{\mathrm{tors}}$ such that $P_1, P_2 \in \mathbb{Z}G_1 + \mathbb{Z}G_2$. 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 P_1 and P_2 in $\mathbb{Z}G_1 + \mathbb{Z}G_2$ satisfies*

$$\nu \leq \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{R(P_1, P_2)}}{\lambda},$$

where

$$R(P_1, P_2) = \hat{h}(P_1)\hat{h}(P_2) - \tfrac{1}{4}(\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2.$$

LEMMA 5.3.

$$0.5 \log n - 0.347 < \hat{h}(P_i) < 0.5 \log n + 0.463$$

for $i \in \{1,2\}$, *and*

$$\log n < \hat{h}(P_1 + P_2) < \log n + 1.864,$$
$$\log n - 1.04 < \hat{h}(P_1 - P_2) < \log n + 0.463.$$

Proof. It is easy to see from Lemma 4.2 that

$$-\tfrac{1}{2}\log 2 \le \hat{h}_{\mathrm{fin}}(P_i) = \hat{h}_2(P_i) \le 0$$

and from (4.2) that

$$0 \le \hat{\lambda}_\infty(P_i) - \tfrac{1}{2}\log(x(P_i)^2 + n) \le \tfrac{1}{6}\log 2.$$

Since $n < x(P_i)^2 + n < 2n$, we have

$$\tfrac{1}{2}\log n < \hat{\lambda}_\infty(P_i) < \tfrac{1}{2}\log n + \tfrac{2}{3}\log 2.$$

Hence, we obtain

$$0.5\log n - 0.347 < \hat{h}(P_i) < 0.5\log n + 0.463.$$

Let us compute $\hat{h}(P_1 \pm P_2)$. Since

$$x(P_1 \pm P_2) = (s^2 \pm st + t^2)^2/(s \pm t)^2$$

is odd and

$$\gcd(s \pm t, s^2 \pm st + t^2) = \gcd(s \pm t, t^2) = 1,$$

we see from Lemma 4.2 that

$$\hat{h}_{\mathrm{fin}}(P_1 \pm P_2) = \log(s \pm t)^2 + \hat{h}_2(P_1 \pm P_2)$$

and $-(\log 2)/2 \le \hat{h}_2(P_1 \pm P_2) \le 0$. Moreover, (4.2) implies that

$$0 \le \hat{\lambda}_\infty(P_1 \pm P_2) - \tfrac{1}{2}\log\left(\frac{(s^2 \pm st + t^2)^4}{(s \pm t)^4} + n\right) \le \tfrac{1}{6}\log 2.$$

Hence, we obtain

$$\tfrac{1}{2}\log A_\pm - \tfrac{1}{2}\log 2 \le \hat{h}(P_1 \pm P_2) \le \tfrac{1}{2}\log A_\pm + \tfrac{1}{6}\log 2,$$

where

$$A_\pm = (s^2 \pm st + t^2)^4 + (s \pm t)^4 n$$

and the signs are taken simultaneously. Now, since

$$5n - (s^2 + st + t^2)^2 = (s^2 - st + t^2)^2 + 3(s^2 - t^2)^2 > 0,$$
$$8n - (s + t)^4 = (s - t)^4 + 6(s^2 - t^2)^2 > 0,$$

we have $2n^2 < A_+ < 33n^2$. Hence, we obtain

$$\log n \le \hat{h}(P_1 + P_2) < \log n + 1.864.$$

Moreover, since $n/2 < (s^2 - st + t^2)^2 < n$ and $0 < (s - t)^4 < n$, we have $n^2/4 < A_- < 2n^2$, which shows that

$$\log n - 1.04 < \hat{h}(P_1 - P_2) < \log n + 0.463. \blacksquare$$

Proof of Theorem 1.5(1). By Lemmas 4.3 and 5.3, we have

$$\nu < \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{\hat{h}(P_1)\hat{h}(P_2)}}{c} < \frac{2}{\sqrt{3}} \cdot \frac{0.5\log n + 0.463}{0.125\log n + 0.3917} < \frac{2}{\sqrt{3}} \cdot \frac{0.5}{0.125} < 4.7.$$

Since we already know by Lemma 5.1 that ν is odd, it suffices to show that $\nu \neq 3$, which is equivalent to

$$P_1, P_2, P_1 + P_2, P_1 - P_2 \notin 3E(\mathbb{Q}).$$

Suppose that $P \in 3E(\mathbb{Q})$ for some $P \in \{P_1, P_2, P_1 + P_2, P_1 - P_2\}$. Letting $P = 3Q$ for $Q \in E(\mathbb{Q})$, we see from Lemma 4.3 that

$$\hat{h}(P) = \hat{h}(3Q) = 9\hat{h}(Q) > 1.125\log n.$$

On the other hand, Lemma 5.3 implies that $\hat{h}(P) < \log n + 1.864$. Thus, we have $n < 3.0 \cdot 10^6$. For n in this range, one can easily check by using Magma [1] that $P \notin 3E(\mathbb{Q})$. Therefore, we obtain $\nu = 1$, which completes the proof of Theorem 1.5(1). ∎

In order to examine the integer points on E, we need the following lemma, analogous to Lemma 3.1.

LEMMA 5.4 ([3, Lemma 2 in Chapter 14]). *The map* $\varphi : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ *defined by*

$$\varphi(X) = \begin{cases} x(\mathbb{Q}^\times)^2 & \text{if } X = (x, y) \notin \{O, T\}, \\ -n(\mathbb{Q}^\times)^2 & \text{if } X = T, \\ (\mathbb{Q}^\times)^2 & \text{if } X = O, \end{cases}$$

is a group homomorphism.

Proof of Theorem 1.5(2). Let $X = (x, y)$ be a point in Z. By Lemma 5.1, $X \equiv X_1 \pmod{2E(\mathbb{Q})}$, where

$$X_1 \in \{O, T, P_1, P_2, P_1 + T, P_2 + T, P_1 + P_2, P_1 + P_2 + T\}.$$

Suppose first that $X_1 \in \{P_1 + T, P_2 + T\}$. Since $x(P_i + T) = n\square$ for $i \in \{1, 2\}$, Lemma 5.4 implies that $x = nx_0^2$ for some positive integer x_0. By $y^2 = x^3 - nx$, there exists a positive integer y_0 such that

$$y_0^2 - nx_0^4 = -1. \tag{5.1}$$

Since by Lemma 2.3 the Diophantine equation (5.1) has at most one positive solution, there exists at most one pair of integers m_1, m_2 with $m_1 \not\equiv m_2 \pmod 2$ such that $X = \pm(m_1P_1 + m_2P_2) + T$. In particular, if $n = s^4 + 1$, then (5.1) has the solution $(x_0, y_0) = (1, s^2)$, and hence $X = (n, \pm ns^2) = \pm P_1 + T$. Note that m_1 and m_2 above are coprime, since otherwise the point $(m_1/d)P_1 + (m_2/d)P_2 + T$ (with $d = \gcd(m_1, m_2)$) would also be integral and give another solution of (5.1).

Suppose secondly that $X_1 \in \{O, T, P_1, P_2, P_1+P_2, P_1+P_2+T\}$. If $X_1 \in \{T, P_1, P_2, P_1+P_2+T\}$, then $X_1 \notin E(\mathbb{R})^0$ and hence $X \notin E(\mathbb{R})^0$. It follows that $|x| \le \sqrt{n}$. If $X_1 \in \{O, P_1+P_2\}$, then Lemma 5.4 implies that $x = x_0^2$ for some positive integer x_0, since $x(P_1+P_2) = \square$. By $y^2 = x^3 - nx$, we have $x_0^4 - n = y_0^2$ for some positive integer y_0. Thus

$$n = (x_0^2 + y_0)(x_0^2 - y_0) \ge x_0^2 + y_0 > x_0^2 = x.$$

In any case, it suffices to consider the case $|x| < n$.

Suppose that $n > 3000$. By Lemma 5.3, the canonical height pairing

$$\langle P_1, P_2 \rangle = \tfrac{1}{2}\big(\hat{h}(P_1+P_2) - \hat{h}(P_1) - \hat{h}(P_2)\big)$$

of P_1 and P_2 satisfies

$$-0.926 < 2\langle P_1, P_2 \rangle < 2.558.$$

Thus, putting $X = l_1P_1 + l_2P_2 + \epsilon T$ with $l_1, l_2 \in \mathbb{Z}$ and $\epsilon \in \{0,1\}$, we have

$$\begin{aligned} \hat{h}(X) &= \hat{h}(l_1P_1) + \hat{h}(l_2P_2) + 2\langle l_1P_1, l_2P_2 \rangle \\ &= l_1^2\hat{h}(P_1) + l_2^2\hat{h}(P_2) + 2l_1l_2\langle P_1, P_2 \rangle \\ &> \{0.456(l_1^2 + l_2^2) - 0.32|l_1l_2|\}\log n \\ &> 0.456\{(|l_1| - 0.351|l_2|)^2 + 0.876l_2^2\}\log n. \end{aligned} \tag{5.2}$$

On the other hand, since we are considering the case where $|x| < n$, we can obtain an upper bound for $\hat{h}(X)$ using a result on the difference between h and $\hat{h}$; in fact, Theorem and Proposition 4 in [26] together yield

$$\hat{h}(X) \le h(X) + \tfrac{1}{2}\log n + \tfrac{4}{3}\log 2 < \tfrac{3}{2}\log n + \tfrac{4}{3}\log 2 < 1.616\log n. \tag{5.3}$$

Combining the estimates (5.2) and (5.3), we get

$$(|l_1| - 0.351|l_2|)^2 + 0.876l_2^2 < 3.544,$$

which implies

$$(|l_1|, |l_2|) \in \{(0,0), (0,1), (1,0), (1,1)\}.$$

Since $X_1 \in \{O, T, P_1, P_2, P_1+P_2, P_1+P_2+T\}$, we obtain

$$X \in \{T, \pm P_1, \pm P_2, \pm(P_1+P_2), \pm(P_1-P_2), \pm(P_1+P_2)+T, \pm(P_1-P_2)+T\}.$$

We always have $T, \pm P_1, \pm P_2 \in Z$. Since

$$x(P_1 \pm P_2) = \frac{(s^2 \pm st + t^2)^2}{(s \pm t)^2}, \qquad x(P_1 \pm P_2 + T) = -\frac{n(s \pm t)^2}{(s^2 \pm st + t^2)^2},$$

and since $\gcd(s \pm t, s^2 \pm st + t^2) = 1$, it is not difficult to see that $\pm(P_1+P_2)$, $\pm(P_1 \pm P_2) + T \notin Z$, and that $\pm(P_1 - P_2) \in Z$ if and only if $t = s-1$.

If $(17 <)\ n \le 3000$, then by Magma [1] one can easily check the following:

- if $t = 1$, then $Z = \{T, \pm P_1, \pm P_2, \pm P_1 + T\}$;
- if $t = s-1$, then $Z = \{T, \pm P_1, \pm P_2, \pm(P_1 - P_2)\}$;
- in all other cases, $Z = \{T, \pm P_1, \pm P_2\}$.

This completes the proof of Theorem 1.5(2). ∎

Remark 5.5. It is quite simple to find a further parameterization of $n = s^4 + t^4$, other than $n = s^4 + 1$, such that the set Z can be completely determined. For example, let

$$s = |17k^2 - 12kl - 13l^2|, \qquad t = |17k^2 + 12kl - 13l^2| \tag{5.4}$$

with positive integers k, l. Then $s^4 + t^4 = u^2 + v^4$, where

$$u = |289k^4 + 14k^2l^2 - 239l^4|, \qquad v = |17k^2 - l^2|$$

(cf. [17, Part 7]). If $v = 1$, then the Diophantine equation (5.1) has the solution $(y_0, x_0) = (u, 1)$, which together with Lemma 2.3 implies that $Z = \{T, \pm P_1, \pm P_2, \pm P_1 + T\}$. In this case, $17k^2 - l^2 = \pm 1$ has the positive solutions

$$l + k\sqrt{17} = (4 + \sqrt{17})^m$$

for positive integers m, whence k, l are parameterized as follows:

$$l = \tfrac{1}{2}\{(4+\sqrt{17})^m + (4-\sqrt{17})^m\},$$
$$k = \frac{1}{2\sqrt{17}}\{(4+\sqrt{17})^m - (4-\sqrt{17})^m\}.$$

We have seen so far that the set Z of integer points can be completely determined for several parameterizations of n. We conclude this paper by noting the infinity of such square-free integers n. The family $n = N^2$ with $N = (s^4+t^4)/2$ or $N = s^4+4t^4$ in Corollary 1.4 certainly represents infinitely many square-free integers by a theorem of Greaves [13], since it is a binary form of degree four. Each of the families $n = st(s^2 + t^2)/2$ with $|s - t| = 1$ in Theorem 1.3 and $n = s^4 + 1$ in Theorem 1.5 represents infinitely many square-free integers if the ABC conjecture is valid (cf. [12, Theorem 1]). We do not have a criterion for $n = s^4 + t^4$ with (5.4) and $|17k^2 - l^2| = 1$ to represent infinitely many square-free integers.

Acknowledgments. The authors thank the referee for pertinent suggestions.

References

[1] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Dept. of Math., Univ. of Sydney; http://magma.maths.usyd.edu.au/magma/.

[2] A. Bremner, J. H. Silverman and N. Tzanakis, *Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$*, J. Number Theory 80 (2000), 187–208.

[3] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge Univ. Press, 1991.

[4] J. H. Chen and P. Voutier, *Complete solution of the Diophantine equation $X^2+1 = dY^4$ and a related family of quartic Thue equations*, J. Number Theory 62 (1997), 71–99.

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.

[6] J. H. E. Cohn, *The Diophantine equation $x^4 - Dy^2 = 1$, II*, Acta Arith. 78 (1997), 401–403.
[7] A. Dujella and A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen 56 (2000), 321–335.
[8] S. Duquesne, *Integral points on elliptic curves defined by simplest cubic fields*, Experiment. Math. 10 (2001), 91–102.
[9] S. Duquesne, *Elliptic curves associated with simplest quartic fields*, J. Théor. Nombres Bordeaux 19 (2007), 81–100.
[10] Y. Fujita and N. Terai, *Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$*, Tokyo J. Math. 34 (2011), 289–303.
[11] Y. Fujita and N. Terai, *Generators for the elliptic curve $y^2 = x^3 - nx$*, J. Théor. Nombres Bordeaux 23 (2011), 403–416.
[12] A. Granville, *ABC allows us to count squarefrees*, Int. Math. Res. Notices 1998, no. 19, 991–1009.
[13] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) 43 (1992), 45–65.
[14] P. Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory 129 (2009), 182–208.
[15] A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.
[16] W. Ljunggren, *Über die Gleichung $x^4 - Dy^2 = 1$*, Arch. Math. Naturvid. 45 (1942), no. 5, 61–70.
[17] T. Piezas, *A collection of algebraic identities*, http://sites.google.com/site/tpiezas/Home.
[18] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, A. Pethő et al. (eds.), de Gruyter, 1991, 227–238.
[19] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. 25 (1995), 1501–1538.
[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[21] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.
[22] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.
[23] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.
[24] B. K. Spearman, *Elliptic curves $y^2 = x^3 - px$ of rank two*, Math. J. Okayama Univ. 49 (2007), 183–184.
[25] P. G. Walsh, *On integer solutions to $x^2 - dy^2 = 1$, $z^2 - 2dy^2 = 1$*, Acta Arith. 82 (1997), 69–76.
[26] H. G. Zimmer and S. Schmitt, *Height estimates for elliptic curves in short Weierstraß form over global fields and a comparison*, Arch. Math. (Basel) 77 (2001), 22–31.

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 Information System Design
Ashikaga Institute of Technology
268-1 Omae
Ashikaga, Tochigi 326-8558, Japan
E-mail: terai@ashitech.ac.jp

Received on 25.6.2012
and in revised form on 2.3.2013 (7110)