GLASNIK MATEMATIČKI
Vol. 54(74)(2019), 321 – 343

GENERATORS AND INTEGRAL POINTS ON CERTAIN QUARTIC CURVES

Yasutsugu Fujita and Tadahisa Nara
Nihon University, Japan and Tohoku-Gakuin University, Japan

Abstract. In this paper, we study integral points and generators on quartic curves of the forms $u^2 \pm v^4 = m$ for a nonzero integer m. The main results assert that certain integral points on the curves can be extended to bases for the Mordell-Weil groups of the elliptic curves attached to the quartic curves in the cases where the Mordell-Weil ranks are at most two. As corollaries, we explicitly describe the integral points on the quartic curves in each case where the ranks are one and two.

1. Introduction

Let m be a nonzero integer. Denote by C_m^- and C_m^+ the quartic curves defined by

$$u^2 - v^4 = m$$

and

$$u^2 + v^4 = m,$$

respectively.

Consider first the curve C_m^-, which is birationally equivalent to the elliptic curve E_m^- defined by

$$y^2 = x^3 - 4mx.$$

In fact, a birational map φ^- from C_m^- to E_m^- is defined by

$$\varphi^-(u, v) = (2(u + v^2), 4v(u + v^2)) \tag{1.1}$$

2010 *Mathematics Subject Classification.* 11G05, 11D25, 11G50.
Key words and phrases. Elliptic curve, quartic curve, canonical height, integral points.
The first author was supported by JSPS KAKENHI Grant Number 16K05079.

and its inverse ψ^- from E_m^- to C_m^- is defined by

$$\psi^-(x,y) = \left(\frac{2x^3 - y^2}{4x^2}, \frac{y}{2x}\right). \tag{1.2}$$

Note that there are two points at infinity on C_m^- corresponding to the points $(\pm 1, 0)$ on the "dual" model of C_m^- defined by $u^2 = mw^4 + 1$, via the map φ^- one of the points at infinity maps to the identity element $\mathcal{O}^-$ on E_m^- and the other maps to the torsion point $T^- = (0,0)$ on E_m^-. Denote by T the point at infinity on C_m^- corresponding to T^- on E_m^-. So we regard $C_m^-(\mathbb{Q})$ as a group consisting of the rational points with the two points at infinity, isomorphic to $E_m^-(\mathbb{Q})$.

Theorem 1.1. *Let m be a fourth-power-free integer. If $P_1 = (a_1, b_1)$ is an integral point on C_m^- with $a_1 b_1 \neq 0$, then P_1 can be extended to a basis for $C_m^-(\mathbb{Q})$ modulo $C_m^-(\mathbb{Q})_{\mathrm{tors}}$.*

Corollary 1.2. *Let m be a fourth-power-free integer. Assume that the rank of $C_m^-(\mathbb{Q})$ is one. If m is a non-square, then C_m^- has at most four integral points, which can be expressed as $(a_1, \pm b_1)$, $(-a_1, \pm b_1)$, and if m is a square of some positive integer m_0, then C_m^- has at most six integral points, which can be expressed as $(a_1, \pm b_1)$, $(-a_1, \pm b_1)$, $(\pm m_0, 0)$ for some integers a_1 and b_1.*

Theorem 1.3. *Let m be a square-free integer. Assume that P_1 and P_2 are integral points on C_m^- such that $(|x(P_1)|, |y(P_1)|) \neq (|x(P_2)|, |y(P_2)|)$. If neither $P_1 + P_2$ nor $P_1 - P_2$ has a 3-division point in $C_m^-(\mathbb{Q})$, then $\{P_1, P_2\}$ can be extended to a basis for $C_m^-(\mathbb{Q})$ modulo $C_m^-(\mathbb{Q})_{\mathrm{tors}}$.*

Using the identity

$$(2s^2 + st + 2t^2)^2 - (s+t)^4 = (2s^2 - st + 2t^2)^2 - (s-t)^4, \tag{1.3}$$

we can give an explicit example of an infinite family of m satisfying the assumption of Theorem 1.3.

Corollary 1.4. *Let m be a square-free integer expressed as $m = 3(s^4 + s^2t^2 + t^4)$ with coprime integers s, t. Put*

$$P_1 = (st + 2(s^2 + t^2), s + t), \quad P_2 = (st - 2(s^2 + t^2), s - t). \tag{1.4}$$

Then, $\{P_1, P_2\}$ can be extended to a basis for $C_m^-(\mathbb{Q})$ modulo $C_m^-(\mathbb{Q})_{\mathrm{tors}}$.

If we assume that the rank of $C_m^-(\mathbb{Q})$ is two, then the integral points can be explicitly described without the assumption on 3-division points as in Theorem 1.3.

Theorem 1.5. *Let m be a square-free integer. Assume that the rank of $C_m^-(\mathbb{Q})$ is two. Then, C_m^- has at most eight integral points, which can be expressed as*

$$(a_1, \pm b_1),\ (-a_1, \pm b_1),\ (a_2, \pm b_2),\ (-a_2, \pm b_2) \tag{1.5}$$

for some integers a_1, b_1, a_2 and b_2. In particular, if C_m^- has two integral points (a_1, b_1) and (a_2, b_2) with $(|a_1|, |b_1|) \neq (|a_2|, |b_2|)$, then the integral points on C_m^- are exactly given by (1.5).

Consider next the curve C_m^+. Let $P_1 = (a_1, b_1)$ be a point in $C_m^+(\mathbb{Q})$, and E_m^+ the elliptic curve defined by

$$y^2 = x^3 + 4mx.$$

Then, there exists a birational map φ^+ from C_m^+ to E_m^+ defined by

$$\varphi^+(u,v) = \left(\frac{(u+a_1)^2 + (v^2 - b_1^2)^2}{(v+b_1)^2}, \frac{4\left\{(u+a_1)m + b_1 v(a_1 v^2 + b_1^2 u)\right\}}{(v+b_1)^3} \right), \tag{1.6}$$

with the inverse map ψ^+ defined by

$$\psi^+(x,y) = \left(\frac{a_1^3 x^3 - 12 a_1 b_1^2 m x^2 - 4 a_1^3 m x + 8 b_1 (a_1^2 + 2 b_1^4) m y - 16 a_1 b_1^2 m^2}{(a_1 y - 2 b_1^3 x - 4 b_1 m)^2}, \frac{2mx - a_1 b_1 y - 4 b_1^2 m}{a_1 y - 2 b_1^3 x - 4 b_1 m} \right). \tag{1.7}$$

Note that

$$\begin{aligned} \varphi^+(a_1, -b_1) = \mathcal{O}^+, \quad \varphi^+(-a_1, b_1) &= (0,0) =: T^+, \\ \varphi^+(a_1, b_1) &= \left(\frac{a_1^2}{b_1^2}, \frac{a_1(a_1^2 + 2b_1^4)}{b_1^3} \right) =: P_1^+, \\ \varphi^+(-a_1, -b_1) &= \left(\frac{4b_1^2 m}{a_1^2}, -\frac{4b_1(a_1^2 + 2b_1^4)m}{a_1^3} \right) = P_1^+ + T^+. \end{aligned}$$

The latter two equalities follow from

$$\begin{aligned} \frac{u+a_1}{v+b_1} &= \frac{(b_1 - v)(b_1^2 + v^2)}{u - a_1}, \\ \frac{b_1 u - a_1 v}{v + b_1} &= \frac{(b_1 - v)(m + b_1^2 v^2)}{b_1 u + a_1 v}, \end{aligned}$$

by $u^2 + v^4 = a_1^2 + b_1^4$. Thus, C_m^+ can be regarded as an elliptic curve with the identity element $\mathcal{O} = (a_1, -b_1)$, the 2-torsion point $T = (-a_1, b_1)$ and the non-torsion point $P_1 = (a_1, b_1)$.

THEOREM 1.6. *Let m be a fourth-power-free integer. If $P_1 = (a_1, b_1)$ is an integral point on C_m^+ with $a_1 b_1 \neq 0$, then P_1 can be extended to a basis for $C_m^+(\mathbb{Q})$ modulo $C_m^+(\mathbb{Q})_{\text{tors}}$.*

COROLLARY 1.7. *Let m be a fourth-power-free integer. Assume that the rank of $C_m^+(\mathbb{Q})$ is one. If m is a non-square, then C_m^+ has at most four integral points, which can be expressed as $(a_1, \pm b_1)$, $(-a_1, \pm b_1)$, and if m is a square of some positive integer m_0, then C_m^+ has at most six integral points, which* *can be expressed as* $(a_1, \pm b_1),\ (-a_1, \pm b_1),\ (\pm m_0, 0)$ *for some integers* a_1 *and* b_1.

THEOREM 1.8. *Let* m *be a non-square, fourth-power-free integer. Assume that* $P_1 = (a_1, b_1)$ *and* $P_2 = (a_2, b_2)$ *are integral points on* C_m^+ *such that* $\{|a_1|, b_1^2\} \neq \{|a_2|, b_2^2\}$. *Assume further that either of the following holds*:

(i) m *is square-free.*

(ii) *Neither* $(a_1 + a_2)^2 + (b_1^2 - b_2^2)^2$ *nor* $(a_1 - a_2)^2 + (b_1^2 - b_2^2)^2$ *is a square.*

If neither P_2 *nor* $P_1 - P_2$ *has a* 3*-division point in* $C_m^+(\mathbb{Q})$, *then* $\{P_1, P_2\}$ *can be extended to a basis for* $C_m^+(\mathbb{Q})$ *modulo* $C_m^+(\mathbb{Q})_{\mathrm{tors}}$.

Identity (1.3) also gives an explicit example satisfying assumption (i) of Theorem 1.8.

COROLLARY 1.9. *Let* m *be a square-free integer expressed as* $m = 5\,(s^4 + 3s^2t^2 + t^4)$ *with coprime integers* s, t. *Put*

$$P_1 = (st + 2(s^2 + t^2), s - t), \quad P_2 = (st - 2(s^2 + t^2), s + t). \tag{1.8}$$

Then, $\{P_1, P_2\}$ *can be extended to a basis for* $C_m^+(\mathbb{Q})$ *modulo* $C_m^+(\mathbb{Q})_{\mathrm{tors}}$.

THEOREM 1.10. *Let* m *be a square-free integer. If the rank of* $C_m^+(\mathbb{Q})$ *is two, then* C_m^+ *has at most eight integral points, which can be expressed as*

$$(a_1, \pm b_1),\ (-a_1, \pm b_1),\ (a_2, \pm b_2),\ (-a_2, \pm b_2) \tag{1.9}$$

for some integers a_1, b_1, a_2 *and* b_2. *In particular, if* C_m^+ *has two integral points* (a_1, b_1) *and* (a_2, b_2) *with* $(|a_1|, |b_1|) \neq (|a_2|, |b_2|)$, *then the integral points on* C_m^+ *are exactly given by* (1.9).

Let Q_m^+ be the quartic curve defined by $u^4 + v^4 = m$. For a point $P = (u, v)$ in $Q_m^+(\mathbb{Q})$, denote by $\hat{P}$ the "dual" point (v, u) of P and denote by P_q and $\hat{P}_q$ the images of P and $\hat{P}$, respectively, in $C_m^+(\mathbb{Q})$ via the natural map $(u, v) \mapsto (u^2, v)$.

Let (a, b) be an integral point on Q_m^+. When we take $(a_1, b_1) = (a^2, b)$ and regard C_m^+ as an elliptic curve via the map φ^+, we obtain the following, which is an immediate consequence of [5, Theorem 1.5 (1)].

THEOREM 1.11. *Let* m *be a fourth-power-free integer. Assume that* Q_m^+ *has an integral point* $P = (a, b)$. *Then,* $\{P_q, \hat{P}_q\}$ *can be extended to a basis for* $C_m^+(\mathbb{Q})$ *modulo* $C_m^+(\mathbb{Q})_{\mathrm{tors}}$.

The final result of this paper asserts that the integral points on Q_m^+ can be completely described under the assumptions that the rank of $C_m^+(\mathbb{Q})$ is two and m is fourth-power-free (not necessarily square-free, unlike Theorem 1.10).

THEOREM 1.12. *Let* m *be a fourth-power-free integer. If the rank of* $C_m^+(\mathbb{Q})$ *is two, then* Q_m^+ *has at most eight integral points, which can be expressed as* $(a, \pm b),\ (-a, \pm b),\ (b, \pm a),\ (-b, \pm a)$ *for some integers* a *and* b.

Note that the main strategy of the proofs is similar to that of the proofs of theorems and corollaries in [3]; after transforming a given model into the Weierstrass form, we combine divisibility considerations with height estimates. However, we need other devices than those used in [3]. In fact, in the cases of C_m^+, we often use another map φ' from C_m^+ to E_m^+ defined by $\varphi'(u,v) = (-v^2, uv)$, and the proof of Theorem 1.10 needs an argument over $\mathbb{Q}(i)$ instead of $\mathbb{Q}$.

The organization of this paper is as follows. In Section 2, we refer to two lemmas, one of which will be used to show that some rational points on an elliptic curve are not divisible by 2 over $\mathbb{Q}$, and the other of which will be needed for determining the integral points on an elliptic curve. In Section 3, we show that some rational points on an elliptic curve are not divisible by 2 over $\mathbb{Q}$. Some of the results (Lemmas 3.2 and 3.3) imply that certain two points are independent modulo torsion (see Remark 3.4). In Section 4, we quote the work of Voutier and Yabuta ([11, Theorem 1.2]), which gives a uniform lower bound for canonical heights, and bound canonical heights from above by computing local heights. Finally, in Section 5, we give the proofs of theorems and corollaries.

We now fix the notation. Throughout this paper, let m be a fourth-power-free integer. Let C_m^-, C_m^+ be the quartic curves defined by $u^2 - v^4 = m$, $u^2 + v^4 = m$, respectively, and E_m^-, E_m^+ the elliptic curves defined by $y^2 = x^3 - 4mx$, $y^2 = x^3 + 4mx$, respectively. Note that C_m^- and E_m^- are birationally equivalent via φ^- and ψ^- defined by (1.1) and (1.2), respectively, and that C_m^+ and E_m^+ are birationally equivalent via φ^+ and ψ^+ defined by (1.6) and (1.7), respectively, under the assumption that C_m^+ has a rational point $P_1 = (a_1, b_1)$. For a point P in $C_m^-(\mathbb{Q})$ or in $C_m^+(\mathbb{Q})$, denote by $P^- = \varphi^-(P)$ or $P^+ = \varphi^+(P)$ the corresponding point in $E_m^-(\mathbb{Q})$ or in $E_m^+(\mathbb{Q})$, respectively. Let $T^- = (0,0)$ be the torsion point in $E_m^-(\mathbb{Q})$, which is the image by φ^- of one of the points at infinity T on C_m^-, whereas let $T^+ = (0,0)$ be the torsion point in $E_m^+(\mathbb{Q})$, which is the image by φ^+ of the point $(-a_1, b_1)$ on C_m^+. We also use the map φ' from C_m^+ to $\bar{E}_m^+$ defined by $\varphi'(u,v) = (-v^2, uv)$, where $\bar{E}_m^+$ is defined by $y^2 = x^3 - mx$. In case $m = m_0^2$ for some positive integer m_0, let $T_1^- = (-2m_0, 0)$, $T_2^- = (2m_0, 0)$ be the remaining 2-torsion points in $E_m^-(\mathbb{Q})$, and denote by $T_1 = (-m_0, 0)$, $T_2 = (m_0, 0)$ the corresponding points on C_m^-, respectively.

2. Preliminary Lemmas

Let K be a number field, E an elliptic curve defined by

$$y^2 = x^3 - 4Ax$$

for some $A \in K$ and $\bar{E}$ the elliptic curve defined by

$$y^2 = x^3 + Ax.$$

Then, there is an isogeny g of degree two from E to $\bar{E}$ defined by

$$g(P) = \begin{cases} \left(\dfrac{y^2}{4x^2}, \dfrac{y(x^2+4A)}{8x^2}\right) & \text{if } P=(x,y) \notin \{\mathcal{O}, T\}, \\ \bar{\mathcal{O}} & \text{if } P \in \{\mathcal{O}, T\}, \end{cases}$$

and the dual isogeny $\hat{g}$ of g is

$$\hat{g}(\bar{P}) = \begin{cases} \left(\dfrac{\bar{y}^2}{\bar{x}^2}, \dfrac{\bar{y}(\bar{x}^2 - A)}{\bar{x}^2}\right) & \text{if } \bar{P}=(\bar{x},\bar{y}) \notin \{\bar{\mathcal{O}}, \bar{T}\}, \\ \mathcal{O} & \text{if } \bar{P} \in \{\bar{\mathcal{O}}, \bar{T}\}, \end{cases} \tag{2.1}$$

where $\mathcal{O}$, $\bar{\mathcal{O}}$ are the identity elements on E, $\bar{E}$, and T, $\bar{T}$ are the 2-torsion points $(0,0)$ on E, $\bar{E}$, respectively.

In order to examine whether a rational point has a 2-division point or not in $E(K)$, we need the following lemma.

LEMMA 2.1. *Let $P \neq O$ be a point in $E(K)$.*

(1) $P \in \hat{g}(\bar{E}(K))$ if and only if $x(P)$ is a square. In this case, putting $P=(x_0^2, y)$ with x_0 positive, one can express $\bar{P} \in \bar{E}(K)$ with $g(\bar{P}) = P$ as

$$\bar{P} = \left(\frac{1}{2}\left(x_0^2 \pm \frac{y}{x_0}\right), \pm x_0 x(\bar{P})\right),$$

where the signs are taken simultaneously.

(2) $P \in 2E(K)$ if and only if both $x(P)$ and $x(\bar{P})$ are squares for some $\bar{P} \in \bar{E}(K)$ with $g(\bar{P}) = P$.

PROOF. The assertion in the case where $K = \mathbb{Q}$ follows immediately from (iii) in [10, p. 83]. The same argument applies to the case where K is a general number field (see [2, p. 342]). ∎

The following lemma is used in the proofs of Theorems 1.5 and 1.10, i.e., in determining integral points on C_m^- and C_m^+ in the rank two cases.

LEMMA 2.2. *The map $\Phi : E(K) \to K^\times/(K^\times)^2$, defined by*

$$\Phi(P) = \begin{cases} x(K^\times)^2 & \text{if } P=(x,y) \notin \{\mathcal{O}, T\}, \\ -A(K^\times)^2 & \text{if } P = T, \\ (K^\times)^2 & \text{if } P = \mathcal{O}, \end{cases}$$

is a group homomorphism.

PROOF. The assertion is an immediate consequence of [1, Lemma 2 in Chapter 14] if $K = \mathbb{Q}$. The same argument applies to a general K, see [2, Proposition 3.2.1 (a)]. ∎

Note that we use Lemmas 2.1 and 2.2 only for $K = \mathbb{Q}$ and $K = \mathbb{Q}(i)$.

3. Divisibility and independence of points

Let us first examine the divisibility of integral points on C_m^-.

Lemma 3.1. *Assume that C_m^- has an integral point P. Then $P^-, P^- + T^- \notin 2E_m^-(\mathbb{Q})$. Moreover, if $m = m_0^2$ for some positive integer m_0, then $P^- + T_1^-, P^- + T_2^- \notin 2E_m^-(\mathbb{Q})$.*

Proof. Suppose that $P = (u, v) \in 2C_m^-(\mathbb{Q})$, which implies $P^- = \varphi(P) = (2(u+v^2), 4v(u+v^2)) \in 2E_m^-(\mathbb{Q})$. From Lemma 2.1 we see that both $x(P^-)$ and $x(\bar{P}^-)$ are squares. Thus, we may write $x(P^-) = 2(u+v^2) = 4w^2$ and $x(\bar{P}^-) = 2w(w \pm v)$ with w a positive integer. Since $u - v^2$ must be even by $u + v^2 = 2w^2$, it holds that w is odd and square-free. If a prime p divides $\gcd(u, v)$, then p also divides w and hence p^2 divides $u + v^2$. Therefore, p^2 divides either of v^2 and u and thus $u - v^2$, which shows that p^4 divides m, a contradiction. It follows that $\gcd(u, v) = \gcd(v, w) = 1$. This implies that any odd prime p dividing w does not divide $w \pm v$, which contradicts the fact that $x(\bar{P}^-)$ is a square. Hence, we obtain $P^- \notin 2E_m^-(\mathbb{Q})$.

Since $P^- + T^- = (2(-u+v^2), -4v(-u+v^2))$, if we replace u, v by $-u$, $-v$ in the argument above, we see that $P^- + T^- \notin 2E_m^-(\mathbb{Q})$.

Consider the case where $m = m_0^2$. We may write $u - v^2 = km_1^2$, $u + v^2 = km_2^2$ and $m_0 = km_1m_2$ for some integers k, m_1, m_2 with $\gcd(m_1, m_2) = 1$. Then, we have

$$x(P^- + T_1^-) = \frac{2km_1m_2(m_1 - m_2)}{m_1 + m_2}, \quad x(P^- + T_2^-) = \frac{2km_1m_2(m_1 + m_2)}{-m_1 + m_2}.$$

Since $m_0 = km_1m_2$ is square-free and $\gcd(m_1, m_2) = 1$, we conclude that neither $x(P^- + T_1^-)$ nor $x(P^- + T_2^-)$ can be a square.

□

Consider the case where C_m^- has integral points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ with $(|a_1|, |b_1|) \neq (|a_2|, |b_2|)$.

Lemma 3.2. *Let m be a square-free integer. Assume that C_m^- has integral points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ with $(|a_1|, |b_1|) \neq (|a_2|, |b_2|)$. Then, $P_1^-, P_1^- + T^-, P_2^-, P_2^- + T^-, P_1^- + P_2^-, P_1^- + P_2^- + T^- \notin 2E_m^-(\mathbb{Q})$.*

Proof. By Lemma 3.1 it suffices to show that $P_1^- + P_2^-, P_1^- + P_2^- + T^- \notin 2E_m^-(\mathbb{Q})$, which is obvious from

$$x(P_1^- + P_2^-) = \frac{4(a_1 + b_1^2)(a_2 + b_2^2)(b_1 - b_2)^2}{(a_1 + b_1^2 - a_2 - b_2^2)^2},$$
$$x(P_1^- + P_2^- + T^-) = \frac{4(-a_1 + b_1^2)(a_2 + b_2^2)(b_1 + b_2)^2}{(-a_1 + b_1^2 - a_2 - b_2^2)^2}$$

and the assumption that $m = a_1^2 - b_1^4 = a_2^2 - b_2^4$ is square-free. □

Second, examine the divisibility of integral points on C_m^+.

LEMMA 3.3. *Let m be a non-square, fourth-power-free integer. If C_m^+ has an integral point $P_1 = (a_1, b_1)$, then P_1^+, $P_1^+ + T^+ \notin 2E_m^+(\mathbb{Q})$. Moreover, assume that there exists another integral point $P_2 = (a_2, b_2)$ with $\{|a_1|, |b_1|\} \neq \{|a_2|, |b_2|\}$. Assume further that either of the following holds*:

(i) *m is square-free.*
(ii) *Neither $(a_1 + a_2)^2 + (b_1^2 - b_2^2)^2$ nor $(a_1 - a_2)^2 + (b_1^2 - b_2^2)^2$ is a square.*

Then, P_1^+, P_2^+, $P_1^+ + T^+$, $P_2^+ + T^+$, $P_1^+ + P_2^+$, $P_1^+ + P_2^+ + T^+ \notin 2E_m^+(\mathbb{Q})$.

PROOF. Noting that $(a_1 \pm a_2)^2 + (b_1^2 - b_2^2)^2 = 2(m - b_1^2 b_2^2 \pm a_1 a_2)$, one sees that this lemma follows, more or less, from [4, Lemma 3.2]. However, [4, Lemma 3.2] examines the divisibility of points on an elliptic curve of the form $y^2 = x^3 - mx$, which is 2-isogenous to E_m^+. Therefore, we give the proof of this lemma.

It is clear that $P_1^+ + T^+ \notin 2E_m^+(\mathbb{Q})$, since $x(P_1^+ + T^+) = 4b_1^2 m / a_1^2$ and m is non-square. Moreover, since the point P_1^+ satisfies $\hat{g}(-b_1^2, a_1 b_1) = P_1^+$, where $\hat{g} : \bar{E}_m^+ \to E_m^+$ is the dual isogeny of g defined by (2.1) with $A = -m$, it follows from Lemma 2.1 that $P_1^+ \notin 2E_m^+(\mathbb{Q})$.

Consider next the point P_2^+. Since

$$x(P_2^+) = \frac{(a_1 + a_2)^2 + (b_1^2 - b_2^2)^2}{(b_1 + b_2)^2},$$

the assumption and Lemma 2.1 together imply that $P_2^+ \notin 2E_m^+(\mathbb{Q})$. Since

$$x(P_2^+ + T^+) = \frac{(a_1 - a_2)^2 + (b_1^2 - b_2^2)^2}{(b_1 - b_2)^2},$$

it also holds that $P_2^+ + T^+ \notin 2E_m^+(\mathbb{Q})$. Moreover, since $g(P_1^+) = 2(-b_1^2, a_1 b_1)$, it is necessary for $P_1^+ + P_2^+ \in 2E_m^+(\mathbb{Q})$ that $P_2^+ \in \hat{g}(\bar{E}_m^+(\mathbb{Q}))$, which is impossible by the assumption and Lemma 2.1. Thus, $P_1^+ + P_2^+ \notin 2E_m^+(\mathbb{Q})$. Similarly, it is easily checked that $P_1^+ + P_2^+ + T^+ \notin 2E_m^+(\mathbb{Q})$. ∎

REMARK 3.4. On the assumption of Lemma 3.2, it can be deduced that P_1^- and P_2^- are independent modulo $E_m^-(\mathbb{Q})_{\text{tors}}$. Indeed, suppose on the contrary that P_1^- and P_2^- are dependent. Then, there exist integers n_1, n_2 and n_3 with $(n_1, n_2, n_3) \neq (0, 0, 0)$ such that $n_1 P_1^- + n_2 P_2^- + n_3 T^- = \mathcal{O}$. Considering this equality modulo $2E_m^-(\mathbb{Q})$, we have $\delta_1 P_1^- + \delta_2 P_2^- + \delta_3 T^- \in 2E_m^-(\mathbb{Q})$ with $\delta_1, \delta_2, \delta_3 \in \{0, 1\}$, which contradicts Lemma 3.2. Similarly, on the assumption of Lemma 3.3, one sees that P_1^+ and P_2^+ are independent modulo $E_m^+(\mathbb{Q})_{\text{tors}}$.

In order to prove Theorem 1.10, we have to consider the divisibility of points on E_m^+ over the quadratic field $\mathbb{Q}(i)$ so that the points at infinity become rational. Let us now denote by φ_i^+ the isomorphism over $\mathbb{Q}(i)$ from C_m^+ to E_m^+ defined by

$$\varphi_i^+(u,v) = \left(2(iu+v^2), 4v(iu+v^2)\right).$$

In view of the following lemma, the torsion subgroup of $E_m^+(\mathbb{Q}(i))$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

LEMMA 3.5. *Let A be a non-square, positive integer, and E the elliptic curve defined by $y^2 = x^3 + Ax$. Then, $E(\mathbb{Q}(i))_{\text{tors}} = \langle (0,0) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.*

PROOF. Since the j-invariant of E is 1728, we know from [7, Theorem 7] that $E(\mathbb{Q}(i))_{\text{tors}}$ has no element of odd order. If there is a 2-torsion point $(x,y) \in E(\mathbb{Q}(i))$ with $(x,y) \neq (0,0)$, then $x^2 + A = 0$ has a solution in $\mathbb{Q}(i)$. Hence, A or $-A$ has to be a square in $\mathbb{Q}(i)$, which contradicts the assumption. If the point $(0,0)$ has a 2-division point (x,y) in $E_m^+(\mathbb{Q}(i))$, then the duplication formula implies that $x^4 - 2Ax^2 + A^2 = 0$, that is, $x^2 = A$, which is again a contradiction. ∎

For a point $P \in C_m^+(\mathbb{Q})$, put $P^i := \varphi_i^+(P)$. With the help of Lemma 3.5, an analogous result to Lemma 3.2 can be shown.

LEMMA 3.6. *Let m be a square-free integer. Assume that C_m^+ has integral points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ with $\{|a_1|, |b_1|\} \neq \{|a_2|, |b_2|\}$. Then, P_1^i, $P_1^i + T^+$, P_2^i, $P_2^i + T^+$, $P_1^i + P_2^i$, $P_1^i + P_2^i + T^+ \notin 2E_m^+(\mathbb{Q})$.*

PROOF. If $P_1^i = \left(2(ia_1 + b_1^2), 4b_1(ia_1 + b_1^2)\right) \in 2E_m^+(\mathbb{Q}(i))$, then Lemma 2.1 with $K = \mathbb{Q}(i)$ implies that $2(ia_1 + b_1^2)$ is a square, which is equivalent to that $2(-ia_1 + b_1^2)$ is a square. Thus, $4m = 4(a_1^2 + b_1^4)$ must be a square in $\mathbb{Q}(i)$, i.e., in $\mathbb{Q}$, which contradicts the assumption. Hence, $P_1^i \notin 2E_m^+(\mathbb{Q}(i))$. Since $x(P_1^i + T^+) = 2(-ia_1 + b_1^2)$, we also have $P_1^i + T^+ \notin 2E_m^+(\mathbb{Q}(i))$. Similarly, it is easy to see that P_2^i, $P_2^i + T^+ \notin 2E_m^+(\mathbb{Q}(i))$.

Assume that $P_1^i + P_2^i \in 2E_m^+(\mathbb{Q}(i))$. Then,

$$x(P_1^i + P_2^i) = \frac{4(ia_1 + b_1^2)(ia_2 + b_2^2)(b_1 - b_2)^2}{(ia_1 + b_1^2 - ia_2 - b_2^2)^2}$$

is a square by Lemma 2.1. Since $m = a_1^2 + b_1^4 = a_2^2 + b_2^4$ is square-free, we have $ia_1 + b_1^2 = \pm(ia_2 + b_2^2)$ and hence $(a_1, b_1^2) = (a_2, b_2^2)$, which contradicts the assumption. Therefore, $P_1^i + P_2^i \notin 2E_m^+(\mathbb{Q}(i))$. In the same way, it can be shown that $P_1^i + P_2^i + T^+ \notin 2E_m^+(\mathbb{Q}(i))$, since

$$x(P_1^i + P_2^i + T^+) = \frac{4(-ia_1 + b_1^2)(ia_2 + b_2^2)(b_1 + b_2)^2}{(-ia_1 + b_1^2 - ia_2 - b_2^2)^2}.$$

∎

In the case of Q_m^+, we can replace the assumption "square-free" by "fourth-power-free".

Lemma 3.7. *Let m be a fourth-power-free integer. Assume that Q_m^+ has an integral point $P=(a,b)$. Then, P_1^i, $P_1^i+T^+$, P_2^i, $P_2^i+T^+$, $P_1^i+P_2^i$, $P_1^i+P_2^i+T^+ \notin 2E_m^+(\mathbb{Q})$.*

Proof. One can prove P_1^i, $P_1^i+T^+$, P_2^i, $P_2^i+T^+ \notin 2E_m^+(\mathbb{Q})$ in exactly the same way as in Lemma 3.6. Moreover, we have

$$x(P_1^i+P_{2k}^+)=-\frac{2m}{(a+b)^2} \quad \text{and} \quad x(P_1^i+P_2^i+T^+)=-2(a+b)^2.$$

Since $m=a^4+b^4$ cannot be twice a square and $2=i(1-i)^2$ is not a square, none of the x-coordinates above can be a square in $\mathbb{Q}(i)$. It follows from Lemma 2.1 that $P_1^i+P_2^i$, $P_1^i+P_2^i+T^+ \notin 2E_m^+(\mathbb{Q}(i))$. ∎

4. Estimates on canonical heights

Voutier and Yabuta ([11, Theorem 1.2]) showed a uniform lower bound, which is best-possible, for the canonical height of a rational point on an elliptic curve E of the form $y^2=x^3+Ax$ with A a fourth-power-free integer. For $P\in E(\mathbb{Q})$, the canonical height $\hat{h}$ is defined by

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

where $h(Q)=\log\max\{|a|,|b|\}$ for $Q=(a/b,*)\in E(\mathbb{Q})$ with $\gcd(a,b)=1$. In view of

$$a^2-b^4\equiv 0,1,3,4,8,9,15 \pmod{16}$$

and

$$a^2+b^4\equiv 1,2,4,5,9,10 \pmod{16}$$

for integers a and b, the following are immediate consequences of [11, Theorem 1.2].

Lemma 4.1. *Let a and b be integers and let $m=a^2-b^4$ be fourth-power-free. Let E_m^- be the elliptic curve defined by $y^2=x^3-4mx$ and P^- a non-torsion point in $E_m^-(\mathbb{Q})$. Then,*

$$\hat{h}(P^-)>\frac{1}{16}\log|m|+C,$$

where in case $m\not\equiv 0 \pmod 4$, we have

$$C=\begin{cases}\frac{3}{8}\log 2 & \text{if } m<0 \text{ and } m\equiv 1 \pmod 8,\\ 0 & \text{if } m<0 \text{ and } m\equiv 15 \pmod{16},\\ \frac{7}{16}\log 2 & \text{if } m>0 \text{ and } m\equiv 1 \pmod 8,\\ \frac{1}{16}\log 2 & \text{if } m>0 \text{ and } m\equiv 15 \pmod{16},\end{cases}$$

and in case $m \equiv 0 \pmod 4$*, we have*

$$C = \begin{cases} \frac{1}{8}\log 2 & \textit{if } m < 0 \textit{ and } m \equiv 8, 24, 40, 56 \pmod{64}, \\ \frac{3}{16}\log 2 & \textit{if } m > 0 \textit{ and } m \equiv 8, 24, 40, 56 \pmod{64}. \end{cases}$$

Lemma 4.2. *Let* a *and* b *be integers and let* $m = a^2 + b^4$ *be fourth-power-free. Let* $\bar{E}_m^+$ *be the elliptic curve defined by* $y^2 = x^3 - mx$ *and* P' *a non-torsion point in* $\bar{E}_m^+(\mathbb{Q})$*. Then*

$$\hat{h}(P') > \frac{1}{16}\log|m| + C,$$

where

$$C = \begin{cases} \frac{9}{16}\log 2 & \textit{if } m \equiv 1, 9 \pmod{16}, \\ \frac{5}{16}\log 2 & \textit{if } m \equiv 2, 4, 10 \pmod{16}. \end{cases}$$

Next we should compute upper bounds for $\hat{h}(P^-)$, where P is an integral point on C_m^-, and for $\hat{h}(P')$, where $P' = (-v^2, uv)$ and $P = (u, v)$ is an integral point on C_m^+.

Note that on computing the canonical heights we can assume $u, v \geq 1$ for integral points $\varphi^-(u,v) = (2(u+v^2), 4v(u+v^2)) \in E_m^-(\mathbb{Q})$, since

$$\begin{aligned} \hat{h}(\varphi^-(u,-v)) &= \hat{h}(-\varphi^-(u,v)) = \hat{h}(\varphi^-(u,v)), \\ \hat{h}(\varphi^-(-u,v)) &= \hat{h}(-\varphi^-(u,v) + T^-) = \hat{h}(\varphi^-(u,v)). \end{aligned}$$

Lemma 4.3. *Let* m *be a nonzero fourth-power-free integer and* P *an integral point on* C_m^-*. Then*

$$\hat{h}(P^-) \leq \begin{cases} \frac{1}{4}\log(|m|+1) + \frac{1}{12}\log 2 & \textit{if } m > 0, \\ \frac{1}{4}\log|m| + \frac{1}{4}\log 2 & \textit{if } m < 0. \end{cases}$$

Lemma 4.4. *Let* m *be a nonzero fourth-power-free integer and* P *an integral point on* C_m^+ *(hence* $m > 0$*). Then*

$$\hat{h}(P') \leq \frac{1}{4}\log m + \frac{1}{3}\log 2.$$

To prove the lemmas we can use the decomposition of the canonical height into local heights:

$$\hat{h}(Q) = \hat{h}_\infty(Q) + \sum_{p:\text{prime}} \hat{h}_p(Q) = \hat{h}_\infty(Q) + \hat{h}_{\text{fin}}(Q).$$

If $A < 0$, then $E(\mathbb{R})$ has two connected components and

$$x(2^k Q) \geq \sqrt{-A} \tag{4.1}$$

holds for $k \geq 1$. Hence by Tate's series, on the curve of the form $E : y^2 = x^3 + Ax$, we have

$$
\begin{aligned}
\hat{h}_\infty(Q) &= \frac{1}{2}\log|x(Q)| + \frac{1}{8}\sum_{k=0}^{\infty}\frac{\log|z_k(Q)|}{4^k} \\
&= \frac{1}{8}\log|x^4(Q)z_0(Q)| + \frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z_k(Q)|}{4^k} \qquad (4.2)\\
&= \frac{1}{4}\log|x^2(Q) - A| + \frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z_k(Q)|}{4^k},
\end{aligned}
$$

where $z_k(Q) = z(2^kQ)$, $z(Q) = (1 - A/x(Q)^2)^2$, which are generally defined by

$$z(Q) = 1 - b_4x(Q)^{-2} + 2b_6x(Q)^{-3} - b_8x(Q)^{-4}$$

with the usual quantities associated with the Weierstrass equation. Note that we omit the term $(\log|\Delta(E)|)/12$ in $\hat{h}_\infty(\mathbb{Q})$ and $(\log|\Delta(E)|_v)/12$ in $\hat{h}_v(\mathbb{Q})$, since they are canceled out in summing up the local heights. Now inequality (4.1) implies for $k \geq 1$

$$z_k(Q) = \Big(1 + \frac{-A}{x(2^kQ)^2}\Big)^2 \in [1, 4],$$

and so

$$\frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z_k(Q)|}{4^k} \in \Big[0, \frac{1}{12}\log 2\Big]. \qquad (4.3)$$

If $A > 0$, then $E(\mathbb{R})$ has only one connected component and $x(2^kQ)$ may be close to 0, which causes difficulties with estimates of $z_k(Q)$. So as in [11, Lemma 3.3] we use the shifted model

$$E' : (y')^2 = (x')^3 - 3A^{1/2}(x')^2 + 4Ax' - 2A^{3/2}$$

over $\mathbb{R}$ of $y^2 = x^3 + Ax$ $(A > 0)$ via $x' = x + A^{1/2}$. Concerning the model, $x'(Q) \geq A^{1/2}$ for $Q \in E'(\mathbb{R})$ and

$$z'(Q) = 1 - 8Ax'(Q)^{-2} + 16A^{3/2}x'(Q)^{-3} - 8A^2x'(Q)^{-4}$$

and $z'_k(Q) = z'(2^k Q)$. By the definition of the local height, $\hat{h}_\infty$ is invariant under such shifting and so again by Tate's series

$$\begin{aligned}\hat{h}_\infty(Q) &= \frac{1}{2}\log|x'(Q)| + \frac{1}{8}\sum_{k=0}^{\infty}\frac{\log|z'_k(Q)|}{4^k}\\ &= \frac{1}{8}\log|x'(Q)^4 z'_0(Q)| + \frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z'_k(Q)|}{4^k}\\ &= \frac{1}{8}\log|x'(Q)^4 - 8Ax'(Q)^2 + 16A^{3/2}x'(Q) - 8A^2|\\ &\quad + \frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z'_k(Q)|}{4^k}.\end{aligned} \tag{4.4}$$

By a bit of calculus we can see

$$\frac{dz'}{dx'} = \frac{16A(x' - A^{1/2})(x' - 2A^{1/2})}{(x')^5},$$

which gives the estimate of $z'(Q)$ under the condition $x'(Q) \geq A^{1/2}$:

$$z'_k(Q) \in [1/2, 1],$$

hence

$$\frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z'_k(Q)|}{4^k} \leq 0. \tag{4.5}$$

Proof of Lemma 4.3. Write $P = (u, v)$ and $P^- = (2(u+v^2), 4v(u+v^2))$ with integers u, v.

First to compute $\hat{h}_{\mathrm{fin}}(P^-)$ we use [11, Lemmas 4.1 and 5.1]. Note that we omit the contribution of the terms $(\log|\Delta(E)|_v)/12$, as explained above. So we have

$$\hat{h}_{\mathrm{fin}}(P^-) = -\frac{1}{4}\log\prod_{2\neq p_i|U,m} p_i^{e_i} - \frac{1}{2}\log 2 \leq -\frac{1}{4}\log|U| - \frac{1}{2}\log 2, \tag{4.6}$$

where $U = u + v^2$ and $e_i = v_{p_i}(4m)$.

Now assume $m > 0$. Then by (4.2) and (4.3) with $A = -4m$ we have

$$\begin{aligned}\hat{h}_\infty(P^-) &= \frac{1}{4}\log|4U^2 + 4m| + \frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z_k(P^-)|}{4^k}\\ &\leq \frac{1}{4}\log(U^2 + |m|) + \frac{1}{2}\log 2 + \frac{1}{12}\log 2.\end{aligned} \tag{4.7}$$

Hence we have

$$\begin{aligned}\hat{h}(P^-) &\le \frac{1}{4}\log(U^2+|m|)+\frac{1}{2}\log 2+\frac{1}{12}\log 2-\frac{1}{4}\log|U|-\frac{1}{2}\log 2\\ &\le \frac{1}{4}\log(|U|+\frac{|m|}{|U|})+\frac{1}{12}\log 2\\ &\le \frac{1}{4}\log(|m|+1)+\frac{1}{12}\log 2,\end{aligned}$$

where we use the fact that $f(x)=x+k/x\le f(1)=k+1$ for $1\le x\le k$ with $k>1$.

Next assume $m<0$. Then we use (4.4) with (4.5). By substituting $x'(Q)=x'(P^-)=2(u+v^2)+A^{1/2}$ with $A=-4m=-4(u^2-v^4)$, we find

$$\begin{aligned}&x'(Q)^4-8Ax'(Q)^2+16A^{3/2}x'(Q)-8A^2\\ &\quad=64\big(v^2+u\big)^2\left(2v^2\sqrt{v^4-u^2}+u^2\right)\\ &\quad=64U^2(2v^2|m|^{1/2}+u^2).\end{aligned}$$

Since $v^2=U-u\le|m|-u$, we have $u\le|m|$ and

$$2v^2\,|m|^{1/2}+u^2\le 2(|m|-u)|m|^{1/2}+u^2=\left(u-|m|^{1/2}\right)^2-|m|+2|m|^{3/2}=:F(u).$$

Then it is not difficult to see, for $1\le u\le|m|$,

$$F(u)\le F(|m|)=|m|^2.$$

Consequently we have

$$\hat{h}_\infty(P^-)\le\frac{1}{8}\log(64\cdot U^2|m|^2)$$

and so

$$\hat{h}(P^-)\le\frac{1}{8}\log(64\cdot U^2|m|^2)-\frac{1}{4}\log|U|-\frac{1}{2}\log 2=\frac{1}{4}\log|m|+\frac{1}{4}\log 2.$$

□

Proof of Lemma 4.4. We can prove this by the same manner as above.

Write $P=(u,v)$ and $P'=(-v^2,uv)$ with integers u,v. By [11, Lemmas 4.1 and 5.1] we have

$$\hat{h}_{\text{fin}}(P')=-\frac{1}{4}\log\prod_{2\ne p_i|v,m}p_i^{e_i}+0\le 0.$$

Also by (4.2) with (4.3)

$$\begin{aligned}\hat{h}_\infty(P')&=\frac{1}{4}\log|v^4+m|+\frac{1}{8}\sum_{k=1}^{\infty}\frac{\log|z_k(P')|}{4^k}\\ &\le\frac{1}{4}\log(m+m)+\frac{1}{12}\log 2=\frac{1}{4}\log m+\frac{1}{3}\log 2,\end{aligned}$$

where we note $v^4 \le u^2 + v^4 = m$. Hence we have

$$\hat{h}(P') \le \frac{1}{4}\log m + \frac{1}{3}\log 2.$$

□

5. Proofs of the theorems

Proof of Theorem 1.1. We claim that if $uv \neq 0$, then $P = (u, v)$ is a non-torsion point. Indeed, by [6, Theorem 5.2] we have $E_m^-(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$ unless $m \neq -1$. So any rational torsion point is a 2-torsion point and thus $v(u+v^2) = 0$. If $u+v^2 = 0$, then $m = 0$, a contradiction and so $v = 0$. In the case $m = -1$ we have $E_m^-(\mathbb{Q})_{\text{tors}} = \langle(2,4)\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $\psi((2,4)) = (0,1)$.

Suppose either $\varphi^-(P_1) = P_1^- = kQ$ or $\varphi^-(P_1 + T) = P_1^- + T^- = kQ$ for some rational point $Q \in E_m^-(\mathbb{Q})$ with a positive integer k. Note that $\hat{h}(P_1^- + T^-) = \hat{h}(P_1^-)$. If $|m| \ge 2$, then by Lemmas 4.1 and 4.3 we have

$$k^2 = \frac{\hat{h}(P_1^-)}{\hat{h}(Q)} < \frac{\frac{1}{4}\log|2m|}{\frac{1}{16}\log|m|} \le 8,$$

since $\frac{1}{4}\log|2m| \ge \frac{1}{4}\log(|m|+1) + \frac{1}{12}\log 2$ for $|m| \ge 2$, which means $k = 1, 2$. But the latter is impossible by Lemma 3.1. Now the proof for $|m| \ge 2$ is complete.

On the other hand, the only integral points on C_m^- are $(u, v) = (\pm 1, 0)$ if $m = 1$ and $(u, v) = (0, \pm 1)$ if $m = -1$, in each case of which there is no points satisfying $uv \neq 0$. □

Proof of Corollary 1.2. Let P_1 be an integral point on C_m^-. (If there exists no integral point, then we have nothing to prove.) Recall that if $Q \in C_m^-(\mathbb{Q})$ is an integral point, then $Q^- \in E_m^-(\mathbb{Q})$ is also an integral point.

If m is not a square, then $E_m^-(\mathbb{Q}) = \langle P_1^-, T^-\rangle$ by Theorem 1.1. So for any rational non-torsion point $Q \in C_m^-(\mathbb{Q})$, we have $Q^- = kP_1^- + lT^-$, $k \in \mathbb{Z}, l \in \mathbb{Z}/2\mathbb{Z}$. Further if Q is an integral point, then $|k| \le 1$ by Theorem 1.1. The four relevant points are actually integral as $P_1 = (a_1, b_1)$, $-P_1 = (a_1, -b_1)$, $P_1 + T = (-a_1, -b_1)$ and $-P_1 + T = (-a_1, b_1)$. Recall that the torsion point $T^- = (0, 0)$ corresponds to one of the points at infinity on C_m^-, which is not integral.

If m is a square, say $m = m_0^2$, then $E_m^-(\mathbb{Q}) = \langle P_1^-, T^-, T_1^-\rangle$ by Theorem 1.1. So if a non-torsion point $Q^- = kP^- + l_0T^- + l_1T_1^- \in E_m^-(\mathbb{Q})$ for some integers k, l_0, l_1 is an integral point, then $|k| = 1$. The points $\pm P_1^-$, $\pm P_1^- + T^-$, $T_1^- = (-m_0, 0)$ and $T^- + T_1^- = (m_0, 0)$ are always integral points on E_m^-, and the corresponding points $\pm P_1$, $\pm P_1 + T$, T_1, $T + T_1$ on C_m^- are also integral. We now claim that none of the points $\pm P_1 + T_1$, $\pm P_1 + T + T_1 (= \pm P_1 + T_2)$ is integral on C_m^-, which shows that C_m^- has exactly six integral points $\pm P_1$, $\pm P_1 + T$, T_1, $T + T_1$. It suffices to show that neither $P_1 + T_1 =$

$\psi^-(P_1^- + T_1^-)$ nor $P_1 + T_2 = \psi^-(P_1^- + T_2^-)$ is integral on C_m^-. Indeed, let $d = \gcd(a_1, b_1)$, $a_1' = a_1/d$ and $b_1' = b_1/d$. Then, $m = m_0^2 = a_1^2 - b_1^4 = d^2((a_1')^2 - d^2(b_1')^4)$. Putting $m_0' = m_0/d$, we have

$$(m_0')^2 = (a_1')^2 - d^2(b_1')^4.$$

Since m_0 is square-free and $\gcd(a_1', db_1') = 1$, we see that b_1' is even and we may write

$$a_1' = A^2 + B^2,\ m_0' = A^2 - B^2,\ d(b_1')^2 = 2AB$$

for some coprime integers A and B with $A \not\equiv B \pmod 2$. We then have

$$P_1^- + T_1^- = \left(-\frac{4B^2(A^2 - B^2)}{(b_1')^2}, -\frac{8B^2(A^2 - B^2)^2}{(b_1')^3}\right).$$

It follows from (1.2) that

$$v(P_1 + T_1)\left(= v(\psi^-(P_1^- + T_1^-))\right) = \frac{A^2 - B^2}{b_1'}.$$

However, since $2AB \equiv 0 \pmod{b_1'}$, $\gcd(2AB, A^2 - B^2) = 1$ and b_1' is even (hence $b_1' > 1$), $v(P_1 + T_1)$ cannot be an integer. Therefore, we conclude that $P_1 + T_1$ is not an integral point on C_m^-. It can be similarly shown that $P_1 + T_2 = P_1 + T + T_1$ cannot be integral by noting that

$$P_1^- + T_2^- = \left(\frac{4A^2(A^2 - B^2)}{(b_1')^2}, -\frac{8A^2(A^2 - B^2)^2}{(b_1')^3}\right).$$

□

Proof of Theorem 1.3. Let ν be the group index of the sublattice generated by $\{P_1, P_2\}$ in the full lattice of rank 2 in $C_m^-(\mathbb{Q})/C_m^-(\mathbb{Q})_{\text{tors}}$ and λ a positive number such that $\hat{h}(P^-) > \lambda$ for any non-torsion point P^- in $E_m^-(\mathbb{Q})$. We know from Lemma 3.2 (see also Remark 3.4) that P_1^- and P_2^- are independent modulo $E_m^-(\mathbb{Q})_{\text{tors}}$. Then by Siksek's theorem ([9, Theorem 3.1]) with Lemmas 4.1 and 4.3 we have, for $|m| \geq 5000$,

$$\nu \leq \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_1^-)\hat{h}(P_2^-)}}{\lambda} \leq \frac{2}{\sqrt{3}} \frac{\frac{1}{4}\log|2m|}{\frac{1}{16}\log|m|} < 5,$$

which means $\nu = 1, 2, 3, 4$. But we have $2 \nmid \nu$ by Lemma 3.2. Further by Theorem 1.1, we have $P_1^-, P_2^- \notin 3E_m^-(\mathbb{Q})$. So with the assumption $P_1^- \pm P_2^- \notin 3E_m^-(\mathbb{Q})$ we conclude $3 \nmid \nu$, which means $\nu = 1$.

For $|m| < 5000$ we have $\nu < 10$, so it suffices to see that any linear combination of P_1^-, P_2^- and T^- (and further T_1^- in case m is a square) does not have a p-division point in $E_m^-(\mathbb{Q})$ for $p \in \{5, 7\}$ as long as m is fourth-power-free. We checked this using a program written in Sage ([8]). □

PROOF OF COROLLARY 1.4. Note s, t are nonzero for m to be square-free. Since

$$\begin{aligned} m = 3(s^4 + s^2t^2 + t^4) &= (2s^2 + st + 2t^2)^2 - (s+t)^4 \\ &= (2s^2 - st + 2t^2)^2 - (s-t)^4, \end{aligned}$$

we see that P_1 and P_2 defined by (1.4) are integral points on C_m^-. So to use Theorem 1.3 it suffices to show that both $P_1^- \pm P_2^-$ are indivisible by 3 in $E_m^-(\mathbb{Q})$. We do this by height estimation.

By the formula in the proof of Lemma 3.2 with

$$\begin{aligned} a_1 &= st + 2(s^2 + t^2),\ b_1 = s + t, \\ a_2 &= st - 2(s^2 + t^2),\ b_2 = s - t, \end{aligned}$$

we have

$$x(P_1^- + P_2^-) = -3t^2, \quad x(P_1^- - P_2^-) = -3s^2.$$

(Note if $P = (u, v)$, then $-P = (u, -v)$ on C_m^-.) Now by (4.2) and (4.3) we have

$$\hat{h}_\infty(P_1^- + P_2^-) \le \frac{1}{4}\log|9t^4 + 4m| + \frac{1}{12}\log 2$$

and also we have

$$\hat{h}_{\text{fin}}(P_1^- + P_2^-) \le -\frac{1}{4}\log 3$$

by [11, Lemmas 4.1 and 5.1], which may not be the best. Summing them up, we have

$$\begin{aligned} \hat{h}(P_1^- + P_2^-) &\le \frac{1}{4}\log|9t^4 + 4m| + \frac{1}{12}\log 2 - \frac{1}{4}\log 3 \\ &\le \frac{1}{4}\log|9m + 4m| + \frac{1}{12}\log 2 - \frac{1}{4}\log 3 \\ &= \frac{1}{4}\log m + \frac{1}{4}\log 13 + \frac{1}{12}\log 2 - \frac{1}{4}\log 3 \\ &\le \frac{1}{4}\log m + 0.425. \end{aligned}$$

Similarly

$$\hat{h}(P_1^- - P_2^-) \le \frac{1}{4}\log m + 0.425.$$

Now any non-torsion rational point $Q \in 3E_m^-(\mathbb{Q})$ satisfies $\hat{h}(Q) > 3^2 \cdot \frac{1}{16}\log m$ by Lemma 4.1. But

$$\frac{1}{4}\log m + 0.425 < \frac{9}{16}\log m$$

holds for $m \ge 4$, which contradicts $s, t \ge 1$. So we have $P_1^- \pm P_2^- \notin 3E_m^-(\mathbb{Q})$ and by Theorem 1.3 the proof is complete. □

Proof of Theorem 1.5. Assume that C_m^- has integral points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ with $(|a_1|, |b_1|) \neq (|a_2|, |b_2|)$ (otherwise, there is nothing to prove). Then, Lemma 3.2 implies that P_1^-, P_2^- and T^- are independent in $E_m^-(\mathbb{Q})$. Now, let $P = (u, v)$ be an integral point on C_m^-. Since the rank of $E_m^-(\mathbb{Q})$ is two and $E_m^-(\mathbb{Q})_{\mathrm{tors}} = \langle T^- \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, there exist integers k_0, k_1, k_2, k_3 such that

$$k_0 P^- = k_1 P_1 - k_2 P_2^- + k_3 T^-.$$

We may assume that $\gcd(k_0, k_1, k_2, k_3) = 1$, and hence we see from Lemma 3.2 that k_0 is odd. Therefore, we have

$$P^- \equiv P_0^- \pmod{2E_m^-(\mathbb{Q})},$$

where

$$P_0^- \in \{\mathcal{O}^-, T^-, P_1^-, P_1^- + T^-, P_2^-, P_2^- + T^-, P_1^- + P_2^-, P_1^- + P_2^- + T^-\}.$$

We examine each case using Lemma 2.2 with $A = m$ and $K = \mathbb{Q}$. Note that $\Phi(P^-) = 2(u + v^2)\Box$, where $\Box$ denotes the square of a rational number.

If $P_0^- = \mathcal{O}^-$, then $2(u + v^2) = \Box$, which cannot happen, since $m = (u + v^2)(u - v^2)$ is square-free and odd.

If $P_0^- = P^-$, then $2(u + v^2) = -4m\Box$, that is, $u + v^2 = -2m\Box$, which is impossible, since m is odd.

If $P_0^- \in \{P_1^-, P_1^- + T^-\}$, then $u + v^2 = (\pm a_1 + b_1^2)\Box$. Since $m = (u + v^2)(u - v^2) = (\pm a_1 + b_1^2)(\pm a_1 - b_1^2)$ is square-free, $u + v^2 = \pm a_1 + b_1^2$, which is equivalent to $u - v^2 = \pm a_1 - b_1^2$. Hence, $u = \pm a_1$ and $v^2 = b_1^2$. It follows that $P \in \{(a_1, \pm b_1), (-a_1, \pm b_1)\}$.

Similarly, if $P_0^- \in m\{P_2^-, P_2^- + T^-\}$, then $P \in \{(a_2, \pm b_2), (-a_2, \pm b_2)\}$.

Finally, if $P_0^- \in \{P_1^- + P_2^-, P_1^- + P_2^- + T^-\}$, then

$$2(u + v^2) = (\pm a_1 + b_1^2)(a_2 + b_2^2)\Box,$$

which again contradicts the assumption that m is odd. ∎

Now we proceed to proofs for C_m^+.

Proof of Theorem 1.6. It suffices to show that the point $P_1' := (-b_1^2, a_1 b_1)$ can be extended to a basis for $\bar{E}_m^+(\mathbb{Q})$ modulo $\bar{E}_m^+(\mathbb{Q})_{\mathrm{tors}}$. Indeed, since $g(P_1^+) = 2P_1'$, we then see that the point $g(P_1^+)$ with the torsion point $T_0' = (0, 0)$ generates a rank one subgroup of $\bar{E}_m^+(\mathbb{Q})$. Thus, for any point $P^+ \in E_m^+(\mathbb{Q})$, we have $2g(P^+) = l_1 g(P_1^+) + l_2 T_0'$ with some integers l_1, l_2, and hence $4P^+ = 2l_1 P_1^+$, which yields $2P^+ = \pm l_1 P_1^+ + l_2' T^+$ with $l_2' \in \{0, 1\}$. It follows from Lemma 3.3 that l_1, l_2' are even and $\{P_1^+, T^+\}$ can be extended to a basis for $E_m^+(\mathbb{Q})$.

Suppose $P_1' = kQ' + lT_0'$ for some rational point $Q' \in E_m^+(\mathbb{Q})$ with a positive integer k and $l \in \{0,1\}$. By Lemmas 4.2 and 4.4 we have

$$k^2 = \frac{\hat{h}(P_1' + lT_0')}{\hat{h}(Q')} = \frac{\hat{h}(P_1')}{\hat{h}(Q')} \leq \frac{\frac{1}{4}\log m + \frac{1}{3}\log 2}{\frac{1}{16}\log m + \frac{5}{16}\log 2} < 4,$$

which means $k = 1$. Hence we can conclude that P_1' can be extended to a basis for $\bar{E}_m^+(\mathbb{Q})$ modulo $\bar{E}_m^+(\mathbb{Q})_{\mathrm{tors}}$. ∎

Proof of Corollary 1.7. Let $P_1 = (a_1, b_1)$ be an integral point in $C_m^+(\mathbb{Q})$. Then by the proof of Theorem 1.6, for any integral point P on C_m^+ we can write

$$P' = k_1 P_1' + l_1 T',$$

where k_1 is an integer, $l_1 \in \{0,1\}$ and $T' \in \bar{E}_m^+(\mathbb{Q})_{\mathrm{tors}}$. Then, the proof of Theorem 1.6 implies that $|k_1| \leq 1$.

It is obvious that $\pm P_1' = (-b_1^2, \pm a_1 b_1)$ correspond to the integral points

$$(a_1, \pm b_1),\ (-a_1, \pm b_1)$$

on C_m^+. Let $T_0' = (0,0)$. Since

$$\pm P_1' + T_0' = \left(\frac{m}{b_1^2}, \pm\frac{a_1 m}{b_1^3}\right),$$

the x-coordinates of points $\pm P_1' + T_0'$ are positive (note that $m = a_1^2 + b_1^4 > 0$). On the other hand, the x-coordinate of the image $P' = (-b^2, ab)$ of any integral point $P = (a,b)$ on C_m^+ is always negative. Thus, neither of the points $\pm P_1' + T_0'$ corresponds to an integral point on C_m^+. This shows the assertion in the case where m is non-square.

Suppose now that $m = m_0^2$ for a square-free positive integer m_0. In this case, we have additional integral points $(\pm m_0, 0)$ on C_m^+, which map to $T_0' = (0,0)$ in $\bar{E}_m^+(\mathbb{Q})$. Let $T_1' = (-m_0, 0)$ and $T_2' = (m_0, 0)$ be the remaining 2-torsion points in $\bar{E}_m^+(\mathbb{Q})$. We have

$$x(\pm P_1' + T_1') = \frac{m_0(m_0 + b_1^2)}{m_0 - b_1^2} = \frac{m_0 a_1^2}{(m_0 - b_1^2)^2}$$

and

$$x(\pm P_1' + T_2') = -\frac{m_0(m_0 - b_1^2)}{m_0 + b_1^2} = -\frac{m_0 a_1^2}{(m_0 + b_1^2)^2}.$$

Since m_0 is square-free, we see that any integral point on C_m^+ does not map to a point Q via φ', where

$$Q \in \{T_1', T_2', \pm P_1' + T_1', \pm P_1' + T_2'\}.$$

This shows that C_m^+ has at most six integral points, expressed as $(a_1, \pm b_1)$, $(-a_1, \pm b_1)$, $(\pm m_0, 0)$. ∎

Proof of Theorem 1.8. It suffices to show that the points $P_1' := (-b_1^2, a_1b_1)$ and $P_2' := (-b_2^2, a_2b_2)$ can be extended to a basis for $\bar{E}_m^+(\mathbb{Q})$ modulo $\bar{E}_m^+(\mathbb{Q})_{\rm tors}$. Indeed, since $g(P_1^+) = 2P_1'$ and $g(P_2^+) = P_1' + P_2'$, we then see that the points $g(P_1^+)$ and $g(P_2^+)$ with the torsion point $\bar{T}^+ = (0,0)$ generate a rank two subgroup of $\bar{E}_m^+(\mathbb{Q})$. Thus, for any point $P^+ \in E_m^+(\mathbb{Q})$, we have $2g(P^+) = l_1 g(P_1^+) + l_2 g(P_2^+) + l_3\bar{T}^+$ with some integers l_1, l_2, l_3, and hence $4P^+ = 2l_1P_1^+ + 2l_2P_2^+$, which yields $2P^+ = \pm l_1 P_1^+ \pm l_2 P_2^+ + l_3' T^+$ with $l_3' \in \{0,1\}$. It follows from Lemma 3.3 that l_1, l_2, l_3' are even and P_1^+, P_2^+, T^+ can be extended to a basis for $E_m^+(\mathbb{Q})$.

Let ν be the lattice index of $\{P_1', P_2'\}$. Combining Siksek's theorem with Lemmas 4.2 and 4.4 shows that

$$\nu \le \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_1')\hat{h}(P_2')}}{\lambda} \le \frac{2}{\sqrt{3}} \frac{\frac{1}{4}\log m + \frac{1}{3}\log 2}{\frac{1}{16}\log m + \frac{5}{16}\log 2} < 5,$$

which means $\nu = 1, 2, 3, 4$. But we have $2 \nmid \nu$ by Lemma 3.3. Further in the proof of Theorem 1.6, we have showed $P_1', P_2' \notin 3\bar{E}_m^+(\mathbb{Q})$. Now the assumption $P_2 \notin 3C_m^+(\mathbb{Q})$ implies $P_1' + P_2' \notin 3\bar{E}_m^+(\mathbb{Q})$, since otherwise $g(P_2^+) = P_1' + P_2' = 3Q$ for some Q in $\bar{E}_m^+(\mathbb{Q})$, which leads to $2P_2^+ = 3\hat{g}(Q)$, a contradiction. Similarly $P_1 - P_2 \notin 3C_m^+(\mathbb{Q})$ implies $P_1' - P_2' \notin 3\bar{E}_m^+(\mathbb{Q})$.

So we conclude $3 \nmid \nu$, which means $\nu = 1$. ∎

Proof of Corollary 1.9. Since

$$\begin{aligned} m = 5(s^4 + 3s^2t^2 + t^4) &= (2s^2 + st + 2t^2)^2 + (s-t)^4 \\ &= (2s^2 - st + 2t^2)^2 + (s+t)^4, \end{aligned}$$

the points P_1 and P_2 defined by (1.8) are integral points on C_m^+. Thus, it suffices to show that $P_1' \pm P_2'$ is indivisible by 3 in $\bar{E}_m^+(\mathbb{Q})$.

By the addition formula on $\bar{E}_m^+ : y^2 = x^3 - mx$ we have

$$\begin{aligned} P_1' - P_2' &= \left(\frac{(3s^2+2t^2)^2}{(2s)^2}, \ -\frac{(3s^2+2t^2)(s^4 - 12s^2t^2 - 4t^4)}{(2s)^3} \right), \\ P_1' + P_2' &= \left(\frac{(3t^2+2s^2)^2}{(2t)^2}, \ +\frac{(3t^2+2s^2)(t^4 - 12t^2s^2 - 4s^4)}{(2t)^3} \right), \end{aligned}$$

from which we can see that if we write $P_1' - P_2' = (a/d^2, b/d^3)$ with $\gcd(a,d) = \gcd(b,d) = 1$ and $d > 0$, then $d \le |2s|$. So we have

$$\hat{h}_{\rm fin}(P_1' - P_2') \le \log|2s|$$

by [11, Lemmas 4.1 and 5.1]. Further by (4.2) and (4.3) we have

$$\hat{h}_\infty(P_1' - P_2') \le \frac{1}{4}\log\left| \frac{(3s^2+2t^2)^4}{(2s)^4} + m \right| + \frac{1}{12}\log 2.$$

Summing them up, we have

$$\begin{aligned}\hat{h}(P_1' - P_2') &\leq \frac{1}{4}\log|(3s^2+2t^2)^4+(2s)^4 m| + \frac{1}{12}\log 2\\ &\leq \frac{1}{4}\log|(161/25)m^2| + \frac{1}{12}\log 2\\ &= \frac{1}{2}\log m + \frac{1}{4}\log(161/25) + \frac{1}{12}\log 2 \leq \frac{1}{2}\log m + 0.5234,\end{aligned}$$

where the second inequality comes from a direct estimate of $(161/25)m^2 - (3s^2+2t^2)^4 - (2s)^4 m$, to be positive. By almost the same computation we have

$$\hat{h}(P_1' + P_2') \leq \frac{1}{2}\log m + 0.5234.$$

Now any non-torsion rational point $Q \in 3\bar{E}_m^+(\mathbb{Q})$ satisfies

$$\hat{h}(Q) > 3^2\,(\frac{1}{16}\log m + \frac{5}{16}\log 2)$$

by Lemma 4.2. But clearly

$$\frac{1}{2}\log m + 0.5234 < 3^2\,\left(\frac{1}{16}\log m + \frac{5}{16}\log 2\right).$$

So we have $P_1' \pm P_2' \notin 3\bar{E}_m^+(\mathbb{Q})$ and by Theorem 1.8 the proof is complete. ☐

Proof of Theorem 1.10. The proof proceeds along similar lines to that of Theorem 1.5, except that we have to replace $E_m^-(\mathbb{Q})$ by $E_m^+(\mathbb{Q}(i))$.

Assume that C_m^+ has integral points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ with $(|a_1|, b_1^2) \neq (|a_2|, b_2^2)$. Let $P = (u, v)$ be an integral point on C_m^+. Then, by the same argument as in the proof of Theorem 1.5, we see from Lemma 3.6 that

$$P^+ \equiv P_0^+ \pmod{2E_m^+(\mathbb{Q}(i))},$$

where

$$P_0^+ \in \{\mathcal{O}^+,\, T^+,\, P_1^i,\, P_1^i + T^+,\, P_2^i,\, P_2^i + T^+,\, P_1^i + P_2^i,\, P_1^i + P_2^i + T^+\}.$$

We apply Lemma 2.2 with $A = -m$ and $K = \mathbb{Q}(i)$.

If $P_0^+ = \mathcal{O}^+$, then $2(iu+v^2) = \square$, since $2 = -i(1+i)^2$, we have $u - iv^2 = \square$, where $\square$ denotes the square of an element in $\mathbb{Q}(i)$. Since this also implies $u + iv^2 = \square$, we have $m = u^2 + v^4 = \square$, which contradicts the assumption.

If $P_0^+ = T^+$, then $iu + v^2 = 2m\square$, that is $u + iv^2 = \square$. In the same way as the previous case, we obtain a contradiction.

If $P_0^+ \in \{P_1^i,\, P_1^i + T^+\}$, then $iu + v^2 = (\pm i a_1 + b_1^2)\square$. Since m is square-free, we have $iu + v^2 \in \{ia_1 + b_1^2,\, -ia_1 + b_1^2\}$, and therefore, $P \in \{(a_1, \pm b_1), (-a_1, \pm b_1)\}$.

If $P_0^+ \in \{P_2^i,\, P_2^i + T^+\}$, then similarly we have $P \in \{(a_2, \pm b_2),\, (-a_2, \pm b_2)\}$.

If $P_0^+ \in \{P_1^i + P_2^i,\, P_1^i + P_2^i + T^+\}$, then

$$2(iu + v^2) = (\pm i a_1 + b_1^2)(i a_2 + b_2^2)\square,$$

that is,

$$(u - iv^2)(\pm ia_1 + b_1^2)(ia_2 + b_2^2) = \square.$$

Since this is equivalent to

$$(u + iv^2)(\mp ia_1 + b_1^2)(-ia_2 + b_2^2) = \square.$$

we obtain $m = \square$, which is a contradiction. ∎

Proof of Theorem 1.11. By Lemma 3.7 and the argument given in the proof of Theorem 1.8, it suffices to show that the points $P_q' := (-b^2, a^2b)$ and $\hat{P}_q' := (-a^2, ab^2)$ can be extended to a basis for $\bar{E}_m^+(\mathbb{Q})$ modulo $\bar{E}_m^+(\mathbb{Q})_{\text{tors}}$, which is nothing but the assertion of [5, Theorem 1.5 (1)]. ∎

Proof of Theorem 1.12. Assume that Q_m^+ has an integral point $P = (a, b)$. Let $R = (u, v)$ be an integral point on Q_m^+. Then, $R' = (-v^2, u^2v)$ is an integral point on $\bar{E}_m^+$. Since $v^2 \le \sqrt{u^2 + v^4} = \sqrt{m}$, we may examine the integral points (x, y) on $\bar{E}_m^+$ with $-\sqrt{m} \le x \le 0$. However, [5, Theorem 1.5 (2)] and its proof imply that if $\operatorname{rank} \bar{E}_m^+(\mathbb{Q}) = 2$, then such points are

$$T_0' = (0,0),\ \pm P_q' = (-b^2, \pm a^2 b),\ \pm \hat{P}_q' = (-a^2, \pm ab^2).$$

Note that since

$$x\left(\pm P_q' + T_0'\right) = \frac{m}{b^2} \quad \text{and} \quad x\left(\pm(P_q' - \hat{P}_q')\right) = \frac{(a^2 - ab + b^2)^2}{(a-b)^2},$$

none of the points $\pm P_q' + T_0'$ and $\pm(P_q' - \hat{P}_q')$ corresponds to an integral point on Q_m^+, even if $b = 1$ or $|a - b| = 1$, because each x-coordinate is positive. Moreover, T_0' also does not correspond to an integral point on Q_m^+, since if it does, then it would correspond to a point $(u, 0)$ on Q_m^+ and $m = u^4$, a contradiction. Therefore, we obtain eight integral points on Q_m^+ displayed in the theorem. ∎

Acknowledgements.

The authors thank the referees for their careful reading and helpful suggestions.

References

[1] J. W. S. Cassels, Lectures on elliptic curves, Cambridge University Press, Cambridge, 1991.

[2] I. Connell, Elliptic curve handbook, available online at `http://webs.ucm.es/BUCM/mat/doc8354.pdf`.

[3] Y. Fujita and T. Nara, *Generators and integral points on twists of the Fermat cubic,* Acta Arith. **168** (2015), 1–16.

[4] Y. Fujita and N. Terai, *On the rank of the elliptic curve $y^2 = x^3 - nx$,* Int. J. Algebra **6** (2012), 885–901.

[5] Y. Fujita and N. Terai, *Generators and integer points on the elliptic curve $y^2 = x^3 - nx$,* Acta Arith. **160** (2013), 333–348.

[6] A. Knapp, Elliptic Curves, Princeton University Press, Princeton, NJ, 1992.

[7] B. Newman, *Growth of torsion of elliptic curves with odd-order torsion over quadratic cyclotomic fields,* preprint, https://arxiv.org/abs/1604.01153.
[8] Sage, Open Source Mathematics Software, http://www.sagemath.org/.
[9] S. Siksek, *Infinite descent on elliptic curves,* Rocky Mountain J. Math. **25** (1995), 1501–1538.
[10] J. H. Silverman and J. Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
[11] P. Voutier and M. Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves $y^2 = x^3 + ax$,* Int. J. Number Theory **9** (2013), 1141–1170.

Y. 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

T. Nara
Faculty of Engineering
Tohoku-Gakuin University
1-13-1 Chuo, Tagajo, Miyagi 985-8537
Japan
E-mail: sa4m19@math.tohoku.ac.jp

Received: 15.1.2019.
Revised: 6.6.2019.