ACTA ARITHMETICA
168.1 (2015)

# Generators and integral points on twists of the Fermat cubic

by

YASUTSUGU FUJITA (Narashino) and TADAHISA NARA (Tagajo)

**1. Introduction.** Consider a cubic twist of the Fermat cubic $x^3+y^3=1$. Let $m$ be a non-zero integer and

$$C_m : x^3 + y^3 = m \tag{1.1}$$

the elliptic curve. In this paper we study integral points on $C_m$ (i.e. integral solutions of (1.1)) and generators for the Mordell–Weil group when we vary $m$. In what follows, we assume that $m$ is positive and cube-free, since $C_m$ is isomorphic over $\mathbb{Q}$ to the elliptic curve $x^3 + y^3 = mu^3$ for $u \in \mathbb{Q}^\times$. The coordinate transformation

$$x \mapsto \frac{36m + y}{6x}, \quad y \mapsto \frac{36m - y}{6x}$$

gives a birational equivalence between $C_m$ and the elliptic curve

$$E_m : y^2 = x^3 - 432m^2. \tag{1.2}$$

The transformation $C_m \to E_m$, denoted by $\varphi$, can be expressed as

$$\varphi(x, y) = \big(12(x^2 - xy + y^2), 36(x - y)(x^2 - xy + y^2)\big),$$

and via the birational equivalence the addition law on $C_m$ is defined. Note that if $P = (x, y) \in C_m$, then $-P = (y, x)$.

Jędrzejak [5] estimated the canonical height on the elliptic curve $E_m$, which resulted in showing that a rank one subgroup of the Mordell–Weil group contains no integral arithmetic progressions if the defining equation is global minimal.

The first main theorem of this paper is the following.

THEOREM 1.3. *Let $m$ be a positive cube-free integer. If $P_1 \in C_m(\mathbb{Q})$ is an integral point, then $P_1$ can be in a system of generators for $C_m(\mathbb{Q})$. In particular, if the rank of $C_m(\mathbb{Q})$ is one, then $P_1$ generates $C_m(\mathbb{Q})$.*

---

2010 *Mathematics Subject Classification*: Primary 11G05, 11D59; Secondary 11G50.
*Key words and phrases*: elliptic curve, Fermat cubic, Thue equation, canonical height.

DOI: 10.4064/aa168-1-1

Corollary 1.4 ([3, Corollary 1.3]). *Let $m$ be a positive cube-free integer. If the rank of $C_m(\mathbb{Q})$ is one, then $C_m$ has at most two integral points, either of which generates $C_m(\mathbb{Q})$.*

In [3], Everest, Ingram and Stevens studied an elliptic divisibility sequence on the curve

$$X^3 + Y^3 = mZ^3,$$

that is, the sequence $W_n$ defined by

$$n(U : V : W) = (U_n : V_n : W_n),$$

where $n(U : V : W)$ is the $n$-fold multiple of the point $(U : V : W)$ on the curve. They showed that $W_n$ has a primitive divisor for $n > 1$, from which Corollary 1.4 immediately follows (see Remark 1.9 below).

The second main theorem is concerned with the case where the rank of $C_m$ is greater than one.

Theorem 1.5. *Let $m$ be a positive cube-free integer. If $P_1$ and $P_2$ are integral points on $C_m$ such that $P_1 \neq \pm P_2$, then they can be in a system of generators for $C_m(\mathbb{Q})$. In particular, if the rank of $C_m(\mathbb{Q})$ is two, then $P_1$ and $P_2$ generate $C_m(\mathbb{Q})$.*

Corollary 1.6. *Let $m$ be a positive cube-free integer. If the rank of $C_m(\mathbb{Q})$ is two, then $C_m$ has at most six integral points, which can be expressed as $\pm P_1, \pm P_2, \pm(P_1 + P_2)$ with generators $P_1$ and $P_2$ for $C_m(\mathbb{Q})$.*

Remark 1.7. (1) The upper bound of 6 for integral points on $C_m$ in Corollary 1.6 is optimal. In fact, if $m = 3367$, then the rank of $C_m(\mathbb{Q})$ is two and the set of integral points on $C_m$ equals $\{\pm P_1, \pm P_2, \pm(P_1 + P_2)\}$, where $P_1 = (15, -2)$, $P_2 = (-9, 16)$ and $P_1 + P_2 = (34, -13)$.

(2) Several parameterizations of the equation $a_1^3 + b_1^3 = a_2^3 + b_2^3$ (coming from two integral points on $C_m$) with binary quadratic forms are known. For example, Ramanujan found

$$(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3 = (6a^2-4ab+4b^2)^3+(-5a^2+5ab+3b^2)^3$$

(see [4, p. 260]). For further examples, see Womack's thesis [13].

In general, Silverman [8] showed that if $f(x, y)$ is a cubic form with non-zero discriminant and $m$ is a cube-free integer, then the elliptic curve $C_{f,m} : f(x, y) = m$ has at most $\kappa^{R_{f,m}} + 1$ integral points for some absolute constant $\kappa$, where $R_{f,m}$ is the rank of $C_{f,m}(\mathbb{Q})$.

The third main theorem of the paper is an explicit version of the above mentioned result of Silverman in the case when $f(x, y) = x^3 + y^3$.

Theorem 1.8. *Let $m$ be a positive cube-free integer. If the rank of $C_m(\mathbb{Q})$ is $r$, then $C_m$ has at most $3^r - 1$ integral points.*

REMARK 1.9. If $m = 2$, then it is easy to see that $C_m(\mathbb{Q}) = \{O, (1,1)\} \simeq \mathbb{Z}/2\mathbb{Z}$ by using the Magma function "MordellWeilGroup" [1]. Moreover this is the only case where $C_m(\mathbb{Q})$ has a non-trivial torsion point by [6, p. 134, Theorem 5.3]. So we may assume $m > 2$ in our proofs.

The theoretical key to proving the above theorems is to obtain "good" estimates for the canonical heights $\hat{h}$. In particular, it is essential to give a uniform lower bound for $\hat{h}$ (see Remark 2.16), since the known lower bound, Lemma 2.13 (see [5, Proposition 1] or [3, Lemma 4.3]), is of little use in proving Theorem 1.5, as one can see even from "the main term" of the estimate (see Remark 4.3). On the other hand, we cannot complete the proofs of theorems without numerical devices, among which the hardest part is checking $P + Q \notin 2C_m(\mathbb{Q})$ for integral points $P$ and $Q$ on $C_m$ in the proof of Theorem 1.5.

The organization of this paper is as follows. In Section 2 after reviewing the canonical height and the local height function, we estimate their values on our elliptic curve (1.2). In Section 3 by an algebraic argument we consider divisibility of integral points, which leads us to showing the independence of integral points. In Section 4 we prove the main theorems.

REMARK 1.10. After this paper had been submitted, P. Voutier informed us that together with M. Yabuta they recently obtained the best possible results on lower bounds for the canonical heights on the Mordell curves in [12, Theorem 1.4], where they give a better estimate on error terms than ours in Proposition 2.15. We would like to thank Professor Voutier for this helpful information.

## 2. Estimates of the canonical heights.

**2. Estimates of the canonical heights.** The notion of the canonical height is important to consider integral points or generators on elliptic curves. For a rational point $P = (n/d, *)$ ($\gcd(n, d) = 1$) on an elliptic curve over $\mathbb{Q}$, we define the *naïve height* $h$ by

$$h(P) = \log \max\{|n|, |d|\}$$

and the *canonical height* $\hat{h}$ by

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

For estimates of the canonical height, we usually consider the local height functions $\lambda_p$ for places $p$, because of the equality over $\mathbb{Q}$ (see [10, Section VI])

$$\hat{h}(P) = \sum_{p\le\infty} \lambda_p(P).$$

**2.1. The reduction of $E_m$.** In order to compute the local height functions, it is useful to know the reduction type of the elliptic curve. The following lemma summarizes the considerations in [5, p. 180], which used Tate's algorithm (cf. [10, p. 364]).

Lemma 2.1. *Let $E_m$ be the elliptic curve defined by the equation*

$$y^2 = x^3 - 432m^2. \tag{2.2}$$

*Then the reduction type (the Kodaira symbol) of $E_m$ is given in Tables 1–3, where $E_m(\mathbb{Q}_p)^0$ is the subgroup of $E_m(\mathbb{Q}_p)$ consisting of points with non-singular reduction modulo $p$, $c_p = |E_m(\mathbb{Q}_p)/E_m(\mathbb{Q}_p)^0|$ and $[u, r, s, t]$ denotes the transformation*

$$x \mapsto u^2x + r, \qquad y \mapsto u^3y + su^2x + t$$

*of $E_m$ which is performed in Tate's algorithm.*

**Table 1.** The reduction of $E_m$ modulo 3

| $m \pmod 9$ | 0 | $\pm 1$ | $\pm 2$ | $\pm 3$ | $\pm 4$ |
|---|---|---|---|---|---|
| reduction type | II | IV$^*$ | III$^*$ | II$^*$ | IV$^*$ |
| $c_3$ | 1 | 3 | 2 | 1 | 1 |
| $[u, r, s, t]$ | $[3, 0, 0, 0]$ | $[1, -6, 0, 0]$ | $[1, -6, 0, 0]$ | $[1, 0, 0, 0]$ | $[1, -6, 0, 0]$ |

**Table 2.** The reduction of $E_m$ modulo 2

| $m \pmod 4$ | 0 | $\pm 1$ | 2 |
|---|---|---|---|
| reduction type | IV$^*$ | I$_0$ | IV |
| $c_2$ | 1 | 1 | 1 |
| $[u, r, s, t]$ | $[2, 0, 0, 16]$ | $[2, 0, 0, -4]$ | $[2, 0, 0, 8]$ |

**Table 3.** The reduction of $E_m$ modulo $p$ $(> 3)$

| $m \pmod{p^2}$ | 0 | $p, 2p, \dots, (p-1)p$ | otherwise |
|---|---|---|---|
| reduction type | IV$^*$ | IV | I$_0$ |
| $c_p$ | 1 or 3 | 1 or 3 | 1 |
| $[u, r, s, t]$ | $[1, 0, 0, 0]$ | $[1, 0, 0, 0]$ | $[1, 0, 0, 0]$ |

Remark 2.3. In Table 3, we have $c_p = 3$ if and only if $\left(\frac{-3}{p}\right) = 1$.

**2.2. Height bounds for integral points on $C_m$.** Let $m$ be a cube-free positive integer, and let $P = (X, Y)$ be an integral point on the curve

$$C_m : x^3 + y^3 = m.$$

Then $P' = \varphi(P) = (12(X^2 - XY + Y^2), 36(X^2 - XY + Y^2)(X - Y))$ is an integral point on the curve

$$E_m : y^2 = x^3 - 432m^2. \tag{2.4}$$

Note that if $m \equiv \pm 3, \pm 4 \pmod 9$, then there is no integral point on $C_m$.

Now we set $U = X^2 - XY + Y^2$ $(\geq 0)$, $V = X - Y$, and so

$$P' = (12U, 36UV).$$

Since $m$ is cube-free, we have $U \equiv 1 \pmod 2$ and

$$\text{(2.5)}\qquad \operatorname{ord}_3 U = \begin{cases} 1 & \text{if } m \equiv 0 \pmod 9, \\ 0 & \text{if } m \equiv \pm 1, \pm 2 \pmod 9. \end{cases}$$

PROPOSITION 2.6. *Let $P$ be an integral point on $C_m$. Then for $P' = \varphi(P)$,*

$$\hat{h}(P') < \tfrac{1}{6}\log U + 0.1832 \leq \tfrac{1}{6}\log m + 0.1832.$$

*Further if $XY > 0$, then*

$$\hat{h}(P') < \tfrac{1}{9}\log m + 0.1832.$$

*Proof.* Using Tate's series [9, Theorem 1.2] we have

$$\text{(2.7)}\qquad \lambda_\infty(P') = \tfrac{1}{2}\log|x(P')| + \tfrac{1}{8}\sum_{r=0}^{\infty} 4^{-r}\log|z(2^r P')| - \tfrac{1}{12}\log|\Delta_m|,$$

where $z(R) = 1 + 8\cdot 432m^2/x(R)^3$ and $\Delta_m$ is the discriminant of $E_m$. Note that in this paper the local height function $\lambda_v$ is defined to be that in [9] with $-(1/12)\log|\Delta|_v$ added. In other words, our $\lambda_v$ corresponds to $\hat{\lambda}'_v$ in [9, p. 341]. Since $x(R) \geq (432m^2)^{1/3}$ for $R \in E_m(\mathbb{R})$, we have $\log|z(2^r P')| = \log z(2^r P') \leq \log 9$, and so

$$\text{(2.8)}\qquad \begin{aligned} \lambda_\infty(P') &\leq \tfrac{1}{2}\log|12U| + \tfrac{1}{8}\sum_{r=0}^{\infty} 4^{-r}\log 9 - \tfrac{1}{12}\log|\Delta_m| \\ &= \tfrac{1}{2}\log U + \log 2 + \tfrac{5}{6}\log 3 - \tfrac{1}{12}\log|\Delta_m|. \end{aligned}$$

Next we consider $\lambda_p(P')$ for a finite place $p$ using [9, Theorem 5.2]. Note that $E_m(\mathbb{Q}_p)^0$ is equal to the set of points $P \in E_m(\mathbb{Q}_p)$ satisfying either

$$\begin{aligned} &\operatorname{ord}_p(2y(P) + a_1x(P) + a_3) \leq 0, \quad \text{or} \\ &\operatorname{ord}_p(3x(P)^2 + 2a_2x(P) + a_4 - a_1y) \leq 0 \end{aligned}$$

if the Weierstrass equation is $p$-minimal.

For $p > 3$ not dividing $U$, we have $P' \in E_m(\mathbb{Q}_p)^0$, and by [9, Theorem 5.2],

$$\text{(2.9)}\qquad \lambda_p(P') = \tfrac{1}{2}\max\{-v_p(12U), 0\} + \tfrac{1}{12}v_p(\Delta_m) = \tfrac{1}{12}v_p(\Delta_m),$$

where $v_p(\cdot) = -\log|\cdot|_p$ $(= \operatorname{ord}_p(\cdot)\log p)$. For $p > 3$ dividing $U$, we have $P' \notin E_m(\mathbb{Q}_p)^0$. Then by Table 1 the reduction type is IV or IV*, and so by [9, Theorem 5.2],

$$\text{(2.10)}\qquad \begin{aligned} \lambda_p(P') &= \tfrac{1}{3}\log|\psi_2(P')|_p + \tfrac{1}{12}v_p(\Delta_m) \\ &= \tfrac{1}{3}\log|72UV|_p + \tfrac{1}{12}v_p(\Delta_m) = \tfrac{1}{3}\log|U|_p + \tfrac{1}{12}v_p(\Delta_m), \end{aligned}$$

where $\psi_2 = 2y$ is the division polynomial of $E_m$ (cf. [10, Exercise 3.7]).

For $p = 2$, we have $E_m(\mathbb{Q}_2) = E_m(\mathbb{Q}_2)^0$ by Table 2 and we consider the following minimal equations:

$$\begin{aligned} (y')^2 + y' &= (x')^3 - (27m^2+1)/4 && \text{if } m \text{ is odd,} \\ (y')^2 &= (x')^3 - 27m^2/4 && \text{if } m \text{ is even.} \end{aligned}$$

In any case the discriminant is $2^{-12}\Delta_m$ and $x'(P') = 2^{-2}12U$. Therefore

$$\begin{aligned} \lambda_2(P') &= \tfrac{1}{2}\max\{-v_2(2^{-2}12U), 0\} + \tfrac{1}{12}v_2(2^{-12}\Delta_m) \\ &= -\log 2 + \tfrac{1}{12}v_2(\Delta_m). \end{aligned} \tag{2.11}$$

For $p = 3$, in the case $m \equiv 0 \pmod 9$, we have $E_m(\mathbb{Q}_3) = E_m(\mathbb{Q}_3)^0$, and by considering the minimal equation

$$(y')^2 = (x')^3 - 16m^2/27,$$

we obtain

$$\begin{aligned} \lambda_3(P') &= \tfrac{1}{2}\max\{-v_3(3^{-2}12U), 0\} + \tfrac{1}{12}v_3(3^{-12}\Delta_m) \\ &= -\log 3 + \tfrac{1}{12}v_3(\Delta_m). \end{aligned}$$

If $m \equiv \pm 1, \pm 2 \pmod 9$ (then $U \not\equiv 0 \pmod 3$), we have $P' \notin E_m(\mathbb{Q}_3)^0$ and the reduction type is IV$^*$ or III$^*$ by Table 1. So

$$\lambda_3(P') = \tfrac{1}{3}\log|\psi_2(P')|_3 + \tfrac{1}{12}v_3(\Delta_m) \quad \text{or} \quad \tfrac{1}{8}\log|\psi_3(P')|_3 + \tfrac{1}{12}v_3(\Delta_m),$$

where $\psi_2 = 2y$, $\psi_3 = 3x(x^3 - 1728m^2)$ are the division polynomials of $E_m$. Now we use the identity

$$2^4 3x(Q)^2\psi_3(Q) - (2^2 3^2 x(Q)^3 - 2^6 3^6 m^2)\psi_2(Q)^2 = \Delta_m = -2^{12}3^9 m^4,$$

which we can verify by a straightforward computation. By this identity we have $\mathrm{ord}_3\psi_3(P') \geq 6$, since $\mathrm{ord}_3\psi_2(P') \geq 2$ and $\mathrm{ord}_3 x(P') = 1$. So in any case

$$\lambda_3(P') \leq -\tfrac{2}{3}\log 3 + \tfrac{1}{12}v_3(\Delta_m).$$

To summarize,

$$\lambda_3(P') \leq \begin{cases} -\log 3 + \tfrac{1}{12}v_3(\Delta_m) & \text{if } m \equiv 0 \pmod 9, \\ -\tfrac{2}{3}\log 3 + \tfrac{1}{12}v_3(\Delta_m) & \text{if } m \equiv \pm 1, \pm 2 \pmod 9. \end{cases} \tag{2.12}$$

Now recalling $U \not\equiv 0 \pmod 2$ and (2.5), we have

$$\sum_{p>3,\, p|U} \log|U|_p = \begin{cases} -\log U + \log 3 & \text{if } m \equiv 0 \pmod 9, \\ -\log U & \text{if } m \equiv \pm 1, \pm 2 \pmod 9, \end{cases}$$

and therefore by (2.8)–(2.12),

$$\begin{aligned}\hat{h}(P') &= \lambda_\infty(P') + \sum_p \lambda_p(P')\\ &\le \tfrac{1}{2}\log U + \log 2 + \tfrac{5}{6}\log 3 - \tfrac{1}{12}\log|\Delta_m|\\ &\quad + \sum_{p>3,\, p\mid U} \tfrac{1}{3}\log|U|_p + \sum_{p>3} \tfrac{1}{12} v_p(\Delta_m) + \lambda_2(P') + \lambda_3(P')\\ &\le \tfrac{1}{6}\log U + \tfrac{1}{6}\log 3 < \tfrac{1}{6}\log U + 0.1832 \le \tfrac{1}{6}\log m + 0.1832.\end{aligned}$$

Further if $XY > 0$, then

$$U = U^{2/3}U^{1/3} = U^{2/3}(X^2 - XY + Y^2)^{1/3} < U^{2/3}(X+Y)^{2/3} = m^{2/3},$$

and this leads to the last assertion of the proposition. ■

**2.3. A uniform lower bound of $\hat{h}$ on $E_m$.** The following result by Jędrzejak gives a uniform lower bound of $\hat{h}$, which will be used in the proof of Theorem 1.3.

LEMMA 2.13 ([5, Proposition 1]). *Let $P'$ be a rational non-torsion point on $E_m$. Then $\hat{h}(P') \ge f(m)$, where*

$$f(m) = \begin{cases} \frac{1}{108}\log\frac{m}{2} + \frac{1}{48}\log 3 & \text{if } m \not\equiv 0 \pmod 9,\\ \frac{1}{27}\log\frac{m}{2} - \frac{1}{36}\log 3 & \text{if } m \equiv 0 \pmod 9.\end{cases} \tag{2.14}$$

The goal of this section is to show the following.

PROPOSITION 2.15. *Let $P'$ be a rational non-torsion point on $E_m$. Then*

$$\hat{h}(P') > \tfrac{1}{9}\log m - \tfrac{1}{9}\log 2 - \tfrac{5}{8}\log 3 > \tfrac{1}{9}\log m - 0.7637.$$

REMARK 2.16. This estimate is an improvement of [5, Proposition 1] and [3, Lemma 4.3] in the sense that the main term is $(1/9)\log m$ unconditionally, which enables us to prove Theorem 1.5 (see Remark 4.3). A uniform lower bound for $\hat{h}(P')$ can be obtained with relative ease by computing $\lambda_p(3P')$ using the fact that $3P'$ reduces modulo $p$ ($\neq 3$) to a non-singular point, as in [3] and [5]. Our improvement comes from a direct computation of $\lambda_p(P')$ by means of an exhaustive investigation. In other words, we precisely estimate $\lambda_p(P')$ for each finite place $p$, as well as $\lambda_\infty(P')$, by considering separately whether $p$ divides the numerator of the $x$-coordinate of $P'$, and sum them up. Then we can find a contribution to "the main term" of the lower bound for $\hat{h}(P')$, which was neglected in [5, Proposition 1] and [3, Lemma 4.3].

*Proof of Proposition 2.15.* Let $P = (\alpha/\gamma, \beta/\gamma) \in C_m(\mathbb{Q})$, where $\alpha, \beta, \gamma$ are integers with $\gcd(\alpha,\gamma) = \gcd(\beta,\gamma) = 1$. Note that $\gcd(\alpha,\beta) = 1$, since $m$ is cube-free. Then $P' = (12u/\gamma^2, 36uv/\gamma^3)$, where $u = \alpha^2 - \alpha\beta + \beta^2$ and $v = \alpha - \beta$. We can also see that $u \not\equiv 0 \pmod 2$ and $u \not\equiv 0 \pmod 9$ from $\gcd(\alpha,\beta) = 1$.

First of all, we claim that we may write

$$u = u_0 d^3, \quad \gamma = \gamma_0 d, \tag{2.17}$$

where $u_0, \gamma_0, d$ are integers with $u_0, d > 0$ such that $\gcd(u_0, \gamma_0)$ divides 3 and $\gcd(d, 6\gamma_0) = 1$. Indeed, for a prime $p > 3$, if $p$ divides $\gcd(u, \gamma)$, then $\alpha+\beta \not\equiv 0 \pmod p$, since $\gcd(u, \alpha+\beta)$ divides 3. So by the equality $(\alpha+\beta)u = m\gamma^3$, we have $\gcd(u, \gamma^3) = 3^s d^3$ for some $s \in \{0, 1\}$ and some integer $d > 0$ such that $\gcd(d, 3) = 1$ since $u \not\equiv 0 \pmod 9$. Therefore $u = u' 3^s d^3$ and $\gamma^3 = \gamma' 3^s d^3$ for some $u', \gamma' \in \mathbb{Z}$ with $\gcd(u', \gamma') = 1$. Now set $u_0 = u' 3^s$ and $\gamma_0 = (\gamma' 3^s)^{1/3} (\in \mathbb{Z})$. It is clear that $\gcd(u_0, \gamma_0)$ divides 3 and from $u \not\equiv 0 \pmod 2$ we have $\gcd(d, 6) = 1$. Moreover, from $\gcd(d, \alpha+\beta) = 1$ and $(\alpha+\beta)u_0 = m\gamma_0^3$ we see that $\gcd(d, \gamma_0)$ divides $\gcd(d, 3(\alpha+\beta)) = 1$, which completes the proof of the claim.

Now we compute the archimedean part $\lambda_\infty(P')$. By Tate's series (2.7) we have

$$\begin{aligned}\lambda_\infty(P') &> \tfrac{1}{2}\log|x(P')| - \tfrac{1}{12}\log|\Delta_m| = \tfrac{1}{2}\log|12u/\gamma^2| - \tfrac{1}{12}\log|\Delta_m| \\ &= \tfrac{1}{2}\log u_0 + \tfrac{1}{2}\log d - \log|\gamma_0| + \tfrac{1}{2}\log 12 - \tfrac{1}{12}\log|\Delta_m|.\end{aligned}$$

Next we consider $\lambda_p(P')$ for a finite place $p$. For $p > 3$ not dividing $u_0$, we have $P' \in E_m(\mathbb{Q}_p)^0$, and so

$$\begin{aligned}\lambda_p(P') &= \tfrac{1}{2}\max\{-v_p(12u/\gamma^2), 0\} + \tfrac{1}{12}v_p(\Delta_m) \\ &= \tfrac{1}{2}\max\{-v_p(d/\gamma_0^2), 0\} + \tfrac{1}{12}v_p(\Delta_m).\end{aligned}$$

Since $\gcd(d, \gamma_0) = 1$, we obtain

$$\lambda_p(P') = -\log|\gamma_0|_p + \tfrac{1}{12}v_p(\Delta_m).$$

For $p > 3$ dividing $u_0$, we have $P' \notin E_m(\mathbb{Q}_p)^0$. Then since the reduction type is IV or IV$^*$ and $\gcd(v, m)$ divides 2, [9, Theorem 5.2] shows that

$$\begin{aligned}\lambda_p(P') &= \tfrac{1}{3}\log|\psi_2(P')|_p + \tfrac{1}{12}v_p(\Delta_m) \\ &= \tfrac{1}{3}\log|72uv/\gamma^3|_p + \tfrac{1}{12}v_p(\Delta_m) = \tfrac{1}{3}\log|u_0|_p - \log|\gamma_0|_p + \tfrac{1}{12}v_p(\Delta_m).\end{aligned}$$

For $p = 2$, recalling $E_m(\mathbb{Q}_2) = E_m(\mathbb{Q}_2)^0$ and noting that $u = u_0 d^3 \not\equiv 0 \pmod 2$ we have

$$\begin{aligned}\lambda_2(P') &= \tfrac{1}{2}\max\{-v_2(2^{-2}12u/\gamma^2), 0\} + \tfrac{1}{12}v_2(2^{-12}\Delta_m) \\ &= -\log|\gamma_0|_2 - \log 2 + \tfrac{1}{12}v_2(\Delta_m).\end{aligned}$$

For $p = 3$, in the case $m \equiv 0 \pmod 9$, we have $P' \in E_m(\mathbb{Q}_3)^0$, and noting that $u \not\equiv 0 \pmod 9$ and $d \not\equiv 0 \pmod 3$ we obtain

$$\begin{aligned}\lambda_3(P') &= \tfrac{1}{2}\max\{-v_3(3^{-2}12u/\gamma^2), 0\} + \tfrac{1}{12}v_3(3^{-12}\Delta_m) \\ &= \tfrac{1}{2}\max\{-v_3(3^{-1}u_0/\gamma_0^2), 0\} + \tfrac{1}{12}v_3(3^{-12}\Delta_m) \\ &\ge -\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m).\end{aligned}$$

In the case $m \equiv \pm 3, \pm 4 \pmod 9$, similarly we have $P' \in E_m(\mathbb{Q}_3)^0$ and

$$\lambda_3(P') = \tfrac{1}{2}\max\{-v_3(12u/\gamma^2), 0\} + \tfrac{1}{12}v_3(\Delta_m) \geq -\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m). \tag{2.18}$$

Note that the bound (2.18) is also valid in the case $m \equiv \pm 1, \pm 2 \pmod 9$ if $P' \in E_m(\mathbb{Q}_3)^0$. So now assume $P' \notin E_m(\mathbb{Q}_3)^0$. In the case $m \equiv \pm 1 \pmod 9$, we see from $\alpha^3 + \beta^3 = m\gamma^3 \equiv 0, \pm 1 \pmod 9$ that $v \not\equiv 0 \pmod 3$. Since the reduction type is IV* by Table 1, [9, Theorem 5.2] implies that

$$\lambda_3(P') = \tfrac{1}{3}\log|72uv/\gamma^3|_3 + \tfrac{1}{12}v_3(\Delta_m) \geq -\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m).$$

In the case $m \equiv \pm 2 \pmod 9$, the reduction type is III* and we have

$$\begin{aligned}\lambda_3(P') &= \tfrac{1}{8}\log|\psi_3(P')|_3 + \tfrac{1}{12}v_3(\Delta_m)\\ &= \tfrac{1}{8}\log|3^5\gamma^{-8}u(u^3 - m^2\gamma^6)|_3 + \tfrac{1}{12}v_3(\Delta_m)\\ &= \tfrac{1}{8}\log|3^5\gamma_0^{-8}u_0 d(u_0^3 d^3 - m^2\gamma_0^6)|_3 + \tfrac{1}{12}v_3(\Delta_m).\end{aligned}$$

If $u \equiv 3 \pmod 9$, then $\gamma_0 \equiv 0 \pmod 3$ and

$$\lambda_3(P') = \tfrac{1}{8}\log|3^9\gamma_0^{-8}|_3 + \tfrac{1}{12}v_3(\Delta_m) = -\tfrac{9}{8}\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m).$$

If $u \not\equiv 0 \pmod 3$, then $(\alpha, \beta) \not\equiv (0,0), (\pm 1, \mp 1) \pmod 3$, and so $u \equiv 1 \pmod 3$ and $\gamma \not\equiv 0 \pmod 3$, which implies that $u^3 \equiv 1 \pmod 9$, $m\gamma^3 \equiv \pm 2 \pmod 9$ and $u^3 - m^2\gamma^6 \equiv -3 \pmod 9$. Thus,

$$\begin{aligned}\lambda_3(P') &= \tfrac{1}{8}\log|3^5 \cdot 3|_3 + \tfrac{1}{12}v_3(\Delta_m)\\ &= -\tfrac{3}{4}\log 3 + \tfrac{1}{12}v_3(\Delta_m) = -\tfrac{3}{4}\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m).\end{aligned}$$

Hence, in any case

$$\lambda_3(P') \geq -\tfrac{9}{8}\log 3 - \log|\gamma_0|_3 + \tfrac{1}{12}v_3(\Delta_m).$$

To sum up, we obtain

$$\begin{aligned}\hat{h}(P') &> \tfrac{1}{2}\log u_0 + \tfrac{1}{2}\log d - \log|\gamma_0| + \tfrac{1}{2}\log 12\\ &\quad + \tfrac{1}{3}\sum_{p>3,\, p\mid u_0}\log|u_0|_p - \sum_p \log|\gamma_0|_p - \log 2 - \tfrac{9}{8}\log 3\\ &\geq \tfrac{1}{6}\log u_0 + \tfrac{1}{2}\log d - \tfrac{5}{8}\log 3.\end{aligned}$$

Since we see from $u_0 d^3 = \alpha^2 - \alpha\beta + \beta^2 \geq (\alpha+\beta)^2/4$ that

$$u_0^3 \geq \frac{(\alpha+\beta)^2 u_0^2}{4d^3} = \frac{m^2\gamma_0^6}{4d^3},$$

we conclude that

$$\begin{aligned}\hat{h}(P') &> \tfrac{1}{6}\log\left(\frac{m^{2/3}\gamma_0^2}{\sqrt[3]{4}\,d}\right) + \tfrac{1}{2}\log d - \tfrac{5}{8}\log 3\\ &= \tfrac{1}{9}\log m + \tfrac{1}{3}\log\gamma_0 + \tfrac{1}{3}\log d - \tfrac{1}{9}\log 2 - \tfrac{5}{8}\log 3 \geq \tfrac{1}{9}\log m - 0.7637. \quad \blacksquare\end{aligned}$$

**3. Divisibility and independence of points.** We begin this section by showing that the duplicated point of any point in $C_m(\mathbb{Q})$ cannot be integral.

LEMMA 3.1. *$2P$ cannot be integral for any $P \in C_m(\mathbb{Q})$.*

*Proof.* Let $P = (x, y)$ be a point in $C_m(\mathbb{Q})$ and set $P' = \varphi(P)$. Then

$$P' = (12u_{x,y}, 36(x-y)u_{x,y})$$

and

$$2P' = \left(\frac{12u_{x,y}(x^2+xy+y^2)}{(x-y)^2}, -\frac{36u_{x,y}(x^4+2x^3y+2xy^3+y^4)}{(x-y)^3}\right),$$

where $u_{x,y} = x^2 - xy + y^2$. Since $2P = \varphi^{-1}(2P')$, we have

$$x(2P) = \frac{36m - y(2P')}{6x(2P')} = \frac{(2x^3+y^3)y}{x^3-y^3}.$$

Now, set $x = \alpha/\gamma$ and $y = \beta/\gamma$, where $\alpha, \beta, \gamma$ are integers with $\gcd(\alpha, \gamma) = \gcd(\beta, \gamma) = 1$. Since $m$ is cube-free, we also have $\gcd(\alpha, \beta) = 1$. If

$$x(2P) = \frac{(2\alpha^3+\beta^3)\beta}{(\alpha^3-\beta^3)\gamma}$$

is an integer, then $\alpha^3 - \beta^3$ must divide $(2\alpha^3+\beta^3)\beta$. This implies that $\alpha^3 - \beta^3 = 1$ or $3$, which is impossible. Therefore, $2P$ is non-integral. ∎

Next we assume that $C_m$ has integral points $P_1 = (a_1, b_1)$, $P_2 = (a_2, b_2)$ such that $P_1 \neq \pm P_2$. Equivalently, the positive cube-free integer $m$ can be expressed as

$$m = a_1^3 + b_1^3 = a_2^3 + b_2^3$$

with $\{a_1, b_1\} \neq \{a_2, b_2\}$. Then $P_1$, $P_2$ correspond to the integral points on $E_m$,

$$P_1' = \varphi(P_1) = \big(12(a_1^2 - a_1b_1 + b_1^2), 36(a_1 - b_1)(a_1^2 - a_1b_1 + b_1^2)\big),$$
$$P_2' = \varphi(P_2) = \big(12(a_2^2 - a_2b_2 + b_2^2), 36(a_2 - b_2)(a_2^2 - a_2b_2 + b_2^2)\big).$$

PROPOSITION 3.2. *None of the points $P_1'$, $P_2'$, $P_1' + P_2'$, $P_1' - P_2'$ is in $3E_m(\mathbb{Q})$.*

*Proof.* Since $\varphi : C_m \to E_m$ is a birational equivalence, for any point $P'$ in $E_m(\mathbb{Q})$ there exists a point $P = (\alpha/\gamma, \beta/\gamma)$ in $C_m(\mathbb{Q})$ with $\gcd(\alpha, \gamma) = \gcd(\beta, \gamma) = 1$ such that

$$P' = \varphi(P) = \left(\frac{12(\alpha^2 - \alpha\beta + \beta^2)}{\gamma^2}, \frac{36(\alpha - \beta)(\alpha^2 - \alpha\beta + \beta^2)}{\gamma^3}\right)$$

and

$$x(3P') = \frac{4(\alpha^6 + \alpha^3\beta^3 + \beta^6)}{\alpha^2\beta^2\gamma^2}.$$

Since $m$ is cube-free, we know from $\alpha^3+\beta^3 = m\gamma^3$ that $\gcd(\alpha,\beta) = 1$. Thus,

$$\gcd(m, \alpha^6 + \alpha^3\beta^3 + \beta^6) = \gcd(m, \alpha^3\beta^3) = 1,$$

in other words, the numerator of $x(3P')$ is not divisible by any odd prime divisor of $m$.

On the other hand, $x(P'_i) = 12(a_i^2 - a_ib_i + b_i^2)$ for $i \in \{1,2\}$ and

$$x(P'_1 + P'_2) = \frac{12(a_1+b_1)(a_2+b_2)\{(a_1-a_2)^2 - (a_1-a_2)(b_1-b_2) + (b_1-b_2)^2\}}{(a_1+b_1-a_2-b_2)^2},$$

$$x(P'_1 - P'_2) = \frac{12(a_1+b_1)(a_2+b_2)\{(a_1-b_2)^2 + (a_1-b_2)(a_2-b_1) + (a_2-b_1)^2\}}{(a_1+b_1-a_2-b_2)^2}.$$

Since $m$ is cube-free, $a_i^2-a_ib_i+b_i^2$ is an odd divisor of $m$ for $i \in \{1,2\}$. Hence, it is obvious that $P'_1, P'_2 \notin 3E_m(\mathbb{Q})$. In order to show that $P'_1 \pm P'_2 \notin 3E_m(\mathbb{Q})$, it suffices to check that each numerator of $x(P'_1 \pm P'_2)$ is divisible by an odd prime divisor of $m$.

For $i \in \{1,2\}$ we have $\gcd(a_i + b_i, a_i^2 - a_ib_i + b_i^2) = \gcd(a_i + b_i, 3a_ib_i)$, which divides 3, since $\gcd(a_i, b_i) = 1$. Moreover, $m \equiv 0 \pmod 3$ if and only if $a_i + b_i \equiv a_i^2 - a_ib_i + b_i^2 \equiv 0 \pmod 3$, which shows that

$$a_i + b_i \not\equiv 0 \pmod 9 \tag{3.3}$$

for any $i \in \{1,2\}$. Suppose now that the set of prime divisors of $a_1+b_1$ is the same as the set of prime divisors of $a_2 + b_2$. Then $a_1 + b_1 \neq a_2 + b_2$ implies that there exists a prime $p$ such that

$$a_i + b_i \equiv 0 \pmod{p^2}, \quad a_j + b_j \equiv 0 \pmod p, \quad a_j + b_j \not\equiv 0 \pmod{p^2}$$

for some $i, j$ with $\{i, j\} = \{1,2\}$. However, since $m = (a_j+b_j)(a_j^2-a_jb_j+b_j^2)$ is divisible by $p^2$, we have $a_j^2 - a_jb_j + b_j^2 \equiv 0 \pmod p$, yielding $p = 3$. Hence, $a_i + b_i \equiv 0 \pmod 9$, which contradicts (3.3). Thus, there exists a prime $p$ such that

$$a_i + b_i \equiv 0 \pmod p \quad \text{and} \quad a_j + b_j \not\equiv 0 \pmod p$$

for some $i, j$ with $\{i, j\} = \{1,2\}$, whence $p$ satisfies $a_1 + b_1 - a_2 - b_2 \not\equiv 0 \pmod p$. It is clear that $p \neq 2$ (note that $a_1^3 + b_1^3 = a_2^3 + b_2^3$) and that $p$ is a divisor of $m$. Therefore, we conclude that there exists an odd prime divisor $p$ of $m$ such that the numerators of $x(P'_1 \pm P'_2)$ are divisible by $p$. This completes the proof of Proposition 3.2. ∎

Proposition 3.2 immediately implies the following.

COROLLARY 3.4. *The points $P'_1$ and $P'_2$ are independent in $E_m(\mathbb{Q})$.*

*Proof.* Suppose that $P_1'$ and $P_2'$ are dependent. Then there exist integers $n_1$ and $n_2$ with $(n_1, n_2) \neq (0, 0)$ such that

$$n_1 P_1' + n_2 P_2' = O.$$

Considering this equality modulo $3E_m(\mathbb{Q})$, we see that

$$\epsilon_1 P_1' + \epsilon_2 P_2' \in 3E_m(\mathbb{Q}),$$

where $(\epsilon_1, \epsilon_2) \in \{(1,0), (0,1), (1,1), (1,-1)\}$. However, Proposition 3.2 ensures that this cannot occur. Therefore, $P_1'$ and $P_2'$ are independent. ∎

**4. Proofs of the main theorems.** We say that a rational point $P$ in $C_m(\mathbb{Q})$ is *divisible* by an integer $l$ if there exists a rational point $Q$ in $C_m(\mathbb{Q})$ such that $P = lQ$. Recall we assume $m > 2$, and so $C_m(\mathbb{Q})$ is torsion-free.

*Proof of Theorem 1.3.* It suffices to show that $P_1$ is not divisible by any integer greater than 1 in $C_m(\mathbb{Q})$. By Lemma 3.1 and Proposition 3.2 the point $P_1$ is divisible by neither 2 nor 3 in $C_m(\mathbb{Q})$. Suppose that $P_1' = \varphi(P_1)$ is divisible by an integer $l$. Then

$$\hat{h}(P_1') = l^2 \hat{h}(Q')$$

for some $Q' \in E_m(\mathbb{Q})$. Noting that if $3 \leq m \leq 6$, then $C_m$ has no integral point, we see from the assumption $m > 2$ that $m \geq 7$. Hence $f(m) > 0$, where $f(m)$ is the function defined in (2.14). It follows from Proposition 2.6 and Lemma 2.13 that

$$l^2 = \frac{\hat{h}(P_1')}{\hat{h}(Q')} < \frac{\frac{1}{6}\log m + 0.1832}{f(m)},$$

which shows that if $m \geq 9$, then $l < 5$, and if $m = 7$, then $l < 7$. Therefore, it remains to check that if $m = 7$, then $P_1'$ is not divisible by 5 in $E_5(\mathbb{Q})$. This can be easily done by using the function "elldivpoint" in Cremona's script `ell_ff.gp` [2] for PARI [11], or by the Magma function "IsDivisibleBy" [1]. ∎

*Proof of Corollary 1.4.* If $C_m$ has more than three integral points, then two of them, say $P$ and $Q$, satisfy $P \neq \pm Q$. But since the rank is one, each point of the two can be a generator by Theorem 1.3, which is a contradiction. ∎

*Proof of Theorem 1.5.* Let $P_1, P_2 \in C_m(\mathbb{Q})$ be integral points such that $P_1 \neq \pm P_2$. Then they are independent by Corollary 3.4. So it suffices to show that the index $\nu$ of the span of $P_1'$ and $P_2'$ in $\mathbb{Z}Q_1 + \mathbb{Z}Q_2$ is less than 2, where $Q_1$ and $Q_2$ are points in a system of generators for $E_m(\mathbb{Q})$ such that $P_1', P_2' \in \mathbb{Z}Q_1 + \mathbb{Z}Q_2$.

First we shall show that $\nu < 5$ if $m \geq 66093$. By Siksek's theorem [7, Theorem 3.1] we have

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

where

$$\begin{aligned} R(P_1', P_2') &= \hat{h}(P_1')\hat{h}(P_2') - \langle P_1', P_2' \rangle^2 \\ &= \hat{h}(P_1')\hat{h}(P_2') - \tfrac{1}{4}\big(\hat{h}(P_1' + P_2') - \hat{h}(P_1') - \hat{h}(P_2')\big)^2 \end{aligned}$$

if $\hat{h}(Q) > \lambda$ for any non-torsion point $Q \in E_m(\mathbb{Q})$. Using this theorem, for $m \geq 967$ (so $(1/9)\log m - 0.7637 > 0$) we have, by Propositions 2.6 and 2.15,

$$\begin{aligned} (4.1) \qquad \nu &\leq \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_1')\hat{h}(P_2')}}{\lambda} \leq \frac{2}{\sqrt{3}} \frac{\sqrt{\big(\frac{1}{6}\log m + 0.1832\big)^2}}{\frac{1}{9}\log m - 0.7637} \\ &= \frac{2}{\sqrt{3}} \frac{\frac{1}{6}\log m + 0.1832}{\frac{1}{9}\log m - 0.7637}. \end{aligned}$$

We see that the right-hand side is less than 5 for $m \geq 66093$.

Next, in view of $\nu \neq 3$ by Proposition 3.2, we shall show that $\nu$ is indivisible by 2. Since we have already shown that $P_1'$ and $P_2'$ are indivisible by 2 by Lemma 3.1, it suffices to show that $P_1' + P_2'$ (or equivalently $P_1' - P_2'$) is indivisible by 2, which is possible for sufficiently large $m$ by using heights as follows. By the parallelogram law and Proposition 2.6 we have

$$\hat{h}(P_1' + P_2') + \hat{h}(P_1' - P_2') = 2\hat{h}(P_1') + 2\hat{h}(P_2') < 4\big(\tfrac{1}{6}\log U_m + 0.1832\big),$$

where

$$U_m = \max\{x^2 - xy + y^2 : (x, y) \text{ is an integral point on } C_m\}.$$

Hence there exists $R' \in \{P_1' + P_2', P_1' - P_2'\}$ such that

$$\hat{h}(R') < 2\big(\tfrac{1}{6}\log U_m + 0.1832\big).$$

If $R'$ is divisible by 2, then we see from Proposition 2.15 that

$$\hat{h}(R') > 2^2\big(\tfrac{1}{9}\log m - 0.7637\big),$$

and so

$$2^2\big(\tfrac{1}{9}\log m - 0.7637\big) < 2\big(\tfrac{1}{6}\log U_m + 0.1832\big).$$

This indicates that $P_1' + P_2'$ is indivisible by 2 for $m$ such that $mT_m^3 \geq 2.3566 \times 10^{13}$, where $T_m = m/U_m$, in other words,

$$T_m = \min\{x + y \in \mathbb{Z}_{>0} : (x, y) \text{ is an integral point on } C_m\}.$$

Hence we have shown that $\nu$ is indivisible by 2 for $m$ such that $mT_m^3 \geq 2.3566 \times 10^{13}$.

Now we have shown that $P_1$ and $P_2$ can be in a system of generators for $m \geq 66093$ such that $mT_m^3 \geq 2.3566 \times 10^{13}$. Since in the remaining cases the number of $m$ for which we have to show the statement of the theorem is finite and not so large, we can check all the cases with a computer. This process is divided into three parts as follows. Note that if $m$ is numerically given, it is possible to obtain all the integral points on $C_m$ by solving the Thue equation.

(i) For $m \geq 66093$ such that $mT_m^3 < 2.3566 \times 10^{13}$, it suffices to show that $P + Q$ is indivisible by 2 for any integral points $P$ and $Q$ satisfying $P \neq \pm Q$. For this purpose, we first solve the Thue equation $x^3 + y^3 = m$ for each $m \geq 66093$ such that $mT_m^3 < 2.3566 \times 10^{13}$ by using the PARI function "thue" [11] to obtain all the integral points. Then for all pairs $\{P, Q\}$ of integral points satisfying $P \neq \pm Q$, we can check that $P' + Q'$ is indivisible by 2 by using the function "elldivpoint" of [2] for PARI, where $P' = \varphi(P)$ and $Q' = \varphi(Q)$. Since it takes too much time to check this part in a routine manner, we need a technical argument, which is described in Remark 4.2 below.

(ii) For $3300 < m < 66093$ we can see that $\nu < 13$ by (4.1), and so it suffices to check that $kP + lQ \notin pE_m(\mathbb{Q})$ for $(k, l) \in \{\pm 1, \pm 2, ..., \pm (p-1)\}^2$ with $p = 2, 5, 7, 11$ for any integral points $P$ and $Q$ satisfying $P \neq \pm Q$. This can be done by solving the Thue equation $x^3 + y^3 = m$ and using the function "elldivpoint" or the Magma function "IsDivisibleBy" as in part (i).

(iii) Finally, for $m \leq 3300$ we can check directly by using the Magma function "Generators" that any pair $\{P, Q\}$ of integral points satisfying $P \neq \pm Q$ can be in a system of generators. Indeed, since we consider the case where $C_m$ has at least four integral points, all the $m$ we have to check turn out to be $m = 91, 217, 721, 1027, 1729$ and we can obtain a system of generators by the function "Generators". (For any such $m$ the rank of $E_m(\mathbb{Q})$ is two.) ∎

Remark 4.2. We explain in detail how to check part (i). Set

$$A = 2.3566 \times 10^{13}, \quad B = 66093,$$
$$M = \{m \in \mathbb{Z}_{>0} : B \leq m,\ mT_m^3 < A,\ m \text{ cube-free}\},$$

and for $k \in \mathbb{Z}$ set

$$M_k = \{m \in \mathbb{Z}_{>0} : B \leq m,\ mT_m^3 < A,\ T_m = k,\ m \text{ cube-free}\},$$
$$M_k' = \left\{ a^3 + (k-a)^3 : \begin{array}{c} B \leq a^3 + (k-a)^3,\ (a^3 + (k-a)^3)k^3 < A, \\ a \in \mathbb{Z},\ 1 \leq a < (A/k^3)^{1/2}, \\ a^3 + (k-a)^3 \text{ cube-free} \end{array} \right\}.$$

Note we may check the desired indivisibility for $m \in M$. Since $T_m < A^{1/3}$ for $m \in M$, we have $M \subset \bigcup_{k=1}^{\lfloor A^{1/3} \rfloor} M_k$. Next we shall see that $M_k \subset M_k'$. Let $m$ be in $M_k$. Then since $T_m = k$, there exist integers $a > 0$ and $b$ such that $a^3 + b^3 = m$, $a + b = k$ and $a > |b|$. So $m$ is of the form $m = a^3 + (k-a)^3$ with $a \in \mathbb{Z}$ such that $a > |k - a|$, by replacing $b$ with $k - a$. Note that if $k - a < 0$, then $m = a^3 + (k-a)^3 = k\{a^2 - a(k-a) + (k-a)^2\} > a^2$ and that if $k - a > 0$, then $m > a^3$. Since $a$ is a positive integer, in any case $a^2 < m < A/k^3$. So $1 \leq a < (A/k^3)^{1/2}$, and therefore $M_k \subset M_k'$. Now we have $M \subset \bigcup_{k=1}^{\lfloor A^{1/3} \rfloor} M'_k$ and we can write a program to check the indivisibility for $m$ in the right-hand side. A crucial point of this method is that we vary $k$ and $a$ instead of $m$, which considerably reduces the running time.

REMARK 4.3. If we use [3, Lemma 4.3], then the upper bound for $\nu$ in (4.1) would be greater than

$$\frac{2}{\sqrt{3}}\frac{27}{6} > 5,$$

from which the assertion of Theorem 1.5 cannot be deduced.

*Proof of Corollary 1.6.* Assume the rank is two and $P_1$, $P_2$ ($P_1 \neq \pm P_2$) are integral points on $C_m$. Then by Theorem 1.5, $\{P_1, P_2\}$ is a system of generators. Let $R = kP_1 + lP_2$ ($kl \neq 0$) be an integral point on $C_m$ and so

$$\begin{bmatrix} R \\ P_2 \end{bmatrix} = \begin{bmatrix} k & l \\ 0 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}.$$

Now since $\{R, P_2\}$ is also a system of generators by Theorem 1.5, we have $k = \pm 1$. Similarly, $l = \pm 1$.

Further by the equation

$$\begin{bmatrix} P_1 + P_2 \\ P_1 - P_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix},$$

noting that the determinant of the matrix is not $\pm 1$, either $P_1 + P_2$ or $P_1 - P_2$ is non-integral, since otherwise this contradicts Theorem 1.5. ∎

*Proof of Theorem 1.8.* Recall $E_m(\mathbb{Q})$ is torsion-free for $m > 2$, since $m$ is cube-free. For $m \geq 967$, let $N_m$ be the least integer greater than

$$2\sqrt{\left(\tfrac{1}{6}\log U_m + 0.1832\right)/\left(\tfrac{1}{9}\log m - 0.7637\right)}. \tag{4.4}$$

Then we have an injection

$$\left\{P \in E_m(\mathbb{Q}) : \hat{h}(P) < \tfrac{1}{6}\log U_m + 0.1832\right\} \to E_m(\mathbb{Q})/N_m E_m(\mathbb{Q})$$

by the argument in the proof of [8, Lemma 6]. The number of integral points on $C_m$ is less than or equal to the cardinality of the left-hand side by Proposition 2.6. Now by solving the inequality (4.4) $< 3$ we see that if $mT_m^2 \geq 8125718565$, then $N_m = 3$. So for such $m$, $C_m$ has at most $3^r$ integral points, where $r$ is the rank of $C_m(\mathbb{Q})$. But the number of integral points is even, since the equation of $C_m$ is symmetrical and $m$ is cube-free. Therefore $C_m$ has at most $3^r - 1$ integral points.

For $m$ such that $mT_m^2 < 8125718565$, using PARI in the same manner as in the proof of Theorem 1.5 we can verify the assertion of the theorem. ∎

REMARK 4.5. In the proofs of Theorems 1.5 and 1.8, theoretically we may replace $U_m$ by $m$ (therefore replace $T_m$ by 1), which might make the argument simpler. But then we need to check all $m < 2.3566 \times 10^{13}$ of the form $m = a^3 + b^3$, which seems to take too much time for ordinary personal computers. The reason we use PARI in the proofs is that PARI is much faster than Magma in this computation.

**Acknowledgements.** The authors are deeply grateful to the referee for his/her thorough review and valuable suggestions, which significantly contributed to improving the quality and presentation of this paper. The first author was partially supported by JSPS KAKENHI Grant Number 25400025.

## References

[1] W. Bosma and J. Cannon, *Handbook of magma functions*, Department of Mathematics, Univ. of Sydney; http://magma.maths.usyd.edu.au/magma/.

[2] J. Cremona, ell_ff.gp; http://homepages.warwick.ac.uk/~masgaj/ftp/progs/pari/ell_ff.gp.

[3] G. Everest, P. Ingram and S. Stevens, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. 12 (2009), 54–81.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford Univ. Press, 2008.

[5] T. Jędrzejak, *Height estimates on cubic twists of the Fermat elliptic curve*, Bull. Austral. Math. Soc. 72 (2005), 177–186.

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

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

[8] J. H. Silverman, *Integer points and the rank of Thue elliptic curves*, Invent. Math. 66 (1982), 395–404.

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

[10] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[11] The PARI Group, *PARI/GP, version 2.6.0*, Bordeaux, 2012; http://pari.math.u-bordeaux.fr/.

[12] P. Voutier and M. Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves* $y^2 = x^3 + b$, arXiv:1305.6560.

[13] T. Womack, *Equal sum of power*, Master's thesis, Oxford Univ., 1999; http://tom.womack.net/maths/dissert_abstract.htm.

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

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

*Received on 18.11.2013*
*and in revised form on 27.10.2014* (7644)