Publ. Math. Debrecen
92/1-2 (2018), 79–99
DOI: 10.5486/PMD.2018.7719

The Mordell–Weil bases for the elliptic curve of the form $y^2 = x^3 - m^2x + n^2$

By YASUTSUGU FUJITA (Narashino) and TADAHISA NARA (Tagajo)

Abstract. Let $E_{m,n}$ be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 - m^2x + n^2$, where m and n are positive integers. Brown and Myers showed that the curve $E_{1,n}$ has rank at least two for all n. In the present paper, we specify the two points which can be extended to a basis for $E_{1,n}(\mathbb{Q})$ under certain conditions described explicitly. Moreover, we verify a similar result for the curve $E_{m,1}$, which, however, gives a basis for the rank three part of $E_{m,1}(\mathbb{Q})$.

1. Introduction

Let m, n be positive integers and $E_{m,n}$ the elliptic curve defined by

$$y^2 = x^3 - m^2x + n^2.$$

Brown and Myers ([3]) examined the curve $E_{1,n}$ and found that the group $E_{1,n}(\mathbb{Q})$ of rational points on $E_{1,n}$ over $\mathbb{Q}$ has rank at least two as far as $n \geq 2$. After that, the curve $E_{m,1}$ was studied by Antoniewicz ([1]), who showed that the group $E_{m,1}(\mathbb{Q})$ has rank at least two if $m \geq 2$, and has rank at least three if $m \geq 4$ with $m \equiv 0 \pmod 4$ or $m = 7$, which partially gave an answer to the problem raised in ([3]). Both curves above were further investigated in Eikenberg's dissertation ([5]), where it was shown that the group $E_{1,n}(\mathbb{Q}(n))$ of $\mathbb{Q}(n)$-rational points is generated by the points $(0, n)$ and $(1, n)$ ([5, Corollary 3.1.2]), and that

Mathematics Subject Classification: Primary: 11G05, 11D59; Secondary: 11G50.
Key words and phrases: elliptic curve, canonical height, Mordell–Weil group, square-free.
The first author is supported by JSPS KAKENHI Grant Number 16K05079.
A version with codes for computations is available on arXiv:1705.00308.

the group $E_{m,1}(\mathbb{Q}(m))$ of $\mathbb{Q}(m)$-rational points is generated by the points $(0,1)$, $(m,1)$ and $(-1,m)$ ([5, Theorem 5.1.1]). Note that $\mathbb{Q}(n)$ and $\mathbb{Q}(m)$ in the assertions above are function fields. For high rank curves of the forms $E_{1,n}$ and $E_{m,1}$, see TADIĆ's papers ([19], [20]).

Let $P_0 = (0,n)$ and $P_{\pm 1} = (\pm m, n)$ be integral points on $E_{m,n}$. It is easy to see that these points satisfy the relation

$$P_0 + P_{+1} + P_{-1} = O.$$

Denote by $\Delta_{m,n}$ the discriminant of $E_{m,n}$, which equals $-16(27n^4 - 4m^6)$. The purpose of the present paper is to determine the bases for $E_{1,n}(\mathbb{Q})$ and $E_{m,1}(\mathbb{Q})$ under certain conditions described explicitly.

Theorem 1.1. *Let m, n be coprime positive integers. Assume that the p-primary part of $\Delta_{m,n}$ is square-free for any prime $p > 3$.*

(1) *If $m = 1$ and $n \geq 2$, then $\{P_0, P_{-1}\}$ can be extended to a basis for $E_{m,n}(\mathbb{Q})$.*
(2) *If $n = 1$ and $m \geq 4$, then $\{P_0, P_{-1}, P_2\}$ can be extended to a basis for $E_{m,n}(\mathbb{Q})$, where $P_2 = (-1,m) \in E_{m,1}(\mathbb{Q})$.*

Remark 1.2. For some particular cases with $n = 1$, we have the following results:

- $E_{1,1}(\mathbb{Q}) = \langle P_{+1} \rangle$ and $P_0 = -3P_{+1}$;
- $E_{2,1}(\mathbb{Q}) = \langle P_0, P_{-1} \rangle$;
- $E_{3,1}(\mathbb{Q}) = \langle P_0, P_2 \rangle$ and $P_{+1} = 2P_2$;
- $E_{7,1}(\mathbb{Q}) = \langle P_0, P_2, (-3,11) \rangle$ and $P_{+1} = -2(-3,11)$;
- $E_{24,1}(\mathbb{Q}) = \langle P_0, P_2, (-10,69) \rangle$ and $P_{+1} = -2(-10,69)$;

where $E_{7,1}$ and $E_{24,1}$ do not satisfy the above assumption about $\Delta_{m,n}$.

While Eikenberg used the theory of Mordell–Weil lattices (see [14]) to find the bases for $E_{1,n}(\mathbb{Q}(n))$ and $E_{m,1}(\mathbb{Q}(m))$, we appeal to explicit estimates of canonical heights to show Theorem 1.1. There are several literatures describing explicitly the bases for the Mordell–Weil groups of parametric families of elliptic curves E over $\mathbb{Q}$ under the assumption that E has rank two or three (see, e.g., [4], [7]–[11]). However, as far as we can see, Theorem 1.1 is the first result giving the bases in the cases where the j-invariants of E are not equal to 0 or 1728. Although in general it is needed in order to get better lower bounds for canonical heights (see Propositions 4.1 and 5.4), in case $n = 1$, the assumption on $\Delta_{m,n}$ is crucial because, otherwise, the assertion does not hold for $m \in \{7, 24\}$, as seen in Remark 1.2. Furthermore, one can expect that almost all of m or n satisfy the

assumption on $\Delta_{m,n}$. More precisely, assuming that the *abc* conjecture is true, we can estimate the density of n (resp. m) satisfying the assumption on $\Delta_{1,n}$ (resp. $\Delta_{m,1}$) in Theorem 1.1.

Proposition 1.3. *For $x > 0$, define*

$$\mathcal{N}(x) = \#\{n \in (0, x]; \textit{the } p\textit{-primary part of } \Delta_{1,n} \textit{ is square-free for any } p > 3\},$$
$$\mathcal{M}(x) = \#\{m \in (0, x]; \textit{the } p\textit{-primary part of } \Delta_{m,1} \textit{ is square-free for any } p > 3\}.$$

Suppose the abc conjecture is true. Then there exist constants κ_1, $\kappa_2 > 0.97$ such that

$$\mathcal{N}(x) \sim \kappa_1 x, \quad \mathcal{M}(x) \sim \kappa_2 x.$$

The organization of this paper is as follows. In Section 2, we quote the results from [3] and [1] which show that $E_{m,n}(\mathbb{Q})$ is torsion-free and has rank at least two under the assumptions in Theorem 1.1. In Section 3, we examine the reduction types and the x-intercepts of $E_{m,n}$, which are needed in computing the canonical heights in the following sections. Section 4 is devoted to prove Theorem 1.1 (1). In Section 5, we prove Theorem 1.1 (2) and Proposition 1.3.

2. Preliminaries

First, we have the following proposition by Brown and Myers ([3, Theorem 3]) and Antoniewicz ([1, Theorem 2.3]).

Proposition 2.1. *Assume that one of the following holds*:

- $m = 1$ *and* $n \geq 1$;
- $n = 1$ *and* $m \geq 1$.

Then, $E_{m,n}(\mathbb{Q})_{\mathrm{tors}} = \{O\}$.

Next, in view of Lemma 6 in [3] and Lemmas 3.1 and 3.9 in [1], we have the following proposition.

Proposition 2.2. *Assume that one of the following holds*:

- $m = 1$ *and* $n \geq 2$;
- $n = 1$ *and* $m \notin \{1, 3, 7, 24\}$.

Then, P_0, P_{+1}, $P_0 + P_{+1} \notin 2E_{m,n}(\mathbb{Q})$. *In particular, the points* P_0 *and* P_{+1} *are independent modulo* $E_{m,n}(\mathbb{Q})_{\mathrm{tors}}$.

3. Local study of the curve

Lemma 3.1. *If* $\gcd(m,n)=1$, *then the Weierstrass equation*

$$y^2 = x^3 - m^2x + n^2, \tag{3.2}$$

for $E_{m,n}$ *is global minimal.*

Proof. In view of [16, VII, Remark 1.1], it suffices to show that at least one of $v_p(c_4) < 4, v_p(c_6) < 6$ and $v_p(\Delta) < 12$ holds for every prime p. Now we have

$$c_4 = 2^4 \cdot 3m^2, \qquad c_6 = -2^5 \cdot 3^3 n^2, \qquad \Delta = 2^4(2^2m^6 - 3^3n^4).$$

If $p > 3$, then either $v_p(c_4) < 4$ or $v_p(c_6) < 6$ always holds. If $p \in \{2,3\}$, then $v_p(\Delta) < 12$ always holds. □

Lemma 3.3. *If* $\gcd(m,n)=1$, *then for a prime* $p>3$, *the reduction type of* $E_{m,n}$ *at* p *is* I_k *(the Kodaira symbol), where* $k = \mathrm{ord}_p(\Delta_{m,n})$.

Proof. There exists a minimal Weierstrass equation $y^2 = x^3 + a_4x + a_6$ for $E_{m,n}$ such that a_4, a_6 and the discriminant Δ are as described in the table of Exercise 4.47 in [18]. Since the equation $y^2 = x^3 - m^2x + n^2$ is also minimal, we can transform $y^2 = x^3 + a_4x + a_6$ to $y^2 = x^3 - m^2x + n^2$ by some $[1, r, s, t]$, where $[u, r, s, t]$ means the transformation

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

Then it turns out that $r = s = t = 0$, and so definitively $a_4 = -m^2, a_6 = n^2$. Since if p divides $\Delta_{m,n}$, then p divides neither m nor n, we see that the possible reduction type is I_k by the table of Exercise 4.47. □

Lemma 3.4. *If* $\gcd(m,n)=1$, *then the reduction type of* $E_{m,n}$ *at* 3 *is as follows:*

(1) I_0 *if* $m \not\equiv 0 \pmod 3$;

(2) II *if* $m \equiv 0 \pmod 3$ *and* $n \not\equiv \pm 1 \pmod 9$;

(3) III *otherwise.*

Proof. If $m \not\equiv 0 \pmod 3$, then $\Delta_{m,n}$ is not divisible by 3 and we have I_0.

Next assume $m \equiv 0 \pmod 3$. Then $n \not\equiv 0 \pmod 3$ and $\mathrm{ord}_3(\Delta_{m,n}) = 3$. Now, there exists a minimal Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$ for $E_{m,n}$ such that a_2, a_4, a_6 and the discriminant Δ are as described in the table of Exercise 4.48 in [18]. Since the equation $y^2 = x^3 - m^2x + n^2$ is also minimal,

we can transform $y^2 = x^3 + a_2x^2 + a_4x + a_6$ to $y^2 = x^3 - m^2x + n^2$ by some $[1, r, s, t]$. In particular, the discriminants of the two equations are the same. Then we have $a_2 = -3r$. So since a_2 is divisible by 3, the possible reduction type is II or III by the table. Transforming $y^2 = x^3 - m^2x + n^2$ by $[1, -1, 0, 0]$, we have the equation

$$y^2 = x^3 - 3x^2 - (m^2 - 3)x + m^2 + n^2 - 1.$$

Note that $m^2 + n^2 - 1$ is divisible by 3, since $n \not\equiv 0 \pmod 3$. Further it turns out that $m^2 + n^2 - 1$ is divisible by 9 if and only if $n \equiv \pm 1 \pmod 9$. Tate's algorithm ([18, p. 366]) with the fact completes the proof. □

Lemma 3.5. *The reduction type of $E_{m,n}$ at 2 is as follows:*

(1) IV *if* $n \equiv 1 \pmod 2$;

(2) III *if* $n \equiv 0 \pmod 2$ *and* $m \equiv 1 \pmod 2$.

Remark 3.6. If $n \equiv m \equiv 0 \pmod 2$, then various reduction types are possible.

Proof. First assume $n \equiv 1, m \equiv 0 \pmod 2$. By transforming equation (3.2) by $[1, 0, 0, 1]$, we have the equation

$$y^2 + 2y = x^3 - m^2x + n^2 - 1$$

with the quantities

$$b_8 = -m^4, \qquad b_6 = 4n^2.$$

Then $b_8 \equiv 0 \pmod 8$ and $b_6 \equiv 4 \pmod 8$, which indicate type IV by Tate's algorithm ([18, p. 366]).

Next assume $n \equiv 1, m \equiv 1 \pmod 2$. By transforming equation (3.2) by $[1, 1, 1, 1]$, we have the equation

$$y^2 + 2xy + 2y = x^3 + 2x^2 + (1 - m^2)x - m^2 + n^2$$

with the quantities

$$b_8 = -m^4 - 6m^2 + 12n^2 + 3, \qquad b_6 = -4m^2 + 4n^2 + 4.$$

Then $b_8 \equiv -1 - 6 + 12 + 3 \equiv 0 \pmod 8$ and $b_6 \equiv -4 + 4 + 4 \equiv 4 \pmod 8$, which indicate type IV by Tate's algorithm.

Assume $n \equiv 0, m \equiv 1 \pmod 2$. By transforming the equation (3.2) by $[1, 1, 1, 0]$, we have the equation

$$y^2 + 2xy = x^3 + 2x^2 + (3 - m^2)x - m^2 + n^2 + 1$$

with the quantities

$$b_8 = -m^4 - 6m^2 + 12n^2 + 3.$$

Then $b_8 \equiv -1-6+3 \equiv 4 \pmod 8$ which indicates type III by Tate's algorithm. □

The next lemma is related to bounds for the real components of $E_{m,n}$.

Lemma 3.7. *Put $f(x) = x^3 - m^2x + n^2$ and $l = n^{2/3} > 0$. If $27n^4 - 4m^6 > 0$, then $f(x)$ has only one real root, which is bounded below by each of*

$$-l\left(1 + \frac{m^2}{3l^2}\right), \qquad -m\left(1 + \frac{l^3}{2m^3}\right).$$

If $27n^4 - 4m^6 < 0$, then $f(x)$ has three real roots α, β, γ. Further, if we assume $m/l \geq 3^{1/3} = 1.4422\cdots$ and $\alpha < \beta < \gamma$, then we have the estimates

$$-m\left(1 + \frac{l^3}{2m^3}\right) < \alpha < 0 < \beta < \frac{2l^3}{m^2} \leq m\left(1 - \frac{l^3}{m^3}\right) < \gamma.$$

Proof. It is widely known that the number of the real roots of a cubic polynomial depends on the sign of the discriminant $\Delta = -16(27n^4 - 4m^6)$, and so we only show about the bounds.

We have

$$f\left(-l - \frac{m^2}{3l}\right) = -m^6/(27l^3) < 0, \qquad f\left(-m - \frac{l^3}{2m^2}\right) = -\frac{l^6\left(6\,m^3 + l^3\right)}{8\,m^6} < 0,$$

which gives a proof for the one-real-root case.

Next, we have

$$f\left(\frac{2l^3}{m^2}\right) = -\frac{l^3\left(m^2 - 2\,l^2\right)\left(m^4 + 2\,l^2\,m^2 + 4\,l^4\right)}{m^6} < 0,$$

$$f\left(m\left(1 - \frac{l^3}{m^3}\right)\right) = -\frac{l^3\left(m^6 - 3\,l^3\,m^3 + l^6\right)}{m^6} = -\frac{l^3\,m^3\left(m^3 - 3\,l^3\right) + l^9}{m^6} < 0,$$

$$m\left(1 - \frac{l^3}{m^3}\right) - \frac{2l^3}{m^2} = \frac{m^3 - 3\,l^3}{m^2} \geq 0,$$

by the assumption $m/l \geq 3^{1/3}$. Those facts with $f(0) = n^2 > 0$ give the estimates for α, β, γ. □

Remark 3.8. The values $-l - m^2/(3l)$ and $-m - l^3/(2m^2)$ are obtained from the leading terms of the Taylor expansions around $m = 0$ and $l = 0$, respectively, of the explicit roots

$$x_0 = \left(\frac{\sqrt{27\,l^6 - 4\,m^6}}{6\sqrt{3}} - \frac{l^3}{2}\right)^{\frac{1}{3}} - \left(\frac{\sqrt{27\,l^6 - 4\,m^6}}{6\sqrt{3}} + \frac{l^3}{2}\right)^{\frac{1}{3}}$$

of $f(x)$.

4. Generators for $E_{1,n}(\mathbb{Q})$

In this section, we consider the curve $E = E_{1,n} : y^2 = x^3 - x + n^2$ over $\mathbb{Q}$ and show that $\{P_0, P_{-1}\}$ can be extended to a basis for $E(\mathbb{Q})$. Our method largely depends on estimates of the canonical height. We compute it through the decomposition into the sum of the local height functions. In this paper, the definition of the local height function follows [18, Chapter VI].

Proposition 4.1. *Assume that $n \geq 27$, and that the p-primary part of $\Delta_{1,n} = -16(27n^4 - 4)$ is square-free for any $p > 3$. Then, for any rational non-torsion point $P \in E_{1,n}(\mathbb{Q})$, we have*

$$\hat{h}(P) > \frac{1}{3}\log n - 0.619.$$

Proof. We denote the local height function on E for a place p by λ_p, and put $v_p(\cdot) = -\log|\cdot|_p$.

First, we compute λ_∞. To ease notation, put $l = n^{2/3} \geq 9$. Further, to use Tate's series, we take the Weierstrass model $E' : y^2 = f(x - 2l - 1/(3l))$, where $f(x) = x^3 - x + n^2$. (Our local height function is independent of models.) Then, for any $Q' \in E'(\mathbb{R})$, we have $x(Q') > l$ by Lemma 3.7. By Tate's series, we have

$$\lambda_\infty(P) = \frac{1}{2}\log|x(P')| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log|z(2^k P')| + \frac{1}{12}v_\infty(\Delta),$$

where P' is the corresponding point on E' to P,

$$z(P) = \frac{27\,l^4\,x^4 + \left(-648\,l^6 - 162\,l^4 - 18\,l^2\right)\,x^2 + \left(1512\,l^7 + 432\,l^5 + 72\,l^3 + 8\,l\right)\,x}{27\,l^4\,x^4} - \frac{648\,l^8 + 108\,l^6 - 27\,l^4 + 6\,l^2 + 1}{27\,l^4\,x^4}$$

and $x = x(P)$. We can regard $z(P)$ as a function of the variable x and l in the domain $\mathcal{D} : 9 \leq l \leq x$ and denote it by $z(x, l)$. Here by using the Mathematica functions "MaxValue" and "MinValue" ([22]), we can evaluate the maximum and the minimum of $z(x, l)$ in $\mathcal{D}$ to $z(9, 9) = 9.0745\cdots$ and $z(x_0, 9) = 0.09801\cdots$, respectively, where $x_0 = 25.054819\cdots$.

Therefore, for $l \geq 9$ and $P \in E'(\mathbb{R})$, we have

$$0.098 < z(P) < 9.075. \tag{4.2}$$

(The upper bound is not necessary here, but used in Proposition 4.3.) So we have

$$\begin{aligned}\lambda_\infty(P) &> \frac{1}{2}\log l + \log(0.098) \times \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k} + \frac{1}{12}v_\infty(\Delta) \\ &= \frac{1}{3}\log n + \frac{\log(0.098)}{6} + \frac{1}{12}v_\infty(\Delta).\end{aligned}$$

Next, we compute the local height for non-Archimedean places. Let ψ_2 and ψ_3 be the division polynomials of E. Explicitly we have

$$\psi_2 = 2y, \qquad \psi_3 = 3x^4 - 6x^2 + 12n^2x - 1.$$

If P reduces to a nonsingular point modulo 2, then

$$\lambda_2(P) = \frac{1}{2}\log\max\{1, |x(P)|_2\} + \frac{1}{12}v_2(\Delta) \geq \frac{1}{12}v_2(\Delta).$$

Put $X = x(P)$ and $Y = y(P)$. Assume P reduces to a singular point modulo 2. Then it is necessary that $v_2(X) = 0$, since $v_2(f_x(X)) = v_2(3X^2 - 1) > 0$ is needed, where $f(x) = x^3 - x + n^2$. If $n \equiv 1 \pmod 2$, then $v_2(Y^2) = v_2(X^3 - X + n^2) = 0$, and by Lemma 3.5 with [17, p. 353, (32)], we have

$$\lambda_2(P) = \frac{1}{3}\log|\psi_2(P)|_2 + \frac{1}{12}v_2(\Delta) = \frac{1}{3}\log|2Y|_2 + \frac{1}{12}v_2(\Delta) = -\frac{1}{3}\log 2 + \frac{1}{12}v_2(\Delta).$$

Similarly, if $n \equiv 0 \pmod 2$, then since $\psi_3(P) = 3X^4 - 6X^2 + 12n^2X - 1 \equiv 3 - 6 - 1 \equiv 4 \pmod 8$, we have

$$\lambda_2(P) = \frac{1}{8}\log|\psi_3(P)|_2 + \frac{1}{12}v_2(\Delta) = -\frac{1}{4}\log 2 + \frac{1}{12}v_2(\Delta).$$

In any case,

$$\lambda_2(P) \geq -\frac{1}{3}\log 2 + \frac{1}{12}v_2(\Delta).$$

For $p = 3$, by Lemma 3.4 the reduction type is I_0, and so

$$\lambda_3(P) = \frac{1}{2}\log\max\{1, |x(P)|_3\} + \frac{1}{12}v_3(\Delta) \geq \frac{1}{12}v_3(\Delta).$$

For $p > 3$, by Lemma 3.3 with the assumption that the p-primary part of $27n^4 - 4$ is square-free, the reduction type is either I_0 or I_1. So P always reduces to a nonsingular point modulo p (e.g., [18, p. 365]), and we have

$$\lambda_p(P) = \frac{1}{2}\log\max\{1, |x(P)|_p\} + \frac{1}{12}v_p(\Delta) \geq \frac{1}{12}v_p(\Delta).$$

Finally, we have

$$\hat{h}(P) = \sum_{p\le\infty} \lambda_p(P) > \frac{1}{3}\log n + \frac{\log(0.098)}{6} - \frac{1}{3}\log 2 + \sum_{p\le\infty}\frac{1}{12}v_p(\Delta)$$
$$> \frac{1}{3}\log n - 0.619. \qquad \square$$

Proposition 4.3. *Let $P_0 = (0, n)$ and $P_{-1} = (-1, n)$ be integral points on $E_{1,n}$. Assume that $n > 27$. Then*

$$\hat{h}(P_0) < \frac{1}{3}\log n + 0.716, \quad \hat{h}(P_{-1}) < \frac{1}{3}\log n + 0.541.$$

Proof. As in the proof of Proposition 4.1, we compute local heights of P_0 and P_{-1}.

For $p = \infty$, again we take the model $E' : y^2 = (x - 2l - 1/(3l))^3 - (x - 2l - 1/(3l)) + l^3$, where $l = n^{2/3} > 9$. Then on E' the points

$$P'_0 = (2l + 1/(3l), n), \qquad P'_{-1} = (-1 + 2l + 1/(3l), n)$$

correspond to P_0 and P_{-1}, respectively. By Tate's series with the bound (4.2), we have

$$\lambda_\infty(P_0) = \frac{1}{2}\log|2l + 1/(3l)| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k} z(2^k P'_0) + \frac{1}{12}v_\infty(\Delta)$$
$$< \frac{1}{2}\log|(2 + 9^{-2}\cdot 3^{-1})l| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\cdot\log(9.075) + \frac{1}{12}v_\infty(\Delta)$$
$$= \frac{1}{3}\log n + \frac{1}{2}\log(2 + 9^{-2}\cdot 3^{-1}) + \frac{1}{6}\log(9.075) + \frac{1}{12}v_\infty(\Delta)$$

and

$$\lambda_\infty(P_{-1}) = \frac{1}{2}\log|-1 + 2l + 1/(3l)| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log|z(2^k P'_{-1})| + \frac{1}{12}v_\infty(\Delta)$$
$$< \frac{1}{2}\log|2l| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\cdot\log(9.075) + \frac{1}{12}v_\infty(\Delta)$$
$$= \frac{1}{3}\log n + \frac{1}{2}\log 2 + \frac{1}{6}\log(9.075) + \frac{1}{12}v_\infty(\Delta).$$

For $p = 2$, since $v_2(x(P_0)) > 0$ and $v_2(x(P_{-1})) = 0$, P_0 and P_{-1} reduce to a nonsingular point and a singular point, respectively, modulo 2. Further, recall

if it is singular, then the reduction type is IV or III. So the same argument in the proof of Proposition 4.1 shows that

$$\lambda_2(P_0) = \frac{1}{2}\log\max\{1, |x(P_0)|_2\} + \frac{1}{12}v_2(\Delta) = \frac{1}{12}v_2(\Delta),$$
$$\lambda_2(P_{-1}) \leq -\frac{1}{4}\log 2 + \frac{1}{12}v_2(\Delta).$$

For $p \geq 3$, we have the trivial bounds valid for any integral point:

$$\lambda_p(P_0) \leq \frac{1}{12}v_p(\Delta), \quad \lambda_p(P_{-1}) \leq \frac{1}{12}v_p(\Delta).$$

By summing them up, we have

$$\begin{aligned}\hat{h}(P_0) &< \frac{1}{3}\log n + \frac{1}{2}\log(2 + 9^{-2}\cdot 3^{-1}) + \frac{1}{6}\log(9.075) + \sum_{p\leq\infty}\frac{1}{12}v_p(\Delta)\\ &< \frac{1}{3}\log n + 0.716\end{aligned}$$

and

$$\begin{aligned}\hat{h}(P_{-1}) &< \frac{1}{3}\log n + \frac{1}{2}\log 2 + \frac{1}{6}\log(9.075) - \frac{1}{4}\log 2 + \sum_{p\leq\infty}\frac{1}{12}v_p(\Delta)\\ &< \frac{1}{3}\log n + 0.541.\end{aligned}$$

□

Theorem 4.4. *Let $P_0 = (0, n)$ and $P_{-1} = (-1, n)$ be integral points on $E_{1,n}$. Assume that $n > 1$, and the p-primary part of $\Delta_{1,n}$ is square-free for any $p > 3$. Then $\{P_0, P_{-1}\}$ can be extended to a basis for $E_{1,n}(\mathbb{Q})$.*

Proof. By Proposition 2.1, $E_{1,n}(\mathbb{Q})$ is torsion-free, and by Proposition 2.2, if $n > 1$, then P_0 and P_{+1} are independent, and so are P_0 and P_{-1}. Let ν be the index of the span of P_0 and P_{-1} in $\mathbb{Z}G_1 + \mathbb{Z}G_2$, where G_1 and G_2 are points contained in a basis for $E_{1,n}(\mathbb{Q})$ such that $P_0, P_{-1} \in \mathbb{Z}G_1 + \mathbb{Z}G_2$. It is sufficient to show $\nu = 1$. By Siksek's theorem ([15]), we have

$$\nu \leq \frac{2}{\sqrt{3}}\frac{\sqrt{R(P_0, P_{-1})}}{\lambda},$$

where $R(P_0, P_{-1})$ is the regulator of $\{P_0, P_{-1}\}$, explicitly,

$$\begin{aligned}R(P_0, P_{-1}) &= \hat{h}(P_0)\hat{h}(P_{-1}) - \langle P_0, P_{-1}\rangle^2\\ &= \hat{h}(P_0)\hat{h}(P_{-1}) - \frac{1}{4}\left(\hat{h}(P_0 + P_{-1}) - \hat{h}(P_0) - \hat{h}(P_{-1})\right)^2,\end{aligned}$$

and λ is any positive lower bound of $\hat{h}$ for non-torsion points in $E_{1,n}(\mathbb{Q})$. Hence by Propositions 4.1 and 4.3, we have

$$\nu \le \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_0)\hat{h}(P_{-1})}}{\lambda} \le \frac{2}{\sqrt{3}} \frac{\sqrt{\left(\frac{1}{3}\log n + 0.716\right)\left(\frac{1}{3}\log n + 0.541\right)}}{\frac{1}{3}\log n - 0.619}$$

for $n > 27$. By calculation we see that the right hand side is less than 3 for $n > 66$, and less than 5 for $n > 19$, which imply $\nu = 1$ for $n > 66$, and $\nu = 1$ or 3 for $27 < n \le 66$, respectively. (Note that $2 \nmid \nu$ by Proposition 2.2.) Now by using the Magma function "DivisionPoints" ([2]), we can confirm that $P_0, P_{-1}, P_0 \pm P_{-1} \notin 3E(\mathbb{Q})$ for $27 < n \le 66$, which implies even $\nu = 1$ for $27 < n \le 66$. Finally, for $1 < n \le 27$ we can check that $\{P_0, P_{-1}\}$ can be extended to a basis by using the Magma function "Generators". Indeed, we can obtain a basis for each $n \le 27$. Then all we have to do is to check that the ratio R'/R is much less than four (and nonzero), where R is the regulator of the given basis and R' is the regulator of a set which consists of P_0, P_{-1} and appropriate points in the given basis. □

5. Generators for $E_{m,1}(\mathbb{Q})$

From this section we consider the curve $E = E_{m,1} : y^2 = x^3 - m^2x + 1$ over $\mathbb{Q}$. The argument is essentially the same as that for $E_{1,n}$. However, owing to a geometrical property, estimates of the canonical height are slightly easier.

We use the following modified Tate's series for the computation of the local height function.

Lemma 5.1. *Let $E/\mathbb{R}$ be an elliptic curve*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Assume that $x(Q) > 0$ for any Q in the connected component of O in $E(\mathbb{R})$. Then for any $P \in E(\mathbb{R}) \setminus E[2]$, the following convergent series gives the Archimedean part of the local height function:

$$\lambda_\infty(P) = \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|z(2^kP)| + \frac{1}{12}v_\infty(\Delta), \tag{5.2}$$

where

$$u(Q) = x^4(Q) - b_4x^2(Q) - 2b_6x(Q) - b_8, \qquad z(Q) = u(Q)/x^4(Q).$$

PROOF. First note $u(Q) = 0$ if and only if $x(2Q) = 0$, since

$$x(2Q) = \frac{u(Q)}{4x^3(Q) + b_2x^2(Q) + 2b_4x(Q) + b_6},$$

whose numerator and denominator have no common roots ([18, p. 458]). Note also we have the equality

$$(2y(Q) + a_1x(Q) + a_3)^2 = 4x^3(Q) + b_2x^2(Q) + 2b_4x(Q) + b_6,$$

whose value is nonzero if $Q \notin E[2]$.

Whether $x(P) = 0$ or not, we can use the original series of TATE ([21]) for $2P$ under our assumption. So, by the property of λ_∞ (e.g., [18, Ch. VI, Theorem 1.1]):

$$\lambda_\infty(2P) = 4\lambda_\infty(P) - \log|2y(P) + a_1x(P) + a_3| - \frac{1}{4}v_\infty(\Delta) \quad \text{for } P \in E(\mathbb{R}) \setminus E[2],$$

we have

$$\begin{aligned}
\lambda_\infty(P) &= \frac{1}{4}\lambda_\infty(2P) + \frac{1}{4}\log|2y(P) + a_1x(P) + a_3| + \frac{1}{16}v_\infty(\Delta) \\
&= \frac{1}{4}\left(\frac{1}{2}\log|x(2P)| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log|z(2^{k+1}P)| + \frac{1}{12}v_\infty(\Delta)\right) \\
&\quad + \frac{1}{4}\log|2y(P) + a_1x(P) + a_3| + \frac{1}{16}v_\infty(\Delta) \\
&= \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|z(2^kP)| + \frac{1}{12}v_\infty(\Delta). \qquad \square
\end{aligned}$$

The following fact is also used for estimates of the local height function.

Lemma 5.3. *Let E be an elliptic curve defined by a simple form*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

and let

$$\begin{aligned}
k &= 3\,x^2 + 2\,a_2\,x + 4\,a_4 - {a_2}^2, \\
l &= 9\,x^3 + 9\,a_2\,x^2 + (21\,a_4 - 4\,{a_2}^2)\,x + 27\,a_6 - 2\,a_2\,a_4
\end{aligned}$$

be functions on E. Then the identity

$$16\,k \cdot \psi_3 - 4\,l \cdot \psi_2^2 = \Delta$$

holds, where ψ_3 and ψ_2 are the division polynomials defined by

$$\psi_3 = 3\,x^4 + 4\,a_2\,x^3 + 6\,a_4\,x^2 + 12\,a_6\,x + 4\,a_2\,a_6 - a_4^2, \qquad \psi_2 = 2y,$$

regarded as functions on E.

PROOF. The substitution

$$\psi_2^2 = 4(x^3 + a_2x^2 + a_4x + a_6)$$

and computation give the result. □

Proposition 5.4. *Assume that $m \geq 10$, and that the p-primary part of $\Delta_{m,1} = -16(27 - 4m^6)$ is square-free for any $p > 3$. Then for any rational non-torsion point $P \in E_{m,1}(\mathbb{Q})$, we have*

$$\hat{h}(P) > \frac{1}{2}\log m - 0.509.$$

PROOF. By Lemma 5.1, for $P \in E(\mathbb{R}) \setminus E[2]$ we have

$$\lambda_\infty(P) = \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|z(2^kP)| + \frac{1}{12}v_\infty(\Delta),$$

where

$$u(P) = (x(P)^2 + m^2)^2 - 8x(P), \qquad z(2^kP) = \frac{(x(2^kP)^2 + m^2)^2 - 8x(2^kP)}{x^4(2^kP)}.$$

So we have the estimates

$$(x(P)^2 + m^2 - 1)^2 < u(P) < (x(P)^2 + m^2)^2 + 8(m+1), \tag{5.5}$$

$$1 < \left(1 + \frac{m^2-1}{x^2(2^kP)}\right)^2 < z(2^kP) < \left(1 + \frac{m^2}{x^2(2^kP)}\right)^2 < \left(1 + \frac{m^2}{(m-1)^2}\right)^2, \tag{5.6}$$

where the upper bounds are due to $x(P) > -(m+1)$ and $x(2^kP) > m-1$ implied by Lemma 3.7. (The upper bounds are for later use.) Hence

$$\begin{aligned}\lambda_\infty(P) &> \frac{1}{8}\log(m^2-1)^2 + \frac{1}{12}v_\infty(\Delta) = \frac{1}{4}\log\left\{m^2\left(1 - \frac{1}{m^2}\right)\right\} + \frac{1}{12}v_\infty(\Delta)\\ &> \frac{1}{4}\log\left\{m^2\left(1 - \frac{1}{10^2}\right)\right\} + \frac{1}{12}v_\infty(\Delta) = \frac{1}{2}\log m + \frac{1}{4}\log\frac{99}{100} + \frac{1}{12}v_\infty(\Delta).\end{aligned}$$

Next, we compute the local height for non-Archimedean places. Let

$$\psi_2 = 2y, \qquad \psi_3 = 3\,x^4 - 6\,m^2\,x^2 + 12\,x - m^4$$

be the division polynomials of E. Put $X = x(P)$ and $Y = y(P)$.

We claim that

$$\lambda_2(P)\begin{cases}\geq \frac{1}{12}v_2(\Delta) & \text{if } P \text{ reduces to a nonsingular point modulo 2,}\\ = -\frac{1}{3}\log 2 + \frac{1}{12}v_2(\Delta) & \text{otherwise.}\end{cases} \tag{5.7}$$

Indeed, if nonsingular, it is clear and we assume that P reduces to a singular point modulo 2. Then by Lemma 3.5, the reduction type is IV, and so

$$\lambda_2(P) = \frac{1}{3}\log|\psi_2(P)|_2 + \frac{1}{12}v_2(\Delta) = \frac{1}{3}\log|2Y|_2 + \frac{1}{12}v_2(\Delta).$$

If $v_2(m) > 0$, then $v_2(X) > 0$, since $v_2(3X^2 - m^2) > 0$. So $v_2(Y^2) = v_2(X^3 - m^2X + 1) = 0$. If $v_2(m) = 0$, then $v_2(X) = 0$, since $v_2(3X^2 - m^2) > 0$. So $v_2(Y^2) = v_2(X^3 - m^2X + 1) = 0$. In any case, $v_2(Y) = 0$, and we have

$$\lambda_2(P) = -\frac{1}{3}\log 2 + \frac{1}{12}v_2(\Delta).$$

Similarly, we claim that

$$\lambda_3(P) \geq \begin{cases}\frac{1}{12}v_3(\Delta) & \text{if } P \text{ reduces to a nonsingular point modulo 3,}\\ -\frac{1}{4}\log 3 + \frac{1}{12}v_3(\Delta) & \text{otherwise.}\end{cases} \tag{5.8}$$

Indeed, if nonsingular, it is clear and we assume that P reduces to a singular point modulo 3. Then it is necessary that $v_3(Y) > 0$ and $v_3(m) > 0$, since $\frac{\partial}{\partial x}(x^3 - m^2x + 1 - y^2) = 3x^2 - m^2$ and $\frac{\partial}{\partial y}(x^3 - m^2x + 1 - y^2) = -2y$. Further, note $v_3(X) \geq 0$, since $v_3(3X^2 - m^2) > 0$. Now the reduction type is III by Lemma 3.4, and

$$\lambda_3(P) = \frac{1}{8}\log|\psi_3(P)|_3 + \frac{1}{12}v_3(\Delta).$$

By Lemma 5.3, we have the identity

$$16\,(3\,X^2 - 4\,m^2)\cdot\psi_3(P) - 4\,(9\,X^3 - 21\,m^2\,X + 27)\cdot\psi_2^2(P) = \Delta.$$

Note that $\mathrm{ord}_3\Delta = 3$ and

$$\mathrm{ord}_3((9\,X^3 - 21\,m^2\,X + 27)\cdot\psi_2^2(P)) \geq 4, \qquad \mathrm{ord}_3(3X^2 - 4m^2) \geq 1.$$

This indicates $\mathrm{ord}_3\psi_3(P) \leq 2$, and so

$$\lambda_3(P) \geq \frac{1}{8}\cdot(-2\log 3) + \frac{1}{12}v_3(\Delta) = -\frac{1}{4}\log 3 + \frac{1}{12}v_3(\Delta).$$

For $p > 3$, by Lemma 3.3 with the assumption that $27 - 4m^6$ has no square factor, the reduction type is either I_0 or I_1, and so

$$\lambda_p(P) = \frac{1}{2}\log\max\{1, |x(P)|_p\} + \frac{1}{12}v_p(\Delta) \geq \frac{1}{12}v_p(\Delta). \tag{5.9}$$

Finally, we obtain

$$\hat{h}(P) = \sum_{p\leq\infty}\lambda_p(P) > \frac{1}{2}\log m + \frac{1}{4}\log\frac{99}{100} - \frac{1}{3}\log 2 - \frac{1}{4}\log 3 > \frac{1}{2}\log m - 0.509.$$

□

Proposition 5.10. *Let $P_0 = (0,1)$, $P_{-1} = (-m,1)$ and $P_2 = (-1,m)$ be integral points on $E_{m,1}$. Assume that $m \geq 10$. Then for $P \in \{P_0, P_{-1}, P_2, P_0 + P_{-1}, P_{-1} + P_2, P_0 + P_{-1} + P_2\}$,*

$$\hat{h}(P) < \frac{1}{2}\log m + 0.290.$$

Further, if we assume the p-primary part of $\Delta_{m,1}$ is square-free for any $p > 3$, then

$$\log m - 0.634 < \hat{h}(P_2 + P_0) < \log m + 0.068.$$

Proof. First we have the explicit expressions

$$\begin{aligned}
&P_0 + P_{-1} = -P_{+1} = (m, -1),\\
&P_{-1} + P_2 = (m+2, -2m-3), \quad P_2 + P_0 = (m^2-2m+2, m^3-3m^2+4m-3),\\
&P_0 + P_{-1} + P_2 = (-m+2, -2m+3).
\end{aligned}$$

So we have

$$\begin{aligned}
&u(P_0) = m^4, \quad u(P_{-1}) = 4m^4 + 8m, \quad u(P_2) = m^4 + 2m^2 + 9,\\
&u(P_0 + P_{-1}) = 4m^4 - 8m, \quad u(P_{-1} + P_2) = 4m^4 + 16m^3 + 32m^2 + 24m,\\
&u(P_0 + P_{-1} + P_2) = 4m^4 - 16m^3 + 32m^2 - 24m,
\end{aligned}$$

where $u(Q) = (x(Q)^2 + m^2)^2 - 8x(Q)$ as defined in Lemma 5.1. Therefore, for $P \in \{P_0, P_{-1}, P_2, P_0 + P_{-1}, P_{-1} + P_2, P_0 + P_{-1} + P_2\}$, we have

$$\begin{aligned}
u(P) &\leq 4m^4 + 16m^3 + 32m^2 + 24m = 4m^4(1 + 4/m + 8/m^2 + 6/m^3)\\
&\leq 4m^4(1 + 4/10 + 8/10^2 + 6/10^3) = 4m^4 \cdot \frac{743}{500}.
\end{aligned}$$

On the other hand,

$$u(P_2+P_0)=m^8-8\,m^7+34\,m^6-88\,m^5+153\,m^4-176\,m^3+128\,m^2-48\,m\le m^8$$

for $m \geq 10$.

By (5.6), we have

$$z(2^kQ) < \left(1+\frac{m^2}{(m-1)^2}\right)^2 \leq \left(1+\frac{10^2}{9^2}\right)^2 = \left(\frac{181}{81}\right)^2$$

for any Q. So for $P \in \{P_0, P_{-1}, P_2, P_0+P_{-1}, P_{-1}+P_2, P_0+P_{-1}+P_2\}$,

$$\begin{aligned}\lambda_\infty(P) &= \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|z(2^kP)| + \frac{1}{12}v_\infty(\Delta)\\ &< \frac{1}{8}\log 4m^4\left(\frac{743}{500}\right) + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\cdot\log\left(\frac{181}{81}\right)^2 + \frac{1}{12}v_\infty(\Delta)\\ &= \frac{1}{2}\log m + \frac{1}{8}\log 4 + \frac{1}{8}\log\frac{743}{500} + \frac{1}{12}\log\frac{181}{81} + \frac{1}{12}v_\infty(\Delta)\end{aligned}$$

and similarly,

$$\begin{aligned}\lambda_\infty(P_2+P_0) &< \frac{1}{8}\log m^8 + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\cdot\log\left(\frac{181}{81}\right)^2 + \frac{1}{12}v_\infty(\Delta)\\ &= \log m + \frac{1}{12}\log\frac{181}{81} + \frac{1}{12}v_\infty(\Delta).\end{aligned}$$

Now since the relevant points are integral, we clearly have

$$\lambda_p(P) \leq \frac{1}{12}v_p(\Delta)$$

for $p < \infty$.

By summing them up, for $P \in \{P_0, P_{-1}, P_2, P_0+P_{-1}, P_{-1}+P_2, P_0+P_{-1}+P_2\}$,

$$\hat{h}(P) < \frac{1}{2}\log m + \frac{1}{8}\log 4 + \frac{1}{8}\log\frac{743}{500} + \frac{1}{12}\log\frac{181}{81} < \frac{1}{2}\log m + 0.290,$$

and

$$\hat{h}(P_2+P_0) < \log m + \frac{1}{12}\log\frac{181}{81} < \log m + 0.068.$$

Next, we shall obtain a lower bound for $\hat{h}(P_2+P_0)$. By (5.5) and (5.6), we have

$$\begin{aligned}\lambda_\infty(P_2+P_0) &\geq \frac{1}{8}\log|x(P_2+P_0)^2+m^2-1|^2+\frac{1}{12}v_\infty(\Delta)\\ &= \frac{1}{4}\log(m^4-4m^3+9m^2-8m+3)+\frac{1}{12}v_\infty(\Delta)\\ &> \frac{1}{4}\log(m^4-4m^3)+\frac{1}{12}v_\infty(\Delta) > \frac{1}{4}\log\left\{m^4\left(1-\frac{4}{10}\right)\right\}+\frac{1}{12}v_\infty(\Delta)\\ &= \log m+\frac{1}{4}\log\frac{3}{5}+\frac{1}{12}v_\infty(\Delta).\end{aligned}$$

Finally, with using (5.7), (5.8) and (5.9), we obtain

$$\hat{h}(P_2+P_0) \geq \log m+\frac{1}{4}\log\frac{3}{5}-\frac{1}{3}\log 2-\frac{1}{4}\log 3 > \log m-0.634. \qquad \square$$

Theorem 5.11. *Let $P_0=(0,1)$, $P_{-1}=(-m,1)$ and $P_2=(-1,m)$ be integral points on $E_{m,1}$. Assume that $m>3$, and that the p-primary part of $\Delta_{m,1}=-16(27-4m^6)$ is square-free for any $p>3$. Then $\{P_0,P_{-1},P_2\}$ can be extended to a basis for $E_{m,1}(\mathbb{Q})$.*

Proof. Assume $m\geq 10$. By Proposition 2.1, $E_{m,1}(\mathbb{Q})$ is torsion-free, and by Proposition 2.2, if $m\neq 24$, then $\{P_0,P_{+1},P_0+P_{+1}\}\notin 2E_{m,1}(\mathbb{Q})$, equivalently, $\{P_0,P_{-1},P_0+P_{-1}\}\notin 2E_{m,1}(\mathbb{Q})$. Further, the facts

$$2^2\left(\frac{1}{2}\log m-0.509\right) > \frac{1}{2}\log m+0.290, \quad 2^2\left(\frac{1}{2}\log m-0.509\right) > \log m+0.068$$

with Propositions 5.4 and 5.10 imply $\{P_2,P_{-1}+P_2,P_2+P_0,P_0+P_{-1}+P_2\}\notin 2E_{m,1}(\mathbb{Q})$. Consequently, P_0,P_{-1},P_2 are independent for $m\geq 10, m\neq 24$.

Let ν be the index of the span of P_0,P_{-1},P_2 in $\mathbb{Z}G_1+\mathbb{Z}G_2+\mathbb{Z}G_3$, where G_1,G_2,G_3 are points contained in a basis for $E_{m,1}(\mathbb{Q})$ such that $P_0,P_{-1},P_2\in\mathbb{Z}G_1+\mathbb{Z}G_2+\mathbb{Z}G_3$. We should show $\nu=1$. First, we estimate the height paring:

$$2\langle P_i,\,P_j\rangle=\hat{h}(P_i+P_j)-\hat{h}(P_i)-\hat{h}(P_j).$$

By Propositions 5.4 and 5.10,

$$\begin{aligned}-\frac{1}{2}\log m-1.089 < 2\langle P_0,\,P_{-1}\rangle < \frac{1}{2}\log m+1.308,\\ -\frac{1}{2}\log m-1.089 < 2\langle P_{-1},\,P_2\rangle < \frac{1}{2}\log m+1.308,\\ -1.214 < 2\langle P_2,\,P_0\rangle < 1.086.\end{aligned}$$

As the proof of Theorem 4.4, by Siksek's theorem

$$\nu \le \sqrt{2}\sqrt{\frac{R(P_0, P_{-1}, P_2)}{\lambda^3}}.$$

Since by definition,

$$\begin{aligned} R(P_0, P_{-1}, P_2) &= |\det(\langle P_i,\, P_j\rangle)_{i,j=0,-1,2}| \\ &< \hat{h}(P_0)\,\hat{h}(P_{-1})\,\hat{h}(P_2) + 2\langle P_0,\, P_{-1}\rangle\langle P_{-1},\, P_2\rangle\langle P_2,\, P_0\rangle, \end{aligned}$$

we have

$$\sqrt{2}\sqrt{\frac{R(P_0, P_{-1}, P_2)}{\lambda^3}} < \sqrt{2}\sqrt{\frac{\left(\frac{1}{2}\log m + 0.290\right)^3 + 2\left(\frac{1}{4}\log m + \frac{1.308}{2}\right)^2 \times \frac{1.214}{2}}{\left(\frac{1}{2}\log m - 0.509\right)^3}}$$

for $m \ge 10$. By calculation, we see that the right hand side is less than 3 for $m \ge 59$, which implies $\nu = 1$ for $m \ge 59$. (Note that $2 \nmid \nu$ by the above argument.) For $m < 59$, we can check that $\{P_0, P_{-1}, P_2\}$ can be extended to a basis by using the Magma function "Generators" by the same manner as in Theorem 4.4. □

Remark 5.12. During the check, we can find that in the cases where $m = 7, 24$, $\{P_0, P_{-1}, P_2\}$ cannot be extended to a basis (in fact $\nu = 2$), but in such cases the assumption that the p-primary part of Δ is square-free for $p > 3$ is not satisfied. In the cases where $m = 1, 2, 3$ the rank of $E_{m,1}(\mathbb{Q})$ is less than three.

At the end of the paper we prove Proposition 1.3. Before this, we review the outline of the proof of [12, Theorem 1].

For any polynomial f such that $\{f(n); n \in \mathbb{Z}\}$ have no common square factor, put

$$\begin{aligned} S_1(x) &= \#\{n \in (0, x]; p^2 \nmid f(n) \text{ for any } p \le (\log x)/3\}, \\ S_2(x) &= \#\{n \in (0, x]; p^2 \mid f(n) \text{ for some } p \in ((\log x)/3, x]\}, \\ S_3(x) &= \#\{n \in (0, x]; p^2 \mid f(n) \text{ for some } p > x\}. \end{aligned}$$

Then

$$S_1(x) \sim \prod_p \left(1 - \frac{\omega_f(p)}{p^2}\right) \cdot x, \quad S_2(x) = o(x), \quad S_3(x) = o(x),$$

where

$$\omega_f(p) = \#\{n \pmod{p^2}; f(n) \equiv 0 \pmod{p^2}\}.$$

The first estimate is due to the prime number theorem with the fact that the number of integers $n \in (a, a + \prod_{p \le x_0} p^2]$ such that $p^2 \nmid f(n)$ for any $p \le x_0$ is exactly

$$\prod_{p \le x_0} p^2 \prod_{p \le x_0} \left(1 - \frac{\omega_f(p)}{p^2}\right),$$

independently of a, which is essentially from the Chinese remainder theorem. The estimate for S_3 needs the *abc* conjecture. Consequently, [12, Theorem 1] is proved.

So in our setting, we have only to remove the factors $\left(1-\frac{\omega_f(2)}{2^2}\right)$ and $\left(1-\frac{\omega_f(3)}{3^2}\right)$ from the first estimate, since we allow the discriminants $\Delta_{1,n}$ and $\Delta_{m,1}$ to be divisible by the square of 2 or 3, which does not alter the estimate for S_2 and S_3.

Proof of Proposition 1.3. Put $D_{m,n} = 27n^4 - 4m^6$, so that $\Delta_{m,n} = -16D_{m,n}$. Further, define

$$\Omega_1(p) = \{n \pmod{p^2}; D_{1,n} \equiv 0 \pmod{p^2}\},$$
$$\Omega_2(p) = \{m \pmod{p^2}; D_{m,1} \equiv 0 \pmod{p^2}\}.$$

Since the discriminants of $D_{1,n}$ and $D_{m,1}$ (as polynomials in n and m, respectively) have no prime divisor other than 2 or 3, we have $\omega_1(p) := \#\Omega_1(p) \le 4$ and $\omega_2(p) := \#\Omega_2(p) \le 6$ for $p > 3$ by [13, Lemma 5.2].

In view of the argument just before the proof, we see that

$$\kappa_1 = \prod_{p>3} \left(1 - \frac{\omega_1(p)}{p^2}\right) = \prod_{k=3}^{\infty} \left(1 - \frac{\omega_1(p_k)}{p_k^2}\right),$$

where p_k is the k-th prime number. Now by using the inequality

$$\prod_{k=1}^{N} (1 - a_k) \ge 1 - \sum_{k=1}^{N} a_k$$

for $0 < a_k < 1$, which can be seen by induction, we have

$$\kappa_1 = \prod_{k=3}^{60} \left(1 - \frac{\omega_1(p_k)}{p_k^2}\right) \prod_{k=61}^{\infty} \left(1 - \frac{\omega_1(p_k)}{p_k^2}\right) \ge \prod_{k=3}^{60} \left(1 - \frac{\omega_1(p_k)}{p_k^2}\right) \prod_{k=61}^{\infty} \left(1 - \frac{4}{p_k^2}\right)$$
$$\ge \prod_{k=3}^{60} \left(1 - \frac{\omega_1(p_k)}{p_k^2}\right) \left(1 - \sum_{k=61}^{\infty} \frac{4}{p_k^2}\right) = 0.972866\cdots \times 0.997939\cdots > 0.97,$$

where we compute $\omega_1(p_k)$ for $k \le 60$ directly and use the known result of the prime zeta function (e.g. [6, p. 95]):

$$\sum_{k=1}^{\infty} \frac{1}{p_k^2} = 0.4522474200\cdots .$$

By the same argument,

$$\kappa_2 = \prod_{k=3}^{60}\left(1-\frac{\omega_2(p_k)}{p_k^2}\right)\prod_{k=61}^{\infty}\left(1-\frac{\omega_2(p_k)}{p_k^2}\right) \ge \prod_{k=3}^{60}\left(1-\frac{\omega_2(p_k)}{p_k^2}\right)\prod_{k=61}^{\infty}\left(1-\frac{6}{p_k^2}\right)$$
$$\ge \prod_{k=3}^{60}\left(1-\frac{\omega_2(p_k)}{p_k^2}\right)\left(1-\sum_{k=61}^{\infty}\frac{6}{p_k^2}\right) = 0.976111\cdots\times 0.996909\cdots > 0.97. \quad \square$$

Acknowledgements. The authors are grateful to the referee and the editor for valuable suggestions.

References

[1] A. Antoniewicz, On a family of elliptic curves, *Univ. Iagel. Acta Math.* **43** (2005), 21–32.

[2] W. Bosma, J. Cannon, W. Bosma and C. Fieker (eds.), Handbook of Magma Functions, *Department of Mathematics, University of Sydney*, http://magma.maths.usyd.edu.au/magma/.

[3] E. Brown and B. T. Myers, Elliptic curves from Mordell to Diophantus and back, *Amer. Math. Monthly* **109** (2002), 639–649.

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

[5] E. V. Eikenberg, Rational points on some families of elliptic curves, PhD thesis, *University of Maryland*, 2004.

[6] S. R. Finch, Mathematical Constants, *Cambridge University Press*, *Cambridge*, 2003.

[7] Y. Fujita and N. Terai, Generators for the elliptic curve $y^2 = x^3 - nx$, *J. Théor. Nombres Bordeaux* **23** (2011), 403–416.

[8] Y. Fujita and T. Nara, On the Mordell–Weil group of the elliptic curve $y^2 = x^3 + n$, *J. Number Theory* **132** (2012), 448–466.

[9] Y. Fujita, Generators for the elliptic curve $y^2 = x^3 - nx$ of rank at least three, *J. Number Theory* **133** (2013), 1645–1662.

[10] Y. Fujita, Generators for congruent number curves of ranks at least two and three, *J. Ramanujan Math. Soc.* **29** (2014), 307–319.

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

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

[13] M. R. Murty and H. Pasten, Counting squarefree values of polynomials with error term, *Int. J. Number Theory* **10** (2014), 1743–1760.

[14] T. Shioda, On the Mordell–Weil lattices, *Comment. Math. Univ. St. Paul* **39** (1990), 211–240.

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

[16] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer-Verlag, New York*, 1986.

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

[18] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, *Springer-Verlag, New York*, 1994.

[19] P. Tadić, On the family of elliptic curves $Y^2 = X^3 - T^2X + 1$, *Glas. Mat. Ser. III* **47** (2012), 81–93.

[20] P. Tadić, The rank of certain subfamilies of the elliptic curve $Y^2 = X^3 - X + T^2$, *Ann. Math. Inform.* **40** (2012), 145–153.

[21] J. Tate, Letter to J.-P. Serre, *arXiv:1207.5765* (1979).

[22] Wolfram Research, Inc., Mathematica, Version 10.3, *Wolfram Research, Inc., Champaign, IL*, 2015.

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 May 21, 2016)