Czechoslovak Mathematical Journal, 71 (146) (2021), 1133–1147

THE MORDELL-WEIL BASES FOR THE ELLIPTIC CURVE $y^2 = x^3 - m^2x + m^2$

Sudhansu Sekhar Rout, Bhubaneswar, Abhishek Juyal, Chennai

Received June 7, 2020. Published online March 22, 2021.

Abstract. Let D_m be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 - m^2x + m^2$, where m is an integer. In this paper we prove that the two points $P_{-1} = (-m, m)$ and $P_0 = (0, m)$ on D_m can be extended to a basis for $D_m(\mathbb{Q})$ under certain conditions described explicitly.

Keywords: elliptic curve; Mordell-Weil group; canonical height

MSC 2020: 11G05, 11D59

1. Introduction

The family $E_{m,n}\colon\ y^2 = x^3 - m^2x + n^2$ of elliptic curves has been extensively studied by several mathematicians, see [1], [2], [4], [9], [10], [17], [18]. Many papers have been devoted on this family to study its different properties. In [2], Brown and Myers constructed an infinite family of elliptic curves $E_{1,n}\colon\ y^2 = x^3 - x + n^2$ and showed that the rank of the Mordell-Weil group $E_{1,n}(\mathbb{Q}) \geqslant 2$. Antoniewicz in [1] produced another family of elliptic curves $E_{m,1}\colon\ y^2 = x^3 - m^2x + 1$ and proved that the rank of the Mordell-Weil group $E_{m,1}(\mathbb{Q}) \geqslant 3$. Eikenberg in [4] studied the curves $E_{1,n}$ and $E_{m,1}$ over function fields. In particular, Eikenberg used the theory of Mordell-Weil lattices (see [12]) to find the basis for $E_{1,n}(\mathbb{Q}(n))$ and $E_{m,1}(\mathbb{Q}(m))$, where $\mathbb{Q}(n)$ and $\mathbb{Q}(m)$ are function fields. Later in [8], Fujita and Nara, exploiting the estimates of canonical heights, proved that the explicit points in the families of elliptic curves $E_{1,n}$ and $E_{m,1}$ can always be in system generators of the Mordell-Weil group. There are several references describing explicitly the basis 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. [5], [6], [7], [8], [9].

A. Juyal's research was supported by IMSc Chennai (HBNI) Post-Doctoral Fellowship.

DOI: 10.21136/CMJ.2021.0238-20

In this paper we attempt to study an infinite family of elliptic curves of the form

$$D_m\colon\ y^2 = x^3 - m^2x + m^2, \tag{1}$$

where m is an integer. We put

$$P_{\pm 1} = (\pm m, m) \quad \text{and} \quad P_0 = (0, m).$$

It is easy to see that the points $P_{\pm 1}, P_0$ are in $D_m(\mathbb{Q})$.

The classification of rational elliptic surfaces (see [11]) implies the following result.

Theorem 1.1. *The Mordell-Weil group $D_m(\bar{\mathbb{Q}}(m))$ has rank 2 with the trivial torsion subgroup, generated by the points P_{-1} and P_0.*

Since both of the generators of this group are rational, the entire group must be defined over $\mathbb{Q}(m)$, therefore, we have the following corollary.

Corollary 1.2. *$D_m(\mathbb{Q}(m))$ has rank 2 generated by the points P_{-1} and P_0.*

Let C be a curve defined over a field k, let S be an elliptic surface over C, and let $K = k(C)$. Then one can view S as an elliptic curve E over the field K. For any $t \in C(\overline{k})$, we denote by $E_{(t)}$ the specialization of E at t. Now we state the Silverman Specialization Theorem.

Theorem 1.3 ([15], Theorem 11.4, page 271)**.** *The specialization map $\sigma_t\colon E(K) \to E_{(t)}(\overline{k})$ is injective for all but finitely many $t \in C(\overline{k})$.*

Since the rank of $D_m(\mathbb{Q}(m))$ is equal to 2, by the Silverman Specialization Theorem we obtain the rank of $D_m(\mathbb{Q}) \geqslant 2$ for all but finitely many values of m and hence the points P_{-1} and P_0 are independent for all but finitely many m. Therefore the immediate question one can ask is "can the set $\{P_{-1}, P_0\}$ be extended to a basis of $D_m(\mathbb{Q})$?" In this paper, we answer this question affirmatively. The main result of the paper is the following.

Theorem 1.4. *Let m be a square-free integer, $m \equiv 1 \pmod 4$. Let $P_{-1} = (-m, m)$ and $P_0 = (0, m)$ be integral points of $D_m(\mathbb{Q})$. Assume that $m > 4$ and the p primary part of $27 - 4m^2$ is square-free for any $p > 3$. Then for all but finitely many m the set of points $\{P_0, P_{-1}\}$ can be extended to a basis for $D_m(\mathbb{Q})$.*

The family of elliptic curves D_m has a unique property (*double lift*) in comparison to the curves $E_{1,n}$ and $E_{m,1}$ considered in [8]. Brown and Myers in [2] proved that $E_{1,n}(\mathbb{Q}(n))$ has rank 2 generated by $P = (0, n)$ and $Q = (1, n)$. Further, they

proved that there are infinitely many values of n such that $E_{1,n}(\mathbb{Q})$ has rank at least 3 by constructing some infinite families of curves with rank at least 3. For example, suppose $n(t) = 54t^2 - 165t - 90$. Then the subfamily $E_{1,n(t)}(\mathbb{Q}(t))$ contains an additional point $R(t) = (36t+17, 54t^2+267t+114)$ and it is independent from the points P and Q, see [2]. This can be viewed as a *lift* of the point $(17, 114) \in E_{1,90}(\mathbb{Q})$, since this is obtained when specializing to $t = 0$. This particular lift increases the rank of $E_{1,n}$ by 1. But, there exists a quadratic polynomial $m(t)$ such that $D_{m(t)}(\mathbb{Q}(t))$ contains four independent points. Two of these points can be chosen as lifts of the point $(-7, 35) \in D_{14}(\mathbb{Q})$, see [4]. This results in a *double lift* of the point $(-7, 35)$ and hence increases the rank by 2. For more general criteria for lifting the points of $E_{1,n}$ and $E_{m,1}$ one may refer to [4].

The organization of this paper is as follows. In Section 2 we review basic notions from the field of elliptic curves. In Section 3 we study the local properties of the curve D_m and also compute the bounds of the canonical heights for P_{-1}, P_0. At the end we complete the proof of Theorem 1.4. Our proofs closely follow the arguments from [8].

2. Preliminaries

In this section we develop necessary background material needed for a better exposition and clarity of presentation of this paper.

Let E be an elliptic curve over a number field K. It is known by the Mordell-Weil Theorem that the set of K-rational points $E(K)$ is a finitely generated abelian group. If the absolute value of the discriminant of E is large, then it is very difficult to compute $E(K)$ even if $K = \mathbb{Q}$. The main difficulties arise from the free part of the group. The Weierstrass equation for the elliptic curve E over a number field K is

$$E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. By completing the square of the left hand side of (2), we have

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{3}$$

where

$$\begin{gathered} b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{gathered} \tag{4}$$

We also have

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^2b_8 + 36b_2b_4 - 216b_6.$$

The discriminant of the elliptic curve E is defined as

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6. \tag{5}$$

Denote by $x(P)$ the x-coordinate of a point P on E. For $P = (x, y) \in E(\mathbb{Q})$, we have the duplication formula

$$x(2P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}. \tag{6}$$

Next we define the canonical height. Let $P = (x, y) \in E(\mathbb{Q})$. If $x = b/a$ and $\gcd(a, b) = 1$, then the naive height $h\colon E(\mathbb{Q}) \to \mathbb{R}$ is defined by

$$h(P) = \max\{\log |a|, \log |b|\}$$

and the canonical height $\hat{h}\colon E(\mathbb{Q}) \to \mathbb{R}$ is defined by

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

We compute the canonical height using the local height. One can refer to [14], page 341 for the existence of the local height function. The canonical height can be decomposed as the sum of local heights. In this paper the definition of the local height function follows, see [15], Chapter VI. We denote the local height function on E for a place p by λ_p. For $K = \mathbb{Q}$, we have the decomposition

$$\hat{h}(P) = \sum_{p\colon \text{prime}} \lambda_p(P) + \lambda_\infty(P) \quad \text{for } P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}. \tag{7}$$

In addition, the canonical height gives a bilinear pairing on $E(\mathbb{Q})$ called the canonical height pairing (or Néron-Tate height pairing):

$$\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)). \tag{8}$$

Finally, for a prime number p denote by v_p the valuation on $\mathbb{Q}$, i.e., $v_p(\cdot) = -\log |\cdot|_p$. Now we prove few lemmas which we use in the proof of our main theorem.

Lemma 2.1. *Let $A = (x', y')$ and $B = (x, y)$ be points in $D_m(\mathbb{Q})$ such that $A = 2B$ and $x' \in \mathbb{Z}$. Then*

(1) $x \in \mathbb{Z}$,

(2) $x \equiv m \pmod 2$.

P r o o f. Equating the x-coordinates of A and $2B$, where the x-coordinate of $2B$ is calculated using the formula given in (6), and then substituting $x = u/s$ with $\gcd(u, s) = 1$, we get, after simplifying,

$$(m^4 - 4m^2x')s^4 + (4m^2x' - 8m^2)us^3 + 2m^2u^2s^2 - 4x'u^3s + u^4 = 0. \tag{9}$$

From (9), it is clear that $s \mid u^4$. Since $\gcd(u, s) = 1$, we have $s = \pm 1$ and hence $x \in \mathbb{Z}$. Further, rewriting (9) as

$$(x^2 + m^2)^2 = 4(x'(x^3 - m^2x + m^2) + 2xm^2),$$

we have $2 \mid (x^2 + m^2)$, i.e., $x \equiv m \pmod 2$. □

Lemma 2.2. *Let m be a positive integer with $m \equiv 1 \pmod 4$. Then the point $A_m = (0, m)$ is an element of $D_m(\mathbb{Q}) \setminus 2D_m(\mathbb{Q})$.*

P r o o f. Suppose $A_m = 2G$ for some $G = (x, y) \in D_m(\mathbb{Q})$. Then from (6), we calculate $x(2G)$ and equating the x-coordinates of $2G$ and A_m, we have

$$\frac{x^4 + 2m^2x^2 + m^4 - 8xm^2}{4(x^3 - m^2x + m^2)} = 0,$$

that is,

$$(x^2 + m^2)^2 = 8xm^2. \tag{10}$$

From (10) we observe that $x = 2k^2$ for some $k \in \mathbb{Z}$. Substituting x into (10), we get

$$16k^8 + 8m^2k^4 + m^4 = 16k^2m^2. \tag{11}$$

It follows that for any integer k, taken modulo 4, the equation (11) has no solution. Consequently the equation (11) has no rational solution. Therefore, $A_m \notin 2D_m(\mathbb{Q})$. □

Lemma 2.3. *Let m be a positive integer with $m \equiv 1 \pmod 4$. Then the point $B_m = (m, m)$ is an element of $D_m(\mathbb{Q}) \setminus 2D_m(\mathbb{Q})$.*

P r o o f. Suppose $B_m = (m, m) = 2G$ for some $G = (x, y) \in D_m(\mathbb{Q})$. Using (6) again we get

$$\frac{x^4 + 2m^2x^2 + m^4 - 8xm^2}{4(x^3 - m^2x + m^2)} = m. \tag{12}$$

A further simplification of (12) yields

$$x^4 - 4mx^3 + 2m^2x^2 + (4m^3 - 8m^2)x + m^4 - 4m^3 = 0,$$

which can be rewritten as

$$(x-m)^4 - 4(x-m)^2m^2 - 8(x-m)m^2 - 12m^3 + 4m^4 = 0. \tag{13}$$

By Lemma 2.1, we substitute $x-m = 2s$, which results in the simplification of (13) as

$$(2s^2 - m^2)^2 = (4s + 3m)m^2.$$

The above equation holds only if $(4s + 3m) = w^2$ for some $w \in \mathbb{Z}$. Since $m \equiv 1 \pmod 4$, $4s + 3m \equiv 3 \pmod 4$ leads to a contradiction that it is a perfect square. This completes the proof. □

Lemma 2.4. *The point $A_m + B_m = (-m, m)$ is an element of $D_m(\mathbb{Q}) \setminus 2D_m(\mathbb{Q})$ for any positive integer m with $m \equiv 1 \pmod 4$.*

P r o o f. The proof is similar to that of Lemma 2.3. □

3. Local study of the curve $D_m\colon\ y^2 = x^3 - m^2x + m^2$

Lemma 3.1. *If m is 3rd power-free and $m \not\equiv 0 \pmod 4$, then the Weierstrass equation*

$$y^2 = x^3 - m^2x + m^2 \tag{14}$$

for D_m is global minimal.

P r o o f. Taking into consideration (see [16], Chapter VII, Remark 1.1), it is enough to show that at least one of the relations $v_p(c_4) < 4$, $v_p(c_6) < 6$ and $v_p(\Delta) < 12$ holds for every prime p. Now we have

$$c_4 = 2^4 \cdot 3m^2,\ c_6 = -2^5 \cdot 3^3m^2,\ \Delta = -2^4m^4(-2^2m^2 + 27).$$

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 3.2. *If $m \not\equiv 0 \pmod 2$, m is square-free and the p primary part of $27 - 4m^2$ is square-free, then the reduction type of D_m at prime p is as follows:*

(1) *IV if $p = 2$ or ($p \geqslant 3$ and $v_p(m) = 1$).*
(2) *I_0 if $p = 3$ and $p \nmid m$.*
(3) *I_k if $p \mid (27 - 4m^2)$, where $k = v_p(\Delta)$.*

P r o o f. First we find the reduction type of D_m at $p = 2$. We have seen from Lemma 3.1 that D_m is minimal. By [16], Chapter VII, Proposition 1.3, every minimal Weierstrass equation is unique up to a change of coordinates by some $[1, r, s, t]$, where $[1, r, s, t]$ means the transformation

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

Thus, by transforming D_m by $[1, 1, 1, 1]$, we get

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

with $b_8 = -m^4+6m^2+3$, $b_6 = 4$. Since $m \equiv 1 \pmod 2$, we have $b_8 \equiv 0 \pmod 8$ and $b_6 \equiv 4 \pmod 8$ which indicates the type IV by Tate's algorithm, see [15], page 366. Next we check the reduction type at $p = 3$. Suppose $m \not\equiv 0 \pmod 3$. Then clearly $3 \nmid (4m^2 + 27)$. Thus, $\Delta = -16m^4(-4m^2 + 27)$ is not divisible by 3 and hence we have reduction type I_0, see [15], Exercise 4.48. Next assume $m \equiv 0 \pmod 3$. As m is square free, we have $v_3(\Delta) = 6$. Now there exists a minimal Weierstrass equation $y^2 = x^3+a_2x^2+a_4x+a_6$ for E_m such that a_2, a_4, a_6 and Δ are as described in the table of Exercise 4.48 in [15]. Since E_m is also minimal, we can transform $y^2 = x^3 + a_2x^2 + a_4x + a_6$ into $y^2 = x^3 - m^2x + m^2$ by some $[1, r, s, t]$. Transforming $y^2 = x^3 - m^2x + m^2$ by $[1, 3, 0, 0]$, we have the equation

$$y^2 = x^3 + 9x^2 + (27 - m^2)x + 27 - 2m^2.$$

So, $v_p(a_2) = v_p(a_4) = v_p(a_6) = 2$. Therefore the possible reduction type is IV, see [15], Exercise 4.48.

Now onwards we assume $p \geqslant 5$ to find the reduction type of E_m at p. Now there exists a minimal Weierstrass equation $y^2 = x^3 + a_4x + a_6$ for E_m such that a_4, a_6 and Δ are as described in the table of Exercise 4.47 in [15]. Since the curve E_m is minimal, we can transform $y^2 = x^3 + a_4x + a_6$ to $y^2 = x^3 - m^2x + m^2$ by the transformation [1, 0, 0, 0]. If p divides Δ then p divides m or p divides $27 - 4m^2$. In the former case, as m is square-free, we have $v_p(\Delta) = 4, v_p(a_4) = v_p(-m^2) = 2$ and $v_p(a_6) = v_p(m^2) = 2$. Therefore the possible reduction type is IV, see [15], Exercise 4.47. If p divides $27 - 4m^2$ then using the Legendre symbol, one can see that $p \equiv \pm 1 \pmod{12}$. Since p primary part of $27 - 4m^2$ is square-free, we have $v_p(a_4) = 0 = v_p(a_6)$. Hence the possible reduction type is I_k, see [15], Exercise 4.47. □

The non-Archimedean part of canonical height can be computed using Silverman's algorithm (see [14], Theorem 5.2) and we use modified Tate's series for the computation of the Archimedean part.

Lemma 3.3 ([8], Lemma 5.2)**.** *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 $\mathcal{O}$ 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:

$$\lambda_\infty(P) = \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|Z(2^kP)| + \frac{1}{12}v_\infty(\Delta), \tag{15}$$

where

$$\begin{aligned} u(Q) &= x^4(Q) - b_4x^2(Q) - 2b_6x(Q) - b_8, \\ Z(Q) &= u(Q)/x^4(Q). \end{aligned} \tag{16}$$

Lemma 3.4 ([8], 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

$$\begin{aligned} k &= 3x^2 + 2a_2x + 4a_4 - a_2^2, \\ l &= 9x^3 + 9a_2x^2 + (21a_4 - 4a_2^2)x + 27a_6 - 2a_2a_4 \end{aligned}$$

be functions on E. Then the identity

$$16k \cdot \psi_3 - 4l \cdot \psi_2^2 = \Delta \tag{17}$$

holds, where ψ_2 and ψ_3 are the division polynomials.

Proposition 3.5. *Assume that m is a square-free integer with $m \geqslant 10$ and that the p-primary part of $(-4m^2+27)$ is square-free for any $p > 3$. Then for any rational non-torsion point $P \in D_m(\mathbb{Q})$ we have*

$$\hat{h}(P) > \frac{1}{6}\log m - \frac{1}{3}\log 2.$$

P r o o f. Since $m \geqslant 10$, we have $27 - 4m^2 < 0$ and hence the discriminant of D_m is positive. Thus the number of real roots of the cubic polynomial $x^3 - m^2x + m^2$ is three. Then for any Q in the connected component of $\mathcal{O}$ in $D_m(\mathbb{R})$ we have $x(Q) > 0$ by [8], Lemma 3.7.

By Lemma 3.3 for $P \in D_m(\mathbb{Q}) \setminus D_m[2]$ we have

$$\lambda_\infty(P) = \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|Z(2^kP)| + \frac{1}{12}v_\infty(\Delta), \tag{18}$$

where

$$u(P) = x^4 - b_4x^2 - 2b_6x - b_8.$$

Note that in the above expression of $u(P)$, we have $x = x(P)$. Using (4), we have

$$b_2 = 0, \quad b_4 = -2m^2, \quad b_6 = 4m^2, \quad b_8 = \frac{b_2b_6 - b_4^2}{4} = -m^4.$$

Thus, from (16),

$$\begin{aligned} u(P) &= (x^2 + m^2)^2 - 8m^2x, \\ Z(P) &= \frac{u(P)}{x^4(P)} = \frac{(x^2 + m^2)^2 - 8m^2x}{x^4}. \end{aligned} \tag{19}$$

As $(x^2+m^2)^2 - 8m^2x - [(x^2+m^2)^2 + 16x^2 - 2(x^2+m^2)4x]$ implies $8x^2(x-2) > 0$ for $x > 2$, we infer that

$$m^4 < (x^2 + m^2 - 4x)^2 < u(P)$$

for $x > 2$. Also,

$$x^4 < (x^2 + m^2 - 4x)^2 < u(P) \tag{20}$$

implies

$$1 < \left(1 + \frac{m^2 - 4x}{x^2}\right)^2 < Z(P). \tag{21}$$

Hence

$$\begin{aligned} \lambda_\infty(P) &= \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|Z(2^kP)| + \frac{1}{12}v_\infty(\Delta) \\ &> \frac{1}{8}\log m^4 + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log 1 + \frac{1}{12}v_\infty(\Delta) > \frac{1}{2}\log m + \frac{1}{12}v_\infty(\Delta). \end{aligned}$$

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

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

be the division polynomials of D_m. Set $x = x(P)$, $y = y(P)$. If P reduces to a nonsingular point modulo 2 then

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

Next assume that P reduces to a singular point modulo 2. Since $m \equiv 1 \pmod 2$ we have $v_2(x) = 0$. Further, since $v_2(3x^2 - m^2) > 0$, so $v_2(y^2) = v_2(x^3 - m^2x + m^2) = 0$ implies $v_2(y) = 0$. Thus,

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

If $p = 3$ and $p \nmid m$, then the reduction type is I_0. So

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

Now for $p > 3$ and $p \mid (27 - 4m^2)$ the reduction type is I_k with $k = v_p(\Delta)$ by Lemma 3.2. For this case,

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

Assume $p \geqslant 3$ and $p \mid m$. In this case the reduction type is IV and hence

$$\lambda_p(P) = \frac{1}{3}\log|\psi_2(P)|_p + \frac{1}{12}v_p(\Delta).$$

Since $v_p(3x^2 - m^2) > 0$ we have $v_p(x) > 0$. Again, $v_p(y^2) = v_p(x^3 - m^2x + m^2) > 0$ implies $v_p(y) > 0$. From (17), we have the identity

$$16(3x^2 - 4m^2)\psi_3(P) - 4(9x^3 - 21m^2x + 27m^2)\psi_2(P)^2 = \Delta. \tag{22}$$

Note that

$$\begin{cases} \operatorname{ord}_p(\Delta) = 4, \\ \operatorname{ord}_p(3x^2 - 4m^2) = 2, \\ \operatorname{ord}_p(9x^3 - 21m^2x + 27m^2) = 2, \\ \operatorname{ord}_p(\psi_3(P)) = 3. \end{cases} \tag{23}$$

Thus from (22) and (23), we deduce that $\operatorname{ord}_p(\psi_2^2(P)) \leqslant 2$ which implies

$$\operatorname{ord}_p(\psi_2(P)) \leqslant 1.$$

Hence,

$$\lambda_p(P) = \frac{1}{3}\log|\psi_2(P)|_p + \frac{1}{12}v_p(\Delta) \geqslant -\frac{1}{3}\log p + \frac{1}{12}v_p(\Delta) > -\frac{1}{3}\log m + \frac{1}{12}v_p(\Delta).$$

Finally, we have

$$\begin{aligned}(24)\qquad \hat{h}(P) &= \sum_{p\colon \text{prime}} \lambda_p(P) + \lambda_\infty(P) > -\frac{1}{3}\log 2 - \frac{1}{3}\log m + \frac{1}{2}\log m \\ &= \frac{1}{6}\log m - \frac{1}{3}\log 2.\end{aligned}$$

This completes the proof of Proposition 3.5. □

Proposition 3.6. *Let $P_0 = (0, m)$, $P_{-1} = (-m, m)$ and $P_1 = (m, m)$ be integral points on*

$$D_m\colon\ y^2 = x^3 - m^2x + m^2.$$

Assume $m \geqslant 10$. Then

$$\hat{h}(P_0) < \frac{1}{6}\log m + 0.46409, \quad \hat{h}(P_{-1}) < \frac{1}{6}\log m + 0.23304.$$

P r o o f. First we have the explicit expression for $P_0 + P_1 = (-m, m)$. In the proof of Proposition 3.5, we saw that

$$u(Q) = (x(Q)^2 + m^2)^2 - 8mx(Q)^2$$

for $Q \in D_m(\mathbb{Q}) \setminus D_m[2]$. Thus we have

$$u(P_0) = m^4, \quad u(P_1) = 4m^4 - 8m^3, \quad u(P_0 + P_1) = 4m^3 + 8m^3.$$

Hence for $P \in \{P_0, P_1, P_0 + P_1\}$,

$$u(P) \leqslant 4m^4 + 8m^3 = 4m^4\Big(1 + \frac{2}{m}\Big) \leqslant 4m^4\Big(1 + \frac{2}{10}\Big) = \frac{24m^4}{5}.$$

Further, from (19), one can deduce the inequality

$$Z(2^kP) < \Big(1 + \frac{m^2}{(m-1)^2}\Big)^2 \leqslant \Big(1 + \frac{10^2}{9^2}\Big)^2 = \Big(\frac{181}{81}\Big)^2$$

for any P. So for $P \in \{P_0, P_1, P_0 + P_1\}$ we have

$$\begin{aligned}\lambda_\infty(P) &= \frac{1}{8}\log|u(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log|Z(2^kP)| + \frac{1}{12}v_\infty(\Delta)\\ &< \frac{1}{8}\log\Big(4m^4 \times \frac{6}{5}\Big) + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k}\log\Big(\frac{181}{81}\Big)^2 + \frac{1}{12}v_\infty(\Delta)\\ &= \frac{1}{8}\log 4 + \frac{1}{2}\log m + \frac{1}{8}\log\frac{6}{5} + \frac{1}{3}\log\Big(\frac{181}{81}\Big) + \frac{1}{12}v_\infty(\Delta).\end{aligned}$$

For $p = 2$, since $v_2(x(P_0)) > 0$ and $v_2(x(P_1)) = 0$, therefore P_0 and P_{-1} reduce to a nonsingular point and a singular point, respectively. If singular, then the reduction type is IV by Lemma 3.2. Hence,

$$\begin{aligned}\lambda_2(P_0) &= \frac{1}{2}\log\max\{1, |x(P_0)|_2\} + \frac{1}{12}v_2(\Delta) = \frac{1}{12}v_2(\Delta),\\ \lambda_2(P_{-1}) &\leqslant -\frac{1}{3}\log 2 + \frac{1}{12}v_2(\Delta).\end{aligned}$$

For $p \geqslant 3$ and $p \mid m$, we have the bound

$$\lambda_p(P) = -\frac{1}{3}\log p + \frac{1}{12}v_2(\Delta)$$

for any integral point $P \in \{P_0, P_{-1}, P_0 + P_{-1}\}$ and this implies

$$\sum_{p\colon \text{prime}} \lambda_p(P) = -\frac{1}{3}\log m + \frac{1}{12}v_2(\Delta).$$

Similarly, when $p \geqslant 3$ and $p \nmid m$, we have $\lambda_p(P) = \frac{1}{12}v_2(\Delta)$ for any integral point.

Thus,

$$\begin{aligned}\hat{h}(P_0) &< \frac{1}{2}\log m + \frac{1}{8}\log 4 + \frac{1}{8}\log\frac{6}{5} + \frac{1}{3}\log\frac{181}{81} - \frac{1}{3}\log m\\ &< \frac{1}{6}\log m + 0.46409\ldots\end{aligned}$$

and

$$\begin{aligned}\hat{h}(P_{-1}) &< \frac{1}{2}\log m + \frac{1}{8}\log 4 + \frac{1}{8}\log\frac{6}{5} + \frac{1}{3}\log\frac{181}{81} - \frac{1}{3}\log 2 - \frac{1}{3}\log m\\ &< \frac{1}{6}\log m + 0.23304\ldots\end{aligned}$$

□

Now we are ready to prove Theorem 1.4.

P r o o f of Theorem 1.4. Let m be a square-free integer with $m \equiv 1 \pmod 4$. Assume that $m \geqslant 10$. We know that the points P_{-1} and P_0 are independent for all but finitely many m. Since the rank of $D_m(\mathbb{Q})$ is at least 2 for all but finitely many m, by the elementary divisor theory, there exist generators G_1 and G_2 of the free part of $D_m(\mathbb{Q})$ such that $P_0, P_{-1} \in \mathbb{Z}G_1 + \mathbb{Z}G_2$. Let ν be the index of the subgroup $\mathbb{Z}P_0 + \mathbb{Z}P_{-1}$ in $\mathbb{Z}G_1 + \mathbb{Z}G_2$. It is sufficient to show $\nu = 1$. By Siksek's theorem (see [13], Theorem 3.1) we have

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

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

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

and λ is any positive lower bound of $\hat{h}$ for non-torsion points in $D_m(\mathbb{Q})$. Note that $\langle \cdot \rangle$ is the Néron-Tate height pairing defined in (8). Hence by Propositions 3.5 and 3.6, we have

$$\nu \leqslant \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_0)\hat{h}(P_{-1})}}{\lambda} \leqslant f(m), \tag{25}$$

where

$$f(m) := \frac{2}{\sqrt{3}} \frac{\sqrt{(\frac{1}{6}\log m + 0.46409)(\frac{1}{2}\log m + 0.23304)}}{(\frac{1}{6}\log m - 0.230)}.$$

One can see that $f(m)$ is a decreasing function. By calculation we find that $f(m)$ is less than 3 for $m \geqslant 34$. From the proof of Lemmas 2.2, 2.3 and 2.4, one can conclude that P_0, P_{-1}, $P_0 + P_{-1} \notin 2D_m(\mathbb{Q})$ and hence $2 \nmid \nu$ for $m \geqslant 10$. Thus, ν is 1 for $m \geqslant 34$. Finally for $m \leqslant 33$, using Magma function "Generators" (see [3]), we check that $\{P_0, P_{-1}\}$ can be extended to a basis. In principle, if we consider that R is the regulator of the given basis and that R' is the regulator of a set which consists of P_0, P_{-1} and an appropriate point of the given basis then we check the ratio R'/R which is less than 4 and nonzero. This completes the proof of Theorem 1.4. □

4. Concluding remark

Consider the elliptic curve $E_{m,n}\colon\ y^2 = x^3 - m^2x + n^2$. In [8], Fujita and Nara proved two results. First they took the curve $E_{1,n}$ and proved that for $n \geqslant 2$ the points $(0,n)$, $(-1,n)$ can be extended to a basis for $E_{1,n}(\mathbb{Q})$. Second, they proved that for the curve $E_{m,1}$ the points $(0,1)$, $(-m,1)$, $(-1,m)$ can be extended to a basis for $E_{m,1}(\mathbb{Q})$. Being inspired with their work, we studied similar properties for the curve $D_m(\mathbb{Q})$. Precisely we proved that the points $(-m,m),(0,m)$ can be extended to a basis for $D_m(\mathbb{Q})$ under some conditions on m, which are stated in Theorem 1.4.

Now if we consider the more general case $E_{m,n}\colon\ y^2 = x^3 - m^2 + n^2$, where m and n are not necessarily coprime and $m \neq n$, we can easily see that the points $P_0 = (0,n)$ and $P_{\pm 1} = (\pm m, n)$ are integral points on $E_{m,n}$. For the curve $E_{m,n}$ we cannot determine the rank of $E_{m,n}(\mathbb{Q}(m,n))$ like we did for the curve $y^2 = x^3 - m^2x + m^2$ in Theorem 1.1. Further, if $m \equiv n \equiv 0 \pmod 2$ then various reduction types of $E_{m,n}$ are possible. But if $m \equiv n \equiv 0 \pmod 3$, then again it is not possible to decide the reduction type of $E_{m,n}$ which essential to estimate the canonical local height. Thus, it seems a new technique is required to study the Mordell-Weil basis for this general case.

Acknowledgment. The authors sincerely thank to Prof. Y. Fujita for his useful suggestions during the preparation of this manuscript. Also, the authors thank to the referee for many valuable suggestions and comments which improved the readability of this paper. This work was started when the second author visited the Institute of Mathematics & Applications Bhubaneswar. He thanks the people of this institute for the hospitality and support. The second author also thanks to the IMSc Chennai for providing research facilities to pursue his research work.

References

[1] *A. Antoniewicz*: On a family of elliptic curves. Univ. Iagell. Acta Math. *43* (2005), 21–32. zbl MR
[2] *E. Brown, B. T. Myers*: Elliptic curves from Mordell to Diophantus and back. Am. Math. Mon. *109* (2002), 639–649. zbl MR doi
[3] *J. Cannon, W. Bosma, C. Fieker, A. Steel* (eds.): Handbook of Magma Functions. Department of Mathematics, University of Sydney, Sydney, 2006.
[4] *E. V. Eikenberg*: Rational Points on Some Families of Elliptic Curves: Ph.D. Thesis. University of Maryland, College Park, 2004. MR
[5] *Y. Fujita*: Generators for the elliptic curve $y^2 = x^3 - nx$ of rank at least three. J. Number Theory *133* (2013), 1645–1662. zbl MR doi
[6] *Y. Fujita*: Generators for congruent number curves of ranks at least two and three. J. Ramanujan Math. Soc. *29* (2014), 307–319. zbl MR
[7] *Y. Fujita, T. Nara*: On the Mordell-Weil group of the elliptic curve $y^2 = x^3 + n$. J. Number Theory *132* (2012), 448–466. zbl MR doi

[8] *Y. Fujita, T. Nara*: The Mordell-Weil bases for the elliptic curve of the form $y^2 = x^3 - m^2x + n^2$. Publ. Math. *92* (2018), 79–99. zbl MR doi
[9] *Y. Fujita, N. Terai*: Generators for the elliptic curve $y^2 = x^3 - nx$. J. Théor. Nombres Bordx. *23* (2011), 403–416. zbl MR doi
[10] *A. Juyal, S. D. Kumar*: On the family of elliptic curves $y^2 = x^3 - m^2x + p^2$. Proc. Indian Acad. Sci., Math. Sci. *128* (2018), Article ID 54, 11 pages. zbl MR doi
[11] *K. Oguiso, T. Shioda*: The Mordell-Weil lattice of a rational elliptic surface. Comment. Math. Univ. St. Pauli *40* (1991), 83–99. zbl MR
[12] *T. Shioda*: On the Mordell-Weil lattices. Comment. Math. Univ. St. Pauli *39* (1990), 211–240. zbl MR
[13] *S. Siksek*: Infinite descent on elliptic curves. Rocky Mt. J. Math. *25* (1995), 1501–1538. zbl MR doi
[14] *J. H. Silverman*: Computing heights on elliptic curves. Math. Comput. *51* (1988), 339–358. zbl MR doi
[15] *J. H. Silverman*: Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 151. Springer, New York, 1994. zbl MR doi
[16] *J. H. Silverman*: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Springer, New York, 2009. zbl MR doi
[17] *P. Tadić*: On the family of elliptic curves $Y^2 = X^3 - T^2X + 1$. Glas. Mat., III. Ser. *47* (2012), 81–93. zbl MR doi
[18] *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. zbl MR

Authors' addresses: Sudhansu Sekhar Rout, Institute of Mathematics & Applications, Andharua, Bhubaneswar 751029, India, e-mail: lbs.sudhansu@gmail.com, sudhansu@iomaorissa.ac.in; Abhishek Juyal (corresponding author), Institute of Mathematical Sciences (HBNI), CIT Campus, Taramani, Chennai 600 113, India, e-mail: abhinfo1402@gmail.com.