LOWER BOUNDS OF THE CANONICAL HEIGHT ON QUADRATIC TWISTS OF ELLIPTIC CURVES

TADAHISA NARA

Abstract. We compute a lower bound of the canonical height on quadratic twists of certain elliptic curves. Also we show a simple method for constructing families of quadratic twists with an explicit rational point. Using the above lower bound, we show that the explicit rational point is primitive as an element of the Mordell–Weil group.

1. Introduction

It is known that for every elliptic curve, there exists a positive lower bound of the canonical heights of non-torsion rational points ([7]). There is also an algorithm which computes a lower bound for a given elliptic curve ([3]).

In the paper [4, Proposition 8.3], Duquesne gave an explicit lower bound of the canonical heights of raional points on a certain family of elliptic curves. The family consists of quartic twists of the elliptic curve $y^2 = x^3 - x$. Similarly Fujita and the auther gave an explicit lower bound on a family consisting of sextic twists of the elliptic curve $y^2 = x^3 + 1$ ([5]). Both results are used to show that some explicit points can always be in a system of generators of the Mordell–Weil groups.

In this paper we give an explicit lower bound for a family consisting of quadratic twists of an elliptic curve. There is already a non-explicit bound ([8, Exercise 8.16]) given by a different method from ours (see Remark 1.2). Making the bound explicit enables us to study explicitly the behavior of a certain family of the quadratic twists of a given elliptic curve. For example, we can proove Theorem 1.3 below.

Our lower bound is computed by using the decomposition of the canonical height into the local heights and they are computed by the combination of Cohen's algorithm ([2, Algorithm 7.5.7]) and Silverman's algorithm ([6, Theorem 5.2]). In [4] and [5], by the simplicity of the forms of the Weierstrass equations, the estimates of the non-archimedean part of the local height were given by ad hoc arguments. However, in our case more systematic argument is required. The key is an identity between division polynomials of elliptic curves (Lemma 4.12).

Our main results are as follows.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve defined by $y^2 = x^3 + a_2x^2 + a_4x + a_6$ $(a_2, a_4, a_6 \in \mathbb{Z})$ with the discriminant Δ. Let D be a square-free integer and $E_D/\mathbb{Q}$ the elliptic curve $y^2 = x^3 + a_2Dx^2 + a_4D^2x + a_6D^3$. Assume that Δ is 6th-power-free. Then for $P \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$,*

$$\hat{h}(P) > \frac{1}{4}\log|D| + \frac{1}{16}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{4}\log\left|\frac{\omega}{2\pi}\right| - \frac{7}{16}\sum_{p|\Delta, p\neq 2}\log p - \frac{5}{12}\log 2,$$

Key words and phrases. elliptic curve, Mordell–Weil group, canonical height, quadratic twist.

where ω_1 *and* ω_2 *are periods of* E *such that* $\omega_1 > 0$, $\mathrm{Im}(\omega_2) > 0$ *and* $\mathrm{Re}(\omega_2/\omega_1) = 0$ *or* $-1/2$, $q = \exp(2\pi i\omega_2/\omega_1)$ *and*

$$\omega = \begin{cases} \omega_1 & (D > 0) \\ \mathrm{Im}(\omega_2) & (D < 0, \Delta > 0) \\ 2\mathrm{Im}(\omega_2) & (D < 0, \Delta < 0) \end{cases}.$$

Remark 1.2. We have $\hat{h}(P) > \frac{1}{4}\log|D| + O(1)$ by [8, Exercise 8.16 (c)]. The proof does not use the local height functions. Note that our $\hat{h}$ is twice of that in [8], [2] and [6].

E_D in Theorem 1.1 is called the quadratic twist of E by D, which is isomorphic over $\mathbb{Q}$ to the curve defined by $Dy^2 = x^3 + a_2x^2 + a_4x + a_6$.

Using Theorem 1.1, we can also show the following theorem.

Theorem 1.3. *Let* $t \in \mathbb{Z}$, $D(t) = t^6+4t^4+30t^3+5t^2+54t+245$, E_D *the elliptic curve* $y^2 = x^3 + 2D(t)x^2 + 163D(t)^2x + 2205D(t)^3$ *and* P *the point* $(D(t)(t^4 + 2t^2 + 12t), D(t)^2(t^3 + t + 3))$ *on* E_D. *We assume that* $D(t)$ *is square-free. Then* P *is a primitive point if* $|t| \geq 2216$. *In particular* $E_D(\mathbb{Q}) \simeq \langle P\rangle$ *if* $\operatorname{rank} E_D(\mathbb{Q}) = 1$.

Remark 1.4. This family of quadratic twists is an example given by the method described in Section 3. For many other families given by the method, we can show similar results.

The organization of this paper is as follows. In Section 2 we review the notions of the canonical height and the local height function. In Section 3 we introduce a method of constructing families of quadratic twists. In Section 4 we compute the local height functions by using Cohen's algorithm and Silverman's algorithm to prove Theorem 1.1. In Section 5 we prove Theorem 1.3, which is a consequence for an example given by the method in Section 3.

2. Preliminaries

Let E be an elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Throughout this paper b_2, b_4, b_6 and c_4, c_6 are the usual quantities defined in [8, III.1]. Further by Δ, we denote the discriminants of E. If we have to specify the elliptic curve, we may use the notation such as Δ_E.

First, we define the notion of the canonical height of elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve and $P = (x, y) \in E(\mathbb{Q})$ with $x = n/d$ and $\gcd(n, d) = 1$. Then the naïve height $h(P)$ is defined by $\max\{\log|n|, \log|d|\}$ and the canonical height $\hat{h}(P)$ is defined by

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

It is known that the canonical height is decomposed to the sum of functions, called the local height functions. We use the decomposition for computations of the canonical heights. The local height function λ_v is defined by the following theorem.

Theorem 2.1. (*Néron, Tate,* [6, p. 341]) *Let* K *be a number field,* v *a place and* K_v *its completion with respect to the absolute value* $|\cdot|_v$. *Let* E/K *be the elliptic curve* $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. *Then there exists a unique function* $\lambda_v : E(K_v) \setminus O \to \mathbb{R}$ *which has the following three properties.*

(1) *For all* $P \in E(K_v)$ *with* $2P \neq O$,

$$\lambda_v(2P) = 4\lambda_v(P) - 2\log|2y(P) + a_1x(P) + a_3|_v.$$

(2) *The limit* $\lim_{\substack{P\to O\\ v\text{-adic}}}(\lambda_v(P) - \log|x(P)|_v)$ *exists.*

(3) λ_v *is bounded on any* v*-adic open subset of* $E(K_v)$ *disjoint from* O.

Remark 2.2. There is an alternative definition of the local height function, which is given by adding $\frac{1}{2}\log|\Delta|$ on the right hand side of (1) ([1, Chapter VI, Theorem 1.1]). This alternative local height function is independent of the Weierstrass equation. With our definition, the local height function depends on the Weierstrass equation, but the function does not change by the substitution $x \mapsto x+r$ (see [5, Lemma 2.11]), which corresponds to the shift of the Weierstrass model in the direction of x-axis.

The definition of the local height function in Cohen's algorithm ([2, Algorithm 7.5.7]), which we shall use later in this paper, agrees with ours except for the multiplication by 1/2.

Now if $K = \mathbb{Q}$ we have the decomposition

$$\hat{h}(P) = \sum_{p:\text{prime},\infty} \lambda_p(P). \tag{2.3}$$

3. Families of quadratic twists

In this section we describe a method to construct families of quadratic twists of elliptic curves with an explicit point.

Let $f \in \mathbb{Z}[t]$ be a monic irreducible cubic polynomial (therefore with no multiple roots), $F \in \mathbb{Z}[t]$ a polynomial such that $F' = mf$ for some $m \in \mathbb{Z}$ and α a root of f. The minimal polynomial of $F(\alpha)$ over $\mathbb{Q}$ is a cubic polynomial, which is denoted by f_1. Then $f_1 \circ F(t)$ has the factor $f(t)^2$, since $f_1 \circ F(\alpha) = 0$ and $\dfrac{d(f_1 \circ F)}{dt}(\alpha) = f_1'(F(\alpha))F'(\alpha) = 0$. Therefore, there exists a polynomial $D(t)$ such that $D(t)f(t)^2 = f_1(F(t))$.

For example, if

$$f = t^3 + t + 3, \quad F = t^4 + 2t^2 + 12t,$$

we have

$$f_1(x) = x^3 + 2x^2 + 163x + 2205, \quad D(t) = t^6 + 4\,t^4 + 30\,t^3 + 5\,t^2 + 54\,t + 245.$$

So we have the quadratic twist $D(t)y^2 = f_1(x)$ of the elliptic curve $y^2 = f_1(x)$, and it has the obvious rational point $(F(t), f(t))$.

If h is a polynomial, we denote its discriminant by $\mathrm{disc}(h)$.

Lemma 3.1. *Let* $A, B \in \mathbb{Z}$, $f = t^3 + At + B$ *and* $F = t^4 + 2At^2 + 4Bt$. *Then the polynomials* f_1 *and* D *as above are as follows.*

$$f_1 = t^3 + 2A^2t^2 + A(A^3 + 18B^2)t + B^2(2A^3 + 27B^2),$$
$$D = t^6 + 4At^4 + 10Bt^3 + 5A^2t^2 + 18ABt + 2A^3 + 27B^2.$$

In particular, $\mathrm{disc}(f_1) = B^2\,\mathrm{disc}(f)^3$.

Proof. If we write $f(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)$, then

$$f_1(t) = (t - F(\alpha_1))(t - F(\alpha_2))(t - F(\alpha_3)).$$

Since

$$\begin{aligned}
&F(\alpha_1) + F(\alpha_2) + F(\alpha_3),\\
&F(\alpha_1)F(\alpha_2) + F(\alpha_2)F(\alpha_3) + F(\alpha_3)F(\alpha_1),\\
&F(\alpha_1)F(\alpha_2)F(\alpha_3)
\end{aligned}$$

are all symmetric polynomials of $\alpha_1, \alpha_2, \alpha_3$, they are polynomials of $\alpha_1+\alpha_2+\alpha_3$ $(=0)$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1$ $(= A)$ and $\alpha_1\alpha_2\alpha_3$ $(= -B)$. It is easy to verify that

$$\begin{aligned}
&F(\alpha_1) + F(\alpha_2) + F(\alpha_3) = -2A^2,\\
&F(\alpha_1)F(\alpha_2) + F(\alpha_2)F(\alpha_3) + F(\alpha_3)F(\alpha_1) = A(A^3 + 18B^2),\\
&F(\alpha_1)F(\alpha_2)F(\alpha_3) = -B^2(2A^3 + 27B^2).
\end{aligned}$$

□

Remark 3.2. Let E' be the elliptic curve $y^2 = f_1(x)$. Then

$$\Delta_{E'} = 16\,\mathrm{disc}(f_1) = 16B^2\,\mathrm{disc}(f)^3 = 16B^2(-4A^3 - 27B^2)^3.$$

So for example, if B is odd, $\gcd(A, B) = 1$ and $\mathrm{disc}(f)$ is square-free, then Theorem 1.1 is applicable to $Dy^2 = f_1(x)$.

4. Uniform lower bound on quadratic twists

In this section we compute a lower bound of the canonical height on quadratic twists of elliptic curves. We use the decomposition (2.3).

Consider an elliptic curve of the form

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

where $a_2, a_4, a_6 \in \mathbb{Z}$ (the point is that $a_1 = a_3 = 0$). For a square-free integer D we put

$$E_D : y^2 = x^3 + a_2Dx^2 + a_4D^2x + a_6D^3. \tag{4.2}$$

Throughout this section, by ω_1 and ω_2 we denote the periods of E such that $\omega_1 > 0$, $\mathrm{Im}(\omega_2) > 0$ and $\mathrm{Re}(\omega_2/\omega_1) = 0$ or $-1/2$ and put $q = \exp(2\pi i\omega_2/\omega_1)$. The periods, discriminant and the usual quantities of E_D are denoted by $\omega_{1,D}$, Δ_D, $a_{i,D}$, $b_{i,D}$ and $c_{i,D}$.

Straightforward computations using [2, Algorithm 7.4.7] show the following lemma.

Lemma 4.3. *We have $\omega_{1,D} = \omega|D|^{-1/2}$, where*

$$\omega = \begin{cases} \omega_1 & (D > 0) \\ \mathrm{Im}(\omega_2) & (D < 0, \Delta > 0) \\ 2\mathrm{Im}(\omega_2) & (D < 0, \Delta < 0) \end{cases}.$$

We first consider the archimedean part, that is λ_∞. Points in $E_D(\mathbb{Q})$ can always be made into the form $(\alpha/\delta^2, \beta/\delta^3)$, where $\alpha, \beta, \delta \in \mathbb{Z}$, $\delta > 0$ and $\gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1$. So in this sectition we always assume the above condition on α, β and δ.

Lemma 4.4. *Let $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$. Then*

$$\begin{aligned}\lambda_\infty(Q) \geq \frac{1}{4}\log|D| + \frac{1}{16}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{4}\log\left|\frac{\omega}{2\pi}\right| \\ - \frac{3}{2}\log\delta + \frac{1}{2}\log|\beta| + \frac{1}{16}\log|\Delta|.\end{aligned} \tag{4.5}$$

Proof. By [2, Algorithm 7.5.7] and the trivial bound $|\theta| \leq 1/(1-|q|)$,

$$\begin{aligned}\lambda_\infty(Q) &= \frac{1}{16}\log\left|\frac{\Delta_D}{q}\right| + \frac{1}{4}\log\left|\left(\frac{\beta}{\delta^3}\right)^2\frac{\omega_{1,D}}{2\pi}\right| - \frac{1}{2}\log|\theta| \\ &= \frac{1}{16}\log\left|\frac{\Delta}{q}\right| + \frac{6}{16}\log|D| + \frac{1}{4}\log\left|\frac{\omega}{2\pi}\right| + \frac{1}{4}\log\left|\frac{\beta^2}{\delta^6}\right| - \frac{1}{4}\log|D|^{\frac{1}{2}} - \frac{1}{2}\log|\theta| \\ &\geq \frac{1}{4}\log|D| + \frac{1}{16}\log\left|\frac{\Delta}{q}\right| + \frac{1}{4}\log\left|\frac{\omega}{2\pi}\right| + \frac{1}{2}\log\left|\frac{\beta}{\delta^3}\right| - \frac{1}{2}\log\frac{1}{1-|q|} \\ &= \frac{1}{4}\log|D| + \frac{1}{16}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{4}\log\left|\frac{\omega}{2\pi}\right| - \frac{3}{2}\log\delta + \frac{1}{2}\log|\beta| + \frac{1}{16}\log|\Delta|.\end{aligned}$$

□

Remark 4.6. Note that we can not use [2, Algorithm 7.5.7] for 2-torsion points.

To prove Theorem 1.1, we shall consider a lower bound of the sum of the last two terms (i.e. $\frac{1}{2}\log|\beta| + \frac{1}{16}\log|\Delta|$) and the non-archimedean part. To compute the non-archimedean part of the canonical height, we use Silverman's algorithm ([6, Theorem 5.2]).

Definition 4.7. For an elliptic curve defined by $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ we define polynomials of x, y as follows.

$$\begin{aligned}\psi_0(x,y) &= 3x^2 + 2a_2x + a_4 - a_1y, \\ \psi_2(x,y) &= 2y + a_1x + a_3, \\ \psi_{2a}(x,y) &= 4x^3 + 2b_2x^2 + b_4x + b_6, \\ \psi_3(x,y) &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8.\end{aligned}$$

Apart from ψ_0, they are known as the division polynomials of elliptic curves. For a point $Q = (x_0, y_0)$, we put $\psi_i(Q) = \psi(x_0, y_0)$. Note that if $Q \in E$, $\psi_2(Q)^2 = \psi_{2a}(Q)$.

Before computing the division polynomials of E_D, we compute the usual quantities of the Weierstrass equation of E in (4.1) as follows. Since $a_1 = a_3 = 0$ in our case, we have

$$\Delta = -16\left(27\,a_6^2 - 18\,a_2\,a_4\,a_6 + 4\,a_2^3\,a_6 + 4\,a_4^3 - a_2^2\,a_4^2\right), \tag{4.8}$$

$$c_4 = -16\left(3\,a_4 - a_2^2\right), \tag{4.9}$$

$$c_6 = -32\left(27\,a_6 - 9\,a_2\,a_4 + 2\,a_2^3\right). \tag{4.10}$$

Note that

$$\Delta = 1728^{-1}(c_4^3 - c_6^2) = 2^{-6}3^{-3}(c_4^3 - c_6^2). \tag{4.11}$$

The usual quantities of the Weierstrass equation of E_D are as follows.

$$a_{1,D} = a_{3,D} = 0, a_{2,D} = a_2 D,\ a_{4,D} = a_4 D^2,\ a_{6,D} = a_6 D^3,$$
$$b_{2,D} = 4a_2 D,\ b_{4,D} = 2a_4 D^2,\ b_{6,D} = 4a_6 D^3,\ b_{8,D} = (4a_2a_6 - a_4^2)D^4,$$
$$c_{4,D} = 16(a_2^2 - 3a_4)D^2,\ c_{6,D} = -32\,(27\,a_6 - 9\,a_2\,a_4 + 2\,a_2^3)D^3,\ \Delta_D = \Delta D^6.$$

Using this, we have the division polynomials of E_D as follows.

$$\begin{aligned}
\psi_{0,D}(x,y) &= 3x^2 + 2a_2Dx + a_4D^2,\\
\psi_{2,D}(x,y) &= 2y,\\
\psi_{2a,D}(x,y) &= 4x^3 + 2b_{2,D}x^2 + b_{4,D}x + b_{6,D}\\
&= 4(x^3 + a_2Dx^2 + a_4D^2x + a_6D^3),\\
\psi_{3,D}(x,y) &= 3x^4 + b_{2,D}x^3 + 3b_{4,D}x^2 + 3b_{6,D}x + b_{8,D}\\
&= 3x^4 + 4a_2Dx^3 + 6a_4D^2x^2 + 12a_6D^3x + (4a_2a_6 - a_4^2)D^4.
\end{aligned}$$

For E_D, $Q(\in E_D)$ and p we put

$$\begin{aligned}
A &= v_p(\psi_{0,D}(Q)),\\
B &= v_p(\psi_{2,D}(Q)) = v_p(\psi_{2a,D}(Q))/2,\\
C &= v_p(\psi_{3,D}(Q)).
\end{aligned}$$

Roughly speaking, by comparing these values for Q, the output of Silverman's algorithm becomes the value of $\lambda_p(Q)$.

Even though the following lemma follows from direct computations, it plays a key role in the subsequent computations.

Lemma 4.12. *Let*

$$\begin{aligned}
k_D(x,y) &:= 3x^2 + 2a_2Dx + (4a_4 - a_2^2)D^2,\\
l_D(x,y) &:= 9x^3 + 9a_2Dx^2 + (21a_4 - 4a_2^2)D^2x + (27a_6 - 2a_2a_4)D^3.
\end{aligned}$$

Then

$$-16k_D \cdot \psi_{3,D} + 4l_D \cdot \psi_{2a,D} = -\Delta D^6. \tag{4.13}$$

In the following consideration, we fix a square-free integer D and a rational point $Q = (x_0, y_0) = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$.

Definition 4.14. Let Ω be the set of all the rational primes. We put

$$\begin{aligned}
&\Omega^+ = \{p \in \Omega; p|\delta\},\ \Omega^- = \{p \in \Omega; p\not|\delta\},\\
&\Omega_1 = \{p \in \Omega^- \setminus \{2,3\}; p\not|\Delta, p\not|D\},\ \Omega_2 = \{p \in \Omega^- \setminus \{2,3\}; p\not|\Delta, p|D\},\\
&\Omega_3 = \{p \in \Omega^- \setminus \{2,3\}; p|\Delta, p\not|D\},\ \Omega_4 = \{p \in \Omega^- \setminus \{2,3\}; p|\Delta, p|D\}.
\end{aligned}$$

If $p \notin \Omega^+$, then $v_p(x_0) \geq 0$ and so

$$v_p(k_D(x_0,y_0)) \geq 0, \quad v_p(l_D(x_0,y_0)) \geq 0, \quad v_p(\psi_{i,D}(x_0,y_0)) \geq 0.$$

To ease the notations, we put

$$\begin{aligned} k_D &= k_D(Q) = k_D(\alpha/\delta^2, \beta/\delta^3), \\ l_D &= l_D(Q) = l_D(\alpha/\delta^2, \beta/\delta^3), \\ \psi_{i,D} &= \psi_{i,D}(Q) = \psi_{i,D}(\alpha/\delta^2, \beta/\delta^3). \end{aligned}$$

Definition 4.15. (1) For a set of primes S and an integer m, we define $m_S = \prod_{p\in S} p^{v_p(m)}$.

(2) We put $\Lambda = \lambda_p(Q)/\log p$ and $N = v_p(\Delta)$ (here we are considering $\Delta = \Delta_E$ and not Δ_D).

Now we compute $\lambda_p(Q)$ using [6, Theorem 5.2] in Lemmas 4.16–4.22. Recall in our definition the value of $\hat{h}$ is twice of that in [6], and so is λ_p. We assume that Δ is 6th-power-free. So (4.2) is a minimal Weierstrass equation at every prime p by [8, VII, Remark 1.1].

Lemma 4.16. *If $p \in \Omega^+$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then $\sum_{p\in\Omega^+} \lambda_p(Q) = 2\log\delta$.*

Proof. Since $p|\delta$, $p\not|\alpha$ and $p\not|\beta$. So the reduction of Q modulo p is nonsingular. Therefore

$$\sum_{p\in\Omega^+} \lambda_p(Q) = \sum_{p\in\Omega^+} \max\{0, -v_p(\alpha/\delta^2)\}\log p = 2\log\delta.$$

□

Lemma 4.17. *If $p \in \Omega_1$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then $\lambda_p(Q) = 0$.*

Proof. Since, $p\not|\Delta_D$, the image of Q under the reduction modulo p is nonsingular. Therefore $\lambda_p(Q) = \max\{0, -v_p(\alpha/\delta^2)\}\log p = 0$. □

Lemma 4.18. *If $p \in \Omega_2$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then $\lambda_p(Q) \geq -\log p$ and $v_p(\beta) \geq 2$. In particular $\sum_{p\in\Omega_2} \lambda_p(Q) + \frac{1}{2}\log|\beta_{\Omega_2}| \geq 0$.*

Proof. To consider a lower bound of λ_p, we may assume $p|\beta$ (so $p\not|\delta$), since otherwise $\lambda_p(Q) = 0$. Recall $\psi_{2,D}(Q)^2 = \psi_{2a,D}(Q)$. Since $p|\psi_{2,D}(Q)$, $p|\psi_{2a,D}(Q)$. So p has to divide α. Then $v_p(\psi_{2a,D}) \geq 3$. On the other hand $v_p(\psi_{2a,D})$ is even, and so $v_p(\psi_{2a,D}) \geq 4$ and $B = v_p(\beta) \geq 2$. Clearly $v_p(k_D) \geq 2$ and $v_p(l_D) \geq 3$. So we have $v_p(\psi_{3,D}) \leq 4$ by (4.13). Then since $3B > C$, $\Lambda = -C/4 \geq -1$. (Note that $p|c_{4,D}$ and so the additive reduction occurs).

□

Lemma 4.19. *If $p \in \Omega_3$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_p(Q) + \frac{1}{2}\log|\beta_{\{p\}}| + \frac{1}{16}\log|\Delta_{\{p\}}| \geq -\frac{1}{12}\log|\Delta_{\{p\}}|.$$

Proof. Note that

$$\lambda_p(Q) + \frac{1}{2}\log|\beta_{\{p\}}| + \frac{1}{16}\log|\Delta_{\{p\}}| = \left(\Lambda + \frac{B}{2} + \frac{N}{16}\right)\log p.$$

At first, we assume that $p|c_4$. Then E_D has the additive reduction at p. By (4.11), $N = v_p(\Delta) = 2, 3$ or 4 since Δ is 6th-power-free. By (4.13) $\min\{v_p(\psi_{2a,D}), v_p(\psi_{3,D})\} \le v_p(\Delta)$. So we rewrite this inequality as $\min\{2B, C\} \le N$. If $(3B >)2B > C$, then

$$\Lambda = -\frac{C}{4}, \ \frac{B}{2} > \frac{C}{4}, \ \frac{N}{16} \ge \frac{C}{16}.$$

So

$$\Lambda + \frac{B}{2} + \frac{N}{16} \ge \frac{C}{16} \ge 0.$$

If $3B > C \ge 2B$ (therefore $3B \ge C + 1$), then

$$\Lambda = -\frac{C}{4} \ge -\frac{3B-1}{4}, \ \frac{N}{16} \ge \frac{2B}{16}.$$

So

$$\Lambda + \frac{B}{2} + \frac{N}{16} \ge -\frac{B}{8} + \frac{1}{4} \ge -\frac{2}{8} + \frac{1}{4} = 0.$$

If $C \ge 3B(> 2B)$, then

$$\Lambda = -\frac{2B}{3}, \ \frac{N}{16} \ge \frac{2B}{16}.$$

So

$$\Lambda + \frac{B}{2} + \frac{N}{16} \ge -\frac{B}{24} \ge -\frac{2}{24} = -\frac{1}{12}.$$

Next we assume that $p \not| c_4$. Then the multiplicative reduction occurs at p. Then $\Lambda = -\frac{n(N-n)}{N}$, where $n = \min\{B, N/2\}$. Since $N \le 5$, $-\frac{n(N-n)}{N} \ge -6/5$. So if $B \ge 3$, clearly $\Lambda + B/2 \ge 0$. For the cases $B = 1, 2$, by case-by-case argument, we can verify that $\Lambda + B/2 + N/16 \ge 0$ for all the case of $N = 1, 2, 3, 4, 5$. □

Lemma 4.20. *If $p \in \Omega_4$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_p(Q) + \frac{1}{2}\log|\beta_{\{p\}}| + \frac{1}{16}\log|\Delta_{\{p\}}| \ge -\frac{7}{16}\log p.$$

Proof. Since $p|c_{4,D}$, the additive reduction occurs at p. We may assume $p|\beta$ as in Lemma 4.18, and so $p|\alpha$. By (4.13), we have $\min\{C + 2, 2B + 3\} \le N + 6$.

If $3B > C$ (therefore $3B \ge C + 1$) and $2B + 3 > C + 2$ (therefore $2B \ge C$), then

$$\Lambda = -\frac{C}{4}, \ \frac{B}{2} \ge \frac{C}{4}, \ \frac{N}{16} > \frac{C-4}{16}.$$

So

$$\Lambda + \frac{B}{2} + \frac{N}{16} \ge \frac{C-4}{16} \ge -\frac{1}{4}.$$

If $3B > C$ (therefore $3B \ge C + 1$) and $C + 2 \ge 2B + 3$, then

$$\Lambda = -\frac{C}{4} \ge -\frac{3B-1}{4}, \ \frac{N}{16} \ge \frac{2B-3}{16}.$$

So

$$\Lambda + \frac{B}{2} + \frac{N}{16} \ge -\frac{B}{8} + \frac{1}{16} \ge -\frac{4}{8} + \frac{1}{16} = -\frac{7}{16}.$$

If $C \geq 3B$, then $C + 2 \geq 2B + 3$. So

$$\Lambda = -\frac{2B}{3}, \ \frac{N}{16} \geq \frac{2B-3}{16}.$$

Therefore

$$\Lambda + \frac{B}{2} + \frac{N}{16} \geq -\frac{B}{24} - \frac{3}{16} \geq -\frac{4}{24} - \frac{3}{16} = -\frac{17}{48}.$$

□

Lemma 4.21. *If $p = 2$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_2(Q) + \frac{1}{2}\log|\beta_{\{2\}}| \geq -\frac{2}{3}\log 2.$$

In particular,

$$\lambda_2(Q) + \frac{1}{2}\log|\beta_{\{2\}}| + \frac{1}{16}\log|\Delta_{\{2\}}| \geq -\frac{5}{12}\log 2.$$

Proof. By (4.9) and (4.10), we can write $v_2(c_4^3) = 3k$ ($k \geq 4$) and $v_2(c_6^2) = 2l$ ($l \geq 5$). So by (4.11), $v_2(\Delta) = 4$ since Δ is 6th-power-free, since $\Delta \in \mathbb{Z}$. Note that $2|c_{4,D}$ and so the additive reduction occurs.

If $2 \nmid \beta$, $B = 1$. Then $\Lambda = -2/3$ or $-1/2$. Therefore, $\Lambda \geq -2/3$.

If $2|\beta$ and $2|D$, then we may assume $2|\alpha$ to consider a lower bound of λ_2, for otherwise $A = 0$. By the same argument as that in Lemma 4.18, we have $v_2(\psi_{2a,D}) \geq 6$ and $v_2(\beta) \geq 2$. Similarly by the identity (4.13), we have $v_2(\psi_{3,D}) \leq 4$ and so $\Lambda \geq -1$.

If $2|\beta$ and $2 \nmid D$, then we may assume $v_2(\psi_{3,D}) \geq 1$, for otherwise $C = 0$ and $\Lambda = 0$. By the identity (4.13), we have $v_2(\psi_{2a,D}) \leq 2$ (actually $v_2(\psi_{2a,D}) = 2$). Then $\Lambda = -2/3$ or $-1/2$. Therefore, $\Lambda \geq -2/3$. □

Lemma 4.22. *If $p = 3$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_3(Q) + \frac{1}{2}\log|\beta_{\{3\}}| + \frac{1}{16}\log|\Delta_{\{3\}}| \geq -\frac{7}{16}\log 3.$$

Proof. We may assume $3|\Delta_D$. If $3 \nmid \Delta$ and $3|D$, then by the same argument as that in Lemma 4.18, $\lambda_3(Q) + \frac{1}{2}\log|\beta_{\{3\}}| \geq 0$. If $3|\Delta$ and $3 \nmid D$, then in the case of $3|c_4$ we cannot deny the possibility of $N = 5$, but anyway $B \leq 2$. So by the same argument as that in Lemma 4.19,

$$\lambda_3(Q) + \frac{1}{2}\log|\beta_{\{3\}}| + \frac{1}{16}\log|\Delta_{\{3\}}| \geq -\frac{1}{12}\log 3.$$

If $3|\Delta$ and $3|D$, then by the same argument as that in Lemma 4.20,

$$\lambda_3(Q) + \frac{1}{2}\log|\beta_{\{3\}}| + \frac{1}{16}\log|\Delta_{\{3\}}| \geq -\frac{7}{16}\log 3.$$

□

We now finish the proof of Theorem 1.1.

proof of Theorem 1.1. By (2.3) and Lemma 4.4

$$\hat{h}(P) \geq \frac{1}{4}\log|D| + \frac{1}{16}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{4}\log|\frac{\omega_1}{2\pi}|$$
$$-\frac{3}{2}\log\delta + \frac{1}{2}\log|\beta| + \frac{1}{16}\log|\Delta| + \sum_{p:\text{prime}} \lambda_p(Q).$$

If $2, 3 \notin \Omega^+$, then

$$\frac{1}{2}\log|\beta| + \frac{1}{16}\log|\Delta| + \sum_{p:\text{prime}} \lambda_p(Q)$$
$$= \sum_{S=\Omega^+,\Omega_1,\Omega_2,\Omega_3,\Omega_4,\{2\},\{3\}} \left(\frac{1}{2}\log|\beta_S| + \frac{1}{16}\log|\Delta_S| + \sum_{p\in S}\lambda_p(Q)\right)$$

and a lower bound of the right hand side is given by Lemmas 4.16-4.22, that is $2\log\delta - \frac{7}{16}\sum_{p|\Delta, p\neq 2}\log p - \frac{5}{12}\log 2$. Even if 2 or 3 $\in \Omega^+$, the same bound is valid, since the lower bounds given in Lemmas 4.21 and 4.22 are negative. □

Corollary 4.23. *Let E_D be the elliptic curve $y^2 = x^3 + 2Dx^2 + 163D^2x + 2205D^3$ $(D > 0)$ and $Q \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$. Then*

$$\hat{h}(Q) > \frac{1}{4}\log D - 3.5472. \tag{4.24}$$

Proof. Let E be the elliptic curve defined by $y^2 = x^3 + 2x^2 + 163x + 2205$. Then we have $\Delta = -2^4 3^2 13^3 19^3$, $\omega_1 = 1.04995090\cdots$, $q = -0.10978666\cdots$ by the following commands in PARI/GP v.2.3.4 and the corollary follows.

```
E=ellinit([0,2,0,163,2205]);
factor(E.disc)
E.omega[1]
exp(2*Pi*I*E.omega[2]/E.omega[1])
```

□

5. An example

In this section we consider a family of quadratic twists of an elliptic curve. The family in the following lemma is constructed by the method described in Section 3.

Lemma 5.1. *Let $t \in \mathbb{Z}$, $D(t) = t^6 + 4t^4 + 30t^3 + 5t^2 + 54t + 245$, E_D the elliptic curve defined by $y^2 = x^3 + 2D(t)x^2 + 163D(t)^2x + 2205D(t)^3$ and P the point $(D(t)(t^4 + 2t^2 + 12t),\ D(t)^2(t^3 + t + 3))$ on E_D. Then*

$$\lambda_\infty(P) < \frac{5}{3}\log D(t) + 1.2177.$$

Proof. We fix an integer t. We transform the Weierstrass equation by $x \mapsto x - 30D(t)$. This yields the elliptic curve defined by

$$y^2 = x^3 - 88D(t)x^2 + 2743D(t)^2x - 27885D(t)^3$$

and P corresponds to the point $(D(t)(t^4+2t^2+12t+30),\ D(t)^2(t^3+t+3))$. We denote them by E'_D and P' respectively. Now $\lambda_\infty(P)$ on E_D equals $\lambda_\infty(P')$ on E'_D (Remark 2.2).

The polynomial $x^3-88x^2+2743x-27885$ has only one real root, which we denote by c, and its approximate value is $20.55166\cdots$ (this can easily be found by softwares like Maple). So the only real root of $x^3-88D(t)x^2+2743D(t)^2x-27885D(t)^3$ is $cD(t)$, and so we have $x(Q)>20.55166D(t)>0$ for $Q\in E'_D(\mathbb{R})$ (it is easy to see that $D(t)>0$ for $t\in\mathbb{R}$). So $\lambda_\infty(P')$ is computable by using Tate's series as follows.

$$\lambda_\infty(P')=\log|x(P')|+\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log|z(2^iP')|,$$

where

$$z(P')=1-\frac{b_{4,D}}{x(P')^2}-\frac{2b_{6,D}}{x(P')^3}-\frac{b_{8,D}}{x(P')^4}.$$

Note that for any $Q\in E'_D(\mathbb{R})$ we have $z(Q)>0$, since $z(Q)$ satisfies the equaliy $z(Q)x(Q)^4=\psi_2(Q)^2x(2Q)$.

By elementary calculus, we can compute the bounds of the series as follows.

$$0<\frac{x(P')}{D(t)^{5/3}}=\frac{t^4+2t^2+12t+30}{(t^6+4t^4+30t^3+5t^2+54t+245)^{2/3}}<3.37933,$$

So

$$\log x(P')<\frac{5}{3}\log D(t)+\log(3.37933)=\frac{5}{3}\log D(t)+1.217674.$$

For any point $Q\in E'_D(\mathbb{R})$, there exists $u(>20.55166)$ such that $x(Q)=D(t)u$. So

$$z(Q)=1-\frac{b_{4,D}}{x(Q)^2}-\frac{2b_{6,D}}{x(Q)^3}-\frac{b_{8,D}}{x(Q)^4}=1-\frac{5486}{u^2}+\frac{223080}{u^3}-\frac{2291471}{u^4}<1.$$

Therefore

$$\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log z(2^iP')<0.$$

□

Lemma 5.2. *We consider the situation of Lemma 5.1, and assume that $D(t)$ is square-free. Then we have*

$$\sum_{p:\text{prime}}\lambda_p(P)\le-\log D(t).$$

Proof. To ease the notation, we write $D(t)=D$. Since the discriminant of E_D is $\Delta_D=D^6\Delta=-D^6\cdot 2^43^213^319^3$ and D is square-free, E_D is a minimal Weierstrass equation. Since P is an integral point, $\lambda_p(P)$ is non-positive for every p and so

$$\sum_{p:\text{prime}}\lambda_p(P)\le\sum_{p|D}\lambda_p(P).$$

E_D has the additive reduction at p dividing D. By the definition of $\psi_{2a,D}$ and $\psi_{3,D}$, it is clear that $v_p(\psi_{2a,D}(P))\ge 3$ and $v_p(\psi_{3,D}(P))\ge 4$. Note that $v_p(\psi_{2a,D}(P))$ is even and so $v_p(\psi_{2a,D}(P)) \geq 4$. So for p such that $p|D$ we have $\lambda_p(P) \leq -\frac{4}{4}\log p$ or $\lambda_p(P) \leq -\frac{4}{3}\log p$ by Silverman's algorithm. In any cases $\lambda_p(P) \leq -\log p$ and so

$$\sum_{p|D} \lambda_p(P) \leq \sum_{p|D}(-\log p) = -\log D.$$

□

Lemmas 5.1, 5.2 imply the following proposition.

Proposition 5.3. *In the situation of Lemma 5.2, we have*

$$\hat{h}(P) < \frac{2}{3}\log D(t) + 1.2177.$$

We now finish the proof of Theorem 1.3.

proof of Theorem 1.3. Since $D(t)^2(t^3+t+3) \neq 0$, P is not a 2-torsion point, and so by Corollary 4.23 not a torsion point for $|t| \geq 11$. By elementary calculus, we have

$$\frac{\frac{2}{3}\log D(t) + 1.2177}{\frac{1}{4}\log D(t) - 3.5472} < 4,$$

for $|t| \geq 2216$. Therefore by the property of the canonical height, there does not exists a point R such that $P = mR$ ($|m| \geq 2$).

□

References

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

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

[3] J. Cremona, S. Siksek. Computing a lower bound for the canonical height on elliptic curves over $\mathbb{Q}$. *in Algorithmic Number Theory, 7th International Symposium*, Vol. ANTS-VII, pp. 275–286, 2006.

[4] S. Duquesne. Elliptic curves associated with simplest quartic fields. *J. Theor. Nombres Bordeaux*, Vol. 19, pp. 81–100, 2007.

[5] Y. Fujita and T. Nara. On the mordell–weil group of the elliptic curve $y^2 = x^3 + n$. *arXiv 1011.1077*, 2010.

[6] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, Vol. 51, pp. 339–358, 1988.

[7] J. H. Silverman. Lower bound for the canonical height on elliptic curves. *Duke Math. J.*, Vol. 48, pp. 633–648, 1981.

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

(T. Nara) Mathematical Institute, Tohoku University, Sendai 980-8578, Japan