ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 44, Number 6, 2014

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 elliptic curves over $\mathbb{Q}$. 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. The canonical height on an elliptic curve over a number field is a non-negative real-valued function on the curve. It is a tool for studying arithmetic of elliptic curves. In studies using the canonical height, it is often useful to estimate its value numerically.

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, 12**]).

In the paper [**4,** Proposition 8.3], Duquesne gave an explicit lower bound of the canonical heights of rational 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 author 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 a set of explicit points is a part of a basis of the Mordell-Weil group.

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

2010 AMS *Mathematics subject classification.* Primary 11G05, 11G50, Secondary 11G07.

Keywords and phrases. Elliptic curve, Mordell-Weil group, canonical height, quadratic twist.

Received by the editors on September 12, 2012, and in revised form on October 9, 2012.

DOI:10.1216/RMJ-2014-44-6-2009

the behavior of a certain family of the quadratic twists of an elliptic curve. For example, we can prove Theorem 1.4 below.

Our lower bound is obtained by using the decomposition of the canonical height into the local heights, and they are estimated by the combination of Cohen's algorithm ([**1,** Algorithm 7.5.7]) and Tate's theorem ([**10,** Theorem 4.1]). Each lower bound in [**4, 5**] is essentially for twists of a single curve. Moreover, by the simplicity of the Weierstrass equations, the estimates of the non-archimedean part of the local height were available by ad hoc arguments. However, in this paper, we give a lower bound for quadratic twists of an arbitrary curve, and more systematic argument is required.

Our main results are as follows.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve and $E_D/\mathbb{Q}$ the quadratic twist of $E/\mathbb{Q}$ by a square-free integer D. If $P \in E_D(\mathbb{Q})$ is not a 2-torsion point, then we have the following lower bound of the canonical height of P,*

$$\begin{aligned}\widehat{h}(P) \geq \frac{1}{8}\log|D| &+ \frac{1}{32}\log\frac{(1-|q|)^8}{|q|}\\ &+\frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right| - \frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}|\\ &-\frac{1}{24}\log|j_E^{\mathrm{dnm}}| - \frac{3}{4}\log 2,\end{aligned}$$

where j_E^{dnm} is the denominator of the j-invariant of E (if $j_E = 0$, then put $j_E^{\mathrm{dnm}} = 1$), $\mathcal{D}_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$, $\omega_1^{\min}$ and $\omega_2^{\min}$ are periods of a minimal Weierstrass equation of $E/\mathbb{Q}$ such that $\omega_1^{\min} > 0$, $\mathrm{Im}(\omega_2^{\min}) > 0$ and $\mathrm{Re}(\omega_2^{\min}/\omega_1^{\min}) = 0$ or $-1/2$,

$$\omega_{E/\mathbb{Q}} = \begin{cases} \omega_1^{\min} & (D>0)\\ \mathrm{Im}(\omega_2^{\min}) & (D<0,\ \mathcal{D}_{E/\mathbb{Q}}>0)\\ 2\mathrm{Im}(\omega_2^{\min}) & (D<0,\ \mathcal{D}_{E/\mathbb{Q}}<0)\end{cases}$$

and $q = \exp(2\pi i\omega_2^{\min}/\omega_1^{\min})$.

Remark 1.2. We have $\widehat{h}(P) > (1/8)\log|D| + O(1)$ by [**8,** Exercise 8.16 (c)]. The proof does not use the (Néron) local height functions.

Remark 1.3. All the quantities in the bound in the theorem (i.e., j_E^{dnm}, $\mathcal{D}_{E/\mathbb{Q}}$, $\omega_{E/\mathbb{Q}}$ and q), do not depend on the choice of a Weierstrass equation of $E/\mathbb{Q}$.

The value of the canonical height is always non-negative and so, unless $|D|$ is sufficiently large, this bound is trivial. But the bound is suited for seeing a behavior of a family of elliptic curves. Indeed, using Theorem 1.1, we can show the following theorem.

Theorem 1.4. *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. *We assume that* $D(t)$ *is square-free. Then* $E_D(\mathbb{Q})$ *does not have torsion points if* $|t| \geq 31$ *and* P *is a primitive point if* $|t| \geq 54485$. *In particular,* $E_D(\mathbb{Q}) \simeq \langle P \rangle$ *if* $\operatorname{rank} E_D(\mathbb{Q}) = 1$ *and* $|t| \geq 54485$.

Remark 1.5. This family of quadratic twists is an example given by the method described in Section 4. For many other families given by the method, we can show similar results. Without the assumption that $D(t)$ is square-free, at least it is true that the set of integers t such that P is primitive has density 1 due to [**6,** Theorem 1].

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 compute the local height functions by using Cohen's algorithm and Tate's theorem to prove Theorem 1.1. In Section 4, we introduce a method of constructing families of quadratic twists. In Section 5, we prove Theorem 1.4, which is a consequence for an example given by the method in Section 4.

2. Preliminaries.

For the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, by b_2, b_4, b_6 and c_4, c_6 we denote the usual quantities defined in [**8,** Chapter III.1]. We use the notation $[u, r, s, t]$ for a transformation of Weierstrass equations given by the substitution $x \mapsto u^2x + r$, $y \mapsto u^3y + u^2sx + t$. (For details see also [**8,** Chapter III.1].)

For an elliptic curve $E/\mathbb{Q}$ we denote the Mordell-Weil group and its m-torsion subgroup by $E(\mathbb{Q})$ and $E(\mathbb{Q})[m]$, respectively. We denote the j-invariant of E by j_E.

First, we recall the definition 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 $\widehat{h}(P)$ is defined by

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

It is known that the canonical height is decomposed to the sum of functions, called the *(Néron) 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 [**11,** Chapter VI, Theorem 1.1])**.** *Let K be a number field, v a place and K_v its completion with respect to the absolute value $|\cdot|_v$, and put $v(\cdot) = -\log|\cdot|_v$. Let E/K be the elliptic curve defined by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then there exists a unique function $\lambda_v : E(K_v) \setminus O \to \mathbb{R}$ which has the following three properties.*

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

$$\lambda_v(2P) = 4\lambda_v(P) + v(2y(P) + a_1x(P) + a_3) - \frac{1}{4}v(\Delta).$$

(ii) *The limit $\lim_{\substack{P\to O\\ v\text{-}adic}} \big(\lambda_v(P) + (1/2)v(x(P))\big)$ exists.*

(iii) *λ_v is continuous on $E(K_v) \setminus \{O\}$ and 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 removing $-(1/4)v(\Delta)$ from the right-hand side of the property (i) (e.g., [**9,** page 341]). Let μ_v be the alternative local height function. Then we have the equality

$$\lambda_v = \mu_v + \frac{1}{12}v(\Delta).$$

Though μ_v depends on the choice of a Weierstrass equation, λ_v is independent of the choice ([**11,** Chapter VI, Theorem 1.1 (b)]).

References [**10, 11**] define the local height function as λ_v. References [**1, 9**] define the local height function as μ_v.

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

$$\widehat{h}(P) = \sum_{p:\text{prime},\infty} \lambda_p(P) = \sum_{p:\text{prime},\infty} \mu_p(P). \tag{2.1}$$

3. 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 (2.1).

Let $C/\mathbb{Q}$ be an elliptic curve defined by

$$C/\mathbb{Q} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1}$$

Definition 3.1. The quadratic twist of C by a square-free integer D is the elliptic curve defined by

$$\begin{aligned} C_D/\mathbb{Q} : y^2 &+ a_1xy + a_3y \\ &= x^3 + \left(a_2D + a_1^2\frac{D-1}{4}\right)x^2 + \left(a_4D^2 + a_1a_3\frac{D^2-1}{2}\right)x \\ &\quad + a_6D^3 + a_3^2\frac{D^3-1}{4}. \end{aligned} \tag{3.2}$$

Remark 3.2. The definition of $C_D/\mathbb{Q}$ is independent of the choice of a Weierstrass equation of $C/\mathbb{Q}$. Indeed, the equation of the quadratic twist of the equation given by transforming (3.1) by $[u, r, s, t]$ is identical with the equation given by transforming (3.2) by $[u, rD, s, t + a_1r(1-D)/2]$ (see [**2,** Proposition 4.3.2 (e)]).

Remark 3.3. If $a_1 = a_3 = 0$, then we have

$$C_D/\mathbb{Q} : y^2 = x^3 + a_2Dx^2 + a_4D^2x + a_6D^3,$$

which is a familiar form.

Lemma 3.4. *Let C be an elliptic curve over $\mathbb{Q}$. Then, for the Weierstrass equation of the curve, we can choose one in the form $y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in \mathbb{Z})$ with the discriminant $2^{12m}\mathcal{D}_{C/\mathbb{Q}}$ $(m = 0, 1)$, where $\mathcal{D}_{C/\mathbb{Q}}$ is the minimal discriminant of $C/\mathbb{Q}$.*

Proof. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $(a_i \in \mathbb{Z})$ be a minimal Weierstrass equation of $C/\mathbb{Q}$, that is, an equation which is minimal at every p prime. Then the discriminant of this equation is $\mathcal{D}_{C/\mathbb{Q}}$.

By the substitution $y \mapsto y - (a_1x + a_3)/2$, we have

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

where b_i are the usual quantities of the Weierstrass equation and they are integral. Through the substitution, the discriminant does not change.

Next, by the substitution $x \mapsto (2^{-2m})x,\ y \mapsto (2^{-3m})y$, we have

$$y^2 = x^3 + (2^{2m})\frac{b_2}{4}x^2 + (2^{4m})\frac{b_4}{2}x + (2^{6m})\frac{b_6}{4}.$$

It suffices to choose $m = 0$ or 1 in order to make all the coefficients of this equation be integral. By the substitution, the discriminant changes to $2^{12m}\mathcal{D}_{C/\mathbb{Q}}$. □

The canonical height is independent of the choice of a Weierstrass equation, and so by Remark 3.2, for a proof of Theorem 1.1, we may choose the equation of $E/\mathbb{Q}$ and $E_D/\mathbb{Q}$ as follows.

$$E/\mathbb{Q} : y^2 = x^3 + a_2x^2 + a_4x + a_6 \ (a_2, a_4, a_6 \in \mathbb{Z}), \tag{3.3}$$

$$E_D/\mathbb{Q} : y^2 = x^3 + a_2Dx^2 + a_4D^2x + a_6D^3. \tag{3.4}$$

We denote the discriminants of these equations by Δ, Δ_D, respectively. By Lemma 3.4, we may also assume

$$\Delta = 2^{12m}\mathcal{D}_{E/\mathbb{Q}} \quad (m = 0, 1),$$

where $\mathcal{D}_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$.

Rational points on an elliptic curve defined by a Weierstrass equation can always be expressed as $(\alpha/\delta^2, \beta/\delta^3)$, where $\alpha, \beta, \delta \in \mathbb{Z}$, $\delta > 0$ and $\gcd(\alpha, \delta) = \gcd(\beta, \delta) = 1$. So let $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})[2]$ with the condition.

We first compute the archimedean part, that is, $\lambda_\infty(Q)$, by using **[1,** Algorithm 7.5.7].

Throughout the paper, we define periods of an elliptic curve as are computed by [**1,** Algorithm 7.4.7], which depend on the choice of a Weierstrass equation. By ω_1, ω_2 and $\omega_1^{\min}$, $\omega_2^{\min}$ we denote the periods of (3.3) and of its minimal equation, respectively. Then we can easily verify $\omega_1 = 2^{-m}\omega_1^{\min}$, $\omega_2 = 2^{-m}\omega_2^{\min}$ $(m = 0, 1)$. Further, if we let $\omega_{1,D}$ be the period of (3.4), then by straightforward computations, we have the following lemma.

Lemma 3.5.

$$\omega_{1,D} = \begin{cases} \omega_1 |D|^{-1/2} & (D > 0) \\ \mathrm{Im}(\omega_2)|D|^{-1/2} & (D < 0, \Delta > 0) \\ 2\mathrm{Im}(\omega_2)|D|^{-1/2} & (D < 0, \Delta < 0) \end{cases}$$

The estimate of the archimedean part is as follows.

Lemma 3.6. *Let* $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$. *Then*

$$\begin{aligned} \lambda_\infty(Q) \geq{}& \frac{1}{8}\log|D| + \frac{1}{32}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right| \\ & - \frac{3}{4}\log\delta + \frac{1}{4}\log|\beta| - \frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}| \\ & - \frac{3}{4}\log 2 - \frac{1}{2}\log|D|, \end{aligned} \tag{3.5}$$

where $q = \exp(2\pi i\omega_2/\omega_1)$, $\mathcal{D}_{E/\mathbb{Q}}$ *is the minimal discriminant of* $E/\mathbb{Q}$ *and*

$$\omega_{E/\mathbb{Q}} = \begin{cases} \omega_1^{\min} & (D > 0) \\ \mathrm{Im}(\omega_2^{\min}) & (D < 0, \Delta > 0) \\ 2\mathrm{Im}(\omega_2^{\min}) & (D < 0, \Delta < 0). \end{cases}$$

Remark 3.7. It is convenient for us to divide the term of $\log|D|$ as above for later computations.

Proof. By [**1,** Algorithm 7.5.7], Lemma 3.5 and the trivial bound $|\theta| \leq 1/(1-|q|)$,

$$\lambda_\infty(Q) = \frac{1}{32}\log\left|\frac{\Delta_D}{q}\right| + \frac{1}{8}\log\left|\left(\frac{\beta}{\delta^3}\right)^2\frac{\omega_{1,D}}{2\pi}\right|$$

$$\begin{aligned}
&-\frac{1}{4}\log|\theta|-\frac{1}{12}\log|\Delta_D|\\
&=\frac{1}{32}\log\left|\frac{2^{12m}\mathcal{D}_{E/\mathbb{Q}}D^6}{q}\right|+\frac{1}{8}\log\left|\frac{\beta^2}{\delta^6}\frac{2^{-m}\omega_{E/\mathbb{Q}}}{2\pi|D|^{1/2}}\right|\\
&\quad-\frac{1}{4}\log|\theta|-\frac{1}{12}\log|2^{12m}\mathcal{D}_{E/\mathbb{Q}}D^6|\\
&=\frac{1}{8}\log|D|+\frac{1}{32}\log\frac{1}{|q|}-\frac{1}{4}\log|\theta|\\
&\quad+\frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right|-\frac{3}{4}\log|2^m|\\
&\quad+\frac{1}{4}\log\left|\frac{\beta}{\delta^3}\right|-\frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}|-\frac{1}{2}\log|D|\\
&\geq\frac{1}{8}\log|D|+\frac{1}{32}\log\frac{(1-|q|)^8}{|q|}\\
&\quad+\frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right|-\frac{3}{4}\log 2\\
&\quad+\frac{1}{4}\log\left|\frac{\beta}{\delta^3}\right|-\frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}|-\frac{1}{2}\log|D|. \qquad \square
\end{aligned}$$

Remark 3.8. Note that we cannot use [**1,** Algorithm 7.5.7] for 2-torsion points.

Next we estimate the non-archimedean part of the canonical height. For this purpose, we use [**10,** Theorem 4.1] and [**11,** Chapter VI, Theorem 4.1].

Definition 3.9. For a Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we define polynomials of x, y as follows.

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

We also put

$$v_p(\cdot)=\mathrm{ord}_p(\cdot)\log p(=-\log|\cdot|_p).$$

Remark 3.10. ψ_2 and ψ_3 are known as the division polynomials of elliptic curves. We use ψ_3 in the proof of Lemma 5.2.

Theorem 3.11 ([**11,** Ch. VI, Theorem 4.1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with p-integral coefficients (i.e. $\mathrm{ord}_p(a_i) \geq 0$). If $P \in E(\mathbb{Q})$ satisfies $\mathrm{ord}_p(\psi_0(P)) \leq 0$ or $\mathrm{ord}_p(\psi_2(P)) \leq 0$, then*

$$\lambda_p(P) = \frac{1}{2}\max\{v_p(x(P)^{-1}), 0\} + \frac{1}{12}v_p(\Delta),$$

where Δ is the discriminant of the equation.

Computing ψ_0, ψ_2 for (3.4) and denoting them by $\psi_{0,D}, \psi_{2,D}$, we have

$$\begin{aligned}\psi_{0,D}(x,y) &= 3x^2 + 2a_2Dx + a_4D^2,\\ \psi_{2,D}(x,y) &= 2y.\end{aligned}$$

In the following consideration, we fix a square-free integer D and a rational point $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$. First for D and Q we divide the set of primes into several subsets.

Definition 3.12. Let Ω be the set of all the rational primes. For Q and D, we put

$$\begin{aligned}S^+ &= \{p \in \Omega;\ p \mid \delta,\ p \neq 2\},\\ S^- &= \{p \in \Omega;\ p \nmid \delta,\ p \neq 2\},\\ T^+ &= \{p \in \Omega;\ p \nmid \delta,\ p \mid \beta,\ p \neq 2\},\\ T^- &= \{p \in \Omega;\ p \nmid \delta,\ p \nmid \beta,\ p \neq 2\},\\ U^+ &= \{p \in \Omega;\ p \nmid \delta,\ p \mid \beta,\ p \mid D,\ p \neq 2\},\\ U^- &= \{p \in \Omega;\ p \nmid \delta,\ p \mid \beta,\ p \nmid D,\ p \neq 2\}.\end{aligned}$$

Remark 3.13. Note that

$$\Omega = S^+ \cup T^- \cup U^+ \cup U^- \cup \{2\}.$$

Lemma 3.14. *If $p \in S^+ \cup T^-$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_p(Q) \geq v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}).$$

Proof. In this case, $\operatorname{ord}_p(\psi_{2,D}(Q)) = \operatorname{ord}_p(2\beta/\delta^3) \leq 0$. So Q reduces modulo p to a nonsingular point. Now, by [**11,** Ch. VI, Theorem 4.1]

$$\begin{aligned}\lambda_p(Q) &= \frac{1}{2}\max\{-v_p(\alpha/\delta^2), 0\} + \frac{1}{12}v_p(D^6\Delta)\\ &\geq v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}).\end{aligned}$$ □

Lemma 3.15. *If $p \in U^+$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_p(Q) \geq -\frac{1}{4}v_p(\beta) + \frac{1}{2}v_p(D) - \frac{1}{24}\max\{v_p(j_E^{-1}), 0\}.$$

Proof. Using [**10,** Theorem 4.1], we have

$$\begin{aligned}\lambda_p(Q) &\geq \frac{1}{2}\max\{-v_p(\alpha/\delta^2), 0\} - \frac{1}{24}\max\{v_p(j_E^{-1}), 0\}\\ &= -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\}.\end{aligned}$$

Next, we have

$$\frac{\beta^2}{\delta^6} = \frac{\alpha^3}{\delta^6} + a_2 D\frac{\alpha^2}{\delta^4} + a_4 D^2\frac{\alpha}{\delta^2} + a_6 D^3,$$

since $Q \in E_D(\mathbb{Q})$. So $p \mid \alpha$, since $p \mid \beta$ and $p \mid D$. Then $\operatorname{ord}_p((\alpha^3/\delta^6) + a_2 D(\alpha^2/\delta^4) + a_4 D^2(\alpha/\delta^2) + a_6 D^3) \geq 3$. On the other hand, $\operatorname{ord}_p(\beta^2/\delta^6)$ is even, and so $\operatorname{ord}_p(\beta^2) \geq 4$ and $\operatorname{ord}_p(\beta) \geq 2$. Therefore, we have

$$\begin{aligned}\lambda_p(Q) + \frac{1}{4}v_p(\beta) &\geq -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\} + \frac{2}{4}\log p\\ &= -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\} + \frac{1}{2}v_p(D),\end{aligned}$$

since D is square-free. □

Lemma 3.16. *If $p \in U^-$ and $Q = (\alpha/\delta^2, \beta/\delta^3) \in E_D(\mathbb{Q})$, then*

$$\lambda_p(Q) \geq -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\}.$$

Proof. Using [**10,** Theorem 4.1], we have

$$\begin{aligned}\lambda_p(Q) &\geq \frac{1}{2}\max\{-v_p(\alpha/\delta^2), 0\} - \frac{1}{24}\max\{v_p(j_E^{-1}), 0\}\\ &= -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\}.\end{aligned}$$ □

Lemma 3.17. *If* $p = 2$, *then*

$$\lambda_p(Q) \geq \begin{cases} -\dfrac{1}{24}\max\{v_p(j_E^{-1}), 0\} - \dfrac{1}{4}v_p(\beta) + \dfrac{1}{2}v_p(D) & (2 \nmid \delta,\ 2 \mid D)\\ -\dfrac{1}{24}\max\{v_p(j_E^{-1}), 0\} & (2 \nmid \delta,\ 2 \nmid D)\\ v_p(\delta) + \dfrac{1}{2}v_p(D) + \dfrac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}) & (2 \mid \delta).\end{cases}$$

Proof. If $2 \mid \delta$, then $2 \nmid \beta$ and so $\operatorname{ord}_2(\psi_{2,D}(Q)) = \operatorname{ord}_2(2\beta/\delta^3) < 0$. Then Q reduces modulo 2 to a nonsingular point, and so

$$\begin{aligned}\lambda_p(Q) &= v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\Delta)\\ &\geq v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}).\end{aligned}$$

Next assume $2 \nmid \delta$. If Q reduces modulo 2 to a nonsingular point, then we have the same bound as above. So we assume Q reduces to a singular point. If $2 \mid D$, then $2 \mid \alpha$ and so $2 \mid \beta$. Therefore, again by the same argument as that in the proof of Lemma 3.15, we obtain

$$\lambda_p(Q) \geq -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\} - \frac{1}{4}v_p(\beta) + \frac{1}{2}v_p(D).$$

If $2 \nmid D$, then by using [**10,** Theorem 4.1], we have

$$\lambda_p(Q) \geq -\frac{1}{24}\max\{v_p(j_E^{-1}), 0\}.$$

These two lower bounds are clearly less than

$$v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}).$$ □

We now finish the proof of Theorem 1.1.

Proof of Theorem 1.1. By (2.1) and Lemma 3.6,

$$\begin{aligned}\widehat{h}(P) \geq{}& \frac{1}{8}\log|D| + \frac{1}{32}\log\frac{(1-|q|)^8}{|q|} + \frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right| \\ &- \frac{3}{4}\log\delta + \frac{1}{4}\log|\beta| - \frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}| \\ &- \frac{3}{4}\log 2 - \frac{1}{2}\log|D| + \sum_{p:\text{prime}}\lambda_p(Q).\end{aligned}$$

If $2 \nmid \delta$ and $2 \mid D$, then by Lemmas 3.14–3.17,

$$\begin{aligned}\sum_{p:\text{prime}}\lambda_p(Q) ={}& \sum_{p\in S^+\cup T^-}\lambda_p(Q) + \sum_{p\in U^+}\lambda_p(Q) + \sum_{p\in U^-}\lambda_p(Q) + \lambda_2(Q) \\ \geq{}& \sum_{p\in S^+\cup T^-}\left(v_p(\delta) + \frac{1}{2}v_p(D) + \frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}})\right) \\ &+ \sum_{p\in U^+\cup\{2\}}\left(-\frac{1}{4}v_p(\beta) + \frac{1}{2}v_p(D) - \frac{1}{24}\max\{v_p(j_E^{-1}),0\}\right) \\ &+ \sum_{p\in U^-}\left(-\frac{1}{24}\max\{v_p(j_E^{-1}),0\}\right) \\ ={}& \sum_{p\mid\delta,\ p\neq 2}v_p(\delta) + \sum_{p\mid D}\frac{1}{2}v_p(D) + \sum_{p\nmid\beta,\ p\neq 2}\frac{1}{12}v_p(\mathcal{D}_{E/\mathbb{Q}}) \\ &+ \sum_{p\nmid\delta,\ p\mid D,\ p\mid\beta}\left(-\frac{1}{4}v_p(\beta)\right) \\ &+ \sum_{p\nmid\delta,\ p\mid\beta}\left(-\frac{1}{24}\max\{v_p(j_E^{-1}),0\}\right) \\ \geq{}& \log\delta + \frac{1}{2}\log|D| + 0 - \frac{1}{4}\log|\beta| \\ &- \sum_{p\mid\mathcal{D}_{E/\mathbb{Q}}}\frac{1}{24}\max\{v_p(j_E^{-1}),0\}.\end{aligned}$$

If $2 \nmid \delta$ and $2 \nmid D$, then by Lemmas 3.14–3.17,

$$\sum_{p:\text{prime}}\lambda_p(Q) = \sum_{p\in S^+\cup T^-}\lambda_p(Q) + \sum_{p\in U^+}\lambda_p(Q) + \sum_{p\in U^-}\lambda_p(Q) + \lambda_2(Q)$$

$$\begin{aligned}
&\geq \sum_{p\in S^{+}\cup T^{-}} \left(v_p(\delta) + \frac{1}{2} v_p(D) + \frac{1}{12} v_p(\mathcal{D}_{E/\mathbb{Q}}) \right) \\
&\quad + \sum_{p\in U^{+}} \left(-\frac{1}{4} v_p(\beta) + \frac{1}{2} v_p(D) - \frac{1}{24} \max\{v_p(j_E^{-1}), 0\} \right) \\
&\quad + \sum_{p\in U^{-}\cup\{2\}} \left(-\frac{1}{24} \max\{v_p(j_E^{-1}), 0\} \right) \\
&= \sum_{\substack{p\mid\delta \\ p\neq 2}} v_p(\delta) + \sum_{\substack{p\mid D \\ p\neq 2}} \frac{1}{2} v_p(D) + \sum_{\substack{p\nmid\beta \\ p\neq 2}} \frac{1}{12} v_p(\mathcal{D}_{E/\mathbb{Q}}) \\
&\quad + \sum_{\substack{p\nmid\delta \\ p\mid D \\ p\mid\beta \\ p\neq 2}} \left(-\frac{1}{4} v_p(\beta) \right) + \sum_{\substack{p\nmid\delta \\ p\mid\beta}} \left(-\frac{1}{24} \max\{v_p(j_E^{-1}), 0\} \right) \\
&\geq \log\delta + \frac{1}{2}\log|D| + 0 - \frac{1}{4}\log|\beta| \\
&\quad - \sum_{p\mid\mathcal{D}_{E/\mathbb{Q}}} \frac{1}{24} \max\{v_p(j_E^{-1}), 0\}.
\end{aligned}$$

If $2 \mid \delta$, then by seeing the decomposition as

$$\sum_{p:\text{prime}} \lambda_p(Q) = \sum_{p\in S^{+}\cup T^{-}\cup\{2\}} \lambda_p(Q) + \sum_{p\in U^{+}} \lambda_p(Q) + \sum_{p\in U^{-}} \lambda_p(Q),$$

we have the same bound by a similar computation.

Therefore,

$$\begin{aligned}
\widehat{h}(P) \geq{}& \frac{1}{8}\log|D| + \frac{1}{32}\log\frac{(1-|q|)^8}{|q|} \\
&+ \frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right| - \frac{3}{4}\log\delta + \frac{1}{4}\log|\beta| \\
&- \frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}| - \frac{3}{4}\log 2 - \frac{1}{2}\log|D| \\
&+ \log\delta + \frac{1}{2}\log|D| - \frac{1}{4}\log|\beta|
\end{aligned}$$

$$
\begin{aligned}
&- \sum_{p \mid \mathcal{D}_{E/\mathbb{Q}}} \frac{1}{24} \max\{v_p(j_E^{-1}), 0\} \\
&\geq \frac{1}{8}\log|D| + \frac{1}{32}\log\frac{(1-|q|)^8}{|q|} \\
&\quad + \frac{1}{8}\log\left|\frac{\omega_{E/\mathbb{Q}}}{2\pi}\right| - \frac{5}{96}\log|\mathcal{D}_{E/\mathbb{Q}}| \\
&\quad - \sum_{p \mid \mathcal{D}_{E/\mathbb{Q}}} \frac{1}{24} \max\{v_p(j_E^{-1}), 0\} - \frac{3}{4}\log 2. \qquad \square
\end{aligned}
$$

Corollary 3.18. *Let E_D be the elliptic curve defined by $y^2 = x^3 + 2Dx^2 + 163D^2x + 2205D^3$ $(D > 0)$ and $Q \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})[2]$. Then*

$$\widehat{h}(Q) \geq \frac{1}{8}\log D - 2.5744.$$

Proof. Let $E/\mathbb{Q}$ be the elliptic curve defined by

$$y^2 = x^3 + 2x^2 + 163x + 2205. \tag{3.6}$$

Then, by using PARI/GP v.2.3.4, we have $\Delta = -2^4 3^2 13^3 19^3$, $j_E = 2^8 5^3 97^3 3^{-2} 13^{-3} 19^{-3}$, $\omega_1 = 1.04995090\cdots$, $q = -0.10978666\cdots$. Since the discriminant is twelfth power-free, the equation (3.6) is minimal, and so $\omega_{E/\mathbb{Q}} = \omega_1, \mathcal{D}_{E/\mathbb{Q}} = \Delta$. By Theorem 1.1 with the values we have the bound. □

4. Families of quadratic twists.

4. 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 $f \in \mathbb{Q}[t]$ be a monic irreducible cubic polynomial (therefore with no multiple roots), $F \in \mathbb{Q}[t]$ a polynomial such that $F' = mf$ for some $m \in \mathbb{Q}$ 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 $[d(f_1 \circ F)]/(dt)(\alpha) = f_1'(F(\alpha))F'(\alpha) = 0$. Therefore, there exists a polynomial $D \in \mathbb{Q}[t]$ such that $D(t)f(t)^2 = f_1(F(t))$. So we obtain a family of the quadratic twists $D(t)y^2 = f_1(x)$ with a rational point $(F(t), f(t))$.

For example, if

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

we have

$$\begin{aligned} f_1 &= t^3 + 2t^2 + 163t + 2205, \\ D &= t^6 + 4\,t^4 + 30\,t^3 + 5\,t^2 + 54\,t + 245. \end{aligned}$$

In general, we can obtain f_1 and D explicitly as follows.

Lemma 4.1. *Let $A, B \in \mathbb{Q}$, $f = t^3 + At + B$ and $F = t^4 + 2At^2 + 4Bt$. Then the polynomials f_1 and D as above are as follows.*

$$\begin{aligned} f_1 &= t^3 + 2A^2t^2 + A(A^3 + 18B^2)t + B^2(2A^3 + 27B^2), \\ D &= t^6 + 4At^4 + 10Bt^3 + 5A^2t^2 + 18ABt + 2A^3 + 27B^2. \end{aligned}$$

In particular, $\operatorname{disc}(f_1) = B^2 \operatorname{disc}(f)^3$, *where we denote discriminants of polynomials by* $\operatorname{disc}(\cdot)$.

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 $\alpha_1\alpha_2\alpha_3$ $(= -B)$. Indeed, we can verify that

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

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 4.

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*

$$\lambda_\infty(P) < \frac{5}{6}\log D(t) + 0.6089 - \frac{1}{12}\log|\Delta_D|.$$

Proof. We fix an integer t. For the computation of $\lambda_\infty(P)$, we use Tate's series ([**9,** Theorem 1.2]). For this purpose, we transform the Weierstrass equation by the substitution $x \mapsto x - 30D(t)$. This yields the equation

$$y^2 = x^3 - 88D(t)x^2 + 2743D(t)^2x - 27885D(t)^3, \tag{5.1}$$

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). Note that the discriminant does not change through the transformation.

The polynomial $x^3 - 88x^2 + 2743x - 27885$ has only one real root, which we denote by c, and its approximate value is $20.55166\cdots$. 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.

$$\lambda_\infty(P') = \frac{1}{2}\log|x(P')| + \frac{1}{2}\sum_{i=0}^{\infty}\frac{1}{4^{i+1}}\log|z(2^iP')| - \frac{1}{12}\log|\Delta_D|,$$

where $b_{i,D}$ are usual quantities of (5.1) and

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

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

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

$$\frac{1}{2}\log x(P') < \frac{5}{6}\log D(t) + \frac{1}{2}\log(3.37933) < \frac{5}{6}\log D(t) + 0.6089.$$

For any point $Q \in E'_D(\mathbb{R})$, if we put $u = x(Q)/D(t)$, then $u > 20.55166$ as mentioned above. So

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

Therefore,

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

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

$$\sum_{p:\text{prime}} \lambda_p(P) \le -\frac{1}{2}\log D(t) + \frac{1}{12}\log|\Delta_D|.$$

Proof. To ease the notation, we write $D(t) = D$. Since the discriminant of E_D is $\Delta_D = D^6\Delta = -D^6 \cdot 2^4 3^2 13^3 19^3$ and D is square-free, the equation defining E_D is minimal. Since P is an integral point, $\lambda_p(P) - (1/12)v_p(\Delta_D)$ is not positive for every p by [**9,** Theorem 5.2]. (Note that the paper defines the local height function as μ_p in Remark 2.2.) So we have

$$\sum_{p:\text{prime}} \left(\lambda_p(P) - \frac{1}{12}v_p(\Delta_D)\right) \le \sum_{p|D} \left(\lambda_p(P) - \frac{1}{12}v_p(\Delta_D)\right).$$

To estimate the right-hand side we use [**9,** Theorem 5.2]. Computing the division polynomials of E_D we have

$$\begin{aligned} &\psi_2 = 2y, \\ &\psi_3 = 3x^4 + 4a_2Dx^3 + 6a_4D^2x^2 + 12a_6D^3x + (4a_2a_6 - a_4^2)D^4, \\ &a_2 = 2, \qquad a_4 = 163, \qquad a_6 = 2205. \end{aligned}$$

E_D has the additive reduction at p dividing D. If $p \mid D$, then $\mathrm{ord}_p(\psi_2(P)) \geq 2$ and $\mathrm{ord}_p(\psi_3(P)) \geq 4$ and so we have

$$\lambda_p(P) \leq -\frac{4}{8}\log p + \frac{1}{12}v_p(\Delta_D)$$

or

$$\lambda_p(P) \leq -\frac{2}{3}\log p + \frac{1}{12}v_p(\Delta_D)$$

by [**9,** Theorem 5.2]. In any case, $\lambda_p(P) \leq -(1/2)\log p + (1/12)v_p(\Delta_D)$, and so

$$\sum_{p|D}\left(\lambda_p(P) - \frac{1}{12}v_p(\Delta_D)\right) \leq \sum_{p|D}\left(-\frac{1}{2}\log p\right) = -\frac{1}{2}\log D. \qquad \square$$

Lemmas 5.1 and 5.2 imply the following proposition.

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

$$\widehat{h}(P) \leq \frac{1}{3}\log D(t) + 0.6089.$$

We now finish the proof of Theorem 1.4.

Proof of Theorem 1.4. The polynomial $x^3 + 2x^2 + 163x + 2205$ does not have rational roots, and neither does $x^3 + 2D(t)x^2 + 163D(t)^2x + 2205D(t)^3$. Therefore, $E_D(\mathbb{Q})$ does not have 2-torsion points. Further, if $|t| \geq 31$, then $\widehat{h}(P) > 0$ for any rational point by Corollary 3.18, and so $E_D(\mathbb{Q})$ does not have any torsion points. By elementary calculus, we have

$$\frac{(1/3)\log D(t) + 0.6089}{(1/8)\log D(t) - 2.5744} < 4,$$

for $|t| \geq 54485$. Therefore, by the property of canonical height, there does not exist a point R such that $P = mR$ ($|m| \geq 2$). $\square$

Acknowledgments. The author is grateful to the referee for valuable comments on an earlier version of this paper, which enabled a much improved result about the main theorem in this paper.

REFERENCES

1. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, New York, 1993.

2. I. Connell, *Elliptic curve handbook*, `http://www.ucm.es/BUCM/mat/doc8354.pdf` or `http://www.math.mcgill.ca/connell/`, 1999.

3. J. Cremona and S. Siksek, *Computing a lower bound for the canonical height on elliptic curves over* $\mathbb{Q}$, in *Algorithmic number theory*, 7th Inter. Sympos., Vol. ANTS-VII (2006), 275–286.

4. S. Duquesne, *Elliptic curves associated with simplest quartic fields*, J. Theor. Nomb. Bordeaux **19** (2007), 81–100.

5. Y. Fujita and T. Nara, *On the Mordell-Weil group of the elliptic curve* $y^2 = x^3 + n$, J. Num. Theor. **132** (2012), 448–466.

6. R. Gupta and K. Ramsay, *Indivisible points on families of elliptic curves*, J. Num. Theor. **63** (1997), 357–372.

7. J.H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), 633–648.

8. ______, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

9. ______, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.

10. ______, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723–743.

11. ______, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

12. T. Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over number fields*, Math. Comp. **79** (2010), 2431–2449.

Mathematical Institute, Tohoku University, Sendai 980-8578, Japan
Email address: **sa4m19@math.tohoku.ac.jp**