ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 263–279

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

The difference between the ordinary height and the canonical height on elliptic curves

Yukihiro Uchida

Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan

Received 20 January 2006; revised 4 August 2007

Communicated by David Goss

Abstract

We estimate the bounds for the difference between the ordinary height and the canonical height on elliptic curves over number fields. Our result is an improvement of the recent result of Cremona, Prickett, and Siksek [J.E. Cremona, M. Prickett, S. Siksek, Height difference bounds for elliptic curves over number fields, J. Number Theory 116 (2006) 42–68]. Our bounds are usually sharper than the other known bounds.

MSC: primary 11G50, 11G05; secondary 11G07, 14G05

Keywords: Elliptic curves; Heights; Canonical height; Height bounds

1. Introduction

Let E be an elliptic curve over a number field K. Height functions on E are real-valued functions on the Mordell–Weil group $E(K)$. In the study of elliptic curves, height functions are important in both the theory and applications. There are several height functions, each having its own advantage. For example, the ordinary (or Weil, naive) height h is easily calculated, and the canonical (or Néron–Tate) height $\hat{h}$ is easy to treat theoretically.

It is known that there are constants c_1, c_2 depending only on the model for the elliptic curve E and the field of definition K such that

$$c_1 \leqslant h(P) - \hat{h}(P) \leqslant c_2$$

E-mail address: m04005y@math.nagoya-u.ac.jp.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.10.002

for all $P \in E(K)$. It is important to estimate the bounds c_1, c_2 effectively. These bounds are used to determine Mordell–Weil bases of elliptic curves, and to determine integral points on elliptic curves. Since these height are logarithmic, we can save much time if we can obtain sharp bounds.

The bounds for the difference $h - \hat{h}$ have been estimated by many authors, for example, Zimmer [10], Silverman [7], Siksek [6], and Cremona, Prickett, and Siksek [2]. Although there are various methods for estimating the bounds, we estimate the bounds as follows.

Let M_K be the set of all places of K. For $v \in M_K$, we denote by K_v the completion of K at v. It is possible to decompose the difference $h - \hat{h}$ as

$$h(P) - \hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \Psi_v(P),$$

where Ψ_v are continuous bounded functions $\Psi_v : E(K_v) \to \mathbb{R}$. If we can estimate the bounds for Ψ_v for all $v \in M_K$, we can estimate the bounds for $h - \hat{h}$. This approach is used in [6,7], and [2]. In particular, using an exhaustive analysis of possible reduction type of elliptic curves, Cremona et al. obtain the extrema of Ψ_v for non-Archimedean places v in [2]. Therefore, it is sufficient to consider Archimedean places. Siksek [6] and Cremona et al. [2] used only the duplication map to obtain the bounds for non-Archimedean places. Using general multiplication maps instead of the duplication map, we obtain sharper bounds than theirs. Moreover, if we have sufficient time, we can obtain the approximation to the extrema of Ψ_v with arbitrary accuracy. In this sense, we obtain the best bound for Ψ_v for Archimedean places.

Our algorithm is quite similar to that in [2]. Hence, it is easy to implement this algorithm. And we can make our bounds entirely rigorous.

This paper is organized as follows. In Section 2, we fix notation used in this paper. Section 3 gives the statement of the main theorem, which gives the bound for the difference $h - \hat{h}$. In Section 4, we give the definition of division polynomials, and describe their properties. In Section 5, we describe local height functions. This section is an important part of this paper. Section 6 gives the proof for the main theorem. In Section 7, we investigate the behavior of the bounds when we replace a multiplication map by another one. Section 8 gives some remarks on actual implementation. In Section 9, we give some examples to compare our bounds with those of Silverman or Zimmer.

The results of this paper are announced without proof in [9].

2. Notation

We fix the following notation.

K	a number field,
$\mathcal{O}_K$	the ring of integers of K,
M_K	the set of all places of K,
M_K^0	the set of non-Archimedean places of K,
M_K^∞	the set of Archimedean places of K,
v	a place of K,
K_v	the completion of K at v,
n_v	the local degree $[K_v : \mathbb{Q}_v]$,
$\lvert\cdot\rvert_v$	the standard absolute value associated to v.

For $v \in M_K^0$, we use the following notation.

k_v the residue field at v,
q_v the cardinality of the residue field k_v.

Let E be an elliptic curve given by the Weierstrass equation

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$. For $v \in M_K^0$, we denote by $E_0(K_v)$ the set of points with non-singular reduction. $E_0(K_v)$ is a subgroup of $E(K_v)$. The index $c_v = [E(K_v) : E_0(K_v)]$ is called Tamagawa index at v.

We define as usual

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= \frac{c_4^3}{\Delta}.
\end{aligned}$$

Let ϕ_m, ψ_m^2 be division polynomials of E (see Section 4).

The ordinary height function $h : E(K) \to \mathbb{R}$ is defined by

$$h(P) = \begin{cases} 0 & \text{if } P = O,\\ \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max\{1, |x(P)|_v\} & \text{if } P \neq O. \end{cases}$$

The canonical height function $\hat{h} : E(K) \to \mathbb{R}$ is defined by

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

3. Statement of the main theorem

For a positive integer m, we define the function $\Phi_{m,v} : E(K_v) \to \mathbb{R}$ by

$$\Phi_{m,v}(P) = \begin{cases} 1 & \text{if } P = O,\\ \frac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}} & \text{if } P \neq O. \end{cases} \tag{1}$$

Table 1
Values of α_v

Kodaira type of E at v	Tamagawa index c_v	α_v
Any	1	0
I_m, m even	2 or m	$m/4$
I_m, m odd	m	$(m^2-1)/4m$
III	2	1/2
IV	3	2/3
I_0^*	2 or 4	1
I_m^*	2	1
I_m^*	4	$(m+4)/4$
IV*	3	4/3
III*	2	3/2

We will prove that $\Phi_{m,v}$ is a bounded continuous function (Proposition 6). We define

$$\varepsilon_{m,v}^{-1} = \inf_{P\in E(K_v)} \Phi_{m,v}(P), \qquad \delta_{m,v}^{-1} = \sup_{P\in E(K_v)} \Phi_{m,v}(P).$$

We will prove that $\varepsilon_{m,v}$ exists, i.e., the infimum appearing in its definition is non-zero (Proposition 6).

Let

$$S_v(m) = \frac{\log \delta_{m,v}}{m^2-1}, \qquad T_v(m) = \frac{\log \varepsilon_{m,v}}{m^2-1}.$$

For each valuation $v \in M_K^0$ let $E_v^{\min}$ be a minimal model for E over K_v, and let $\Delta_v^{\min}$ be the discriminant of $E_v^{\min}$. Note that E_v is already minimal for almost all $v \in M_K^0$. Hence we can take $E_v^{\min} = E_v$ and $\Delta_v^{\min} = \Delta_v$. For $v \in M_K^0$, we define the constants α_v according to the Kodaira type of $E_v^{\min}$ and the Tamagawa index c_v as in Table 1. Then our main theorem is as follows:

Theorem 1. *Let $m \geqslant 2$ be an integer. For all $P \in E(K)$,*

$$\begin{aligned}\frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K^\infty} n_v S_v(m) &\leqslant h(P) - \hat{h}(P) \\ &\leqslant \frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K^\infty} n_v T_v(m) \\ &\quad + \frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K^0} \left(\alpha_v + \frac{1}{6}\operatorname{ord}_v\bigl(\Delta/\Delta_v^{\min}\bigr)\right) \log q_v.\end{aligned}$$

Remark 2. If $m = 2$, Theorem 1 is the same as [2, Theorem 1].

We will prove Theorem 1 in Section 6.

4. Division polynomials

We review the definition and properties of division polynomials. For the details and proofs, see [5, Section 1.3].

We define division polynomials $\phi_m, \psi_m \in K[X, Y]$ as follows:

$$\begin{aligned}
\phi_1(X, Y) &= X,\\
\phi_2(X, Y) &= X^4 - b_4X^2 - 2b_6X - b_8,\\
\psi_0(X, Y) &= 0,\\
\psi_1(X, Y) &= 1,\\
\psi_2(X, Y) &= 2Y + a_1X + a_3,\\
\psi_3(X, Y) &= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,\\
\psi_4(X, Y) &= \psi_2(X, Y)\big(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2\\
&\qquad + (b_2b_8 - b_4b_6)X + \big(b_4b_8 - b_6^2\big)\big),
\end{aligned}$$

for $m \geqslant 2$,

$$\begin{aligned}
\phi_m(X, Y) &= X\psi_m(X, Y)^2 - \psi_{m-1}(X, Y)\psi_{m+1}(X, Y),\\
\psi_{2m+1}(X, Y) &= \psi_{m+2}(X, Y)\psi_m(X, Y)^3 - \psi_{m-1}(X, Y)\psi_{m+1}(X, Y)^3,\\
\psi_2(X, Y)\psi_{2m}(X, Y) &= \psi_m(X, Y)\big(\psi_{m+2}(X, Y)\psi_{m-1}(X, Y)^2 - \psi_{m-2}(X, Y)\psi_{m+1}(X, Y)^2\big).
\end{aligned}$$

It is easy to prove that this definition is well defined, i.e., $\psi_{2m}(X, Y)$ is a polynomial.

Proposition 3. *Let $P = (x, y) \in E(K)$. Let m be a positive integer. Then, $mP = O$ is equivalent to $\psi_m(x, y) = 0$. If $mP \neq O$, then*

$$x(mP) = \frac{\phi_m(x, y)}{\psi_m(x, y)^2}.$$

Proposition 4. *Let $P = (x, y) \in E(K)$. Then, $\phi_m(x, y)$ and $\psi_m(x, y)^2$ are polynomials in x over $\mathbb{Z}[b_2, b_4, b_6, b_8]$. We consider ϕ_m, ψ_m^2 as polynomials in x. Then,*

(a) *ϕ_m is a polynomial of degree m^2 with leading coefficient* 1,
(b) *ψ_m^2 is a polynomial of degree $m^2 - 1$ with leading coefficient m^2.*

By Proposition 4, we can consider ϕ_m, ψ_m^2 as polynomials in x.

Proposition 5. *The polynomials ϕ_m and ψ_m^2 are relatively prime.*

5. Local height functions

In this section, we describe properties of local height functions.

Proposition 6. *$\Phi_{m,v}$ is a bounded continuous function on $E(K_v)$. Furthermore,*

$$\inf_{P\in E(K_v)} \Phi_{m,v}(P) > 0.$$

Proof. It is clear that $\Phi_{m,v}$ is continuous at $P \in E(K_v) \setminus \{O\}$. By Proposition 4,

$$\lim_{P\to O} \Phi_{m,v}(P) = 1.$$

Therefore, $\Phi_{m,v}$ is also continuous at O. Since $E(K_v)$ is compact, $\Phi_{m,v}$ is bounded.

To show the latter part, assume that $\inf_{P\in E(K_v)} \Phi_{m,v}(P) = 0$. Since $E(K_v)$ is compact, there exists $P \in E(K_v)$ such that $\Phi_{m,v}(P) = 0$. By definition, $P \neq O$. Hence, we have $\phi_m(x(P)) = \psi_m^2(x(P)) = 0$. Since ϕ_m and ψ_m^2 are relatively prime by Proposition 5, this is a contradiction. □

We define a local height function $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$ by

$$\lambda_v(P) = \log \max\bigl\{1, \bigl|x(P)\bigr|_v\bigr\} + \sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_{2,v}\bigl(2^i P\bigr).$$

Remark 7. Some authors use different definitions of local height functions. Let λ'_v be the definition of [8,11], or [12]. Then we have

$$\lambda_v = 2\lambda'_v + \frac{1}{6}\log|\Delta|_v.$$

We have the following proposition.

Proposition 8 *(Néron, Tate). The function λ_v satisfies the following properties.*

(a) *The function λ_v is bounded and continuous on the complement of any open neighborhood of O.*
(b) *The limit*

$$\lim_{P\to O} \bigl(\lambda_v(P) - \log\bigl|x(P)\bigr|_v\bigr)$$

exists.
(c) *For all $P, Q \in E(K_v)$ with $P \neq O$, $Q \neq O$, $P \pm Q \neq O$,*

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) - 2\log\bigl|x(P) - x(Q)\bigr|_v.$$

(d) *Let m be any positive integer. For all $P \in E(K_v)$ with $mP \neq O$,*

$$\lambda_v(mP) = m^2\lambda_v(P) - \log\bigl|\psi_m^2\bigl(x(P)\bigr)\bigr|_v.$$

Proof. See [8, Chapter VI], or see [11] and [12]. □

The local height function satisfies the uniqueness property as follows.

Proposition 9. *The function* $\lambda_v : E(K_v) \setminus \{O\} \to \mathbb{R}$ *is uniquely determined by* (a), (b), *and* (d) *for any given integer* $m \geqslant 2$ *of Proposition* 8.

Proof. Suppose that λ_v and λ'_v satisfy (a), (b), and (d) for any given integer $m \geqslant 2$ of Proposition 8. Define $\Lambda : E(K_v) \to \mathbb{R}$ by

$$\Lambda(P) = \begin{cases} \lim_{Q \to O} (\lambda_v(Q) - \lambda'_v(Q)) & \text{if } P = O, \\ \lambda_v(P) - \lambda'_v(P) & \text{if } P \neq O. \end{cases}$$

Then (b) implies that Λ is well defined at $P = O$. And (a) implies that Λ is a bounded continuous function on $E(K_v)$. Therefore, there exists $M > 0$ such that for all $P \in E(K_v)$,

$$\big|\Lambda(P)\big| \leqslant M.$$

From (d), for all $P \in E(K_v)$ with $mP \neq O$,

$$\Lambda(mP) = m^2 \Lambda(P).$$

However, since the set of points with $mP = O$ is a discrete subset of $E(K_v)$, this equality also holds when $mP = O$ by continuity. Hence

$$\big|\Lambda(P)\big| = \left|\frac{\Lambda(m^i P)}{m^{2i}}\right| \leqslant \frac{M}{m^{2i}}.$$

This proves $\Lambda(P) = 0$, hence $\lambda_v = \lambda'_v$. □

Proposition 10. *Let* $m \geqslant 2$ *be an integer. Then, for all* $P \in E(K_v) \setminus \{O\}$,

$$\lambda_v(P) = \log \max\big\{1, \big|x(P)\big|_v\big\} + \sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\big(m^i P\big). \tag{2}$$

Proof. Let $\lambda'_v(P)$ be the right-hand side of (2). It is easy to show that λ'_v satisfies (a) and (b) of Proposition 8. It is sufficient to prove (d) for m:

$$\begin{aligned} \lambda'_v(mP) &= \log \max\big\{1, \big|x(mP)\big|_v\big\} + \sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\big(m^{i+1} P\big) \\ &= \log \max\left\{1, \left|\frac{\phi_m(x(P))}{\psi_m^2(x(P))}\right|_v\right\} + m^2 \sum_{i=1}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\big(m^i P\big) \\ &= m^2 \log \max\big\{1, \big|x(P)\big|_v\big\} + \log \frac{\max\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\}}{\max\{1, |x(P)|_v\}^{m^2}} \end{aligned}$$

$$+ m^2 \sum_{i=1}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\bigl(m^i P\bigr) - \log\bigl|\psi_m^2\bigl(x(P)\bigr)\bigr|_v$$
$$= m^2 \lambda'_v(P) - \log\bigl|\psi_m^2\bigl(x(P)\bigr)\bigr|_v.$$

Therefore, by Proposition 9, $\lambda_v = \lambda'_v$. □

The canonical height function is represented as the summation of the local height functions.

Proposition 11. *For all* $P \in E(K) \setminus \{O\}$,

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \lambda_v(P).$$

Proof. See [8, Chapter VI, Theorem 2.1]. □

By Proposition 11, the difference between the ordinary height and the canonical height is represented as follows:

$$h(P) - \hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \bigl(\log \max\bigl\{1, \bigl|x(P)\bigr|_v\bigr\} - \lambda_v(P)\bigr).$$

We define the function $\Psi_v : E(K_v) \to \mathbb{R}$ by

$$\Psi_v(P) = \begin{cases} 0 & \text{if } P = O, \\ \log \max\{1, |x(P)|_v\} - \lambda_v(P) & \text{if } P \neq O. \end{cases}$$

If we bound Ψ_v, we obtain the bounds for $h - \hat{h}$.

The following proposition says that the bounds for Ψ_v exist.

Proposition 12. *Ψ_v is a bounded continuous function on $E(K_v)$.*

Proof. By definition, for all $P \in E(K_v) \setminus \{O\}$,

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{4^{i+1}} \log \Phi_{2,v}\bigl(2^i P\bigr).$$

This equality holds when $P = O$. By Proposition 6, $\log \Phi_{2,v}$ is bounded and continuous. Therefore, by Weierstrass M-test, Ψ_v is continuous on $E(K_v)$. Since $E(K_v)$ is compact, Ψ_v is bounded on $E(K_v)$. □

For non-Archimedean place, the following bounds are known. Note that these bounds are the best estimates.

Proposition 13. *Let $v \in M_K^0$. Then,*

$$\inf_{P\in E(K_v)} \Psi_v(P) = 0,$$

$$\sup_{P\in E(K_v)} \Psi_v(P) = \left(\alpha_v + \frac{1}{6}\operatorname{ord}_v\left(\Delta/\Delta_v^{\min}\right)\right)\log q_v,$$

where $\Delta_v^{\min}$ is the minimal discriminant of E at v, and α_v is given by Table 1.

Proof. See [2, Proposition 8]. □

6. Proof of the main theorem

Proposition 14. *Let $m \geqslant 2$ be an integer. Then, for all $P \in E(K_v)$,*

$$S_v(m) \leqslant \Psi_v(P) \leqslant T_v(m).$$

Proof. By Proposition 10, for all $P \in E(K_v) \setminus \{O\}$,

$$\Psi_v(P) = -\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\left(m^i P\right). \tag{3}$$

This equality also holds when $P = O$. By the definitions of $\delta_{m,v}$ and $\varepsilon_{m,v}$,

$$\log \delta_{m,v} \leqslant -\log \Phi_{m,v}\left(m^i P\right) \leqslant \log \varepsilon_{m,v}.$$

Therefore, this proposition is proved by the equality

$$\sum_{i=0}^{\infty} \frac{1}{m^{2(i+1)}} = \frac{1}{m^2-1}. \qquad \square$$

Proof of Theorem 1. Theorem 1 follows from Propositions 13 and 14. □

7. Relation between bounds and multipliers

In this section, we consider the relation between the bounds in Theorem 1 and the multiplier m. First, we prove the following proposition.

Proposition 15. *Let $m \geqslant 2$, $l \geqslant 1$ be integers. Then,*

$$S_v(m) \leqslant S_v\left(m^l\right), \qquad T_v\left(m^l\right) \leqslant T_v(m),$$

i.e., the bounds in Theorem 1 *become sharper when we change m to m^l.*

Remark 16. It is not necessarily true that

$$S_v(m) \leqslant S_v(m'), \qquad T_v(m') \leqslant T_v(m),$$

if m is a divisor of m'. We will show some counterexamples in Section 9.

We begin by proving a few lemmas.

Lemma 17. *Let m be a positive integer. Then, for all $P \in E(K_v)$,*

$$\Psi_v(mP) = \log \Phi_{m,v}(P) + m^2 \Psi_v(P).$$

Proof. It is clear when $m = 1$. Let $m \geqslant 2$. By (3),

$$\begin{aligned} m^2 \Psi_v(P) &= -\sum_{i=0}^{\infty} \frac{1}{m^{2i}} \log \Phi_{m,v}\bigl(m^i P\bigr) \\ &= -\log \Phi_{m,v}(P) - \sum_{i=1}^{\infty} \frac{1}{m^{2i}} \log \Phi_{m,v}\bigl(m^i P\bigr) \\ &= -\log \Phi_{m,v}(P) + \Psi_v(mP). \qquad \square \end{aligned}$$

Lemma 18. *Let m and m' be positive integers. Then, for all $P \in E(K_v)$,*

$$\log \Phi_{mm',v}(P) = m'^2 \log \Phi_{m,v}(P) + \log \Phi_{m',v}(mP).$$

Proof. By Lemma 17,

$$\Psi_v(mP) = \log \Phi_{m,v}(P) + m^2 \Psi_v(P), \tag{4}$$

$$\Psi_v(mm'P) = \log \Phi_{m',v}(P) + m'^2 \Psi_v(mP), \tag{5}$$

$$\Psi_v(mm'P) = \log \Phi_{mm',v}(P) + (mm')^2 \Psi_v(P). \tag{6}$$

Multiply (4) by m'^2, add (5), and subtract (6). Then we obtain

$$\log \Phi_{mm',v}(P) = m'^2 \log \Phi_{m,v}(P) + \log \Phi_{m',v}(mP). \qquad \square$$

Corollary 19. *Let $m \geqslant 2$, $l \geqslant 1$ be positive integers. Then, for all $P \in E(K_v)$,*

$$\frac{1}{m^{2l}} \log \Phi_{m^l,v}(P) = \sum_{i=0}^{l-1} \frac{1}{m^{2(i+1)}} \log \Phi_{m,v}\bigl(m^i P\bigr). \tag{7}$$

Proof. By Lemma 18,

$$\begin{aligned}\sum_{i=0}^{l-1}\frac{1}{m^{2(i+1)}}\log\Phi_{m,v}\bigl(m^iP\bigr)&=\sum_{i=0}^{l-1}\frac{1}{m^{2(i+1)}}\bigl(\log\Phi_{m^{i+1},v}(P)-m^2\log\Phi_{m^i,v}(P)\bigr)\\&=\sum_{i=0}^{l-1}\biggl(\frac{1}{m^{2(i+1)}}\log\Phi_{m^{i+1},v}(P)-\frac{1}{m^{2i}}\log\Phi_{m^i,v}(P)\biggr)\\&=\frac{1}{m^{2l}}\log\Phi_{m^l,v}(P),\end{aligned}$$

where we use $\Phi_{1,v}(P)=1$. □

Now we can prove Proposition 15.

Proof of Proposition 15. Take suprema of the both sides of (7). Then we obtain

$$\frac{\log\delta_{m^l,v}^{-1}}{m^{2l}}\leqslant\sum_{i=0}^{l-1}\frac{\log\delta_{m,v}^{-1}}{m^{2(i+1)}}=\frac{m^{2l}-1}{m^{2l}(m^2-1)}\log\delta_{m,v}^{-1}.$$

Hence,

$$\frac{\log\delta_{m,v}}{m^2-1}\leqslant\frac{\log\delta_{m^l,v}}{m^{2l}-1}.$$

The proof for ε is similar. □

Next, we consider the difference between the theoretical bounds and the bounds in Theorem 1.

Proposition 20. *Let $m\geqslant 2$ be an integer. Then,*

$$0\leqslant\inf_{P\in E(K_v)}\Psi_v(P)-S_v(m)\leqslant\frac{1}{m^2-1}\Bigl(\sup_{P\in E(K_v)}\Psi_v(P)-\inf_{P\in E(K_v)}\Psi_v(P)\Bigr),\tag{8}$$

$$0\leqslant T_v(m)-\sup_{P\in E(K_v)}\Psi_v(P)\leqslant\frac{1}{m^2-1}\Bigl(\sup_{P\in E(K_v)}\Psi_v(P)-\inf_{P\in E(K_v)}\Psi_v(P)\Bigr).\tag{9}$$

Proof. By Proposition 14,

$$0\leqslant\inf_{P\in E(K_v)}\Psi_v(P)-S_v(m).$$

By Lemma 17,

$$\log\Phi_{m,v}(P)=\Psi_v(mP)-m^2\Psi_v(P).$$

Take the suprema of the both sides of this equality. We obtain

$$\log \delta_{m,v}^{-1} \leqslant \sup_{P\in E(K_v)} \Psi_v(mP) - m^2 \inf_{P\in E(K_v)} \Psi_v(P).$$

Hence,

$$\inf_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqslant \frac{1}{m^2-1}\Big(\sup_{P\in E(K_v)} \Psi_v(P) - \inf_{P\in E(K_v)} \Psi_v(P)\Big).$$

The proof for $T_v(m)$ is similar. □

The following corollary says that we can bring the bounds in Theorem 1 close to the theoretical bounds arbitrarily.

Corollary 21.

$$\lim_{m\to\infty} S_v(m) = \inf_{P\in E(K_v)} \Psi_v(P), \qquad \lim_{m\to\infty} T_v(m) = \sup_{P\in E(K_v)} \Psi_v(P).$$

Proof. Since Ψ_v is bounded on $E(K_v)$ by Proposition 12, the corollary follows from Proposition 20. □

We can estimate the difference between the theoretical bounds and the bounds in Theorem 1 by the following corollary.

Corollary 22.

$$0 \leqslant \inf_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqslant \frac{1}{m^2}\big(T_v(m) - S_v(m)\big), \tag{10}$$

$$0 \leqslant T_v(m) - \sup_{P\in E(K_v)} \Psi_v(P) \leqslant \frac{1}{m^2}\big(T_v(m) - S_v(m)\big). \tag{11}$$

Proof. By (8),

$$m^2 \inf_{P\in E(K_v)} \Psi_v(P) - \big(m^2-1\big)S_v(m) \leqslant \sup_{P\in E(K_v)} \Psi_v(P).$$

Hence,

$$m^2 \inf_{P\in E(K_v)} \Psi_v(P) - m^2 S_v(m) \leqslant \sup_{P\in E(K_v)} \Psi_v(P) - S_v(m) \leqslant T_v(m) - S_v(m).$$

Therefore we obtain (10). The proof for (11) is similar. □

8. Remarks on implementation

In this section, we describe a method for computing $S_v(m)$ and $T_v(m)$.

When $v \in M_K^0$, it is sufficient to use Tate's algorithm (see [8, Chapter IV, Section 9]).

Let $v \in M_K^\infty$. When v is a complex place, we can use the method based on Gröbner basis, or the repeated quadrisection method. See [2, Sections 8, 9].

When v is a real place, we adapt the method of [2, Section 7]. However, since we need some changes, we describe this case closely.

We can consider $K \subset \mathbb{R}$ and $K_v = \mathbb{R}$. We define polynomials $f(x)$, $g(x)$, $p(x)$ by

$$f(x) = \psi_m^2(x), \qquad g(x) = \phi_m(x), \qquad p(x) = \psi_2^2(x).$$

And we define polynomials $F(x)$, $G(x)$, $P(x)$ by

$$F(x) = x^{m^2} f(1/x), \qquad G(x) = x^{m^2} g(1/x), \qquad P(x) = x^4 p(1/x).$$

Let

$$D = \big\{x \in [-1, 1] \,\big|\, p(x) \geqslant 0\big\},$$
$$D' = \big\{x \in [-1, 1] \,\big|\, P(x) \geqslant 0\big\}.$$

Note that $f(x) = p(x)$ and $F(x) = P(x)$ in [2] since $m = 2$.

We have the following elementary lemma.

Lemma 23. *Define the constants e, e', d, d' by*

$$e = \inf_{x \in D} \max\big\{\big|f(x)\big|, \big|g(x)\big|\big\},$$
$$e' = \inf_{x \in D'} \max\big\{\big|F(x)\big|, \big|G(x)\big|\big\},$$
$$d = \sup_{x \in D} \max\big\{\big|f(x)\big|, \big|g(x)\big|\big\},$$
$$d' = \sup_{x \in D'} \max\big\{\big|F(x)\big|, \big|G(x)\big|\big\}.$$

Then,

$$\varepsilon_{m,v} = \min\{e, e'\}^{-1}, \qquad \delta_{m,v} = \max\{d, d'\}^{-1}.$$

Proof. The lemma follows from the definition of $\varepsilon_{m,v}$ and $\delta_{m,v}$ and the fact that $(x, y) \in E(\mathbb{R})$ if and only if $p(x) = (2y + a_1 x + a_3)^2$. See [6, Lemma 2.3]. □

By definition, D and D' are finite unions of closed intervals. Therefore, we can use the following lemma to determine e, e', d, d'.

Lemma 24. *Let $I \subset \mathbb{R}$ be a closed interval. Let P and Q be continuous real-valued functions on I. Then the extrema of the function* $\max\{|P(X)|, |Q(X)|\}$ *over the interval I are attained at one of the following points*:

(1) *an end point of* I;
(2) *one of the roots of* $P+Q$, $P-Q$ *in the interval* I;
(3) *a turning point of one of the functions* P, Q.

Proof. See [2, Lemma 10]. □

9. Examples

In this section, we compare our result (Theorem 1) with other results. As we noted in Remark 2, our result is the same as [2, Theorem 1] if $m=2$. Therefore we compare our result with Silberman's bounds and Zimmer's bounds. We quickly review their bounds. Note that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$.

Theorem 25. *(See Silverman [7].) For* $x \in K$, *we define*

$$h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max\bigl\{1, |x|_v\bigr\},$$

$$h_\infty(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} n_v \log \max\bigl\{1, |x|_v\bigr\}.$$

And we define

$$2^* = \begin{cases} 2 & \text{if } b_2 \neq 0, \\ 1 & \text{if } b_2 = 0, \end{cases}$$

and

$$\mu(E) = \frac{1}{12} h(\Delta) + \frac{1}{12} h_\infty(j) + \frac{1}{2} h_\infty\left(\frac{b_2}{12}\right) + \frac{1}{2}\log 2^*.$$

Then, for all $P \in E(\overline{K})$,

$$-2\mu(E) - 2.14 \leqslant h(P) - \hat{h}(P) \leqslant \frac{1}{12} h(j) + 2\mu(E) + 1.946.$$

Theorem 26 *(Zimmer). For* $x \in K$, $v \in M_K$, *we define* $v(x) = -\log |x|_v$. *Let*

$$\mu_v = \min\left\{ v(b_2), \frac{v(b_4)}{2}, \frac{v(b_6)}{3}, \frac{v(b_8)}{4} \right\},$$

and

$$\mu_l = -\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \min\{0, \mu_v\},$$

$$\mu_h = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{0, \mu_v\},$$

$$\mu = -\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \mu_v = \mu_l - \mu_h.$$

Then, for all $P \in E(\overline{K})$,

$$-\mu_l - \log 2 \leqslant h(P) - \hat{h}(P) \leqslant 2\mu + \mu_h + \frac{8}{3}\log 2.$$

Proof. The theorem follows from [5, Proposition 5.18(a), Theorem 5.35(c)]. □

To compare the bounds in Theorem 1 with the ones we described above, we give some examples. PARI/GP [4] is used in the computation.

Example 27. Consider the elliptic curve over $\mathbb{Q}$,

$$E: \quad y^2 = x^3 - 459x^2 - 3478x + 169057.$$

This is taken from [2, Example 4]. Theorem 1 gives the following bounds:

$$\begin{aligned}
-6.531924724 &\leqslant h - \hat{h} \leqslant 0.4620981204 \quad (m = 2),\\
-5.228881425 &\leqslant h - \hat{h} \leqslant 0.4620981204 \quad (m = 3),\\
-5.227187136 &\leqslant h - \hat{h} \leqslant 0.4620981204 \quad (m = 4),\\
-5.006931796 &\leqslant h - \hat{h} \leqslant 0.4620981204 \quad (m = 5).
\end{aligned}$$

Silverman's bounds are

$$-15.40309857 \leqslant h - \hat{h} \leqslant 18.74780624,$$

and Zimmer's bounds are

$$-8.208491752 \leqslant h - \hat{h} \leqslant 16.41698351.$$

We observe that the bounds in Theorem 1 are sharper than the other ones.

According to [2, Example 4], the rank of $E(\mathbb{Q})$ is 4, and that $E(\mathbb{Q})$ has a basis

$$P_1 = (16, -1), \qquad P_2 = (-4, -419), \qquad P_3 = (-22, -113), \qquad P_4 = (566, -5699).$$

Furthermore, it says that when $P = 2P_1$,

$$h(P) - \hat{h}(P) = 0.4620980788\ldots,$$

and when $P = P_1 - 3P_2 + P_3 + 3P_4$,

$$h(P) - \hat{h}(P) = -4.900153342\ldots.$$

We observe that the bounds in Theorem 1 are very sharp.

Example 28. As an example with big coefficients, consider

$$E: \quad y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116.$$

It is known that rank $E(\mathbb{Q}) \geqslant 24$ (see [3]). The discriminant of E is factored as

$$\begin{aligned}\Delta = {} & 2^2 \cdot 3^9 \cdot 5^2 \cdot 11^6 \cdot 13^2 \cdot 17^2 \cdot 29^2 \cdot 31^3 \cdot 41^2 \\ & \cdot 458619970494582607679296750333015081 \\ & \cdot 26424097318297169909466115422936023607010597408250 3.\end{aligned}$$

Then, by Theorem 1, we have the following estimates on $E(\mathbb{Q})$:

$$\begin{aligned}-58.454 &\leqslant h - \hat{h} \leqslant 16.560 \quad (m = 2),\\ -49.244 &\leqslant h - \hat{h} \leqslant 21.598 \quad (m = 3),\\ -46.647 &\leqslant h - \hat{h} \leqslant 16.392 \quad (m = 4),\\ -45.516 &\leqslant h - \hat{h} \leqslant 18.044 \quad (m = 5),\\ -44.968 &\leqslant h - \hat{h} \leqslant 16.368 \quad (m = 6),\\ -44.626 &\leqslant h - \hat{h} \leqslant 17.154 \quad (m = 7),\\ -44.422 &\leqslant h - \hat{h} \leqslant 16.360 \quad (m = 8),\\ -44.264 &\leqslant h - \hat{h} \leqslant 16.799 \quad (m = 9).\end{aligned}$$

Silverman's bounds are

$$-48.610 \leqslant h - \hat{h} \leqslant 71.304,$$

and Zimmer's bounds are

$$-44.881 \leqslant h - \hat{h} \leqslant 90.223.$$

We give counterexamples mentioned in Remark 16. These curves are taken from Cremona's elliptic curve data [1].

Example 29. Consider the curve 37a1 (cf. [1])

$$E: \quad y^2 + y = x^3 - x.$$

Then, Theorem 1 gives

$$\begin{aligned}-0.48648 &\leqslant h - \hat{h} \leqslant 0.12298 \quad (m = 3),\\ -0.46933 &\leqslant h - \hat{h} \leqslant 0.12650 \quad (m = 6).\end{aligned}$$

The upper bound with $m = 6$ is worse than that with $m = 3$.

Example 30. Consider the curve 20888a1 (cf. [1])

$$E: \quad y^2 = x^3 - 52x + 100.$$

Then, Theorem 1 gives

$$-2.1041 \leqslant h - \hat{h} \leqslant 1.8394 \quad (m = 5),$$
$$-2.1193 \leqslant h - \hat{h} \leqslant 1.8394 \quad (m = 10).$$

The lower bound with $m = 10$ is worse than that with $m = 5$.

Acknowledgments

The author would like to thank Professors Kazuhiro Fujiwara and Osamu Fujino for valuable suggestions and help. He would also like to thank the referee for useful comments.

References

[1] J.E. Cremona, Elliptic curve data, http://www.warwick.ac.uk/~masgaj/ftp/data/INDEX.html.
[2] J.E. Cremona, M. Prickett, S. Siksek, Height difference bounds for elliptic curves over number fields, J. Number Theory 116 (2006) 42–68.
[3] R. Martin, W. McMillen, An elliptic curve over $\mathbb{Q}$ with rank at least 24, Number Theory Listserver, May 2000.
[4] PARI/GP, version 2.2.10, Bordeaux, 2005, http://pari.math.u-bordeaux.fr/.
[5] S. Schmitt, H.G. Zimmer, Elliptic Curves: A Computational Approach, de Gruyter Stud. Math., vol. 31, Walter de Gruyter, 2003.
[6] S. Siksek, Infinite descent on elliptic curves, Rocky Mountain J. Math. 25 (1995) 1501–1538.
[7] J.H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, Math. Comp. 55 (1990) 723–743.
[8] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 151, Springer-Verlag, 1994.
[9] Y. Uchida, On the difference between the ordinary height and the canonical height on elliptic curves, Proc. Japan Acad. Ser. A Math. Sci. 82 (3) (2006) 56–60.
[10] H.G. Zimmer, On the difference of the Weil height and the Néron–Tate height, Math. Z. 147 (1976) 35–51.
[11] H.G. Zimmer, Quasifunctions on elliptic curves over local fields, J. Reine Angew. Math. 307/308 (1979) 221–246.
[12] H.G. Zimmer, Correction and Remarks concerning: "Quasifunctions on elliptic curves over local fields", J. Reine Angew. Math. 343 (1982) 203–211.