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

By Yukihiro Uchida

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

(Communicated by Heisuke Hironaka, m. j. a., March 13, 2006)

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. Number Theory **116** (2006), 42–68). Our bounds are usually sharper than the other known bounds.

Key words: 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 the application. There are some kinds of height functions, each of them has 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

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

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 basis 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 [4], and Cremona, Prickett, and Siksek [2]. Our bounds (Theorem 2.1) are improvements of the result in [2]. While only the duplication map is used in [2], we use general multiplication maps. Our algorithm (see Section 4) are quite similar to that in [2]. Hence, it is easy to implement this algorithm. And we can make our bounds entirely rigorous.

In this paper, we present the bounds for $h - \hat{h}$ and relations of the bounds and the multiplier m used in the multiplication map. At the end of the paper, we give a few examples to compare our bounds with other bounds. The detailed proof of our result will be published elsewhere ([9]).

2. Statement of the main theorem. We fix the following notations.

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 $[K_v : \mathbf{Q}_v]$,
$\lvert\cdot\rvert_v$	the standard absolute value associated to v.

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

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

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

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 b_i, c_i, the discriminant Δ, and j-invariant j as usual (see [6, Chapter 3, Section 1]).

Let ϕ_m, ψ_m^2 be multiplication polynomials of E (see [5, Section 1.3]). Note that $x(mP) = \phi_m(x(P))/\psi_m^2(x(P))$ if $mP \neq O$.

The ordinary height function $h\colon E(K) \to \mathbf{R}$ is

2000 Mathematics Subject Classification. Primary 11G50, 11G05; Secondary 11G07, 14G05.

Table I. Values of α_v

Kodaira type of $E_v^{\min}$	c_v	α_v
any	1	0
I_r, r even	2 or r	$r/4$
I_r, r odd	r	$(r^2-1)/4r$
III	2	1/2
IV	3	2/3
I_0^*	2 or 4	1
I_r^*	2	1
I_r^*	4	$(r+4)/4$
IV^*	3	4/3
III^*	2	3/2

defined by

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

if $P \neq O$, and $h(O) = 0$.

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

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

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

$$\Phi_{m,v}(P) = \frac{\max\left\{|\phi_m(x(P))|_v, |\psi_m^2(x(P))|_v\right\}}{\max\{1, |x(P)|_v\}^{m^2}} \tag{1}$$

if $P \neq O$, and $\Phi_{m,v}(O) = 1$. We can prove that $\Phi_{m,v}$ is a bounded continuous function. We define

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

We can prove that $\varepsilon_{m,v}$ exists, i.e., the infimum appearing in its definition is positive, especially nonzero.

Let

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

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 $E_v^{\min}$. For almost all $v \in M_K^0$, we can take $E_v^{\min} = E$ and $\Delta_v^{\min} = \Delta$ since E is already minimal at 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 I. Then our main theorem is as follows:

Theorem 2.1 ([9, Theorem 3.1])**.** *Let $m \geq 2$ be an integer. For all $P \in E(K)$,*

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

Remark 2.2. For $v \in M_K^0$ such that $\operatorname{ord}_v(\Delta) = 0$, we have $\alpha_v = 0$ and $\operatorname{ord}_v(\Delta/\Delta_v^{\min}) = 0$. Therefore the summation over M_K^0 is a finite sum.

Remark 2.3. If $m = 2$, Theorem 2.1 is the same as [2, Theorem 1].

3. Relation between bounds and multipliers. In this section, we consider the relation between the bounds in Theorem 2.1 and the multiplier m.

First, we define a local height function $\lambda_v\colon E(K_v) \setminus \{O\} \to \mathbf{R}$ by

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

Remark 3.1. Some authors use different definitions of local height functions. Let λ_v' be the definition of [8, 11, 12]. Then we have

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

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

Proposition 3.2 ([8, Chapter VI, Theorem 2.1])**.** *For all $P \in E(K) \setminus \{O\}$,*

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

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

$$\Psi_v(P) = \log \max\{1, |x(P)|_v\} - \lambda_v(P)$$

if $P \neq O$ and by $\Psi_v(O) = 0$. Then, by Proposition 3.2, the difference between the ordinary height and the canonical height is represented as follows:

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

Hence we obtain the bounds for $h - \hat{h}$ if we bound Ψ_v. Cremona et al. [2] determined the extrema of Ψ_v when v is non-Archimedean.

Proposition 3.3 ([2, Proposition 8]). *Let $v \in M_K^0$. Then,*

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

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

The author proved the following result including the case of Archimedean places.

Proposition 3.4. *Let $v \in M_K$ and $m \geq 2$ be an integer. Then, for all $P \in E(K_v)$,*

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

Theorem 2.1 follows from Propositions 3.3 and 3.4 immediately.

We can estimate the differences between the extrema of Ψ_v and $S_v(m)$, $T_v(m)$ by the following proposition and its corollaries.

Proposition 3.5. *Let $v \in M_K$ and $m \geq 2$ be an integer. Then,*

$$0 \leq \inf_{P \in E(K_v)} \Psi_v(P) - S_v(m) \leq \frac{c}{m^2 - 1},$$

$$0 \leq T_v(m) - \sup_{P \in E(K_v)} \Psi_v(P) \leq \frac{c}{m^2 - 1},$$

where

$$c = \sup_{P \in E(K_v)} \Psi_v(P) - \inf_{P \in E(K_v)} \Psi_v(P).$$

The following corollaries say that we can compute the extrema of Ψ_v with arbitrary precision.

Corollary 3.6.

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

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

Corollary 3.7. *Let $m \geq 2$ be an integer. Then,*

$$0 \leq \inf_{P \in E(K_v)} \Psi_v(P) - S_v(m) \leq c_m,$$

$$0 \leq T_v(m) - \sup_{P \in E(K_v)} \Psi_v(P) \leq c_m,$$

where

$$c_m = \frac{1}{m^2}\left(T_v(m) - S_v(m)\right).$$

Furthermore, we can prove the following proposition.

Proposition 3.8. *Let $m \geq 2$, $l \geq 1$ be integers. Then,*

$$S_v(m) \leq S_v(m^l), \quad T_v(m^l) \leq T_v(m),$$

i.e., the bounds in Theorem 2.1 become sharper when we change m to m^l.

Remark 3.9. By the proposition, we can obtain sharper bounds than those of [2] if we take $m = 2^l$ and $l \geq 2$.

Remark 3.10. There seems to be no relation between the bounds for m and m' generally. For example, it is not necessarily true that

$$S_v(m) \leq S_v(m'), \quad T_v(m') \leq T_v(m)$$

if m is a divisor of m'. We will show some counterexamples in Section 5.

4. 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 can use a method similar to that in [2, Section 7]. However, we need some changes as follows:

We define polynomials $f(x)$, $g(x)$, $p(x)$ by

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

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

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

Let

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

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

Then we can use the same method as that in [2, Section 7].

5. Examples. In order to compare our result with other results, we quickly review Silverman's bounds and Zimmer's bounds. Note that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$.

Theorem 5.1 (Silverman [7]). *For $x \in K$, we define*

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

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

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

Theorem 5.2 (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

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

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

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

This theorem follows from Proposition 5.18 a) and Theorem 5.35 c) in [5].

To compare the bounds in Theorem 2.1 with the ones we described above, we give some examples. PARI/GP [3] is used in the computation.

Example 5.3. Consider the elliptic curve over $\mathbf{Q}$:

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

This is taken from [2, Example 4]. Theorem 2.1 gives the following bounds.

$$-6.531924724 \leq h - \hat{h} \leq 0.4620981204 \quad (m = 2),$$
$$-5.228881425 \leq h - \hat{h} \leq 0.4620981204 \quad (m = 3),$$
$$-5.227187136 \leq h - \hat{h} \leq 0.4620981204 \quad (m = 4),$$
$$-5.006931796 \leq h - \hat{h} \leq 0.4620981204 \quad (m = 5).$$

Silverman's bounds are

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

and Zimmer's bounds are

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

We observe that the bounds in Theorem 2.1 are sharper than the other ones.

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

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

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

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

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

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

We observe that the bounds in Theorem 2.1 are very sharp.

We give counterexamples mentioned in Remark 3.10. These curves are taken from Cremona's Elliptic Curve Data [1].

Example 5.4. Consider the curve 37a1 over $\mathbf{Q}$ (cf. [1]):

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

Then, Theorem 2.1 gives

$$-0.48648 \leq h - \hat{h} \leq 0.12298 \quad (m = 3),$$
$$-0.46933 \leq h - \hat{h} \leq 0.12650 \quad (m = 6).$$

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

Example 5.5. Consider the curve 20888a1 over $\mathbf{Q}$ (cf. [1]):

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

Then, Theorem 2.1 gives

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

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

References

[1] J. E. Cremona, Elliptic Curve Data. http://www.maths.nott.ac.uk/personal/jec/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] PARI/GP, version 2.2.10, Bordeaux, 2005. `http://pari.math.u-bordeaux.fr/`.
[4] S. Siksek, Infinite descent on elliptic curves, Rocky Mountain J. Math. **25** (1995), no. 4, 1501–1538.
[5] S. Schmitt and H. G. Zimmer, *Elliptic curves*, de Gruyter, Berlin, 2003.
[6] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 1986.
[7] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, Math. Comp. **55** (1990), no. 192, 723–743.
[8] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, New York, 1994.
[9] Y. Uchida, The difference between the ordinary height and the canonical height on elliptic curves. (Preprint).
[10] H. G. Zimmer, On the difference of the Weil height and the Néron-Tate height, Math. Z. **147** (1976), no. 1, 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. **307/308** (1979), 221–246], J. Reine Angew. Math. **343** (1983), 203–211.