

## CANONICAL LOCAL HEIGHTS AND MULTIPLICATION FORMULAS FOR THE JACOBIANS OF CURVES OF GENUS 2

YUKIHIRO UCHIDA

### 1. INTRODUCTION

Let  $k$  be a number field. Let  $C$  be a curve of genus 2 over  $k$  defined by

$$Y^2 = F(X),$$

where  $\deg F = 6$ ,  $\text{disc}(F) \neq 0$  and  $F \in k[X]$ . Note that we cannot transform it into  $Y^2 = (\text{quintic})$  over  $k$  in general because  $k$  is not algebraically closed. Let  $J$  be the Jacobian of  $C$ . The set of all the  $k$ -rational points of  $J$  becomes a finitely generated Abelian group. It is called the Mordell-Weil group and denoted by  $J(k)$ . We use *height functions* to study this group. Height functions are functions from  $J(k)$  to  $\mathbb{R}$ . In this report, we consider two height functions:

- naive height  $h$ ,
- canonical height  $\hat{h}$ .

The definitions of these height are given in Section 4. It is known that there exist constants  $c_1$  and  $c_2$  such that

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

for all  $P \in J(k)$ . We need to compute  $c_2$  when we compute the generators of the Mordell-Weil group  $J(k)$ . Therefore it is important to compute the bounds  $c_1$  and  $c_2$ . We use *multiplication formulas* and *local height functions* to compute the bounds.

Note that the multiplication formulas given here is not on the Jacobians but on the Kummer surfaces associated with the Jacobians. For our purpose, it is sufficient to work on the Kummer surfaces.

Local height functions are functions defined for each place of  $k$  and height functions are decomposed to a weighted sum of local height functions.

This report is organized as follows: In Section 2, we review the basic facts of curves of genus 2 and their Jacobians. The multiplication formulas are given in Section 3. In Section 4, we describe height functions on the Jacobians of curves of genus 2. In Section 5, we define local height functions and describe several properties. In Section 6, we give the bounds for the difference  $h - \hat{h}$  by using multiplication formulas and local height functions.

The results in this report also hold for elliptic curves. See [10] and [11].

We cannot include detailed proofs in this report. For proofs, see [12]. In [12], we also discuss computing the canonical heights.

---

2000 *Mathematics Subject Classification*. Primary 11G50, Secondary 11G20, 11G30, 14H40.

## 2. CURVES OF GENUS 2 AND THEIR JACOBIANS

In this section, we review the basic facts described in [2].

We consider a curve of genus 2 over  $k$

$$C: Y^2 = F(X),$$

where

$$F(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 \in k[X]$$

is of degree 6 and has no multiple roots. We denote two points at infinity of  $C$  by  $\infty^+$  and  $\infty^-$ . The points  $\infty^+$  and  $\infty^-$  are defined over  $k$  or a quadratic extension of  $k$ .

Let  $J$  be the Jacobian of  $C$ .  $J$  is an Abelian surface over  $k$ . We can identify  $J$  with  $\text{Pic}^0(C)$  as a group. Let  $\Theta^+$ ,  $\Theta^-$  be the image of  $C$  in  $J$  via the embeddings

$$P \mapsto (P) - (\infty^+), \quad P \mapsto (P) - (\infty^-)$$

respectively. Note that  $\Theta^+$  and  $\Theta^-$  may not be defined over  $k$ . However,  $\Theta^+ + \Theta^-$  is defined over  $k$ .  $\Theta^+ + \Theta^-$  is linearly equivalent to  $2\Theta$ , where  $\Theta$  is a suitable theta divisor on  $J$ . By a theorem of Lefschetz ([7, Section 17, p. 163]),  $\Theta^+ + \Theta^-$  is base-point free, and  $2(\Theta^+ + \Theta^-)$  is very ample. Since  $l(\Theta^+ + \Theta^-) = l(2\Theta) = 4$ , we have a morphism  $\kappa: J \rightarrow \mathbb{P}^3$ . We call the image of  $\kappa$  the *Kummer surface*, and denote it by  $K$ . We write  $\kappa(P) = (\xi_1(P), \dots, \xi_4(P))$ . We define an involution  $\iota_J: J \rightarrow J$  by  $\iota_J(P) = -P$ . Then  $K$  is isomorphic to the quotient variety  $J/\iota_J$ . Note that  $K$  has 16 singular points corresponding to elements of order 2 on  $J$ . We need not to resolve these singular points here.

The defining equation of  $K$  is given by

$$G(\xi_1, \dots, \xi_4) = R\xi_4^2 + S\xi_4 + T = 0,$$

where  $R, S, T$  are homogeneous polynomials of degree 2, 3, 4 respectively. Hence  $G$  is a homogeneous polynomial of degree 4. Furthermore,  $G$  has coefficients in  $\mathbb{Z}[f_0, \dots, f_6]$ . Explicit descriptions of  $\kappa$  and  $K$  are given in [2, Chapter 3].

We denote the multiplication-by- $m$  map on  $J$  by  $[m]$ . Since  $[m](-P) = -([m]P)$ ,  $[m]$  induces a morphism on  $K$ . We denote the morphism on  $K$  induced by the duplication map by  $\delta = (\delta_1, \dots, \delta_4)$ , that is,  $\kappa([2]P) = \delta(\kappa(P))$ . Explicit formulas for  $\delta_i$  are available at [13].

We cannot recover  $\kappa(P + Q)$  from only  $\kappa(P)$  and  $\kappa(Q)$  because  $P$  and  $-P$  are identified through  $\kappa$ . However, we can obtain an unordered pair  $(\kappa(P+Q), \kappa(P-Q))$  from  $\kappa(P)$  and  $\kappa(Q)$ . Precisely, we have the following result:

**Proposition 2.1** ([2, Theorem 3.4.1]). *There are polynomials  $B_{ij}$  biquadratic in the  $\xi_i(P), \xi_i(Q)$  such that*

$$(1) \quad (\xi_i(P+Q)\xi_j(P-Q) + \xi_j(P+Q)\xi_i(P-Q)) = (2B_{ij}(\kappa(P), \kappa(Q)))$$

*as projective coordinates. Furthermore,  $B_{ij}$  have coefficients in  $\mathbb{Z}[f_0, \dots, f_6]$ .*

Explicit formulas for  $B_{ij}$  are also available at [13].

## 3. MULTIPLICATION FORMULAS

The following theorem gives the multiplication formulas on the Kummer surface  $K$ .

**Theorem 3.1.** *There exist homogeneous polynomials  $\mu_{m,i} \in k[\xi_1, \dots, \xi_4]$  ( $m \geq 0, i = 1, 2, 3, 4$ ) such that the following conditions are satisfied:*

(i) *We have*

$$\begin{aligned} \mu_{0,1} &= \mu_{0,2} = \mu_{0,3} = 0, \mu_{0,4} = 1, \\ \mu_{1,i} &= \xi_i, \\ (2) \quad \mu_{2m,i} &= \delta_i(\mu_m) \quad (m \geq 1), \\ (3) \quad \mu_{2m+1,i}\xi_i &= B_{ii}(\mu_{m+1}, \mu_m) \quad (m \geq 1) \end{aligned}$$

*in  $k[\xi_1, \dots, \xi_4]/\langle G \rangle$ , where  $\mu_m = (\mu_{m,1}, \dots, \mu_{m,4})$  and  $G$  is the ideal generated by the polynomial  $G$ .*

(ii) *Let  $\bar{k}$  be the algebraic closure of  $k$ . For all  $P \in J(\bar{k})$ , we have*

$$\kappa([m]P) = (\mu_{m,1}(\kappa(P)), \dots, \mu_{m,4}(\kappa(P))).$$

*Furthermore, the polynomials  $\mu_{m,i}$  are uniquely determined modulo  $G$ .*

**Remark 3.2.** In the case  $\deg(F) = 5$ , Kanayama [5] wrote down the multiplication formulas on the Jacobian  $J$ . He used hyperelliptic  $\wp$ -functions.

**Remark 3.3.** We can compute  $\mu_{m,i}$  inductively.  $\mu_{0,i}$  and  $\mu_{1,i}$  are defined obviously.  $\mu_{2m,i}$  is computed by (2).  $\mu_{2m+1,i}$  satisfies (3), that is, there exists a homogeneous polynomial  $p$  such that

$$(4) \quad \mu_{2m+1,i}\xi_i + pG = B_{ii}(\mu_{m+1}, \mu_m).$$

Such  $\mu_{2m+1,i}$  can be computed by using Gröbner basis (see [1, § 5.6]). We can also compute them by the following elementary operations. In (4), we can assume  $p$  does not contain the variable  $\xi_i$  by replacing  $\mu_{2m+1,i}$  if necessary. We substitute 0 for  $\xi_i$  in (4). Then we have  $pG_i = b_i$ , where  $G_i$  (resp.  $b_i$ ) is the polynomial obtained by substituting 0 for  $\xi_i$  in  $G$  (resp.  $B_{ii}(\mu_{m+1}, \mu_m)$ ). Hence we can calculate  $p = b_i/G_i$  and  $\mu_{2m+1,i} = (b_i - pG)/\xi_i$ .

We describe some properties of  $\mu_{m,i}$ .

**Proposition 3.4.** *For all  $m \geq 0$  and  $i = 1, 2, 3, 4$ , we can choose  $\mu_{m,i}$  such that  $\mu_{m,i}$  has coefficients in  $\mathbb{Z}[f_0, \dots, f_6]$ .*

**Lemma 3.5.** *For all  $m \geq 0$  and  $i = 1, 2, 3, 4$ ,  $\mu_{m,i}$  has degree  $m^2$ .*

**Lemma 3.6.** *Let  $O = (0, 0, 0, 1)$ . Then we have*

$$\mu_{m,1}(O) = \mu_{m,2}(O) = \mu_{m,3}(O) = 0, \mu_{m,4}(O) = 1$$

*for all  $m \geq 0$ .*

**Proposition 3.7.** *We have*

$$\mu_{m+n,i}\mu_{m-n,j} + \mu_{m+n,j}\mu_{m-n,i} = 2B_{ij}(\mu_m, \mu_n)$$

*in  $k[\xi_1, \dots, \xi_4]/\langle G \rangle$  for all  $m, n \geq 0$  such that  $m \geq n$  and for  $i, j = 1, 2, 3, 4$ .*

## 4. HEIGHT FUNCTIONS

Let  $M_k$  be the set of absolute values which extend the  $p$ -adic absolute values or the ordinary absolute value on  $\mathbb{Q}$ .  $M_k$  is naturally identified with the set of places on  $k$ . For  $v \in M_k$ , we denote the completion of  $k$  at  $v$  by  $k_v$ . Let  $n_v = [k_v : \mathbb{Q}_v]$ .

We describe the elements in  $M_k$  closely.

First, let  $v \in M_k$  be an Archimedean absolute value. There is an embedding  $\sigma : k \rightarrow \mathbb{C}$  such that

$$|x|_v = |\sigma(x)|$$

for any  $x \in k$ , where the absolute value in the right-hand side is the ordinary absolute value on  $\mathbb{C}$ . If  $k_v$  is isomorphic to  $\mathbb{R}$ , then the embedding  $\sigma$  is uniquely determined. If  $k_v$  is isomorphic to  $\mathbb{C}$ , then the embedding  $\sigma$  is determined up to complex conjugates.

Next, let  $v \in M_k$  be a non-Archimedean absolute value. Let  $\mathcal{O}_v$  be the ring of integers of  $k_v$  and  $\pi_v$  be a uniformizer of  $\mathcal{O}_v$ . We define  $\text{ord}_v : k_v^\times \rightarrow \mathbb{Z}$  by

$$\text{ord}_v(a\pi_v^n) = n, \quad a \in \mathcal{O}_v^\times.$$

Let  $q_v$  be the cardinality of the residue field  $\mathcal{O}_v/\pi_v\mathcal{O}_v$ . Then we have

$$|x|_v = q_v^{-\text{ord}_v(x)/n_v}$$

for all  $x \in k^\times$ .

We have the product formula:

$$\sum_{v \in M_k} n_v \log |x|_v = 0$$

for all  $x \in k^\times$ .

We define the *naive height function*  $h : J(k) \rightarrow \mathbb{R}$  by

$$h(P) = \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} n_v \log \max_{1 \leq i \leq 4} |\xi_i(P)|_v.$$

$h(P)$  is independent of the choice of the homogeneous coordinates  $(\xi_1(P), \dots, \xi_4(P))$ .

We define the *canonical height function*  $\hat{h} : J(k) \rightarrow \mathbb{R}$  by

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

The right-hand side converges by general theory (see for instance [4, Theorem B.4.1]).

The canonical height function has a good property with respect to the addition.

**Theorem 4.1** (Parallelogram law). *Let  $P, Q \in J(k)$ . We have*

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

*In particular, for any integer  $m$ ,*

$$\hat{h}([m]P) = m^2\hat{h}(P).$$

## 5. LOCAL HEIGHT FUNCTIONS

In this section, we describe local height functions on the Jacobians of curves of genus 2. Our definitions of local height functions are the almost same as those of Flynn-Smart [3]. We consider the  $v$ -adic topology in the rest of this report.

We define divisors  $\Theta_i$  on  $J$  by

$$\Theta_1 = \Theta^+ + \Theta^-, \quad \Theta_i = \Theta_1 + \operatorname{div} \left( \frac{\xi_i}{\xi_1} \right) \quad (i = 2, 3, 4).$$

Note that  $P \in \operatorname{supp}(\Theta_i)$  if and only if  $\xi_i(P) = 0$ .

For  $v \in M_k$ , we define *naive local height functions*  $\lambda_{i,v}: J(k_v) \setminus \operatorname{supp}(\Theta_i) \rightarrow \mathbb{R}$  by

$$\lambda_{i,v}(P) = \log \max_{1 \leq j \leq 4} \left| \frac{\xi_j(P)}{\xi_i(P)} \right|_v.$$

$\lambda_{i,v}$  is independent of the choice of homogeneous coordinates for  $\kappa(P)$ . We have

$$\lambda_{i,v}(P) = \lambda_{j,v}(P) - \log \left| \frac{\xi_i(P)}{\xi_j(P)} \right|_v$$

for any  $P \notin \operatorname{supp}(\Theta_i) \cup \operatorname{supp}(\Theta_j)$ .

To construct canonical local height functions, we define a function  $\Phi_v: J(k_v) \rightarrow \mathbb{R}$  by

$$\Phi_v(P) = \frac{\max_i |\delta_i(\kappa(P))|_v}{\max_i |\xi_i(P)|_v^4}.$$

The right-hand side is independent of the choice of homogeneous coordinates for  $\kappa(P)$  since  $\delta_i$  are homogeneous polynomials of degree 4. We can show that  $\log \Phi_v$  is bounded and continuous on  $J(k_v)$ . Hence we can define functions  $\hat{\lambda}_{i,v}: J(k_v) \setminus \operatorname{supp}(\Theta_i) \rightarrow \mathbb{R}$  by

$$\hat{\lambda}_{i,v}(P) = \lambda_{i,v}(P) + \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

We call them *canonical local height functions* on  $J$ . By definition, we have

$$\hat{\lambda}_{i,v}(P) = \hat{\lambda}_{j,v}(P) - \log \left| \frac{\xi_i(P)}{\xi_j(P)} \right|_v$$

for any  $P \notin \operatorname{supp}(\Theta_i) \cup \operatorname{supp}(\Theta_j)$ .

As in the case of elliptic curves, we have the quasi-parallelogram law.

**Theorem 5.1** (Quasi-parallelogram law). *Let  $P, Q \in J(k_v)$ . If  $P, Q, P+Q, P-Q \notin \operatorname{supp}(\Theta_i)$ , then*

$$\hat{\lambda}_{i,v}(P+Q) + \hat{\lambda}_{i,v}(P-Q) = 2\hat{\lambda}_{i,v}(P) + 2\hat{\lambda}_{i,v}(Q) - \log \left| \frac{B_{ii}(\kappa(P), \kappa(Q))}{\xi_i(P)^2 \xi_i(Q)^2} \right|_v.$$

**Corollary 5.2.** *Let  $P \in J(k_v)$  and  $m > 0$  be an integer. If  $P \notin \operatorname{supp}(\Theta_i)$  and  $[m]P \notin \operatorname{supp}(\Theta_j)$ , then*

$$\hat{\lambda}_{j,v}([m]P) = m^2 \hat{\lambda}_{i,v}(P) - \log \left| \frac{\mu_{m,j}(\kappa(P))}{\xi_i(P)^{m^2}} \right|_v.$$

**Corollary 5.3.** *Let  $m \geq 2$  be an integer. Define a function  $\Phi_{m,v}: J(k_v) \rightarrow \mathbb{R}$  by*

$$\Phi_{m,v}(P) = \frac{\max_{1 \leq i \leq 4} |\mu_{m,i}(\kappa(P))|_v}{\max_{1 \leq i \leq 4} |\xi_i(P)|_v^{m^2}}.$$

Then,

$$\hat{\lambda}_{i,v}(P) = \lambda_{i,v}(P) + \sum_{n=0}^{\infty} \frac{1}{m^{2(n+1)}} \log \Phi_{m,v}([m^n]P)$$

for  $P \in J(k_v) \setminus \text{supp}(\Theta_i)$ .

We consider a relation between global height functions and local height functions. We can decompose these height functions into local height functions.

**Theorem 5.4.** *Let  $P \in J(k) \setminus \text{supp}(\Theta_i)$ . Then,*

$$h(P) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \lambda_{i,v}(P),$$

$$\hat{h}(P) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \hat{\lambda}_{i,v}(P).$$

## 6. APPLICATION: HEIGHT DIFFERENCE BOUNDS

By general theory, it is known that there exists constants  $c_1$  and  $c_2$  such that

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

for all  $P \in J(k)$ . It is important to estimate the bounds  $c_1$  and  $c_2$  effectively. We consider this problem in this section.

Let  $\mathcal{O}_k$  be the ring of integers of  $k$ . We assume that the coefficients  $f_0, \dots, f_6$  belong to  $\mathcal{O}_k$ .

We define a function  $\Psi_v: J(k_v) \rightarrow \mathbb{R}$  by

$$\Psi_v(P) = - \sum_{n=0}^{\infty} \frac{1}{4^{(n+1)}} \log \Phi_v([2^n]P).$$

By definition, we have

$$\lambda_{i,v}(P) - \hat{\lambda}_{i,v}(P) = \Psi_v(P)$$

for all  $P \in J(k_v) \setminus \text{supp}(\Theta_i)$ . Since  $\log \Phi_v$  is bounded and continuous, by Weierstrass  $M$ -test,  $\Psi_v$  is bounded and continuous on  $J(k_v)$  (we consider the  $v$ -adic topology). Furthermore,  $\Psi_v$  has the maximum and the minimum since  $J(k_v)$  is compact. By Theorem 5.4, we have

$$(5) \quad \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} [k_v:\mathbb{Q}_v] \inf_{Q \in J(k_v)} \Psi_v(Q) \leq h(P) - \hat{h}(P) \\ \leq \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} [k_v:\mathbb{Q}_v] \sup_{Q \in J(k_v)} \Psi_v(Q)$$

for all  $P \in J(k)$ . By the assumption that  $f_0, \dots, f_6 \in \mathcal{O}_k$ , we have

$$\sup_{Q \in J(k_v)} \Phi_v(Q) = 1$$

if  $v$  is non-Archimedean (see [3, Lemma 3] or [8, p. 189, the second remark]). Hence we have

$$\inf_{Q \in J(k_v)} \Psi_v(Q) = 0.$$

Therefore the left-hand side of (5) is a finite sum.

For the infimum of  $\Phi_v$ , the following result is known.

**Theorem 6.1** ([8, Theorem 6.1]). *Under the above assumption, if  $v \in M_k$  is non-Archimedean, then*

$$\inf_{Q \in J(k_v)} \Phi_v(Q) \geq |2^4 \operatorname{disc}(F)|_v,$$

where  $\operatorname{disc}(F)$  is the discriminant of  $F$ .

By Theorem 6.1, if  $|2^4 \operatorname{disc}(F)|_v = 1$ , then

$$\inf_{Q \in J(k_v)} \Phi_v(Q) = 1.$$

Therefore the right-hand side of (5) is a finite sum. In [8] and [9], further improvements for non-Archimedean absolute values are described.

From now on, we mainly consider Archimedean absolute values although the following results also hold for non-Archimedean absolute values.

By Corollary 5.3, we have

$$\Psi_v(P) = - \sum_{n=0}^{\infty} \frac{1}{m^{2(n+1)}} \log \Phi_{m,v}([m^n]P)$$

for all  $P \in J(k_v)$ . We define

$$\varepsilon_{m,v}^{-1} = \inf_{Q \in J(k_v)} \Phi_{m,v}(Q), \quad \delta_{m,v}^{-1} = \sup_{Q \in J(k_v)} \Phi_{m,v}(Q).$$

Let

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

Then we have the following proposition:

**Proposition 6.2.** *Let  $v \in M_k$  and  $m \geq 2$  be an integer. Then, for all  $P \in J(k_v)$ ,*

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

*Remark 6.3.* This proposition also holds for elliptic curves. See [10, Proposition 3.4].

**Corollary 6.4.** *Let  $m \geq 2$  be an integer. Then*

$$\frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} n_v S_v(m) \leq h(P) - \hat{h}(P) \leq \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} n_v T_v(m)$$

for all  $P \in J(k)$ .

We have the following results for  $S_v(m)$  and  $T_v(m)$ . The same holds for elliptic curves (see [10]). The proofs of them are the same as those in [11].

**Proposition 6.5.** *Let  $m \geq 2$ ,  $l \geq 1$  be integers. Then,*

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

that is, the bounds in Proposition 6.2 become sharper when we change  $m$  to  $m^l$ .

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

**Proposition 6.6.** *Let  $m \geq 2$  be an integer. Then,*

$$0 \leq \inf_{P \in E(k_v)} \Psi_v(P) - S_v(m) \leq \frac{1}{m^2 - 1} \left( \sup_{P \in E(k_v)} \Psi_v(P) - \inf_{P \in E(k_v)} \Psi_v(P) \right),$$

$$0 \leq T_v(m) - \sup_{P \in E(k_v)} \Psi_v(P) \leq \frac{1}{m^2 - 1} \left( \sup_{P \in E(k_v)} \Psi_v(P) - \inf_{P \in E(k_v)} \Psi_v(P) \right).$$

**Corollary 6.7.**

$$\lim_{m \rightarrow \infty} S_v(m) = \inf_{P \in E(k_v)} \Psi_v(P), \quad \lim_{m \rightarrow \infty} T_v(m) = \sup_{P \in E(k_v)} \Psi_v(P).$$

We can estimate the difference between the theoretical bounds and the bounds in Proposition 6.2 by the following corollary.

**Corollary 6.8.**

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

$$0 \leq T_v(m) - \sup_{P \in E(k_v)} \Psi_v(P) \leq \frac{1}{m^2} (T_v(m) - S_v(m)).$$

As described above, we can estimate  $\Psi_v$  with arbitrary accuracy at least theoretically. However, actual computations are quite difficult because the size of  $\mu_{m,i}$  increases rapidly.

#### REFERENCES

- [1] T. Becker, V. Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics 141, Springer-Verlag, 1993.
- [2] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of genus 2*, Cambridge University Press, Cambridge, 1996.
- [3] E. V. Flynn, N. P. Smart, Canonical heights on the Jacobians of curves of genus 2 and the infinite descent, *Acta Arith.* **89** (1997) 333–352.
- [4] M. Hindry, J. H. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics 201, Springer-Verlag, 2000.
- [5] N. Kanayama, Division polynomials and multiplication formulae of Jacobian varieties of dimension 2, *Math. Proc. Cambridge Philos. Soc.* **139** (2005) 399–409.
- [6] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.
- [7] D. Mumford, *Abelian Varieties*, 2nd edition, Oxford University Press, 1974.
- [8] M. Stoll, On the height constant for curves of genus two, *Acta Arith.* **90** (1999) 183–201.
- [9] M. Stoll, On the height constant for curves of genus two II, *Acta Arith.* **104** (2002) 165–182.
- [10] Y. Uchida, On the difference between the ordinary height and the canonical height on elliptic curves. *Proc. Japan Acad. Ser. A Math. Sci.*, **82**, no. 3, (2006) 56–60.
- [11] Y. Uchida, The difference between the ordinary height and the canonical height on elliptic curves, (Preprint).
- [12] Y. Uchida, Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2, (Preprint).
- [13] Kummer surface formulas, <ftp://ftp.liv.ac.uk/pub/genus2/>.

GRADUATE SCHOOL OF MATHEMATICS, NAGOYA UNIVERSITY, CHIKUSA-KU, NAGOYA 464-8602 JAPAN

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