Math. Proc. Camb. Phil. Soc. (2014), **157**, 357–373
doi:10.1017/S0305004114000371
First published online 14 August 2014

Canonical heights and division polynomials

BY ROBIN DE JONG

Mathematisch Instituut, Universiteit Leiden,
PO Box 9512, 2300 *RA Leiden, The Netherlands.*
e-mail: rdejong@math.leidenuniv.nl

AND J. STEFFEN MÜLLER

Institut für Mathematik, Carl von Ossietzky Universität Oldenburg,
26111 *Oldenburg, Germany.*
e-mail: jan.steffen.mueller@uni-oldenburg.de

(*Received* 26 *June* 2013; *revised* 26 *June* 2014)

Abstract

We discuss a new method to compute the canonical height of an algebraic point on a hyperelliptic jacobian over a number field. The method does not require any geometrical models, neither p-adic nor complex analytic ones. In the case of genus 2 we also present a version that requires no factorisation at all. The method is based on a recurrence relation for the 'division polynomials' associated to hyperelliptic jacobians, and a diophantine approximation result due to Faltings.

1. *Introduction*

In [**3**] G. Everest and T. Ward show how to approximate to high precision the canonical height of an algebraic point on an elliptic curve E over a number field K with a limit formula using the (recurrence) sequence of *division polynomials* ϕ_n associated to E, and a diophantine approximation result.

The ϕ_n have natural analogues for jacobians of hyperelliptic curves. In [**18**] Y. Uchida shows how to obtain recurrence relations for the ϕ_n for hyperelliptic jacobians of dimension $g \geqslant 2$. Further there exists a suitable analogue of the diophantine approximation result employed by Everest and Ward, proved by G. Faltings [**4**]. In this paper we derive a limit formula for the canonical height of an algebraic point on a hyperelliptic jacobian from these inputs.

We have implemented the resulting method for computing canonical heights in `Magma` for $g = 2$. The method does not require geometrical models, neither p-adic nor complex analytic ones. If the curve is defined over $\mathbb{Q}$ and the coordinates of the point are integral, then it also requires no factorisation. It does need either large integer arithmetic or large p-adic and real precision, however. In principle the implementation can be extended to higher genera.

2. *Statement of the main results*

Let K be a number field with ring of integers $\mathcal{O}_K$ and let (X, o) be a pointed hyperelliptic curve of genus $g \geqslant 2$ over K given by an equation $y^2 = f(x)$ with $f \in \mathcal{O}_K[x]$ monic of odd degree $2g+1$, where o is the unique point at infinity. Let J denote the jacobian variety of X. Then the theta divisor Θ on J is the reduced and irreducible divisor on J whose support is given by the set of all points which can be represented by a divisor $(p_1) + \cdots + (p_d) - d(o)$, where all $p_i \in X$ and $d < g$. Equivalently, these are precisely the points whose reduced Mumford representation $(a(x), b(x))$ (cf. Section 5) satisfies $\deg(a) < g$.

For each integer $n \geqslant 1$ there exists a canonical 'division polynomial' ϕ_n in the function field of J over K, see Section 5. We have

$$\operatorname{div} \phi_n = [n]^*\Theta - n^2\Theta\,.$$

For each place v of K we further have a canonical local height function $\widehat{\lambda}_v$, see [**18**, section 7]. These functions are determined by the key relations:

$$\log |\phi_n(p)|_v = -\widehat{\lambda}_v(np) + n^2\widehat{\lambda}_v(p)$$

for each integer $n \geqslant 1$, each place v and generic $p \in J(K_v)$, where $|\cdot|_v$ is the absolute value on K_v, normalized as in Subsection 3·2.

Let p be a point in $J(K)$, not in $\operatorname{supp}(\Theta)$. Let $\widehat{h}\colon J(K) \to \mathbb{R}$ be the canonical height with respect to the canonical principal polarization on J. We have the formula:

$$[K:\mathbb{Q}]\,\widehat{h}(p) = \sum_v n_v\,\widehat{\lambda}_v(p)\,,$$

where n_v is a standard local factor defined in Subsection 3·2. Put

$$T(p) = \{n \in \mathbb{Z}_{>0} \mid np \notin \operatorname{supp}(\Theta)\}.$$

Then one can show that $T(p)$ is an infinite set.

Our first result extends [**3**, theorem 3] and gives a limit formula for the canonical local height $\widehat{\lambda}_v$ in terms of the division polynomials. The proof is based on a diophantine approximation result due to Faltings (Theorem 4·1).

THEOREM 2·1. *Let v be any place of K and let $p \in J(K) \setminus \operatorname{supp}(\Theta)$ be a rational point. Then $T(p)$ is an infinite set and the formula*

$$\widehat{\lambda}_v(p) = \lim_{\substack{n\to\infty \\ n\in T(p)}} \frac{1}{n^2} \log |\phi_n(p)|_v$$

holds.

Let S be a finite set of places of K. We put:

$$\widehat{h}_S(p) = \frac{1}{[K:\mathbb{Q}]} \lim_{\substack{n\to\infty \\ n\in T(p)}} \frac{1}{n^2} \log \prod_{v\in S} |\phi_n(p)|_v^{n_v}\,.$$

Theorem 2·1 implies that the limit $\widehat{h}_S(p)$ exists, and gives the S-part of the canonical height of p.

THEOREM 2·2. *Assume that p is a point in $J(K)$, not in* $\mathrm{supp}(\Theta)$. *Then the limit $\widehat{h}_S(p)$ exists, and the formula*

$$[K:\mathbb{Q}]\,\widehat{h}_S(p) = \sum_{v\in S} n_v\,\widehat{\lambda}_v(p)$$

holds.

Our next result expresses $\widehat{h}(p)$ in terms of $\widehat{h}_S(p)$ and $\widehat{h}_S(2p)$, for a suitable set S. Let $\Delta = 2^{4g}\mathrm{disc}(f)$ denote the discriminant of X. Then the curve X, and hence the jacobian J, has good reduction outside the set S_{bad} of places of K dividing the ideal (Δ). Let S_∞ be the set of archimedean places of K.

THEOREM 2·3. *Let $p \in J(K)$ and assume that both p and $2p$ are not in* $\mathrm{supp}(\Theta)$. *Let S be a finite set of places of K containing $S_{\mathrm{bad}} \cup S_\infty$, such that for all $v \notin S$ one has that neither p nor $2p$ lies on the theta divisor modulo v. Then the formula*

$$\widehat{h}(p) = -\frac{1}{3}\widehat{h}_S(p) + \frac{1}{3}\widehat{h}_S(2p)$$

holds.

Note that, for a finite place v outside S_{bad}, saying that p lies on the theta divisor modulo v is equivalent to saying that p can be represented by a divisor $(p_1)+\cdots+(p_g)-g(o)$, where one of the p_i reduces to o modulo v, or that one of the coefficients of the first polynomial in the Mumford representation of p is not v-integral. We will see that $\widehat{h}_S(p)$ and $\widehat{h}_S(2p)$ are effectively computable for S and p as in Theorem 2·3.

For $g = 2$ we can prove a simpler version of Theorem 2·3.

THEOREM 2·4. *Suppose that $g = 2$ and that $p \in J(K) \setminus \mathrm{supp}(\Theta)$. Let S be a finite set of places of K containing $\{v \in S_{\mathrm{bad}} : \mathrm{ord}_v(\Delta) \geqslant 2\} \cup S_\infty$ such that for all $v \notin S$ the point p does not lie on the theta divisor modulo v. Then we have*

$$\widehat{h}(p) = \widehat{h}_S(p).$$

For the proof of Theorem 2·4, we compare the canonical local height $\widehat{\lambda}_v$ to a canonical local height associated with 2Θ introduced by V. Flynn and N. Smart in [**5**].

The plan of this paper is as follows. Section 3 contains some basic results around canonical local heights on abelian varieties. In Section 4 we recall Faltings's diophantine approximation result and deduce a general limit formula from it. After this we focus on hyperelliptic jacobians. First, in Section 5 we review some facts we need from Uchida's paper [**18**] on hyperelliptic division polynomials.

Then in Sections 6 and 7 we prove Theorems 2·1–2·4. Note that, in principle, these results allow one to approximate values of $\widehat{h}(p)$ effectively. There are two issues to be dealt with. One is the possible occurrence of large 'gaps' in the sets $T(p)$, another is the need to factor the discriminant in order to apply Theorem 2·3. We discuss, and resolve to some extent, both issues in Section 8. In particular we can control the gaps and present a factorisation-free approach to computing $\widehat{h}(p)$ in the genus 2 case, adapting an approach described in [**3**] for the elliptic curves case.

In Section 9 we discuss the actual implementation of our method in `Magma`, and compare our method with earlier ones due to Flynn and Smart [**5**], M. Stoll [**15**], Uchida [**17**], D. Holmes [**6**] and the second author [**12**]. We finish the paper by presenting and analysing some

data in Section 10. In particular we note that assembling enough data may yield predictions on the general convergence rate of our limit formulas.

3. *Canonical local heights*

3·1. *Local theory*

We start with some well-known generalities on canonical local heights on abelian varieties. See for instance, [**10**, chapter 11].

Definition 1. Let A be an abelian variety defined over a local field K with absolute value $|\cdot|$. To each divisor D on A one can associate a function $\lambda_D : A(K) \setminus \operatorname{supp}(D) \to \mathbb{R}$ such that the following conditions are satisfied:

(i) if $D, E \in \operatorname{Div}(A)$, then $\lambda_{D+E} = \lambda_D + \lambda_E + c_1$ for some $c_1 \in \mathbb{R}$;
(ii) if $D = \operatorname{div}(f) \in \operatorname{Div}(A)$ is principal, then $\lambda_D = -\log|f| + c_2$ for some $c_2 \in \mathbb{R}$;
(iii) if $\varphi : A \to A'$ is a morphism of abelian varieties and $D \in \operatorname{Div}(A')$, then we have $\lambda_{\varphi^*(D)} = \lambda_D \circ \varphi + c_3$ for some $c_3 \in \mathbb{R}$.

We call λ_D a *canonical local height (or Néron function) associated with* D.

Given a divisor D on an abelian variety A defined over a local field K, a canonical local height λ_D associated with D is uniquely determined up to a constant. In particular, if λ_D is a canonical local height associated to a symmetric divisor D on A, then by [**10**, proposition 11·1·4], there exists a function $\phi \in K(A)^\times$ such that $\operatorname{div}(\phi) = [2]^*D - 4D$ and

$$\lambda_D(2p) - 4\lambda_D(p) = -\log|\phi(p)|$$

for all $p \in A(K)$ such that both p and $2p$ do not lie in $\operatorname{supp}(D)$. The function ϕ is determined up to a constant factor in $K^\times$ and λ_D is uniquely determined by ϕ.

Assume now that K is non-archimedean and let A be an abelian variety over K. In this case canonical local heights can be related to the Néron model $\mathcal{A}$ of A over the ring of integers $\mathcal{O}_K$ of K. For $D \in \operatorname{Div}(A)$ and $p \in A(K)$ let $\overline{D}$ (resp. $\overline{p}$) denote the Zariski closure of D with multiplicities (resp. of the divisor (p)) in $\mathcal{A}$ and let λ_D denote a canonical local height associated with D. Let v denote the closed point of $\operatorname{Spec}(\mathcal{O}_K)$ and let $i_v(D, p)$ denote the intersection multiplicity of $\overline{D}$ and $\overline{p}$ as defined in [**10**, section 11·5].

PROPOSITION 3·1 (Néron, *cf.* [**10**, section 11·5]).

(i) *If $\mathcal{A}_v$ is connected, then $i_v(D, p)$ is the usual intersection multiplicity of $\overline{D}$ and $\overline{p}$ on $\mathcal{A}_v$.*
(ii) *If $\overline{D}$ is represented by $\alpha \in K(\mathcal{A})$ around $\overline{p} \cap \mathcal{A}_v$, then we have*

$$i_v(D, p) = -\log|\alpha(p)|.$$

(iii) *For each component $\mathcal{C}$ of the special fiber of $\mathcal{A}$ there is a constant $\gamma(\mathcal{C}) \in \mathbb{R}$ such that for all $p \in A(K) \setminus \operatorname{supp}(D)$ reducing to $\mathcal{C}$ we have*

$$\lambda_D(p) = i_v(D, p) + \gamma(\mathcal{C}).$$

3·2. *Global theory*

Let K be a number field. There is a standard way of endowing each completion K_v with an absolute value $|\cdot|_v$, as follows: when v is archimedean, we take the euclidean norm

on K_v. When v is non-archimedean, we normalize $|\cdot|_v$ such that $|\pi|_v = \mathrm{e}^{-1}$, where π is a uniformiser of K_v. Now let M_K be the set of places of K. For each $v \in M_K$ let n_v be the local factor defined as follows: when v is real, then put $n_v = 1$; when v is complex, then put $n_v = 2$; finally if v is non-archimedean, then n_v is the logarithm of the cardinality of the residue field at v. Then we have the product formula $\sum_{v \in M_K} n_v \log |x|_v = 0$ valid for all x in $K^\times$.

The connection between canonical heights and canonical local heights is provided by the following result, again due to Néron:

PROPOSITION 3·2 (Néron). *Let A be an abelian variety over K and let $D \in \mathrm{Div}(A)$ be symmetric. Let $\phi \in K(A)$ such that $\mathrm{div}(\phi) = [2]^* D - 4D$. For each place $v \in M_K$ we let λ_v denote the canonical local height associated with D on $A(K_v)$ which satisfies*

$$\lambda_v(2p) - 4\lambda_v(p) = -\log|\phi(p)|_v$$

for all $p \in A(K_v)$ such that p and $2p$ are not in $\mathrm{supp}(D)$. Then we have

$$[K:\mathbb{Q}]\,\widehat{h}_D(p) = \sum_v n_v\,\lambda_v(p)$$

for all $p \in A(K) \setminus \mathrm{supp}(D)$, where $\widehat{h}_D$ is the canonical height associated to D.

4. *Faltings's result and an application*

The following general diophantine approximation result due to G. Faltings (see [**4**, theorem II]) will be the main ingredient of our method.

THEOREM 4·1. *Let A be an abelian variety over a number field K and suppose that D is an ample divisor on A. Let v be a place of K and let $\lambda_{D,v}$ be a canonical local height function on $A(K_v)$ with respect to D. Let h be a Weil height on A associated to some ample line bundle on A, and let $k \in \mathbb{R}_{>0}$ be arbitrary. Then there exist only finitely many points $p \in A(K) \setminus \mathrm{supp}(D)$ such that $\lambda_{D,v}(p) > k \cdot h(p)$.*

In fact we will use the following corollary.

THEOREM 4·2. *Let A be an abelian variety over a number field K and let D be a symmetric ample divisor on A. Let v be a place of K and let $\lambda_{D,v}$ be a canonical local height function on $A(K_v)$ with respect to D. Let $p \in A(K) \setminus \mathrm{supp}(D)$ be a rational point and put $T(D, p) = \{n \in \mathbb{Z}_{>0} \mid np \notin \mathrm{supp}(D)\}$. Then $T(D, p)$ is infinite and we have $\lambda_{D,v}(np)/n^2 \to 0$ as $n \to \infty$ over $T(D, p)$.*

Proof. We start by showing that $T(D, p)$ is infinite when $p \notin \mathrm{supp}(D)$. For p a torsion point this is immediate. Assume therefore that p is not torsion. We prove that for infinitely many $n \in \mathbb{Z}$ we have $np \notin \mathrm{supp}(D)$. This is sufficient for our purposes: as D is symmetric, we have $np \in \mathrm{supp}(D)$ if and only if $-np \in \mathrm{supp}(D)$. An elementary argument on algebraic groups shows that the Zariski closure Z of the subgroup $\mathbb{Z} \cdot p$ is a closed algebraic subgroup of A. Suppose that only finitely many of the np are outside $\mathrm{supp}(D)$. Then Z is the union of a finite set with a closed subset of $\mathrm{supp}(D)$. It follows that Z has dimension zero, and hence consists of only finitely many points: contradiction.

The limit formula follows immediately if p is torsion since then the set of values $\lambda_{D,v}(np)$ as n ranges over $T(D, p)$ is bounded. Assume therefore that p is not torsion. Then the np

with n running through $T(D, p)$ form an infinite set of K-rational points of $A \setminus \operatorname{supp}(D)$. Let $\widehat{h}$ be the canonical height with respect to D. Since:

$$\frac{\lambda_{D,v}(np)}{n^2} = \widehat{h}(p) \cdot \frac{\lambda_{D,v}(np)}{\widehat{h}(np)},$$

where $\widehat{h}(p) > 0$, Theorem 4·1 can be applied, leading to:

$$\limsup_{\substack{n\to\infty \\ n\in T(D,p)}} \frac{\lambda_{D,v}(np)}{n^2} \leqslant 0.$$

On the other hand, since $\lambda_{D,v}$ is bounded from below we have:

$$\liminf_{\substack{n\to\infty \\ n\in T(D,p)}} \frac{\lambda_{D,v}(np)}{n^2} \geqslant 0.$$

The theorem follows by combining these two estimates.

Remark 1. The above result has the following consequence: let S be a finite set of places of K, and assume that $\widehat{h}(p) > 0$. Then there is an $N \in \mathbb{N}$ such that for all $n \geqslant N$,

$$\sum_{v\notin S} n_v \lambda_{D,v}(np) > 0.$$

It would be interesting to have an effective result in this direction.

5. *Points and division polynomials*

Let K be a field of characteristic not equal to 2 and let X be a hyperelliptic curve of genus $g \geqslant 2$ over K given by an equation $y^2 = f(x)$ with $f \in K[x]$ monic of odd degree $2g + 1$. We write $f(x) = \sum_{i=0}^{2g+1} \mu_i x^i$, where $\mu_{2g+1} = 1$. Note that X has a unique point o at infinity. Let J be the jacobian of X, endowed with its canonical principal polarization. If $p_1 \in X$, then we write p_1^- for the image of p_1 under the hyperelliptic involution.

Then for any point $p \in J$, there is a unique reduced divisor $D = (p_1) + \ldots + (p_d)$ on X such that $D - d(o)$ represents p, which we write as $p = [D - d(o)]$. Here we call an effective degree d divisor D on X *reduced* if $d \leqslant g$ and if we have $o \neq p_i \neq p_j^-$ for all distinct $p_i, p_j \in \operatorname{supp}(D)$. This leads to the *Mumford representation* $(a(x), b(x))$ of a point $p \in J$: If $(p_1) + \cdots + (p_d)$ is the reduced divisor associated to p, then $a(x) = \prod_{i=1}^{d}(x - x(p_i)) \in K[x]$ and $b(x) \in K[x]$ is the uniquely determined polynomial of minimal degree such that $y(p_i) = b(x(p_i))$ for all $i = 1, \ldots, d$. One also defines the Mumford representation of the origin to be $(1, 0)$. Note that the map $X^{(g)} \to J$ given by $(p_1, \ldots, p_g) \mapsto [(p_1) + \cdots + (p_g) - g(o)]$ is birational.

For the construction of the division polynomials ϕ_n Uchida uses certain higher-dimensional generalisations $\wp_{ij}$ and $\wp_{ijk}$, where $i, j, k \in \{1, \ldots, g\}$, of the Weierstrass $\wp$-function from the theory of elliptic curves. Over $\mathbb{C}$, these functions are constructed as second and third order partial logarithmic derivatives of the hyperelliptic σ-function, respectively. They are well-defined on the jacobian, see [**18**, proposition 2·5].

Despite their analytic construction, the $\wp$-functions make sense over an arbitrary field of characteristic zero and in fact this continues to hold in more general situations. Let $p \in J$, then the values $\wp_{ij}(p)$ and $\wp_{ijk}(p)$ can be expressed as polynomials in the coefficients of the Mumford representation $(a(x), b(x))$ of p with coefficients in $\mathbb{Z}[\mu_0, \ldots, \mu_{2g}]$. More

precisely, if we write $a(x) = \sum_{i=0}^{g} a_i x^i$ and $b(x) = \sum_{i=0}^{g-1} b_i x^i$, then we have

$$\wp_{gj} = -a_{j-1} \qquad \text{and} \qquad \wp_{ggk} = 2b_{k-1} \tag{5·1}$$

for $j, k \in \{1, \ldots, g\}$ by [**18**, theorem 2·8]. Furthermore, the $\wp$-functions $\wp_{gj}$ and $\wp_{ggk}$, where $j, k \in \{1, \ldots, g\}$, can be used to embed $J \setminus \operatorname{supp}(\Theta)$ into $\mathbb{C}^{2g}$. In particular, they have a pole only along Θ. The other $\wp$-functions can be expressed as polynomials in the $\wp_{gj}$ and $\wp_{ggk}$ by [**18**, theorem 2·9].

The division polynomials ϕ_n are also defined in terms of the hyperelliptic σ-function and can be expressed as polynomials in terms of the $\wp$-functions with coefficients in $\mathbb{Z}[1/D, \mu_0, \ldots, \mu_{2g}]$. Here D is an integer which can be computed explicitly and is independent of X. See [**18**, theorem 5·8]. In fact Uchida conjectures [**18**, conjecture 4·14] that $\phi_n \in \mathbb{Z}[\mu_0, \ldots, \mu_{2g}][\wp_{ij}, \wp_{ijk}]$ for all n. Moreover, the ϕ_n satisfy certain recurrence relations which make it possible to compute the values they take without the need to construct them as polynomials, cf. [**18**, theorem 6·4].

6. *Proof of Theorems* 2·1 *and* 2·2

Consider the jacobian J of a hyperelliptic curve X of genus $g \geqslant 2$ defined over a number field K, given by an equation $y^2 = f(x)$, where $f \in \mathcal{O}_K[x]$ is monic of degree $2g + 1$. Note that every hyperelliptic curve over K of genus g with a K-rational Weierstrass point has such a model. Let Θ denote the theta divisor on J with respect to the point o at infinity. As $-[(p_1) + \cdots + (p_g) - g(o)] = [(p_1^-) + \ldots + (p_g^-) - g(o)]$, we have that Θ is symmetric. Recall that for the division polynomial ϕ_2 we have

$$\operatorname{div}(\phi_2) = [2]^*\Theta - 4\Theta.$$

Hence there is a canonical local height function $\widehat{\lambda}_v$ associated with Θ for each $v \in M_K$ such that

$$\log|\phi_2(p)|_v = -\widehat{\lambda}_v(2p) + 4\widehat{\lambda}_v(p)$$

for $p \in J(K_v)$ such that $p, 2p \notin \operatorname{supp}(\Theta)$. Therefore Proposition 3·2 implies that we have

$$[K : \mathbb{Q}]\,\widehat{h}(p) = \sum_v n_v\,\widehat{\lambda}_v(p)\,,$$

where $\widehat{h}$ is the canonical height associated to Θ.

More generally, Uchida shows [**18**, theorem 7·5] that

$$\log|\phi_n(p)|_v = -\widehat{\lambda}_v(np) + n^2\widehat{\lambda}_v(p) \tag{6·1}$$

for each integer $n \geqslant 1$ and $p \in J(K_v)$ such that $p, np \notin \operatorname{supp}(\Theta)$.

Using (6·1) and Theorem 4·2, we can prove Theorem 2·1, giving a limit formula for the canonical local height $\widehat{\lambda}_v$ in terms of the division polynomials.

Proof of Theorem 2·1. By equation (6·1) we are done once we prove that $T(p)$ is infinite and that $\widehat{\lambda}_v(np)/n^2 \to 0$ as $n \to \infty$ over $T(p)$. But note that $\widehat{\lambda}_v$ is a canonical local height associated to Θ, which is a symmetric and ample divisor on J. The result follows by applying Theorem 4·2.

The proof of Theorem 2·2 is now almost immediate.

Proof of Theorem 2·2. As S is finite we find:

$$\begin{aligned}[K:\mathbb{Q}]\widehat{h}_S(p) &= \lim_{\substack{n\to\infty\\ n\in T(p)}} \frac{1}{n^2}\log\prod_{v\in S}|\phi_n(p)|_v^{n_v}\\ &= \lim_{\substack{n\to\infty\\ n\in T(p)}} \frac{1}{n^2}\sum_{v\in S} n_v\log|\phi_n(p)|_v\\ &= \sum_{v\in S} n_v \lim_{\substack{n\to\infty\\ n\in T(p)}} \frac{1}{n^2}\log|\phi_n(p)|_v.\end{aligned}$$

By Theorem 2·1 we have

$$\lim_{\substack{n\to\infty\\ n\in T(p)}} \frac{1}{n^2}\log|\phi_n(p)|_v = \widehat{\lambda}_v(p)$$

for each $v\in M_K$. This proves the result.

Remark 2. Unfortunately Theorem 4·2 does not tell us anything about the convergence rate of the sequences $((1/n^2)\widehat{\lambda}_v(np))_{n\in T(p)}$ or $((1/n^2)\log|\phi_n(p)|_v)_{n\in T(p)}$. If v is archimedean, then a conjecture of Lang [**9**, (2·1)] implies that $\widehat{\lambda}_v(np) = \mathcal{O}(\log n)$. For elliptic curves, this bound can be proved unconditionally using the results of David and Hirata–Kohno on linear forms in elliptic logarithms [**2**], see [**19**]. For non-archimedean v, we expect that a more refined analysis of the statements in Proposition 3·1 will give an $\mathcal{O}(\log n)$ bound for $\widehat{\lambda}_v(np)$ as well (in particular one should not need diophantine approximation to prove such a bound).

If the genus is 2, then we can compare $\widehat{\lambda}_v$ to another well-known canonical local height function. In [**5**], Flynn and Smart construct a function $\widehat{\lambda}_v^{\mathrm{FS}} : J(K_v)\to\mathbb{R}$. Uchida [**17**, theorem 5·3] has shown that this is a canonical local height associated to 2Θ for each place v of K. Let $\kappa = (\kappa_1,\dots,\kappa_4) : J\to\mathbb{P}^3$ denote the morphism constructed explicitly in [**1**, chapter 3]. The image of κ is the Kummer surface associated to J embedded into $\mathbb{P}^3$ and we have $\kappa_1(p) = 0$ if and only if $p\in\operatorname{supp}(\Theta)$. There are homogeneous quartic polynomials $\delta_i\in\mathbb{Z}[\mu_0,\dots,\mu_4][x_1,\dots,x_4]$ such that if $p\in J$, then

$$\delta(\kappa(p)) = \kappa(2p),$$

where $\delta = (\delta_1,\dots,\delta_4)$. In addition, the relation $\operatorname{div}(\delta_1\circ\kappa) = [2]^*(2\Theta) - 8\Theta$ holds.

The canonical local height $\widehat{\lambda}_v^{\mathrm{FS}}$ constructed by Flynn and Smart is associated to 2Θ and is determined by the condition that

$$\widehat{\lambda}_v^{\mathrm{FS}}(2p) - 4\widehat{\lambda}_v^{\mathrm{FS}}(p) = -\log\left|\delta_1\left(\frac{\kappa(p)}{\kappa_1(p)}\right)\right|_v \tag{6·2}$$

holds for all $p\in J(K_v)$ such that both p and $2p$ are not in $\operatorname{supp}(2\Theta)$.

PROPOSITION 6·1. *If the genus of X is* 2 *and if $p\in J(K_v)\setminus\operatorname{supp}(\Theta)$, then we have*

$$\widehat{\lambda}_v^{\mathrm{FS}}(p) = 2\widehat{\lambda}_v(p).$$

Proof. Since $\widehat{\lambda}_v$ is a canonical local height associated to Θ, it follows from property (i) of Definition 1 that $2\widehat{\lambda}_v$ is a canonical local height associated to 2Θ. Because of (6·1) and (6·2), it suffices to show that for a point $p\in J\setminus\operatorname{supp}(\Theta)$ we have

$$\delta_1\left(\frac{\kappa(p)}{\kappa_1(p)}\right) = \phi_2(p)^2.$$

We have checked this relation symbolically using explicit expressions for ϕ_2 and δ_1. For this computation we used the computer algebra system `Magma` [**11**].

7. *Proof of Theorems* 2·3 *and* 2·4

Proof of Theorem 2·3. For $v \notin S_{\text{bad}} \cup S_\infty$ the jacobian J has good reduction, so the special fiber $\mathcal{J}_v$ of the Néron model $\mathcal{J}$ of J over $\text{Spec}(\mathcal{O}_{K_v})$ is an abelian variety. Hence for such v we have, for all p not in $\text{supp}(\Theta)$, that $\widehat{\lambda}_v(p) = i_v(p, \Theta) + \gamma_v$ where i_v is the v-adic intersection multiplicity on $\mathcal{J}$, and γ_v is a constant independent of p, see Proposition 3·1. There are only finitely many $v \notin S$ such that γ_v is non-zero. Put $\delta_S = \sum_{v \notin S} n_v \gamma_v$. The assumption on p implies that for $v \notin S$ we have $\widehat{\lambda}_v(p) = \widehat{\lambda}_v(2p) = \gamma_v$. We obtain using Theorem 2·2

$$\begin{aligned}[K : \mathbb{Q}]\,\widehat{h}(p) &= \sum_{v \in S} n_v \widehat{\lambda}_v(p) + \delta_S \\ &= [K : \mathbb{Q}]\,\widehat{h}_S(p) + \delta_S\end{aligned}$$

and similarly

$$[K : \mathbb{Q}]\,\widehat{h}(2p) = [K : \mathbb{Q}]\,\widehat{h}_S(2p) + \delta_S\,.$$

Combining this with $\widehat{h}(2p) = 4\widehat{h}(p)$ we deduce the required formula.

Proof of Theorem 2·4. Suppose that $g = 2$. It clearly suffices to show that if v is a finite place of K such that $\text{ord}_v(\Delta) \leqslant 1$, then we have

$$\widehat{\lambda}_v(p) = i_v(\Theta, p) \tag{7·1}$$

for all $p \in J(K_v) \setminus \text{supp}(\Theta)$.

So let v be such a place. It follows from [**15**, proposition 5·2] that if $p \notin \text{supp}(\Theta)$, then the canonical local height $\widehat{\lambda}_v^{\text{FS}}$ constructed by Flynn and Smart satisfies

$$\widehat{\lambda}_v^{\text{FS}}(p) = \log \max_{1 \leqslant i \leqslant 4} \left| \frac{\kappa_i(p)}{\kappa_1(p)} \right|_v . \tag{7·2}$$

Pick integral coordinates $(x_1, \ldots, x_4)$ for $\kappa(P)$ in such a way that x_j is a unit for some $j \in \{1, \ldots, 4\}$. Then (7·2) implies

$$\widehat{\lambda}_v^{\text{FS}}(p) = -\log \min_{1 \leqslant i \leqslant 4} \left| \frac{x_1}{x_i} \right|_v = -\log \left| \frac{x_1}{x_j} \right|_v = -\log |x_1|_v .$$

But since $\kappa_1(p) = 0$ if and only if $p \in \text{supp}(\Theta)$, Proposition 3·1 (ii) implies

$$-\log |x_1|_v = i_v(2\Theta, p) = 2 i_v(\Theta, p).$$

Combined with Proposition 6·1, this proves (7·1) and hence the theorem.

Remark 3. The above proof shows that $\gamma_v = 0$ if $\text{ord}_v(\Delta) \leqslant 1$ and $g = 2$. For general $g \geqslant 2$, if J has good reduction at v, one has

$$\gamma_v = \frac{-\log |\phi_2(p)|_v}{3}$$

for any p such that p and $2p$ are not in $\text{supp}(\Theta)$ mod v. This implies that $\gamma_v \geqslant 0$ for such v.

8. *Gaps and factorisation*

Suppose now that we want to calculate $\widehat{h}(p)$ for a rational point p on the jacobian associated to the hyperelliptic curve $X : y^2 = \sum_{i=0}^{2g+1} \mu_i x^i$ defined over a number field K, where $g \geqslant 2$, $\mu_{2g+1} = 1$ and all $\mu_i \in \mathcal{O}_K$.

In order to apply Theorem 2·2 or 2·4, a first requirement is that p is not in $\mathrm{supp}\,(\Theta)$ (applying Theorem 2·3 requires, in addition, that $2p$ is not in $\mathrm{supp}\,(\Theta)$). If $p \in \mathrm{supp}\,(\Theta)$, we can simply try to replace p by a multiple.

Next, one wants to know in advance that the set $T(p)$ of multiples to which one is confined does not contain large gaps. Note that a gap of length $g+1$ gives rise to a point in the intersection $\Theta \bigcap \Theta_p \bigcap \cdots \bigcap \Theta_{gp}$ of $g+1$ translates of the theta divisor Θ. These translates are distinct if p is not torsion of order $\leqslant g$, since the morphism $J \to \widehat{J}$ given by $q \mapsto [\Theta - \Theta_q]$ is an isomorphism. Generically one expects the intersection of these translates therefore to be empty.

In the case $g = 2$ we can give the following precise statement.

LEMMA 8·1. *Let K be a field of characteristic not equal to 2 and let X be a genus 2 curve defined over K with jacobian J. Let $p = [(p_1) + (p_2) - 2(o)] \in J$ be a non-zero point. Then we have*:

(i) *if $p \in J[2]$, then $\bigcap_{n=1}^{N} \Theta_{np}$ is non-empty for all $N \geqslant 1$;*
(ii) *assume that neither p_1 nor p_2 is a Weierstrass point. Then $\Theta \bigcap \Theta_p \bigcap \Theta_{2p}$ is empty*;
(iii) *the intersection $\Theta \bigcap \Theta_p \bigcap \Theta_{2p} \bigcap \Theta_{3p}$ is empty for all $p \notin J[2]$.*

Proof. Note that p uniquely determines the unordered pair $\{p_1, p_2\}$ by Riemann–Roch. If $p \in J[2] \setminus \{0\}$, then both p_1 and p_2 are Weierstrass points. One then readily checks that in this situation both $[(p_1) - (o)]$ and $[(p_2) - (o)]$ lie in $\Theta \bigcap \Theta_p$, which proves (i).

Now let $p \in J \setminus \{0\}$ be arbitrary and suppose $q = [(q_1) - (o)] \in \Theta \bigcap \Theta_p$. Then there exists $r = [(r_1) - (o)] \in \Theta$ such that $p = r - q$ and hence

$$(p_1) + (p_2) - 2(o) \sim (r_1) - (q_1)\,.$$

By Riemann–Roch this implies

$$(r_1) - (q_1) \in \{(p_1) - (p_2^-), (p_2) - (p_1^-)\} \tag{8·1}$$

and hence $q_1 = p_1^-$ or $q_1 = p_2^-$. Without loss of generality we assume that $q_1 = p_1^-$.

Suppose that $q \in \Theta \bigcap \Theta_p \bigcap \Theta_s$ where $s = 2p = [(s_1) + (s_2) - 2(o)]$. Similarly as before we find that $q_1 = s_1^-$ or $q_1 = s_2^-$. Hence $s_i = p_1$ for some $i \in \{1, 2\}$, say $s_1 = p_1$. This implies

$$p = s - p = [(s_2) - (p_2)].$$

Again by Riemann–Roch we find

$$(s_2) - (p_2) \in \{(p_1) - (p_2^-), (p_2) - (p_1^-)\}\,,$$

leading to $p_2 = p_1^-$ or $p_2 = p_2^-$. The first possibility implies $p = 0$, which we excluded, so we end up with $p_2 = p_2^-$. This proves (ii).

To prove (iii), we may assume that $p_2 = p_2^-$, so that $2p = [2(p_1) - 2(o)]$. Note that under this assumption $p \notin J[3]$, since otherwise we would have $2p = -p$, which implies $p_1 = p_1^-$ or $p_1 = p_2^-$, and hence $p \in J[2] \bigcap J[3] = \{0\}$.

By the arguments above, we may assume that a point $q \in \Theta \bigcap \Theta_p \bigcap \Theta_{2p}$ satisfies $q_1 = p_1^-$. If we assume, in addition, that $q \in \Theta_t$, where $t = [(t_1) + (t_2) - 2(o)] = 3p \neq 0$, then Riemann-Roch implies $p_1 \in \{t_1, t_2\}$ as in (8·1), say $p_1 = t_1$. But then

$$p = 3p - 2p = [(t_1) + (t_2) - 2(p_1)] = [(t_2) - (p_1)],$$

which implies $p \in J[2]$.

Note that we also need to find the primes dividing the ideal (Δ) if we want to apply Theorem 2·2 or 2·4. In practice, this becomes problematic if $N_{K/\mathbb{Q}}(\Delta)$ is large. The following result generalizes equation (21) in [**3**].

THEOREM 8·2. *Assume that X is defined over $\mathbb{Q}$. Let $p \in J(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$ such that $\phi_n(p) \in \mathbb{Z}$ for all $n \geqslant 1$ and put $E_n = \phi_n(p)$. Let S' be a finite set of prime numbers containing S_{bad} and write $S = S' \cup \{\infty\}$. Assume that l is a positive integer such that for all reductions $\widetilde{J}$ of J modulo primes not in S' we have that $T(\widetilde{p})$ contains no gap larger than l, where $\widetilde{p}$ is the reduction of p. Then we have*

$$\widehat{h}_S(p) = \lim_{\substack{n\to\infty \\ n\in T(p)}} \frac{1}{n^2} \log \left(\frac{|E_n|}{\gcd(|E_n|, |E_{n+1}|, \ldots, |E_{n+l}|)} \right).$$

Proof. Note that

$$\prod_{v\in S} |\phi_n(p)|_v^{n_v} = |E_n| \prod_{v\in S'} |E_n|_v^{n_v},$$

and hence

$$\widehat{h}_S(p) = \lim_{\substack{n\to\infty \\ n\in T(p)}} \frac{1}{n^2} \log |E_n| \prod_{v\in S'} |E_n|_v^{n_v}.$$

By assumption, we have that for each given $n \in T(p)$ a prime $v \notin S'$ does not occur in all of $E_n, \ldots, E_{n+l}$ simultaneously, so that the gcd is only composed of primes in S'. In fact we have

$$\begin{aligned} \gcd(|E_n|, \ldots, |E_{n+l}|) &= \prod_{v\in S'} \min(|E_n|_v^{-1}, \ldots, |E_{n+l}|_v^{-1})^{n_v} \\ &= \prod_{v\in S'} |E_n|_v^{-n_v} \min(1, |E_{n+1}/E_n|_v^{-1}, \ldots, |E_{n+l}/E_n|_v^{-1})^{n_v}. \end{aligned}$$

Thus it suffices to show that in the limit as $n \to \infty$ one has

$$\frac{1}{n^2} \log \min(1, |E_{n+1}/E_n|_v^{-1}, \ldots, |E_{n+l}/E_n|_v^{-1}) \longrightarrow 0 \tag{8·2}$$

for $n \in T(p)$. By Theorem 2·1, the sequence $\left(n^{-2} \log |E_n|_v\right)_{n\in T(p)}$ converges for every $v \in S'$, hence is a Cauchy sequence. This proves (8·2) and therefore the theorem.

Using Theorem 8·2 and Lemma 8·1, we can develop a method for the computation of $\widehat{h}(p)$ if $K = \mathbb{Q}$ and $g = 2$ which requires no factorisation at all.

COROLLARY 8·3. *Suppose that $g = 2$ and that $p \in J(\mathbb{Q})$ satisfies $\wp_{2j}(p), \wp_{22k}(p) \in \mathbb{Z}$ for $j, k \in \{1, 2\}$ and $\gcd(a(x), b(x)) = 1$, where $(a(x), b(x))$ is the Mumford representation of p. Suppose, moreover, that $\phi_n(p) \in \mathbb{Z}$ for all $n \geqslant 1$. Then we have*

$$\widehat{h}(p) = \lim_{\substack{n\to\infty \\ n\in T(p)}} \frac{1}{n^2} \log \left(\frac{|E_n|}{\gcd(|E_n|, |E_{n+1}|, |E_{n+2}|)} \right).$$

Proof. Write $p = [(p_1) + (p_2) - 2(o)]$, where both $p_1, p_2 \in X(K)$ and $K = \mathbb{Q}$ or K is a quadratic extension of $\mathbb{Q}$. The condition $\gcd(a(x), b(x)) = 1$ ensures that neither p_1 nor p_2 is a Weierstrass point on X. In order to apply Theorem 8·2 we let S' denote the union of S_{bad} and the finite set of places v such that p_1 or p_2 reduces to a Weierstrass point modulo w for some place w of K dividing v. By Lemma 8·1 we can then take $l = 2$. Put $S = S' \cup \{\infty\}$.

By Theorem 8·2, the right-hand side of the equality to be proven equals $\widehat{h}_S(p)$. The assumptions that $\wp_{2j}(p), \wp_{22k}(p) \in \mathbb{Z}$ for $j, k \in \{1, 2\}$ imply that for $v \notin S$ the point p does not lie on the theta divisor modulo v. The equality itself then follows by applying Theorem 2·4.

Remark 4. Assuming that all the $\phi_n(p)$ are integers may seem like a strong restriction, but, possibly after applying a simple coordinate transformation to X, we can at least always assume that all $\wp_{gj}(p)$ and $\wp_{ggk}(p)$ are integral. Then, a conjecture of Uchida [**18**, conjecture 4·14] predicts that all $\phi_n(p)$ are integral. So we can simply test along the way whether E_n has a nontrivial denominator for $n = 1, 2, \ldots$; such an n would then yield a counterexample Uchida's conjecture.

Remark 5. We note that if $p = [(x_1, y_1) + \cdots + (x_g, y_g) - g(o)] \in J(\mathbb{Q})$ such that all x_i and y_i are integral, then all $\wp_{gj}(p)$ are integral, but this need not hold for all $\wp_{ggk}(p)$. Consider, for instance, the Jacobian J of the hyperelliptic curve X given by the affine model

$$y^2 = 1 + 2x + 3x^2 + 4x^3 + 5x^4 + x^5$$

and the point $p = [(1, 4) + (-2, 5) - 2(o)] \in J$, satisfying

$$\wp_{21}(p) = -1,\ \wp_{22}(p) = 2,\ \wp_{221}(p) = -2/3,\ \wp_{222}(p) = 26/3.$$

9. *Implementation*

Suppose that $g = 2$. We have implemented the computation of the values of ϕ_n for this case in `Magma`. Expressions for the $\wp$-functions $\wp_{11}$, $\wp_{112}$ and $\wp_{111}$ in terms of $\wp_{12}$, $\wp_{22}$, $\wp_{122}$ and $\wp_{222}$ are given in [**18**, example 5·9]. Uchida shows that all $\phi_n \in \mathbb{Z}[1/2, \mu_0, \ldots, \mu_4]$ and conjectures that in fact $\phi_n \in \mathbb{Z}[\mu_0, \ldots, \mu_4]$. The division polynomials ϕ_n for $n \in \{1, \ldots, 5\}$ were already computed by Uchida and we are grateful to him for sharing them with us. In fact it is not hard to compute these using a method already discussed by Kanayama [**7**] who first constructed the division polynomials in the genus 2 case.

We have not computed any of the polynomials ϕ_n for $n > 5$ because they quickly become rather complicated. Instead we employ a recurrence relation due to Kanayama [**8**, theorem 9 (corrected)] which can be used to compute ϕ_{2n+1} ($n \geqslant 2$) and ϕ_{2n} ($n \geqslant 3$) in terms of $\phi_{n-2}, \ldots, \phi_{n+2}$ and some of their partial derivatives. Given $p \in J(\mathbb{Q}) \setminus \mathrm{supp}(\Theta)$, we apply this method for the calculation of $\phi_n(p)$, where $n = 6, 7, 8$; our method relies on finding partial derivatives of $\phi_2, \ldots, \phi_5$ for our specific J and then evaluating them at p.

Having determined $\phi_1(p), \ldots, \phi_8(p)$, we then proceed to use Uchida's recurrence relations from [**18**, example 6·6] to compute $\phi_n(p)$ for $n \geqslant 9$. These are preferable to Kanayama's recurrence relations since they only need the values $\phi_m(p)$ for $m \in \{1, \ldots, 5\}$ and $m \in \{(n-7)/2, \ldots, (n+7)/2\}$ (resp. $m \in \{(n-8)/2, \ldots, (n+8)/2\}$) if n is odd (resp. even); no derivation of polynomials is required.

We have implemented the computation of $\widehat{h}(p)$ using both Theorem 2·4 and Corollary 8·3. If we can factor Δ, then it is usually much faster to use Theorem 2·4 and work locally at each relevant place. The code is available on the second author's homepage

`http://www.uni-oldenburg.de/fileadmin/user_upload/mathe/personen/steffen.mueller/CanHtsDivPolys.zip`.

Several other methods exist for the computation of canonical heights on hyperelliptic jacobians. For instance, Holmes [**6**] and the second author [**12**] have independently developed algorithms that can be used for arbitrary $g \geqslant 1$; the current record computation has $g = 10$, see [**12**, section 6]. Their methods need integer factorisation, regular models of the curves and theta functions on $\mathbb{C}^g$.

For $g = 2$ other algorithms are available. These all require explicit arithmetic on a model of the Kummer surface associated to J in $\mathbb{P}^3$, see Section 6. The original method of Flynn and Smart [**5**] requires no integer factorisation, but needs the computation of a certain multiple np of the point $p \in J(K)$ whose canonical height we want to compute. As n can become quite large (see [**15**, section 1]), this often becomes impractical. A modified version due to Stoll [**15**] remedies this, but requires integer factorisation. However, one can combine this modified version with the original method of Flynn and Smart to avoid difficult factorisations, see [**15**, section 6]. Further improvements are given in [**14**]. Another algorithm which is very similar to Stoll's method is due to Uchida [**17**]. One could extend these techniques to higher genus if one had formulas for explicit arithmetic on a model of the Kummer variety. This is already quite difficult in genus 3, see for instance [**13**]; Stoll has recently found an analogue of his genus 2 algorithm in genus 3 [**16**].

Currently, `Magma` contains an implementation of the algorithms from [**12**] for general g and [**15**] for $g = 2$. When $g = 2$, then the algorithm from [**15**] is usually faster than the algorithms using Theorem 2·4 or Corollary 8·3, which in turn are usually faster than the implementation of the algorithm from [**12**] if we are only interested in a few digits of precision.

10. *Examples*

10·1. *Height computation*

Let X be given by the affine model

$$y^2 = 1 + 2x + 3x^2 + 4x^3 + 5x^4 + x^5$$

and let J be the Jacobian of X. We want to compute the canonical height $\widehat{h}(p)$ of the point $p = [(1, 4) + (-2, -5) - 2(o)] \in J$, satisfying

$$\wp_{21}(p) = -1,\ \wp_{22}(p) = 2,\ \wp_{221}(p) = 6,\ \wp_{222}(p) = 2.$$

Using the implementation of the Flynn-Smart algorithm [**5**] modified by Stoll [**15**] in `Magma`, we compute $\widehat{h}(p) \sim 0.905661971737515301104367671719$.

We can use Corollary 8·3 to compute $\widehat{h}(p)$ without any factorisations, see Table 1. If we are only interested in a few digits of precision, it suffices to compute $\phi_n(p)$ for $n \leqslant 100$. In this case the bulk of the computation is spent on the computation of $\phi_n(p)$ for $n \leqslant 8$, because, as mentioned in Section 9, we need to manipulate polynomials. For the computation of $\phi_n(p)$ for $n \geqslant 9$ recurrence relations are used which only need the values $\phi_m(p)$ for a few $m < n$, see Section 9.

If we are interested in more than 4 digits of precision, then the computation of $\widehat{h}(p)$ using Theorem 2·4 is much faster, see Table 2. The prime factorisation of the discriminant of X is $\Delta = 2^8 \cdot 86477$, so it suffices to consider the set of places $S = \{2, \infty\}$, since p has integral $\wp_{2j}(p),\ \wp_{22k}(p)$.

Table 1. *Computing* $\widehat{h}(p)$ *using Corollary* 8·3

Iterations	Running time in seconds	Error
10	0.33	$3.60 \cdot 10^{-2}$
100	0.36	$4.67 \cdot 10^{-4}$
200	0.74	$1.27 \cdot 10^{-4}$
300	2.60	$6.92 \cdot 10^{-5}$
400	7.73	$3.49 \cdot 10^{-5}$
500	18.990	$2.45 \cdot 10^{-5}$

Table 2. *Computing* $\widehat{h}(p)$ *using Theorem* 2·4

Iterations	Running time in seconds	Error
10	0.72	$3.60 \cdot 10^{-2}$
100	0.74	$4.67 \cdot 10^{-4}$
1000	0.89	$4.82 \cdot 10^{-6}$
5000	1.58	$1.93 \cdot 10^{-7}$
10000	2.45	$5.86 \cdot 10^{-8}$
15000	3.30	$2.26 \cdot 10^{-8}$
20000	4.14	$1.65 \cdot 10^{-8}$
25000	4.96	$1.21 \cdot 10^{-8}$

10·2. *Order of growth of* $\widehat{\lambda}_v(np)$

As was remarked before, we are not able to say anything about the convergence rate of the sequence $((1/n^2)\log|\phi_n(p)|_v)_{n\in T(p)}$ for a given place v using only Faltings's Theorem 4·1. By (6·1), finding this convergence rate is equivalent to finding the order of growth of $\widehat{\lambda}_v(np)$.

We have applied our implementation described in Section 9 to gather data on the asymptotic behaviour and the implied constants of the sequence $(\widehat{\lambda}_v(np))_{n\in\mathbb{N}}$, where $p \in J(\mathbb{Q})$ is a rational point on a genus 2 jacobian and $v \in M_{\mathbb{Q}}$. To this end we varied the place v, the coefficients μ_i and the point p. More precisely, we considered about 2000 random genus 2 curves with $|\mu_i| \leqslant 50$ for $i \in \{1, \ldots, 4\}$; we computed $\widehat{\lambda}_v(np)$ for $v = \infty$ and all non-archimedean v such that $\mathrm{ord}_v(\Delta) \geqslant 2$, for all $p \notin \mathrm{supp}(\Theta) \bigcap J[2]$ of Kummer surface height bounded by 500 and for all $n \in \{1, \ldots, 15000\} \bigcap T(p)$. We also considered about 100 examples of curves with $50 < |\mu_i| \leqslant 1000$.

10·2·1. *Archimedean places*

Let us first describe the case $v = \infty$. As mentioned in Remark 2, by a conjecture of Lang we should have

$$\widehat{\lambda}_\infty(np) = \mathcal{O}(\log n)$$

for $n \in T(p)$. We have used our implementation to test this prediction.

See Figure 1 for the values of $\widehat{\lambda}_\infty(np)$, where $n \in \{1, \ldots, 15000\}$ and $p \in J_1(\mathbb{Q})$ has Mumford representation

$$(x^2 + 1081/25x + 148/5,\ 13803/125x + 1799/25).$$

Note that every $n \in \{1, \ldots, 15000\}$ lies in $T(p)$. Here J_1 is the jacobian of the genus 2 curve

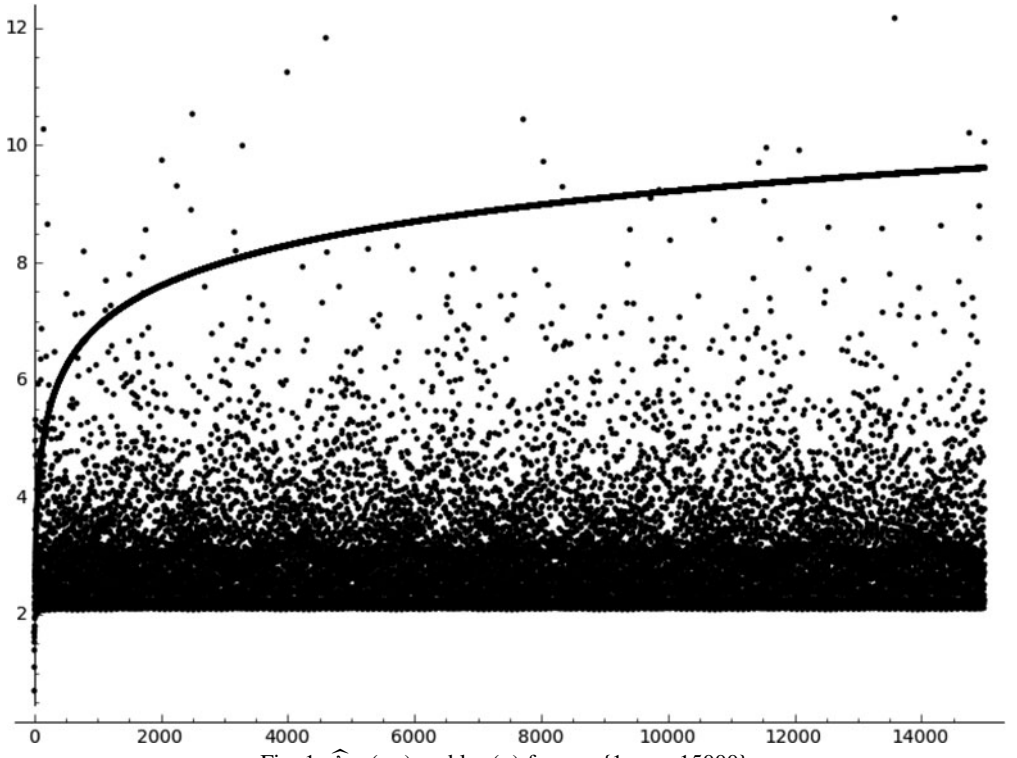

Fig. 1. $\widehat{\lambda}_\infty(np)$ and $\log(n)$ for $n \in \{1, \ldots, 15000\}$.

given by

$$y^2 = 25 + 20x + 30x^2 + 40x^3 + 50x^4 + x^5.$$

All examples we have considered exhibit a similar behavior. The resulting data suggest that we may even have

$$\widehat{\lambda}_\infty(np) = \mathcal{O}((\log n)^A)$$

for some $0 < A < 1$ depending on X and p, and that the implied constant is rather small compared to the coefficients μ_i.

10·2·2. *Non-archimedean places*

Let J_2 be the jacobian of the genus 2 curve given by

$$y^2 = 100 + 200x + 300x^2 + 400x^3 + 500x^4 + x^5$$

and let $q \in J_2(\mathbb{Q})$ have Mumford representation

$$(x^2 + 400x + 200, 3990x + 1990).$$

Then q reduces to a singular point on the reduction of J_2 modulo $v = 2$; the values of $\widehat{\lambda}_2(nq)$ are shown in Figure 2.

Note the apparent formation of finitely many horizontal lines, as well as a set of 'sporadic' points following the graph of $\log n$. This dual behavior can perhaps be explained using Proposition 3·1 (ii) and (iii) as follows: the set of specialisations $n\tilde{p}_2$ of the nq in the special fiber of the Néron model modulo v is a finite group R. The group R has a partition $R = R_1 \sqcup R_2$ into points which are on resp. off the closure of the theta divisor modulo v. The values of

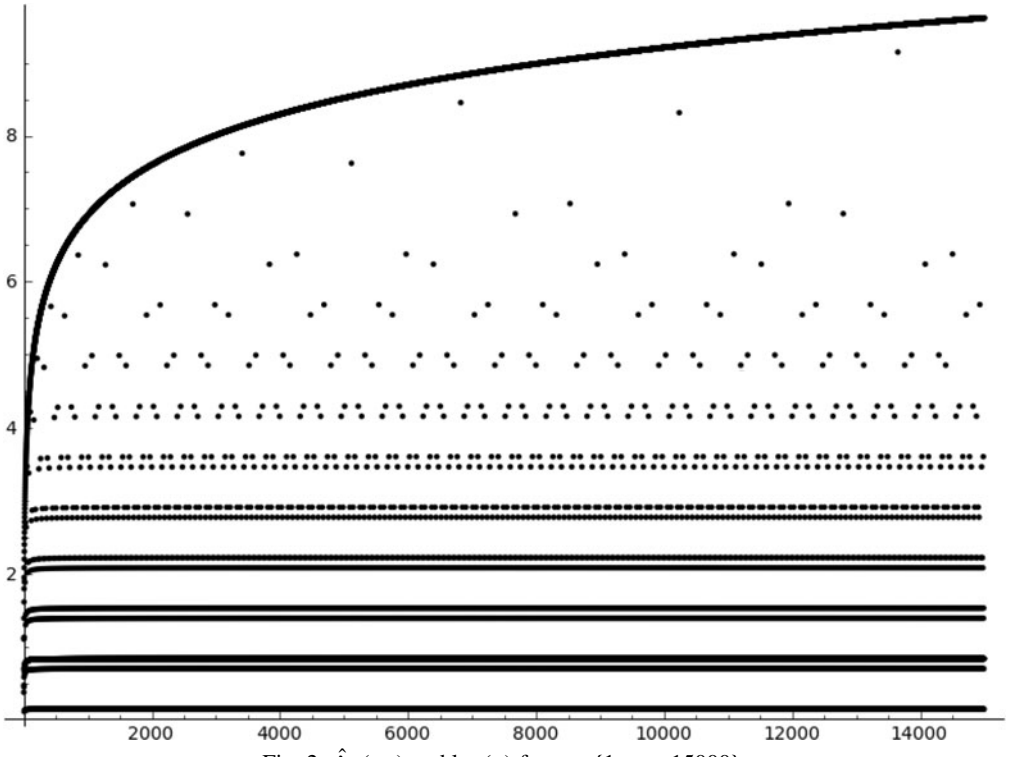

Fig. 2. $\hat{\lambda}_2(nq)$ and $\log(n)$ for $n \in \{1, \ldots, 15000\}$.

$\widehat{\lambda}_2(nq)$ display a $\log n$ behavior for $n\tilde{p}_2 \in R_1$, and are given by $\gamma(\mathcal{C})$, with $\mathcal{C}$ the component containing $n\tilde{p}_2$, when $n\tilde{p}_2 \in R_2$. Again, a similar behaviour occurred in all our examples.

Acknowledgements. We thank Yukihiro Uchida for providing us with formulas for the division polynomials ϕ_n for $n \leqslant 5$ when $g = 2$. Some of the research described here was done while the second author was visiting the University of Leiden and he would like to thank the Mathematical Institute for its hospitality. The second author was supported by DFG grant KU 2359/2-1.

REFERENCES

[1] J. W. S. CASSELS and E. V. FLYNN. *Prolegomena to a middlebrow arithmetic of curves of genus* 2. London Mathematical Society Lecture Note Series no. 230 (Cambridge University Press, 1996).
[2] S. DAVID and N. HIRATA–KOHNO. Linear forms in elliptic logarithms. *J. Reine Angew. Math.* **628** (2009), 37–89.
[3] G. EVEREST and T. WARD. The canonical height of an algebraic point on an elliptic curve. *New York J. Math.* **6** (2000), 331–342.
[4] G. FALTINGS. Diophantine approximation on abelian varieties. *Ann. of Math.* (2) **133** (1991), 549–576.
[5] E. V. FLYNN and N. P. SMART. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.* **79** (1997), 333–352.
[6] D. HOLMES. Computing Néron–Tate heights of points on hyperelliptic Jacobians. *J. Number Theory* **132** (2012), 1295–1305.
[7] N. KANAYAMA. Division polynomials and multiplication formulae of Jacobian varieties of dimension 2. *Math. Proc. Camb. Phil. Soc.* **139** (2005), 399–409.
[8] N. KANAYAMA. Corrections to "Division polynomials and multiplication formulae in dimension 2". *Math. Proc. Camb. Phil. Soc.* **149** (2010), 189–192.
[9] S. LANG. Higher dimensional diophantine problems. *Bull. Amer. Math. Soc.* **80** (1974), 779–787.
[10] S. LANG. *Fundamentals of Diophantine Geometry* (Springer–Verlag, 1983).

[**11**] MAGMA is described in W. BOSMA, J. CANNON and C. PLAYOUST. The Magma algebra system I: The user language. *J. Symb. Comp.* **24** (1997), 235–265.
[**12**] J. S. MÜLLER. Computing canonical heights using arithmetic intersection theory. *Math. Comp.* **83** (2014), 311–336.
[**13**] J. S. MÜLLER. Explicit Kummer varieties of hyperelliptic Jacobian threefolds, to appear in *LMS J. Comput. Math.* (2014).
[**14**] J. S. MÜLLER and M. STOLL. Canonical heights on genus two Jacobians. In preparation.
[**15**] M. STOLL. On the height constant for curves of genus two, II. *Acta Arith.* **104** (2002), 165–182.
[**16**] M. STOLL. An explicit theory of heights for hyperelliptic Jacobians of genus three. In preparation.
[**17**] Y. UCHIDA. Canonical local heights and multiplication formulas. *Acta Arith.* **149** (2011), 111–130.
[**18**] Y. UCHIDA. Division polynomials and canonical local heights on hyperelliptic Jacobians. *Manuscript. Math.* **134** (2011), 273–308.
[**19**] Y. UCHIDA. Valuations of Somos 4 sequences and canonical local heights on elliptic curves. *Math. Proc. Camb. Phil. Soc.* **150** (2011), 385–397.