CANONICAL HEIGHTS ON HYPERELLIPTIC CURVES

DAVID HOLMES

Abstract. It was shown by Faltings ([Fal84]) and Hriljac ([Hri85]) that the canonical height of a point on the Jacobian of a curve can be expressed as the self intersection of a corresponding divisor on a regular model of the curve. We make this explicit and use it to give an algorithm for computing canonical heights on Jacobians of hyperelliptic curves. To demonstrate the practicality of our algorithm, we illustrate it by computing canonical heights on Jacobians of hyperelliptic curves of genus $1 \leq g \leq 9$.

The main work done is firstly to make the algorithm effective without the need to compute a minimal regular model for the curve, and secondly to perform the Green's function computations at infinite places.

1. Introduction

There are two main applications for the computation of canonical (Néron-Tate) heights on the Jacobians of curves; one is in verifying special cases of the conjectures of Birch and Swinnerton-Dyer, and the other is as a step towards saturation, the process of computing generators for the Mordell Weil group of the Jacobian given a finite index subgroup (bounds on the difference between the naive and canonical heights are also required for this). Both of these applications have long been exploited for elliptic curves, and more recently for curves of genus two, see for example [CF96] and [FS97]. However, the approaches used for these low genus curves have been based on computing with explicit equations for projective embeddings of the Jacobian and its Kummer variety together with equations for the duplication maps, which are as yet unknown for curves of genus greater than two.

In [Ara74], Arakelov introduced a theory of intersections for arithmetic surfaces. Faltings ([Fal84]) and Hriljac ([Hri85]) demonstrated many useful properties of these intersection products, including the relationship to canonical heights on Jacobians of curves. The remarkable and useful thing about this for our purposes is that it allows for the computation of canonical heights on the Jacobian of a curve to be expressed purely in terms of equations for divisors on the curve, so we

Date: September 8, 2010.

2010 *Mathematics Subject Classification.* Primary 14G40, Secondary 11G30, 11G50, 37P30.

The author is supported by the EPSRC.

do not need to use, or even consider, explicit projective models of such Jacobians. This extends greatly the class of curves on which we will be able to effectively compute these heights. Prior to this work, height computations had only been carried out on curves of genus one and two, but, as the examples in the final section of this paper will show, hyperelliptic curves of genus up to at least nine can now be tackled.

The remainder of this paper will proceed as follows: in Section 2 we set up the situation over non-Archimedian places, and in Section 3 we give explicit formulae to compute the local contributions at these places, both at primes of good reduction and the rest. The latter we accomplish by results derived in the subsequent section, by showing that intersections for divisors which are 'not too singular' can be computed on the given model of the curve. Then in Section 5 we prove the key result that shows that some multiple of our divisor will avoid the singular locus. This last result may be of some independent interest, since it can be applied to a wide class of arithmetic surfaces.

In the penultimate section of the paper we give a simple new derivation for the expression of the height contribution at an Archimedian place in terms of theta functions based on a theorem of Lang (see [Mül10] for another derivation of this result). Putting all this together we obtain the last section of the paper which contains some examples of canonical heights of points on the Jacobians of hyperelliptic curves of large genus.

The author wishes to thank Samir Siksek for introducing him to this fascinating problem, as well as for much helpful advice and a careful reading of this manuscript. Thanks are also due to Martin Bright and Jan Steffen Müller amongst others for very helpful discussions.

1.1. **Notation.** For the remainder of this paper we fix some notation: K is a number field with integers $\mathcal{O}_K$, and M_K is a complete set of primes of K. K^{alg} is a fixed algebraic closure of K. Let $f \in \mathcal{O}_K[x]$ be an odd degree monic polynomial with no repeated roots over the algebraic closure and having degree at least 5 (since the elliptic case is already well understood). We also assume that the degree of f is odd; the theoretical part of this paper works almost[1] entirely independently of this assumption, but there are additional computational issues when attempting the more general case. Let X denote the arithmetic surface which is constructed by gluing the affine pieces $y^2 = f \subset A^2_{\mathcal{O}_K}$ and $t^2 = s^{(\deg(f)+1)} f(\frac{1}{s}) \subset A^2_{\mathcal{O}_K}$. We assume throughout that f is chosen such that X is normal.

X_η will be the generic fibre of X with function field $k(X)$. For $\nu \in M^0_K$, X_ν will denote the fibre over ν. If D is a prime divisor on X_η, let D_X denote the Zariski closure of D in X viewed as a Weil divisor

[1] The exception is a few curves of even degree which do not have integral special fibre over 2.

on X. Extend this to the whole of $\mathrm{Div}_X(K)$ by linearity. Such D_X will be known as **horizontal** divisors. Intersecting D_X with X_ν yields a divisor D_ν on X_ν.

1.2. **Heights as intersection pairings.** Given a pair of divisors $D, E \in \mathrm{Div}^0(X_\eta)$ without common support, [Fal84] and [Hri85] tell us that the height pairing can be expressed as

$$\hat{h}(D,E) = -\sum_{\nu \in M_K} \langle\langle D, E\rangle\rangle_\nu \tag{1}$$

where the bilinear pairing $\langle\langle D, E\rangle\rangle_\nu$ is the normalised Néron pairing (see Section 2). This pairing respects linear equivalence (essentially by the product formula), so we can define

$$\hat{h}(D) = -\sum_{\nu \in M_K} \langle\langle D, D'\rangle\rangle_\nu \tag{2}$$

where D' is linearly equivalent to D but has disjoint support. Note that we may need to take a finite field extension on order to guarantee the existance of such a D, but $\hat{h}$ is independent of the field of definition so no ambiguity arises. On a hyperelliptic curve we can use the hyperelliptic involution to calculate $\hat{h}(D)$ more easily; suppose D contains no Weierstrass points in its support, and let D^- denote the involution of D. Then observe that

$$\hat{h}(D) = \sum_{\nu \in M_K} \langle\langle D, D^-\rangle\rangle_\nu \tag{3}$$

since $\langle\langle -,-\rangle\rangle_\nu$ is bilinear and D^- is linearly equivalent to $-D$. In practice, we represent D in Mumford form (see Section 3.0.1), then take a high enough multiple so as to avoid containing any finite Weierstrass points, then we let $D' \overset{\mathrm{def}}{=} D_1 - D_2$ where D_1 is the involution of the finite part of D, and $D_2 = \frac{\deg(D_1)}{2}.\mathbb{V}(x-\lambda)$ for some chosen $\lambda \in \mathbb{P}^1$ (where $\mathbb{V}$ denotes the subvariety defined by the given equation).

The computation of the $\langle\langle -,-\rangle\rangle_\nu$ is straightforward at non-Archimedian places of good reduction, and can also be derived in terms of (easily computable) theta functions at Archimedian places. Much of the work we will do is therefore in computing this pairing at bad places. The approach used for theoretical purposes is to replace $X \times_{\mathcal{O}_K} \mathcal{O}_{K,\nu}$ by a regular model, but this can be hard to compute in practice; currently this can be done in MAGMA as long as no components of positive genus have to be blown up in the course of the desingularisation (Jan Steffen Müller is working on an algorithm using this). In this paper we instead prove a $\mathbb{Q}$-factoriality result which allows us to compute the intersection pairing without computing any such desingularisations.

2. Non-Archimedian primes

Since $\operatorname{Spec}(\mathcal{O}_K)$ is excellent (see [Liu02, Chapter 8, Corollary 2.40]), we have that X admits a strong desingularisation $X' \to X$ which is proper and birational ([Liu02, Chapter 8, Corollary 3.45]).

Let ι_ν denote the local intersection symbol in the fibre of X' over ν and $\langle -, - \rangle_\nu$ the Néron pairing, both defined as in [Lan88]. We abuse notation[2] by letting ι_ν also denote the local intersection symbol for divisors on X whose intersection does not contain a non-regular point of X. The **normalised Néron function** $\langle\langle -, - \rangle\rangle_\nu$ is now given by

$$\langle\langle -, - \rangle\rangle_\nu = \log \#\kappa(\nu) \cdot \langle -, - \rangle_\nu$$

Let $\operatorname{comp}(X'_\nu)$ denote the free group generated by the irreducible components of the special fibre, $\mathbb{Q} \otimes_\mathbb{Z} \operatorname{comp}(X'_\nu)$ the base change to $\mathbb{Q}$, and $\mathbb{Q}X'_\nu$ the subgroup consisting of elements corresponding to multiples of the whole fibre X'_ν.

Let Φ_ν denote the unique linear form

$$\Phi_\nu : \operatorname{Div}^0_X(K) \to \frac{\mathbb{Q} \otimes_\mathbb{Z} \operatorname{comp}(X'_\nu)}{\mathbb{Q}X'_\nu} \tag{4}$$

such that for every $D \in \operatorname{Div}^0_X(K)$, we have $D_{X'} + \Phi_\nu(D)$ orthogonal with respect to the pairing ι_ν to the group of $\mathbb{Q}$-divisors on X' supported on X'_ν (see [Lan88, III, Theorem 3.6] for details, and [Mum61] for more motivation for this definition).

We have the following result:

Lemma 1. *Let $D, E \in \operatorname{Div}^0_X(K)$ have disjoint support. Then*

$$\langle D, E \rangle_\nu = \iota_\nu(D_{X'} + \Phi_\nu(D), E_{X'}) = \iota_\nu(D_{X'} + \Phi_\nu(D), E_{X'} + \Phi_\nu(E)).$$

Proof. [Lan88, III,Theorem 5.2]. Note that the second equality is obvious from the definition of Φ_ν. □

Thus the computation of $\langle\langle -, - \rangle\rangle_\nu$ is reduced to the computation of the intersection pairings ι_ν and the linear map Φ_ν. The former will be accomplished using resultants, and the latter will be avoided using $\mathbb{Q}$-factoriality.

2.1. Moving divisors.

We will use linear equivalence to move divisors away from the the locus of points reducing to non-regular points of the special fibre. In order to do this, we need to understand how to compute the Néron pairing $\langle D, E \rangle_\nu$ when one of D, E is principal, even when they meet at a non-regular point of the special fibre. From the definition of the Néron pairing (see [Lan83]) we have that for any rational function $g \in K(X)^*$,

$$\langle \operatorname{div}_{X_\eta}(g), E \rangle_\nu = \operatorname{ord}_\nu(g[E])$$

[2] this abuse is justified as ι_ν is local and the desingularisation map is an isomorphism outside non-regular points.

where $g[E]$ is the product of the values of g at the points in the support of E counted with multiplicities. However, because we want to include divisors E which do **not** have pointwise K-rational support, we need to be more careful in our definition of $g[E]$ as follows.

We begin by restricting to the case where E is a closed point of X_ν (not necessarily a K-point!). Let $\kappa(E)$ denote the residue field, and let $\hat{K}$ denote the ν-adic completion of K. Let L be a[3] finite extension of $\hat{K}$ such that

$$\kappa(E) \otimes_K L = \bigoplus_i L,$$

for example let L contain $\kappa(E)$. By definition, $g(E)$ is the image of g in the residue field $\kappa(E)$, and hence in the $\kappa(E) \otimes_K L$ it breaks up uniquely as $g(E) = \oplus_i \alpha_i$, $\alpha_i \in L$. Now let w denote the unique extension of the valuation ν to L, and define

$$g[E] = \sum_i w(\alpha_i).$$

It is clear that this is independent of the choice of L. Finally we extend to arbitrary divisors $E \in \operatorname{Div}_X(K)$ by linearity:

$$g[E + D] = g[E] \cdot g[D].$$

Note that $\operatorname{div}_{X_\eta}(g)$ determines g up to a constant multiple, so $\langle \operatorname{div}_{X_\eta}(g), E\rangle_\nu = \operatorname{ord}_\nu(g[E])$ makes sense when E has degree zero.

2.2. **Bad primes.** In this section we will outline an approach to computing the Néron pairing at a prime ν over which the fibre X_ν is not smooth. We can work locally, so replace X by $X \times_{\mathcal{O}_K} \mathcal{O}_{K_\nu}$. Our normality assumption implies (by [Liu02, Chapter 8, Lemma 2.21]) that the non-regular points are isolated. Then from Section 4 we have the following:

Theorem 2. *Let* D, $E \in \operatorname{Div}^0_X(K)$ *such that* $\operatorname{Supp}(D) \cap \operatorname{Supp}(E) = \emptyset$.
Let $f \in k(X)$ *such that* $\operatorname{Supp}(\operatorname{div}_{X_\eta}(f) - D) \cap \operatorname{Supp}(D) = \emptyset$.
Set $F \overset{def}{=} D - \operatorname{div}_{X_\eta}(f)$. *Further, suppose:*
1) $F_{X_\eta} \cap \operatorname{Sing}(X) = \emptyset$,*and*
2) $\operatorname{Supp}(F) \cap \operatorname{Supp}(E) = \emptyset$.
Then:

$$\langle D, E\rangle_\nu = \langle \operatorname{div}_{X_\eta}(f), E\rangle_\nu + \iota_\nu(F_X, E_X)$$

By Section 2.1 we can compute $\langle \operatorname{div}_{X_\eta}(f)\rangle_\nu$, and Section 3 will show how to compute $\iota_\nu(F_X, E_X)$. It thus suffices to find a rational function $f \in k(X)$ with properties as in Theorem 2. The only property which is non-trivial to satisfy (if we are prepared to take a finite extension of K to ensure the existence of enough rational points) is $F_{X_\eta} \cap \operatorname{Sing}(X) = \emptyset$, that is that we can move D to avoid the singular locus. This is not

[3] the point of this is to show that the definition is independant of the choice of L.

in general possible, but we will prove in Section 5 that we can move some **multiple** of D to avoid $\operatorname{Sing}(X)$, so we are done by bilinearity of $\langle -, - \rangle_\nu$.

3. Formulae

Continuing with the assumption that ν is non-Archimedian, we now describe an algorithm to rapidly compute $\iota_\nu(D, E)$ when $\operatorname{Supp}(D) \cap \operatorname{Supp}(E) \cap \operatorname{Sing}(X) = \emptyset$. First we recall Mumford's coordinate system on $\operatorname{Jac}_{X_\eta}(K) = \operatorname{Jac}_X(K)$.

3.0.1. *Mumford coordinates.* Recall that we have restricted our attention to the case of an odd degree model for X. Let $\infty = \infty_{X_\eta}$ denote the unique point at infinity of X_η.

We use Mumford coordinates to parametrise divisors on the hyperelliptic curve X. We recall the definitions as in [MM84]:

Suppose X_η is defined by the equation $y^2 = f_{2g+1}(x)$ in $A^2_{x,y}$.

A point on $\operatorname{Jac}_{X_\eta}(K)$ is given by a pair (α, β) where α, β in $K[x, y]$ such that:

1. α is monic of degree at most g.
2. $\deg(\beta) < \deg(\alpha)$.
3. α divides $\beta^2 - f$.

The pair (α, β) corresponds to the divisor $\mathbb{V}(\alpha = 0, y - \beta = 0) - \deg(\alpha).\infty$ on X_η. The coefficients of such α, β are then coordinates on an affine piece of the Jacobian of X_η.

3.1. **Resultants.** We work over the base change $\hat{X} \overset{\text{def}}{=} X \times_{\mathcal{O}_{K,\nu}} \hat{\mathcal{O}}_{K,\nu}$ (where $\hat{\mathcal{O}}_{K,\nu}$ is the ν-adic completion of $\mathcal{O}_{K,\nu}$), so we are working in a complete local ring. [Lan88] tells us that the intersection numbers are invariant under this change. We do this so that factorisation in $k(\hat{X})$ better reflects factorisation in $k(X_\nu)$. We may assume D, E are prime divisors. We write

$$D = \mathbb{V}_{\hat{X}}(a_1, y - b_1), \qquad E = \mathbb{V}_{\hat{X}}(a_2, y - b_2),$$

$a_i, b_i \in \hat{\mathcal{O}}_{K,\nu}[x]$. By comparing the leading and constant coefficients of a_1 and a_2 we know whether there is an affine patch of X_ν containing D_ν, E_ν; if not, then $\operatorname{Supp}(D_{\hat{X}}) \cap \operatorname{Supp}(E_{\hat{X}}) \cap X_\nu = \emptyset$ so $\iota_\nu(D_{\hat{X}}, E_{\hat{X}}) = 0$, and otherwise we take a small local field extension[4] and repeat. If necessary, we can make a change of coordinates, so it now suffices to consider the case where a_1 and a_2 are monic with coefficients in $\hat{\mathcal{O}}_{K,\nu}$. Now we will use the fact (see [Lan88, III], after Theorem 5.1) that $\langle -, - \rangle_\nu$ can be uniquely extended to divisors defined over any finite

[4] In practice, this can be done using fast algorithms in [PR01]. For our later computations we made use of a MAGMA implementation of these algorithms.

extension L of the completion $\hat{K}$. If w is the prime of l extending ν on K, we denote this symbol by $\langle -,-\rangle_w$. We get:

(5)
$$\begin{aligned}\frac{\langle\langle D,E\rangle\rangle_\nu}{\#\kappa(\nu)} &= \langle D,E\rangle_\nu = \langle D,E\rangle_w \\ &= \sum_{i,j}\langle \mathbb{V}_{\hat{X}}(x-\alpha_i, y-b_1(\alpha_i)), \mathbb{V}_{\hat{X}}(x-\beta_j, y-b_2(\beta_j))\rangle_w \\ &\quad \text{where } \alpha_i, \beta_j \text{ are the roots of } a_1, a_2 \text{ respectively} \\ &= \sum_{i,j}\min(w(\alpha_i-\beta_j), w(b_1(\alpha_i)-b_2(\beta_j))).\end{aligned}$$

Now suppose further that the multivariate resultant $\mathrm{res}(a_1(x), a_2(x-t), x)$ is irreducible in $\hat{\mathcal{O}}_{K,v}[t]$ (if not, replace $\hat{\mathcal{O}}_{K,v}$ by a suitable finite local extension and repeat). This means that $w(\alpha_i-\beta_j)$ is independent of i and j. In fact,

$$w(\alpha_i-\beta_j) = w(\mathrm{res}(a_1(x), a_2(x-t), x)(0)) \overset{\mathrm{def}}{=} M$$

where the resultant is scaled so as to be monic.

Now let γ have roots $b_1(\alpha_i) - b_2(\beta_j)$ (again γ can be obtained as a multivariate resultant), then

$$\langle D,E\rangle_\nu = \sum_{u|\gamma}\min\left(M, \nu(u(0))\right)\cdot \mathrm{ord}_u\,\gamma,$$

where the sum is over all monic irreducible factors of γ.

Now all the divisors we will need to consider can be written as sums of divisors of the form above together with divisors of the form $\mathbb{V}(x-a)$ for $a \in \mathrm{Frac}(\hat{\mathcal{O}}_{K,\nu})$. Note that the latter can be written as a sum of divisors in Mumford form after a field extension of degree at most two, so combining this with the bilinearity of the Néron symbol we are done. In practice there are often simpler ways to carry out the calculations in these cases, based around the fact that such divisors are locally principal on some Zariski open subset of the curve containing the support of the second divisor with which we wish to compute the intersection.

Müller has an alternative approach to this computation using Grobner bases, which will appear in [Mül10].

4. Computing on normal models

In this section we will work in somewhat greater generality than before as it creates no additional difficulties. Throughout this section, all schemes are assumed separated. Let R be an excellent[5] Noetherian discrete valuation ring, and let t denote a uniformiser. Let $S \overset{\mathrm{def}}{=} \mathrm{Spec}(R)$,

[5] recall that this includes the case of characteristic zero

and let X be a normal integral projective flat scheme over S, with generic fibre X_η of dimension 1. The situation we have in mind, of course, is $R = \mathcal{O}_K$ and X a normal model of a hyperelliptic curve over S.

As before we have that X admits a strong desingularisation $\varphi : X' \to X$ which is proper and birational ([Liu02, Chapter 8, Corollary 3.45]). Also as before we let $\iota_\nu = \iota$ denote the local intersection symbol in the fibre over ν on X or X', $\langle -, - \rangle_\nu = \langle -, - \rangle$ denote the bilinear pairing corresponding to a Néron function defined as in [Lan88], and Φ the unique linear form as defined by Equation4.

Lemma 3. *Let $D \in \mathrm{Div}^0_{X_\eta}(K)$. Then*

$$\varphi_*(D_{X'}) = D_X$$

Proof. First we note that the canonical map $X_\eta \to X$ is not proper, it is impossible to obtain a slick proof from this. It suffices to show that pushforward commutes with taking Zariski closure for proper maps. Now by definition,

$$\varphi_*(D_{X'}) = \varphi(D'_X).[k(D_{X'}) : k(\varphi(D_{X'}))],$$

and $[k(D_{X'}) : k(\varphi(D_{X'}))] = 1$ since there exists a dense open subset of X' whose intersection with $D_{X'}$ is dense in $D_{X'}$ and on which φ is an isomorphism (for example, take the open subset of X' obtained by deleting all points above the divisor of zeros of t), so $D_{X'}$ is birational to $\varphi(D_{X'})$.

It now suffices to show that

$$\varphi(D_{X'}) = D_X.$$

From elementary topology and the Zariski continuity of φ we have that $\varphi(\overline{u}) \subseteq \overline{\varphi(u)}$. But φ is proper and hence closed, so $\varphi(\overline{u}) = \overline{\varphi(u)}$. □

Lemma 4. *Let D, $E \in \mathrm{Div}^0_X(K)$ such that* $\mathrm{Supp}(D) \cap \mathrm{Supp}(E) = \emptyset$.

Let $f \in k(X)$ such that $\mathrm{Supp}(\mathrm{div}_{X_\eta}(f) - D) \cap \mathrm{Supp}(D) = \emptyset$.

Set $F \overset{def}{=} D - \mathrm{div}_{X_\eta}(f)$. Further, suppose:

1) $F_{X_\eta} \cap \mathrm{Sing}(X) = \emptyset$,and

2)For every irreducible component Y of X'_ν, $\iota(F_{X'}, Y) = 0$.

3) $\mathrm{Supp}(F) \cap \mathrm{Supp}(E) = \emptyset$.

Then:

$$\langle D, E\rangle = \langle \mathrm{div}_{X_\eta}(f), E\rangle + \iota(F_X, E_X)$$

Proof.

$$\langle D, E\rangle = \langle \mathrm{div}_{X_\eta}(f) + F, E\rangle = \langle \mathrm{div}_{X_\eta}(f), E\rangle + \langle F, E\rangle.$$

Assumption 2 implies that $\Phi(F) = 0$, so we get

$$\langle D, E\rangle = \langle \mathrm{div}_{X_\eta}(f), E\rangle + \iota(F_{X'}, E_{X'}).$$

It remains to see that, because F_X does not meet $\mathrm{Sing}(X)$, and φ is an isomorphism outside $\mathrm{Sing}(X)$, the local nature of the symbol ι means that $\iota(F_{X'}, D_{X'}) = \iota(F_X, D_X)$.

□

Lemma 5. *In Lemma 4 we can replace condition 2 by:*
2') For every irreducible component Y of X_ν, $\iota(F_X, Y) = 0$.

Proof. Given the local nature of ι, it suffices to show that for every irreducible component Y' of X'_ν such that $\varphi_*(Y') = 0$, we get

$$\iota(F_{X'}, Y') = 0.$$

Recall

$$\iota(F_{X'}, Y') = \sum_x \mathrm{length}_{\mathcal{O}_{X'.x}} \left(\frac{\mathcal{O}_{X'.x}}{I_{F_{X'}}, T_{Y'}} \right)$$

where the sum is over all closed points of X'_ν contained in $\mathrm{Supp}(F_{X'}) \cap \mathrm{Supp}(Y')$. But $\mathrm{Supp}(F_{X'}) \cap \mathrm{Supp}(Y') = \emptyset$ since otherwise $\mathrm{Supp}(F_{X'})$ contains a point p' lying over a singular point p of X and (from Lemma 3),

$$F_X = \varphi_*(F_{X'}) = \varphi(F_{X'}) \ni \varphi(p') = p.$$

□

We are now in a position to prove the main theorem of this section, Theorem 2. It allows us to calculate the intersection pairing of two divisors on X_η solely on the normal surface X, without the need to know any details of the resolution X'.

Proof of Theorem 2. It is well known that if $g \in R[x]$ is a non-square and R is integral, then $y^2 - g$ is irreducible in $R[x, y]$, so the special fibre of X is geometrically irreducible.

It now suffices to see that condition 2' in Lemma 5 can be dropped. Since $\deg(F) = 0$ we know that $\iota(F_{X'}, X_\nu) = 0$. We also know that $\iota(F'_X, Y) = 0$ for every irreducible component Y of X' such that $\varphi_*(Y) = 0$. Components of X'_ν are either contracted by φ or are X_ν. So we are done.

□

5. $\mathbb{Q}$-factoriality for arithmetic surfaces

Again, because it creates no additional difficulties, we work in greater generality than in the remainder of this paper. Given a degree zero divisor D on the generic fibre of a normal flat arithmetic surface with irreducible special fibre, we construct a representative of the linear equivalence class of some non-zero multiple $c.D$ such that the points in the support of this representative all reduce to smooth points of the special fibre. We also show how to bound c. This is an analogue of the classical fact that multiplying a point on an elliptic curve by the Tamagawa number of the curve yields a point of good reduction. At the end of the section we will briefly discuss the effectiveness of this construction.

Lemma 6. *Let S be the spectrum of the ring of integers of a finite extension K of a p-adic field, with closed point ν and generic point η. Let X/S be a normal proper flat arithmetic surface of genus g with connected special fibre. Suppose also that X/S has a smooth section. Let $\varphi : X' \to X$ denote a strong proper minimal desingularisation of X. Then the canonical map $\psi_\nu : \operatorname{Pic}^0_{X_\nu} \to \operatorname{Pic}^0_{X'_\nu}$ induced by φ^* has finite kernel as a map of commutative group functors.*

Proof. We begin by recalling (from [DG80, Section II, 4, 1.2]) the definition of the Lie algebra of a commutative group functor; let $\mathcal{G}$ be a presheaf from Sch/S (the category of S-schemes) to Ab (the category of abelian groups), and define the functor $\mathcal{L}ie(\mathcal{G})$ from Sch/S to Ab by

$$\mathcal{L}ie(\mathcal{G})(T) = \ker\left(\mathcal{G}\left(T \times_{\mathbb{Z}} \frac{\mathbb{Z}[\epsilon]}{\epsilon^2}\right) \xrightarrow{i} \mathcal{G}(T)\right)$$

where i is induced by the canonical immersion $T \overset{i}{\hookrightarrow} T \times_{\mathbb{Z}} \frac{\mathbb{Z}[\epsilon]}{\epsilon^2}$.

Now consider the exact sequence of sheaves

$$0 \to \ker(\psi) \to \operatorname{Pic}^0_X \xrightarrow{\psi} \operatorname{Pic}^0_{X'}.$$

By [LLR04, Proposition 1.1 a], we have that

$$0 \to \mathcal{L}ie(\ker(\psi)) \to \mathcal{L}ie\left(\operatorname{Pic}^0_X\right) \to \mathcal{L}ie\left(\operatorname{Pic}^0_{X'}\right)$$

is exact. Moreover, by [LLR04, Proposition 1.3 b] we have for any quasi-compact separated morphism $f : T \to S$ a functorial isomorphism

$$\mathcal{L}ie\left(\operatorname{Pic}^0_T\right) \cong \mathcal{L}ie\left(\operatorname{Pic}_T\right) \cong R^1 f_* \mathcal{O}_T.$$

We thus obtain an exact sequence

$$0 \to \mathcal{L}ie(\ker(\psi)) \to R^1 f_* \mathcal{O}_X \to R^1 f'_* \mathcal{O}_{X'}$$

which we evaluate at ν to obtain the exact sequence

$$0 \to \mathcal{L}ie(\ker(\psi))(\nu) \to H^1(X_\nu, \mathcal{O}_{X_\nu}) \to H^1(X'_\nu, \mathcal{O}_{X'_\nu}).$$

However, the final map in this sequence is the first non-trivial map in the Leray spectral sequence of the map φ_ν:

$$0 \to H^1(X_\nu, \mathcal{O}_{X_\nu}) \to H^1(X'_\nu, \mathcal{O}_{X'_\nu}) \to H^0\left(X_\nu, R^1\varphi_{\nu*}\mathcal{O}_{X_\nu}\right) \to \cdots$$

and thus is injective, so $\mathcal{L}ie(\ker(\psi))(\nu) = \mathcal{L}ie(\ker(\psi_\nu))(\nu)$ is trivial. Now $\ker(\psi_\nu)$ is representable, reduced and of finite type over ν, so the triviality of $\mathcal{L}ie(\ker(\psi_\nu))(\nu)$ implies that $\ker(\psi_\nu)$ is finite over ν. This shows that $\psi_\nu : \operatorname{Pic}^0_{X_\nu} \to \operatorname{Pic}^0_{X'_\nu}$ is finite.

□

Theorem 7. *Let S be the spectrum of the ring of integers of a finite extension K of a p-adic field, with closed point ν and generic point η. Let X/S be a normal proper flat arithmetic surface of genus g with connected and* ***integral*** *special fibre. Suppose also that X/S has a smooth section. Then, possibly after replacing K by a finite unramified extension, there exists an integer $c > 0$ such that given any effective divisor $D \in Div_X^g(K)$, the linear equivalence class of $c \cdot D$ contains an effective representative E with* ***smooth reduction****.*

Proof. The proof consists of two stages. First (and hardest) we construct a divisor I to behave as the basepoint for addition in the Jacobian of X, satisfying a number of important properties including smooth reduction. This part makes critical use of Lemma 6. Second we show that the divisor obtained by taking large multiples of D converges p-adicly to I, and thus must have smooth reduction.

Step 1. Let $\varphi : X' \to X$ denote a strong proper minimal desingularisation of X. After replacing K by a finite unramified extension we construct an effective divisor $I \in Div_X^g(K)$ such that for every divisor J_ν in the linear system of effective divisors linearly equivalent to $(I_{X'})_\nu$ we have that $\varphi_*(J_\nu)$ has smooth support.

Now since S is Henselian and the desingularisation X' exists, it suffices to construct a divisor I_ν on the special fibre of X with the desired property as we can then use the regularity of X' and the fact the φ is an isomorphism outside the non-regular locus (and hence outside the non-smooth locus) to lift to the generic fibre.

Let ψ denote the canonical map

$$\begin{aligned} \psi : \mathrm{Pic}_X^0 &\to \mathrm{Pic}_{X'}^0 \\ \mathcal{L} &\mapsto \varphi^* \mathcal{L} \end{aligned} \tag{6}$$

(To reassure the reader, Pic_X^0 and $\mathrm{Pic}_{X'}^0$ are representable by [Ray70, Theorem 8.2.1] and the representability of the morphism ψ is not hard to see.)

Let $\vartheta_{X'}$ denote the locus of $\mathrm{Pic}_{X'_\nu}^0$ on which the map $(X'_\nu)_{\mathrm{sm}}^{(g)} \to \mathrm{Pic}_{X'_\nu}^0$ defined by the smooth section is not an isomorphism (the subscript sm means restrict to smooth points). We begin by showing that the image of ψ_ν is not contained within $\vartheta_{X'}$. Since $\mathrm{Pic}_{X'}^0$ is the connected component of the identity of the Neron model of the Jacobian of X_η we know that $\mathrm{Pic}_{X'_\nu}^0$ has dimension g, and by [Ser88, V, 1.6, Proposition 2] we know that $\mathrm{Pic}_{X_\nu}^0$ also has dimension g since X/S is flat and has integral special fibre. Furthermore, from Lemma 6 we have that $\psi_\nu : \mathrm{Pic}_{X_\nu}^0 \to \mathrm{Pic}_{X'_\nu}^0$ is finite as a map of group schemes, and so the dimension of the image of ψ_ν is g, hence it cannot be contained within the locus $\vartheta_{X'}$.

Let U denote the dense open subscheme of $\mathrm{Pic}^0_{X'_\nu}$ which is the intersection of the image of ψ_ν with the complement of $\vartheta_{X'}$. Since ψ_ν is finite, each point in U has a finite number of preimages. Now the closed and non-open condition on divisors on X_ν of having non-smooth support lifts to a closed and non-open condition on U. We can thus choose I_ν to be an effective divisor corresponding to any k point of U all of whose preimages under ψ_ν are represented by effective divisors with smooth support. This must exist after replacing the residue field at ν by a finite extension - this is the unramified extension of K referred to in the statement of the theorem.

Step 2. Let α denote the map $(X_{\mathrm{sm}})^{(g)} \to \mathrm{Pic}^0_X$ constructed using I as a base-point. Let Q denote the largest separated quotient of the open and closed subscheme of $\mathrm{Pic}_{X'}$ consisting of line bundles of total degree zero (this is the Néron model of the Jacobian of X_η since X'_ν has a component of multiplicity one [BLR90, 9.5, Theorem 4]). Let c be a positive integer which kills the finite group $Q(\nu)$. Now $(D_{X'})_\nu$ is smooth as X' is regular, so we can consider the point $\alpha((D_{X'})_\nu) = (\alpha(D_{X'}))_\nu$ on the special fibre of the Néron model. Be definition of c we have $(c.(\alpha(D_{X'})))_\nu = c.(\alpha(D_{X'})_\nu) = Id_{X'_\nu}$, so set E to be a preimage of $c.\alpha(D)$ under α. Now we see that the special fibre of the flat extension of E to X' is linearly equivalent to $(I_{X'})_\nu$, and thus the special fibre of the flat extension of E to X is smooth by our assumption on I_ν.

□

Much of this algorithm is easily seen to be effective. The only part which may cause problems is the construction of the divisor I_ν, as for this we need information on the special fibre of the minimal regular model of X. However, note that I_ν is supported on the locus on which φ_ν is an isomorphism and so can be constructed on X_ν. Also note that the conditions we impose on I_ν are all open, and so in practice simply picking a candidate I_ν with smooth support is likely to succeed. We thus have a probabilistic algorithm which does not require knowledge of the minimal regular model.

6. Archimedean intersections

Fix an Archimedean place '∞' of K (hopefully no confusion will arise with the point at infinity on the hyperelliptic curve, which we will denote by ∞_X from now on). For the remainder of this section we will work in a complex analytic setting, so let X now denote the Riemann surface corresponding to our curve and the place ∞. Let $\mathrm{Jac}(X)$ denote its Jacobian viewed as a complex torus.

Since this is already well documented, we do not repeat the definitions of intersections at infinite places, but refer the reader to [Lan88]. We summarise what we need below.

6.1. **The pde we need to solve.** As a starting point, we take [Lan83, Chapter 13, Theorem 7.2], which we summarise as follows:

Given a pair of divisors $a, b = \sum_i n_i \cdot b_i$ on X of degree zero with disjoint support, let ω be a differential form on X such that the residue divisor $\operatorname{res}(\omega)$ equals a (such an ω can always be found using the Riemann-Roch Theorem). Normalise ω by adding on holomorphic forms until the periods of ω are purely imaginary. Let

$$dg_a \overset{\text{def}}{=} \omega + \bar{\omega} \tag{7}$$

(this g_a is a Green's function for a). Then:

$$< a, b >_\infty = \frac{1}{2} \cdot \sum_i n_i \cdot g_a(b_i).$$

Thus it remains to find, normalise and integrate such an ω.

6.2. **Application of theta functions to the function theory of hyperelliptic curves.** We can use ϑ-functions to solve the pde (7) of Section 6.1, in a very simple way. For background on ϑ-functions we refer to the first two books of the 'Tata lectures on theta' trilogy, [Mum83], [MM84]. ϑ-functions are complex analytic functions on $\mathbb{C}^g$ which satisfy some quasi-periodicity conditions, thus they are an excellent source of differential forms on the (analytic) Jacobian of X. To get from this a differential form on X we simply use that X is canonically embedded in $\operatorname{Jac}(X)$ by the Abel-Jacobi map, so we can pull back forms from $\operatorname{Jac}(X)$ to X.

Fix a symplectic homology basis A_i, B_i on X as in [MM84]; by this we mean that if $i(-,-)$ denotes the intersection of paths, then we require that the A_i, B_i form a basis of $H_1(X, \mathbb{Z})$ such that

$$i(A_i, A_j) = i(B_i, B_j) = 0 \text{ for } i \neq j$$

and

$$i(A_i, B_j) = \delta_{ij}.$$

We also choose a normalised basis $\omega_1, \ldots \omega_g$ of holomorphic 1-forms on X, normalised such that

$$\int_{A_i} \omega_j = \delta_{ij}.$$

We recall the definition and basic properties of the multivariate ϑ-function:

$$\vartheta(z; \Omega) \overset{\text{def}}{=} \sum_{\underline{n} \text{ in } \mathbb{Z}^g} \exp(\pi i \underline{n} \Omega \underline{n}^{\mathrm{T}} + 2\pi i \underline{n} \cdot z) \tag{8}$$

which converges for z in $\mathbb{C}^g$ and Ω a $g \times g$ complex matrix with positive definite imaginary part. The ϑ-function satisfies the following periodicity conditions for $\underline{m}, \underline{n}$ in $\mathbb{Z}^g$:

$$\vartheta(z + \underline{m}; \Omega) = \vartheta(z; \Omega), \tag{9}$$

$$\vartheta(z + \underline{n}\Omega; \Omega) = \exp(-\pi i \underline{n} \Omega \underline{n}^{\mathrm{T}} - 2\pi i \underline{n} z)\, \vartheta(z; \Omega). \tag{10}$$

We will set Ω to be the period matrix of the analytic Jacobian of X with respect to the fixed symplectic homology basis (as in [MM84]), and z will be a coordinate on the analytic Jacobian. This means that

$$\Omega_{ij} = \int_{B_i} \omega_j.$$

Let

$$\delta' \stackrel{\text{def}}{=} \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g$$

$$\delta'' \stackrel{\text{def}}{=} \left(\frac{g}{2}, \frac{g-1}{2}, \ldots, 1, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g$$

$$\Delta \stackrel{\text{def}}{=} \Omega \cdot \delta' + \delta''.$$

Then [MM84, Theorem 5.3, part 1] tells us that

$$\vartheta(\Delta - z) = 0 \Leftrightarrow \left[\exists P_1, \ldots P_{g-1} \in X \text{ such that } z = \sum_{i=1}^{g-1} \int_{\infty}^{P_i} \underline{\omega} \bmod \Omega\right].$$

This is a crucial result which allows us to construct a quasifunction on $\mathrm{Jac}(X)$ with prescribed zeros, and from this obtain the Green's function we seek.

6.3. **Solution of the pde.** Let D, D_0 be two reduced divisors of degree g on X with disjoint support, containing no Weierstrass points or points at infinity.

For z in $\mathrm{Jac}(X)$ we set

$$G(z) = \frac{\vartheta(z + \Delta - \alpha(D))}{\vartheta(z + \Delta - \alpha(D_0))}.$$

Then for p in X we set $F(p) = G(\alpha(p))$ so

$$F(p) = \frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))}. \tag{11}$$

If we let $\omega = d \log F(p)$ then it is clear that $\mathrm{res}(\omega) = D - D_0$. It then remains to normalise ω to make its periods purely imaginary, and then integrate it. We have a homology basis A_i, B_i, and we find:

$$\int_{A_k} \omega = \int_{A_k} d \log F(p) = \log G(\alpha(p) + e_k) - \log G(\alpha(p)) = 0$$

(where $e_k = (0, 0, \ldots 0, \underbrace{1}_{\text{in } k^{th} \text{ position}}, 0 \ldots, 0)$), and

$$\begin{aligned}\int_{B_k}\omega = \int_{B_k} d\log F(p) &= \log G(\alpha(p)+\Omega.e_k) - \log G(\alpha(p))\\ &= 2\pi i e_k^T\cdot(\alpha(D)-\alpha(D_0)) = 2\pi i \underbrace{[\alpha(D)-\alpha(D_0)]_k}_{k^{th}\text{ component}}\end{aligned}$$

From this we can deduce that the normalisation is

$$\omega = d\log\left[\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right] - 2\pi i\left[(\mathrm{Im}(\Omega))^{-1}\,\mathrm{Im}(\alpha(D)-\alpha(D_0))\right].\begin{bmatrix}\omega_1\\ \omega_2\\ \vdots\\ \omega_g\end{bmatrix}$$

where p is a coordinate on X.

Now we integrate to get the Green's function $g_{D-D_0}(p) = \int_{\infty_X}^p \omega + \overline{\omega}$:

$$g_{D-D_0}(p) = 2\log\left|\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right|$$

$$+\,4\pi\left[(\mathrm{Im}(\Omega))^{-1}\,\mathrm{Im}(\alpha(D)-\alpha(D_0))\right].\mathrm{Im}\left(\int_{\infty_X}^{p}\begin{bmatrix}\omega_1\\ \omega_2\\ \vdots\\ \omega_g\end{bmatrix}\right)$$

$$= 2\log\left|\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right| + 4\pi(\mathrm{Im}(\Omega))^{-1}\cdot\mathrm{Im}(\alpha(D)-\alpha(D_0))\cdot\mathrm{Im}\left(\alpha(p)\right)$$

Again, this has been implemented in MAGMA, so given divisors D, D_0 and E, E_0 containing no Weierstrass points or infinite points and having disjoint support[6] then we have

$$< D-D_0, E-E_0 >_\infty = \frac{1}{2}g_{D-D_0}[E-E_0]$$

where $g_{D-D_0}[E-E_0]$ is simply the product over points $p\in\mathrm{Supp}(E-E_0)$ of the complex absolute value of $g(p)$. So we are done.

7. Examples

The algorithm described above has been implemented in MAGMA, with the exception of that contained in Section 5 - instead of implementing this in full, a simpler algorithm which is not guaranteed to always find a smooth representative has been used. Any results given

[6] Thanks are due to Jan Steffen Müller for pointing out that they need **not** have degree g; this may speed up computations considerably

by the algorithm are provably correct. This section contains some examples computed with this implementation, performed on a 2.50 GHz Intel Core2 Quad CPU Q9300 (timings given are illustrative only, and should not be used for benchmarking).

First, we check the parallelogram law for a genus three curve $y^2 = x^7 - 15x^3 + 11x^2 - 13x + 25$, where we let D and E denote the points on the Jacobian corresponding to the points $(1,3)$ and $(0,-5)$ on the curve respectively. We obtain the following:

$$\begin{aligned}
\hat{h}(D) &= 1.77668\ldots \\
\hat{h}(E) &= 1.94307\ldots \\
\hat{h}(D+E) &= 4.35844\ldots \\
\hat{h}(D-E) &= 3.08107\ldots \\
2\hat{h}(D) + 2\hat{h}(E) - \hat{h}(D+E) - \hat{h}(D-E) &= 1.26217 \times 10^{-28}
\end{aligned}$$

with a total running time of 31.75 seconds.

Next we give two families of curves of increasing genus. Firstly the family $y^2 = x^{2g+1} + 2x^2 - 10x + 11$ with D denoting the point $(1,2) - \infty$ on the Jacobian (all times are in seconds unless otherwise stated):

g	$\hat{h}(D)$	time
1	$1.11466\ldots$	1.94
2	$1.35816\ldots$	6.44
3	$1.50616\ldots$	15.10
4	$1.61569\ldots$	32.71
5	$63.4292\ldots$	72.23
6	$1.77778\ldots$	212.37
7	$51.0115\ldots$	20 minutes
8	$1.89845\ldots$	3 hours
9	$78.8561\ldots$	16 hours

Now we consider the family $y^2 = x^{2g+1} + 6x^2 - 4x + 1$ with D denoting the point $(1,2) + (0,1) - 2 \cdot \infty$ on the Jacobian:

g	$\hat{h}(D)$	time/seconds
1	$1.41617\ldots$	2.06
2	$1.37403\ldots$	6.73
3	$1.50396\ldots$	15.62
4	$1.40959\ldots$	32.60
5	$1.70191\ldots$	76.48
6	$1.81093\ldots$	291.17
7	$1.71980\ldots$	1621.50

References

[Ara74] SY Arakelov. An intersection theory for divisors on an arithmetic surface, Math. *USSR izvestija*, 8:1167–1180, 1974.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Springer, 1990.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[DG80] Michel Demazure and Peter Gabriel. *Introduction to algebraic geometry and algebraic groups*, volume 39 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1980. Translated from the French by J. Bell.

[Fal84] G. Faltings. Calculus on arithmetic surfaces. *The Annals of Mathematics*, 119(2):387–424, 1984.

[FS97] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79(4):333–352, 1997.

[Hri85] P. Hriljac. Heights and Arakelov's intersection theory. *American Journal of Mathematics*, 107(1):23–38, 1985.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Lan88] S. Lang. *Introduction to Arakelov theory*. Springer, 1988.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LLR04] Qing Liu, Dino Lorenzini, and Michel Raynaud. Néron models, Lie algebras, and reduction of curves of genus one. *Invent. Math.*, 157(3):455–518, 2004.

[Mül10] J. S. Müller. Canonical heights on Jacobians. *Preprint*, 2010.

[MM84] D. Mumford and C. Musili. *Tata Lectures on Theta: Jacobian theta functions and differential equations*. Springer, 1984.

[Mum61] David Mumford. The topology of normal singularities of an algebraic surface and a criterion for simplicity. *Inst. Hautes Études Sci. Publ. Math.*, (9):5–22, 1961.

[Mum83] D. Mumford. *Tata lectures on theta I*. Birkhäuser, 1983.

[PR01] S. Pauli and X.F. Roblot. On the computation of all extensions of a p-adic field of a given degree. *Mathematics of Computation*, 70(236):1659, 2001.

[Ray70] M. Raynaud. Spécialisation du foncteur de Picard. *Inst. Hautes Études Sci. Publ. Math.*, (38):27–76, 1970.

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: d.s.t.holmes@warwick.ac.uk