# Canonical heights on Jacobians of hyperelliptic curves

Steffen Müller (Universität Oldenburg)
PIMS Summer School on Explicit Methods for Abelian Varieties
University of Calgary

June 2016

Motivation . . . . . . . . . . 4

Canonical heights on Elliptic Curves . . . . . . . . . . 9

Hyperelliptic curves . . . . . . . . . . 15

Intersection theory on regular models . . . . . . . . . . 21

Green's functions and theta functions . . . . . . . . . . 29

Computing canonical heights using Néron symbols . . . . . . . . . . 35

## Canonical height

Let

- $K$ be a number field,
- $A/K$ be an abelian variety, e.g. an elliptic curve or the Jacobian of a smooth projective curve.

A height function on $A(K)$ is supposed to measure the arithmetic complexity (or size) of a point.

In these lectures we'll discuss the canonical height (or Néron-Tate height)

$$\hat{h} : A(K) \to \mathbb{R}_{\geq 0}\,.$$

It has the following properties:

- $\hat{h}$ is a quadratic form.
- $S_B := \{P \in A(K) : \hat{h}(P) \leq B\}$ is finite for all $B \in \mathbb{R}_{\geq 0}$.
- $\hat{h}(P) = 0$ if and only if $P$ has finite order.

We'll focus on those parts of the theory which are useful for explicit methods.



## Outline

- Motivation
- Canonical heights on elliptic curves
- Hyperelliptic curves
- Intersection theory on regular models
- Green's functions and theta functions
- Canonical heights and Néron symbols

### Mordell-Weil

**Theorem (Mordell-Weil).** The group $A(K)$ is finitely generated. In other words, we have

$$A(K) \cong \mathbb{Z}^r \times T\,,$$

where $r$ is a non-negative integer and $T \cong A(K)_{\mathrm{tors}}$ is finite.

We call

- $A(K)$ the Mordell-Weil group of $A/K$;
- $r$ the rank of $A/K$.

The theorem holds in much greater generality, e.g. over arbitrary global fields.



### Descent Lemma

For the proof of the theorem, canonical heights are useful because of the

**Descent lemma.** Suppose that $G$ is an abelian group such that

1. ${}^{G}\!/_{nG}$ is finite for some $n \geq 2$.
2. There is a quadratic form

$$q : G \to \mathbb{R}_{\geq 0}$$

   such that $S_B := \{g \in G : q(g) \leq B\}$ is finite for all $B \in \mathbb{R}_{\geq 0}$.

Then $G$ is finitely generated.

The proof is left as an exercise.
By the descent lemma and the properties of the canonical height, the Mordell-Weil theorem follows from the

**Weak Mordell-Weil theorem.** If $n \geq 2$, then ${}^{A(K)}\!/_{nA(K)}$ is finite.

## Computing generators of $A(K)$

Suppose we've computed

- the rank $r$,
- independent nontorsion points $Q_1, \ldots, Q_r \in A(K)$,
- generators $Q_{r+1}, \ldots, Q_s$ of $A(K)_{\text{tors}}$.

All known methods to compute generators of $A(K)$ using this information require algorithms to

(i) compute $\hat{h}(P)$ for given $P \in A(K)$;
(ii) enumerate $S_B = \{P \in A(K) : \hat{h}(P) \le B\}$ for given $B \in \mathbb{R}_{\ge 0}$.

For instance, if $Q_1, \ldots, Q_s$ are representatives of ${}^{A(K)}\!/\!_{nA(K)}$ for some $n \ge 2$, then your proof of the descent lemma will probably tell you how to compute generators using (i) and (ii).

There are more efficient methods due to Siksek and to Stoll.



## Regulator

For $P,\, Q \in A(K)$, we write

$$\langle P,\, Q\rangle := \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}$$

Let $P_1, \ldots, P_r$ be generators of $A(K)/A(K)_{\text{tors}}$.
Then

$$\mathrm{Reg}(A/K) := \det(\langle P_i,\, P_j\rangle)_{1 \le i,j \le r}$$

is called the regulator of $A/K$.

It appears in the statement of the full Birch and Swinnerton-Dyer conjecture for abelian varieties.

So we need to compute $\mathrm{Reg}(A/K)$ in order to collect empirical evidence for the conjecture.

## Naive heights on elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve, given by an equation

$$y^2 = x^3 + \alpha x + \beta, \quad \alpha, \beta \in \mathbb{Z}$$

and let $O = (0:1:0) \in E(\mathbb{Q})$. An affine point $P \in E(\mathbb{Q})$ is of the form

$$P = (x_P, y_P) = \left(\frac{a_P}{d_P^2}, \frac{b_P}{d_P^3}\right), \quad a_P, b_P, d_P \in \mathbb{Z}, \quad \gcd(a_P, d_P) = 1 = \gcd(b_P, d_P)\,.$$

**Definition.** The naive height of $P$ is

$$h(P) := \frac{1}{2} \log \max\left\{|a_P|, d_P^2\right\} \in \mathbb{R}_{\geq 0}\,.$$

We also set $h(O) = 0$. Then

- $h$ is quadratic up to a bounded function;
- $S'_B := \{P \in E(\mathbb{Q}) : h(P) \leq B\}$ is finite for all $B \in \mathbb{R}_{\geq 0}$.



## Canonical heights on elliptic curves

**Definition (Tate).** The canonical height of $P \in E(\mathbb{Q})$ is

$$\hat{h}(P) := \lim_{n \to \infty} 4^{-n} h(2^n P) \in \mathbb{R}_{\geq 0}\,.$$

**Properties.**

- $\hat{h}$ is a quadratic form.
- $\Psi := h - \hat{h}$ is bounded.
- $S_B := \{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ is finite for all $B \in \mathbb{R}_{\geq 0}$.
- $\hat{h}(P) = 0$ if and only if $P$ has finite order.

**Idea.** Suppose we can compute $\Psi(P)$ for given $P \in E(\mathbb{Q})$ and bound $|\Psi| \leq D$ on $E(\mathbb{Q})$. Then we can

- compute $\hat{h}(P) = h(P) - \Psi(P)$ for given $P \in E(\mathbb{Q})$,
- enumerate $\{P \in E(\mathbb{Q}) : h(P) \leq B + D\} \supset S_B$ for given $B \in \mathbb{R}$.

## Local decomposition of $\Psi$

To analyze $\Psi$, decompose it into local terms.

**Proposition (Néron).** For every place $v$ of $\mathbb{Q}$ there is a $v$-adically continuous bounded function $\Psi_v : E(\mathbb{Q}_v) \to \mathbb{R}$ such that

$$\Psi(P) = \sum_v \Psi_v(P) \quad \text{for all} \quad P \in E(\mathbb{Q}).$$

For a prime number $p$, let $E_0(\mathbb{Q}_p)$ be the set of points which reduce to a smooth point modulo $p$. Then $\Psi_p$ factors through the finite group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$.

There are simple formulas and optimal bounds for the non-archimedean $\Psi_p$ due to Silverman and Cremona-Prickett-Siksek, respectively.

To use Silverman's formulas, one needs some integer factorisation to find which $\Psi_p(P)$ can be non-trivial. For an algorithm which computes $\Psi(P)$ (and hence $\hat{h}(P)$) without any integer factorisation, and runs in quasi-linear time, come to my talk on Friday next week.

12 / 36

## Simple local decomposition

We normalize the absolute values $|\cdot|_p$ for the primes $p$ so that the product formula holds. Then, for $P \in E(\mathbb{Q}) \setminus \{O\}$, we get:

$$h(P) = -\sum_p \log|d_P|_p + \frac{1}{2}\log\max\left\{\frac{|a_P|}{d_P^2}, 1\right\} = \log|d_P| + \frac{1}{2}\max\{\log|x_P|, 0\}$$

So, if we define the archimedean canonical local height by

$$\lambda_\infty(P) := \Psi_\infty(P) - \frac{1}{2}\max\{\log|x_P|, 0\} \quad \text{for} \quad P \in E(\mathbb{R}) \setminus \{O\},$$

then the canonical height of an affine point $P \in E(\mathbb{Q}) \cap \bigcap_p E_0(\mathbb{Q}_p)$ is

$$\hat{h}(P) = h(P) - \Psi_\infty(P) = \log|d_P| + \lambda_\infty(P).$$

Every $P \in E(\mathbb{Q})$ has a multiple $nP \in E(\mathbb{Q}) \cap \bigcap_p E_0(\mathbb{Q}_p)$, so we can use this to compute $\hat{h}(P) = \hat{h}(nP)/n^2$.

13 / 36

## Archimedean canonical local heights

Let $\widetilde{\theta}$ be a normalized theta function with respect to $\tau \in \mathbb{H}$, where $E(\mathbb{C}) \cong \mathbb{C}/_{\mathbb{Z}+\tau\mathbb{Z}}$, let $H$ be the Riemann form associated to $\widetilde{\theta}$, and let $z_P \in \mathbb{C}$ reduce to $P \in E(\mathbb{C})$.

**Proposition (Néron).** For $P \in E(\mathbb{C}) \setminus \{O\}$ we have

$$\lambda_\infty(P) = -\log|\widetilde{\theta}(z_P)| + \frac{\pi}{2}H(z_P, z_P)\,.$$

For instance, we can use a normalized version of

- the Weierstrass sigma function or
- the Riemann theta function with characteristic $\left(\frac{1}{2}, \frac{1}{2}\right)$.

For the latter, we get $H(z,w) = z\bar{w}/\operatorname{Im}(\tau)$ and

$$\widetilde{\theta}(z) = \exp\left(\frac{\pi z^2}{2\operatorname{Im}\tau}\right) \cdot \sum_{m\in\mathbb{Z}} \exp\left(\pi i\tau\left(m+\frac{1}{2}\right)^2 + 2\pi i\left(m+\frac{1}{2}\right)\left(z+\frac{1}{2}\right)\right).$$



# Hyperelliptic curves



## Hyperelliptic curves

Let $K$ be a field of characteristic $\neq 2$.

A hyperelliptic curve $C/K$ of genus $g \geq 1$ is given by an equation $Y^2 = F(X,Z)$ in the weighted projective plane $\mathbb{P}^2_K(1, g+1, 1)$, where

- $F \in K[X,Z]$ is a binary form of degree $2g+2$,
- $\operatorname{disc}(F) \neq 0$.

$C$ is covered by the two standard affine charts

$$y^2 = f(x) := F(x,1)$$

and

$$t^2 = \widetilde{f}(s) := F(1,s).$$

For simplicity, we will assume that $f$ has degree $2g+1$ and is monic. Then $C(\mathbb{Q}) \ni O = (1:0:0)$ is the unique point of $C$ not on $y^2 = f(x)$.

Let $A$ be the Jacobian of $C$. Then $A(K) \cong \operatorname{Pic}^0(C/K)$, so every $P \in A(K)$ has a representative $D \in \operatorname{Div}^0(C/K) = \{D \in \operatorname{Div}(C/K) : \deg(D) = 0\}$.

## Points on the Jacobian

Let $C/K$ be an odd degree hyperelliptic curve as above.

An effective divisor $D = \sum_{i=1}^{d}(P_i) \in \mathrm{Div}(C/K)$ is called reduced if

- $0 \le d \le g$,
- $P_i \ne O$ for all $i$,
- $P_i \ne w(P_j)$ for all $j \ne i$, where $w(X:Y:Z) = (X:-Y:Z)$ is the hyperelliptic involution on $X$.

If $D$ is a reduced divisor, then there are unique $a, b \in K[x]$ such that

- $a$ is monic of degree $d$ and factors as $a(x) = \prod_{i=1}^{d}(x - x_{P_i})$;
- $b$ has degree at most $d-1$ and we have $b(x_{P_i}) = y_{P_i}$ for all $i$;
- there is a polynomial $c \in K[x]$ such that $b^2 - f = ac$.

**Fact.** If $P \in A(K)$, then there is a unique representative $D - d(O)$ of $P$ such that $D$ is reduced.

We call the pair $(a, b)$ the Mumford representation of $D$ or of $P$.



## Higher genus: The Kummer variety

For the Jacobian $A/\mathbb{Q}$ of a hyperelliptic curve of genus $g$, the naive height can be defined as follows:
Let $\kappa : A \to \mathbb{P}^{2^g-1}$ be such that $\kappa(A)$ is a model for the Kummer variety $\mathcal{K} = {}^{A}\!/_{\{\pm 1\}}$ of $A$.
Define the naive height of $P \in A(\mathbb{Q})$ as

$$h(P) := h(\kappa(P)) = \log\max\{|\kappa_1(P)|, \ldots, |\kappa_{2^g}(P)|\}$$

and the canonical height as

$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h(2^n P)\,.$$

One can use this to compute $\hat{h}(P)$ and bound $\Psi = h - \hat{h}$ when

- $A$ is the Jacobian of a curve of genus 2 (Flynn-Smart, Stoll, M.-Stoll),
- $A$ is the Jacobian of a hyperelliptic curve of genus 3 (Stoll).

For $g > 3$, this seems hopeless in practice, because the explicit arithmetic of $\mathcal{K}$ is too complicated.

## Canonical heights on Jacobians: Idea

Let $C/\mathbb{Q}$ be an odd degree hyperelliptic curve as above and let $A$ denote its Jacobian.

**Idea.** Instead of using the structure of $A$ as a variety, express the canonical height using only data on $C$.

Arakelov conjectured that $\hat{h}$ can be expressed using arithmetic intersection theory. This was proved by Hriljac and Faltings.

We'll develop the theory for general "nice" curves and restrict to the hyperelliptic case for explicit results.

**Remark.** In addition to the computation of the regulator, generators of $A(\mathbb{Q})$ are also needed to apply an algorithm of Bugeaud, Mignotte, Siksek, Stoll and Tengely which computes the integral points on $C$.



## Faltings-Hriljac

Let $C/\mathbb{Q}$ be an odd degree hyperelliptic curve as above and let $A$ denote its Jacobian. Let $P, Q \in A(\mathbb{Q})$ and let $D,\, E \in \mathrm{Div}^0(C/\mathbb{Q})$ be representatives of $P$ and $Q$, respectively, with disjoint support.

For a prime $p$, consider the divisors $D \otimes \mathbb{Q}_p$ and $E \otimes \mathbb{Q}_p$ on the curve $C \otimes \mathbb{Q}_p$. Also consider the divisors $D \otimes \mathbb{C}$ and $E \otimes \mathbb{C}$ on the Riemann surface $C(\mathbb{C})$.

**Theorem (Faltings, Hriljcac).** The canonical height pairing

$$\langle P, Q\rangle = \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}$$

between $P$ and $Q$ is given by

$$\langle P,\, Q\rangle = -\sum_p \langle D \otimes \mathbb{Q}_p, E \otimes \mathbb{Q}_p\rangle_p \cdot \log p - \langle D \otimes \mathbb{C}, E \otimes \mathbb{C}\rangle_\infty \,,$$

where $\langle\ ,\ \rangle_v$ is the Néron symbol on $C \otimes \mathbb{Q}_v$ – to be constructed today.

### Models

Let $R$ be a discrete valuation ring with

- normalized discrete valuation $v$,
- fraction field $K$ of characteristic 0,
- perfect residue field $k$,
- spectrum $S = \operatorname{Spec} R$.

Let $C/K$ be a nice (i.e. smooth projective geometrically irreducible) curve.

A model $\pi : \mathcal{C} \to S$ of $C$ over $S$ is an integral, normal, two-dimensional $S$-scheme which is proper, flat and of finite type over $S$, such that the generic fiber $\mathcal{C}_0 = \mathcal{C} \otimes K$ of $\mathcal{C}$ is isomorphic to $C$.

In other words, a model is a proper arithmetic surface over $R$.

You should think of this as an arithmetic analogue of an algebraic surface which is fibered over a base curve.



### Facts about models

Let $\pi : \mathcal{C} \to S$ be a model of a nice curve $C/K$.

- The special fiber $\mathcal{C}_v = \mathcal{C} \otimes k$ is a connected curve over $k$.
- A section $\mathcal{P} \in \mathcal{C}(R)$ gives rise to a $K$-rational point $P$ on the generic fiber by specialization, so we get a natural map $\mathcal{C}(R) \to C(K)$.
  By the valuative criterion of properness, this map is a bijection, so every $P \in C(K)$ extends to a section $P_{\mathcal{C}} \in \mathcal{C}(R)$.
- If $P \in C(K)$, then we call the specialization of $P_{\mathcal{C}}$ to the special fiber $\mathcal{C}_v$ the reduction of $P$ (or of $P_{\mathcal{C}}$).
- Let $P \in \mathcal{C}$ with local ring $\mathcal{O}_{\mathcal{C},P}$ and maximal ideal $\mathfrak{m}_{\mathcal{C},P}$. We call $P$ regular if the dimension of $\mathfrak{m}_{\mathcal{C},P}/\mathfrak{m}^2_{\mathcal{C},P}$ as an $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$-vector space is 2.
- We call $\mathcal{C}$ regular if all points on $\mathcal{C}$ are regular.
- If $\mathcal{C}$ is regular, then the reduction of every $P \in C(K)$ is a smooth point in $\mathcal{C}_v(k)$.

**Theorem (Abhyankar, Lipman).** Let $C/K$ be a nice curve. Then there is a regular model $\mathcal{C}$ of $C$ over $R$.

## Divisors on regular models

Let $\pi : \mathcal{C} \to S$ be a regular model of a nice curve $C/K$.

An irreducible divisor on $\mathcal{C}$ is either

1. the closure $D_{\mathcal{C}}$ of an irreducible divisor $D \in \mathrm{Div}(C/K)$ (e.g. a section) or
2. an irreducible component $\Gamma$ of $\mathcal{C}_v$.

The divisor group $\mathrm{Div}(\mathcal{C}/R)$ is the free abelian group on these irreducible divisors.

We extend the assignment $D \mapsto D_{\mathcal{C}}$ to arbitrary $D \in \mathrm{Div}(C/K)$ by linearity.

We call $\mathcal{D} = \sum_i n_i \mathcal{D}_i \in \mathrm{Div}(\mathcal{C}/R)$ horizontal if all $\mathcal{D}_i$ are irreducible of type (i) and vertical if all $\mathcal{D}_i$ are irreducible of type (ii).

The vertical divisors form a group $\mathrm{Div}_v(\mathcal{C}/K)$.

24 / 36

## Intersection multiplicity

Let $\pi : \mathcal{C} \to S$ be a regular model of a nice curve $C/K$.

Let $\mathcal{D}, \mathcal{E} \in \mathrm{Div}(\mathcal{C}/R)$ be effective divisors without common component.

Let $z \in \mathcal{C}_v$ be a closed point and let $f, g \in \mathcal{O}_{\mathcal{C},z}$ be respective local equations for $\mathcal{D}, \mathcal{E}$ in $z$.

The intersection multiplicity of $\mathcal{D}$ and $\mathcal{E}$ in $z$ is defined by

$$(\mathcal{D} \cdot \mathcal{E})_z := \dim_k \mathcal{O}_{\mathcal{C},z}/(f,g) \in \mathbb{Z}_{\geq 0} .$$

The total intersection multiplicity of $\mathcal{D}$ and $\mathcal{E}$ is defined by

$$(\mathcal{D} \cdot \mathcal{E}) := \sum_z (\mathcal{D} \cdot \mathcal{E})_z \in \mathbb{Z}_{\geq 0} ,$$

where the sum is over all closed points of $\mathcal{C}_v$.

We extend these to divisors in $\mathrm{Div}(\mathcal{C}/R)$ without common component by linearity.

25 / 36

## Vertical intersection multiplicities

The total intersection multiplicity is symmetric (obviously) and bilinear (less obviously), but in general it does not respect linear equivalence. However, we have:

**Lemma.** Let $E = \operatorname{div}(\varphi) \in \operatorname{Div}(\mathcal{C}/R)$ be a principal divisor and let $\Gamma \in \operatorname{Div}_v(\mathcal{C}/R)$ be vertical. Then $(\Gamma \cdot E) = 0$. In particular, we have $(\Gamma \cdot \mathcal{C}_v) = 0$, if we view $\mathcal{C}_v$ is a (principal) divisor on $\mathcal{C}$.

Hence the intersection of a vertical divisor with an arbitrary divisor class is well-defined.

Let $\mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R) := \operatorname{Div}_v(\mathcal{C}/R) \otimes \mathbb{Q}$ and let $\mathbb{Q}\mathcal{C}_v \subset \mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)$ consist of the rational multiples of $\mathcal{C}_v$.

Then we get a well-defined symmetric bilinear pairing

$$\mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)/\mathbb{Q}\mathcal{C}_v \times \mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)/\mathbb{Q}\mathcal{C}_v \to \mathbb{Q}\,.$$



## Intersection matrix

Let $\mathcal{C}_v = \sum_{i=1}^n a_i\Gamma_i$, where the $\Gamma_i$ are the irreducible components of $\mathcal{C}_v$ and the $a_i$ are positive integers.

Let $M = (m_{ij})_{i,j}$ be the intersection matrix of $\mathcal{C}_v$, where $m_{ij} = (a_i\Gamma_i \cdot a_j\Gamma_j)$.

**Proposition.**

(a) $m_{ij} = m_{ji} \geq 0$ for all $i \neq j$.
(b) $\sum_{j=1}^n m_{ij} = 0$ for all $i \in \{1, \ldots, n\}$.
(c) $M$ is negative semi-definite.
(d) The kernel of $M$ is spanned by the vector ${}^t(1 \ \ldots \ 1)$.

**Corollary.** Let $\Gamma \in \mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)$. Then we have $\Gamma^2 := (\Gamma \cdot \Gamma) \leq 0$ and the following are equivalent:

(i) $\Gamma^2 = 0$,
(ii) $(\Gamma \cdot \Delta) = 0$ for all $\Delta \in \mathbb{Q}\operatorname{Div}_v(\mathcal{C}/R)$,
(iii) $\Gamma = a\,\mathcal{C}_v$ for some $a \in \mathbb{Q}$.

### Non-archimedean Néron symbols

This gives us an (almost) canonical way to extend a divisor $D \in \mathrm{Div}^0(C/K)$ on $C \cong \mathcal{C}_0$ to $\mathcal{C}$.

**Theorem (Manin).** There is a unique linear map

$$\Phi : \mathrm{Div}^0(C/K) \to \mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}/R)/\mathbb{Q}\,\mathcal{C}_v$$

such that for all $D \in \mathrm{Div}^0(C/K)$ and all $\Gamma \in \mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}/R)$, we have

$$(D_{\mathcal{C}} + \Phi(D) \cdot \Gamma) = 0\,.$$

**Definition.** Let $D$, $E \in \mathrm{Div}^0(C/K)$ have disjoint support. Then the Néron symbol of $D$ and $E$ is defined as

$$\langle D, E\rangle_v := (D_{\mathcal{C}} + \Phi(D) \cdot E_{\mathcal{C}} + \Phi(E)) \in \mathbb{Q}\,.$$

**Proposition.** The Néron symbol is bilinear and symmetric. If $D = \mathrm{div}(\varphi)$ is principal, then $\langle D, E\rangle_v = v(\varphi(E))$.

28 / 36

## Green's functions and theta functions

29 / 36

### Green's functions

Let $X$ be a compact Riemann surface, let $D \in \mathrm{Div}(X)$ and let $d\mu$ be a volume form on $X$ such that $\int_X d\mu = 1$.

**Definition.** A Green's function on $X$ with respect to $D$ (and $d\mu$) is a smooth function $g_D : X \setminus \mathrm{supp}(D) \to \mathbb{R}$ such that

(i) $g_D$ has a logarithmic singularity along $D$,
(ii) $i \cdot \partial\overline{\partial} g_D = \pi \deg(D) d\mu\,,$
(iii) $\int_X g_D d\mu = 0\,.$

Note that $g_D$ is uniquely determined and $g_{D_1+D_2} = g_{D_1} + g_{D_2}$.

If $D$ has degree 0, then (ii) means that $g_D$ is harmonic.
If, moreover, $E = \sum_j b_j\,(Q_j) \in \mathrm{Div}^0(X)$ has disjoint support from $D$, then all functions $g_D$ satisfying (i) and (ii) lead to the same value of

$$g_D(E) := \sum_j b_j\, g_D(Q_j)\,.$$

30 / 36

## Archimedean Néron symbols

Let $X$ be a compact Riemann surface of genus $g > 0$ and let $D,\, E \in \mathrm{Div}^0(X)$ have disjoint support.

Then the Néron symbol of $D$ and $E$ is defined by

$$\langle D, E\rangle_\infty := g_D(E)\,,$$

where $g_D$ satisfies (i) and (ii) above.

**Proposition.** The Néron symbol is bilinear and symmetric. If $D = \mathrm{div}(\varphi)$ is principal, then $\langle D, E\rangle_\infty = -\log|\varphi(E)|$.

**Theorem (Hriljac – very vague version).** Let $D \in \mathrm{Div}(X)$ be non-special. Then a function satisfying (i) and (ii) with respect to $D$ and the canonical volume form on $X$ can be constructed by pulling back to $X$ a translate of an archimedean canonical local height on the Jacobian $J$ of $X$ with respect to a theta divisor.



## Riemann $\theta$-function with characteristic

Let

$$J = \mathrm{Jac}(X) \cong \mathbb{C}^g/_{\mathbb{Z}^g + \tau\mathbb{Z}^g} \quad \text{and} \quad \pi : \mathbb{C}^g \twoheadrightarrow J\,,$$

where $\tau \in \mathbb{C}^{g\times g}$ has positive definite imaginary part. Fix a base point $O \in X$, let

$$\iota : X \to J\,;\; P \mapsto [(P) - (O)]$$

be the corresponding Abel-Jacobi map and let

$$\Theta = \{\iota(P_1) + \ldots + \iota(P_{g-1}) : P_1, \ldots, P_{g-1} \in X\}$$

be the corresponding theta divisor on $J$. We linearly extend $\iota$ to $\mathrm{Div}(X)$.
For $a, b \in \left(\frac{1}{2}\mathbb{Z}\right)^g$ and $\tau$ as above we define the Riemann theta function with characteristic $[a; b]$ as a function on $\mathbb{C}^g$ by

$$\theta_{a,b}(z) = \sum_{m\in\mathbb{Z}^g} \exp\left(2\pi i \left(\frac{1}{2}{}^t(m+a)\tau(m+a) + {}^t(m+a)(z+b)\right)\right)\,.$$

## A normalized theta function

Now let $a = \left(\frac{1}{2}, \ldots, \frac{1}{2}\right), b = \left(\frac{g}{2}, \frac{g-1}{2}, \ldots, 1, \frac{1}{2}\right) \in \left(\frac{1}{2}\mathbb{Z}\right)^g$. Then

- $\theta_{a,b}$ is odd and entire;
- the divisor of $\theta_{a,b}$ on $\mathbb{C}^g$ is $\pi^*\Theta$;
- the Riemann form associated to $\theta_{a,b}$ is $H(z,w) = {}^t z \operatorname{Im}(\tau)^{-1}\overline{w}$.

The "normalized" theta function associated to $\theta_{a,b}$ is

$$\widetilde{\theta}_{a,b}(z) := \theta_{a,b}(z) \exp\left(\frac{\pi}{2} {}^t z (\operatorname{Im}\tau)^{-1} z\right).$$

**Theorem.** Let $D \in \operatorname{Div}(X)$ be non-special, i.e. $D$ is effective, $\deg(D) = g$ and $\dim \mathcal{L}(D) = 1$, and define $g_D : X \setminus \operatorname{supp} D \to \mathbb{R}$ by

$$g_D(P) := -\log|\theta_{a,b}(z_{P-D})| + \pi^t \operatorname{Im}(z_{P-D}) \operatorname{Im}(\tau)^{-1} \operatorname{Im}(z_{P-D}),$$

where for $E \in \operatorname{Div}(X)$, $z_E \in \mathbb{C}^g$ is such that $\pi(z_E) = \iota(E) \in J$. Then $g_D$ satisfies properties (i) and (ii) w.r.t. $D$ and the canonical volume form on $X$.



## Néron symbols in terms of $\theta_{a,b}$

**Proposition.** Let $D_1$, $D_2$, $E_1$, $E_2 \in \operatorname{Div}(X)$ be effective divisors with disjoint support such that $D_1$ and $D_2$ are non-special and we have $E_1 = \sum_{i=1}^d (P_i)$ and $E_2 = \sum_{i=1}^d (Q_i)$. Then

$$\begin{aligned}\langle D_1 - D_2, E_1 - E_2\rangle_\infty = &-\log \prod_{i=1}^d \left|\frac{\theta_{a,b}(z_{P_i} - z_{D_1})\,\theta_{a,b}(z_{Q_i} - z_{D_2})}{\theta_{a,b}(z_{P_i} - z_{D_2})\,\theta_{a,b}(z_{Q_i} - z_{D_1})}\right| \\ &- 2\pi \sum_{i=1}^d {}^t \operatorname{Im}(z_{D_1 - D_2}) \operatorname{Im}(\tau)^{-1} \operatorname{Im}(z_{P_i} - z_{Q_i}).\end{aligned}$$

where for $E \in \operatorname{Div}(X)$, $z_E \in \mathbb{C}^g$ is such that $\pi(z_E) = \iota(E) \in J$.

Note that for all $P, Q \in J$ we can find such representatives $E_1 - E_2$ of $Q$ and $D_1 - D_2$ of some multiple $nP$.

### Faltings-Hriljac

Let $C/\mathbb{Q}$ be a nice curve with Jacobian $A$.

Let $P, Q \in A(\mathbb{Q})$ and let $D, E \in \mathrm{Div}^0(C/\mathbb{Q})$ be representatives of $P$ and $Q$, respectively, with disjoint support.

For a prime $p$, consider the divisors $D \otimes \mathbb{Q}_p$ and $E \otimes \mathbb{Q}_p$ on the curve $C \otimes \mathbb{Q}_p$. Also consider the divisors $D \otimes \mathbb{C}$ and $E \otimes \mathbb{C}$ on the Riemann surface $C(\mathbb{C})$.

**Theorem (Faltings, Hriljcac).** The canonical height pairing

$$\langle P, Q \rangle = \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}$$

between $P$ and $Q$ is given by

$$\langle P,\, Q \rangle = -\sum_p \langle D \otimes \mathbb{Q}_p, E \otimes \mathbb{Q}_p \rangle_p \cdot \log p - \langle D \otimes \mathbb{C}, E \otimes \mathbb{C} \rangle_\infty \,.$$

This can be used for an algorithm to compute $\langle P, Q \rangle$ – at least when $C$ is hyperelliptic (Holmes, M.).