Computing canonical heights on Jacobians

Jan Steffen Müller

Universität Bayreuth

Rational Points – Theory & Experiment

Zürich, May 28, 2010

Introduction

- $C/\mathbb{Q}$: smooth projective curve of genus $g \geq 1$ with Jacobian J
- $D \in \mathrm{Div}(J)(\mathbb{Q})$: ample and symmetric
- h_D: Weil height on $J(\bar{\mathbb{Q}})$ defined using a basis of $\mathcal{L}(D)$, called naive height

The canonical height or Néron-Tate height $\hat{h}_D : J(\bar{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ is defined by

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

(a) $\hat{h}_D$ is a positive definite quadratic form on $J(\bar{\mathbb{Q}})$/torsion and $J(\bar{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

(b) $\hat{h}_D - h_D$ is bounded.

(c) $\hat{h}_D = \hat{h}_{D'}$ if D is linearly equivalent to D'.

(d) $\hat{h}_D$ is the unique quadratic form in the class of Weil heights wrt. D.

Mordell-Weil group

- T: Torsion subgroup of $J(\mathbb{Q})$.
- $\Lambda := J(\mathbb{Q})/T \cong \mathbb{Z}^r$, where $r = \mathrm{Rank}(J(\mathbb{Q}))$.

$\Rightarrow (\Lambda, \hat{h}_D)$ is a lattice in $J(\mathbb{Q}) \otimes \mathbb{R}$.

Given a finite index subgroup of Λ, we can use the lattice structure to find generators of $J(\mathbb{Q})$ assuming we have

1. a bound on $\sup_{P \in J(\mathbb{Q})} |\hat{h}_D(P) - h_D(P)|$,
2. an algorithm for the computation of $\hat{h}_D$,
3. a method for enumerating $\{P \in J(\mathbb{Q}) : h_D(P) \leq B\}$ for a given bound B.

We will concentrate on 2 in this talk.

Some other applications

Suppose we have found generators $P_1, \ldots, P_r$ of Λ and generators of T.

Assuming this, Bugeaud, Mignotte, Siksek, Stoll and Tengely have combined a variant of the Mordell-Weil sieve with linear forms in logarithms to provide an algorithm for the computation of all integral points on (hyperelliptic) curves.

Let $m_{ij} := \frac{\hat{h}_D(P_i+P_j)-\hat{h}_D(P_i)-\hat{h}_D(P_j)}{2}$ for $1 \leq i,j \leq r$.

The regulator $R = \det\left((m_{ij})_{1\leq i,j\leq r}\right)$ appears in the statement of the Birch and Swinnerton-Dyer conjecture for abelian varieties.

So we need a method to compute R in order to collect empirical evidence for the conjecture.

Local heights

For each place $v \in M_{\mathbb{Q}}$ there are functions

$$\lambda_v : J(\mathbb{Q}_v) \setminus \mathrm{supp}(D) \to \mathbb{R},$$

called local heights such that (among other properties)

- If $P \in J(\mathbb{Q}) \setminus \mathrm{supp}(D)$, then $h_D(P) = \sum_{v \in M_{\mathbb{Q}}} \lambda_v(P)$.
- If $P \in J(\mathbb{Q}) \setminus \mathrm{supp}(D)$, then $\lambda_v(P) = 0$ for almost all v.
- If $P, 2P \in J(\mathbb{Q}_v) \setminus \mathrm{supp}(D)$, then

  $$\lambda_v(2P) - 4\lambda_v(P) = -\log|\beta(P)|_v + \varepsilon_v(P),$$

  where $[2]^*D = 4D + (\beta)$ and $\varepsilon_v : J(\mathbb{Q}_v) \to \mathbb{R}$ is bounded and continuous.

Then we have

$$h_D(2P) - 4h_D(P) = \sum_{v \in M_{\mathbb{Q}}} \varepsilon_v(P),$$

so ε_v measures locally how far away h_D is from a quadratic form.

Local error functions

We fix a local height λ_v and define

$$\mu_v(P) = \sum_{n=0}^{\infty} 4^{-n-1} \varepsilon_v\left(2^n P\right).$$

Then we get

$$\hat{h}_D(P) = h_D(P) + \sum_{v \in M_{\mathbb{Q}}} \mu_v(P) \text{ if } P \in J(\mathbb{Q}).$$

There are no convergence problems, because $\mu_v(P) = 0$ holds for almost all $v \in M_{\mathbb{Q}}$.

From now on, we want to compute $\mu_v(P)$ for all places v.

$\mu_\infty(P)$ can be approximated using its series expansion if we have an upper bound on $|\varepsilon_\infty(P)|$ or using theta functions.

Néron models

- $v = v_p \in M_{\mathbb{Q}}$ non-archimedean with residue characteristic p
- $\mathcal{C}^{\mathsf{min}}$: minimal regular model of C over Spec($\mathbb{Z}_p$) with special fiber $\mathcal{C}_v^{\mathsf{min}}$
- $\mathcal{J}$: Néron model of J over Spec($\mathbb{Z}_p$) or Spec($\mathbb{Z}_p^{\mathsf{nr}}$)
- $\mathcal{J}^0$: connected component of the identity of the special fiber of $\mathcal{J}$
- $J^0 = \{P \in J(\mathbb{Q}_p^{\mathsf{nr}}) : P \text{ reduces to } \mathcal{J}^0\}$
- $\Phi_v = J(\mathbb{Q}_p^{\mathsf{nr}})/J^0(\mathbb{Q}_p^{\mathsf{nr}})$, a finite group isomorphic to the component group of $\mathcal{J}$

Assumption: The gcd of the geometric multiplicities of the components of $\mathcal{C}_v^{\mathsf{min}}$ equals 1.

Lemma 1. (Raynaud)
Φ_v can be computed from the intersection matrix of $\mathcal{C}_v^{\mathsf{min}}$.

Elliptic curves – setup

- $E/\mathbb{Q}$: elliptic curve given by a Weierstrass equation with identity O,

- $D = 2(O)$

- $\kappa(P) = (x(P) : 1) \in \mathbb{P}^1$

We choose

- $h_D(P) = h(\kappa(P))$

- $\lambda_v(P) = \max\{\log |x(P)|_v, 0\}$ for $v \in M_{\mathbb{Q}}$ and $P \in E(\mathbb{Q}_v) \setminus \{O\}$

Elliptic curves – non-archimedean places

Suppose $v = v_p \in M_{\mathbb{Q}}$ is non-archimedean with residue characteristic p

Proposition 2. (Néron, Tate)
If E is given by a v-minimal Weierstrass model, then ε_v and μ_v factor through the component group Φ_v.

Tate and Silverman used this to find formulas for μ_v, depending on the reduction type of E at v.

Example.
Suppose E has multiplicative reduction at v such that $\Phi_v \cong \mathbb{Z}/m\mathbb{Z}$. Let $P = (x, y) \in E(\mathbb{Q}_p) \setminus E^0(\mathbb{Q}_p)$ and let $i = \min\{\mathrm{ord}_v(2y + a_1x + a_3), m/2\}$.
Then we have

$$\mu_v(P) = -\frac{i(m-i)}{m} \log p.$$

Genus 2 – setup

- $C : y^2 + h(x)y = f(x)$: genus 2 curve over $\mathbb{Q}$ with Jacobian J, where $h(x), f(x) \in \mathbb{Z}[x]$ have degree at most 3,6, respectively

- $K = J/\{\pm 1\}$: Kummer surface of J

- $\kappa = (\kappa_1, \ldots, \kappa_4) : J \to K \hookrightarrow \mathbb{P}^3$ explicit quotient map (Flynn, M.)

- $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$, δ_i suitably normalized homogeneous polynomials on K satisfying $\delta(\kappa(P)) = \kappa(2P)$,

- $D \in \mathrm{Div}(J)(\mathbb{Q})$ such that $\mathcal{L}(D) = \langle \kappa_1, \ldots, \kappa_4 \rangle$ and $P \in \mathrm{supp}(D) \Leftrightarrow \kappa_1(P) = 0$.

(If we have a Weierstrass point $\infty \in C(\mathbb{Q})$, then $D = 2\Theta$, where Θ is the theta divisor on J corresponding to ∞.)

We use $h_D(P) = h(\kappa(P))$.

Genus 2 – local heights

- $v \in M_{\mathbb{Q}}$
- $P \in J(\mathbb{Q}_v) \setminus \mathrm{supp}(D)$
- $x = (x_1, x_2, x_3, x_4)$: a set of projective coordinates for $\kappa(P) \in K$ normalized by $x_i = \frac{\kappa_i(P)}{\kappa_1(P)}$

We use

$$\lambda_v(P) = \max\{\log |x_i|_v)\}.$$

If $P, 2P \notin \mathrm{supp}(D)$, then $\lambda_v(2P) - 4\lambda_v(P) = -\log |\beta(P)|_v + \varepsilon_v(P)$, where

- $\beta(P) = \delta_1(x)$
- $\varepsilon_v(P) = \max\{\log |\delta_i(x)|_v\} - 4\max\{\log |x_i|_v\}$ does not depend on the normalization x of $\kappa(P)$.

There is an algorithm to compute $\widehat{h}_D$ due to Flynn, Smart and Stoll.
Problem: Need to compute possibly large multiples of P.

Genus 2 – non-archimedean places

Let $v = v_p \in M_{\mathbb{Q}}$ be non-archimedean with residue characteristic p.

Idea: Find formulas for μ_v depending on the reduction type.

We say that the given model of C satisfies condition (†) if $\mathcal{C}^{\mathrm{min}}$ can be constructed from the closure of C over Spec($\mathbb{Z}_p$) using only blow-ups.

Proposition 3. (M.)
If condition (†) is satisfied for the given model of C, then ε_v and μ_v factor through the component group Φ_v of the Néron model.

Problems.

- Not all genus 2 curves have a model satisfying condition (†).
- There are more than 100 different reduction types (Namikawa-Ueno)

Genus 2 – simplification

But: There are simple formulas describing the behavior of μ_v under transformations.

Lemma 4. (Stoll)
There is an extension $k/\mathbb{Q}_p$ of ramification degree not divisible by a prime > 5 such that C has a model whose reduction contains no points of multiplicity > 3 and at most one point of multiplicity 3.

We have to find formulas for $\mu_v(P)$ for the possible models in Lemma 4.

- If there are no triple points, there are formulas similar to the genus 1 case.

- Otherwise, condition (†) might not be satisfied.

Genus 2 – an example

Example. $C_m : y^2 = (x^3 + p^{6m+2})(x+1)(x-1), m \geq 0, p > 2$

- C_m satisfies condition $(\dagger) \Leftrightarrow m = 0$
- $\#\Phi_v = 3$ for all $m \geq 0$

Suppose $P \in J^0(\mathbb{Q}_p)$. Then we have

$$\mu_v(P) = -\min\{\mathrm{ord}_v(x_3), \mathrm{ord}_v(x_4), m\} \log(p),$$

where $x = (x_1, x_2, x_3, x_4)$ are v-integral coordinates of $\kappa(P)$ such that some x_i is a unit.

There are similar formulas for all models allowed in Lemma 4.

Genus 3

Now suppose C is hyperelliptic and has genus 3.

Idea: Use the Kummer threefold K associated to J. We have

- an embedding of K into $\mathbb{P}^7$ (Stubbs)
- defining equations (1 quadric, 34 quartics) for this embedding (Stubbs, M.)
- partial results on explicit arithmetic on K (Duquesne).

Proposition 3 continues to hold.

This is still work in progress (joint with Duquesne).

Arakelov theory approach

For other curves the local heights approach is not feasible.

Idea: Suppose $\Theta \in \mathrm{Div}(J)(\mathbb{Q})$. Express $\hat{h}_{\Theta^+ \Theta^-}$ in terms of arithmetic intersection theory on a regular model of C over $\mathrm{Spec}(\mathbb{Z})$ (Faltings, Hriljac).

- Non-archimedean intersection numbers can be computed using resultants (Holmes) or Gröbner bases (M.).

- Archimedean intersection numbers can be computed using theta functions on the analytic Jacobian (Hriljac, Lang).

The algorithm is essentially complete for hyperelliptic curves and it should be practical for general curves of small genus and moderately-sized coefficients.