Computing canonical heights using arithmetic intersection theory

Jan Steffen Müller (Universität Hamburg)

9.12.2011

Kummer variety

Notation.

- $A/\mathbb{Q}$: abelian variety,
- $g = \dim(A)$,
- $K = A/\{\pm 1\}$: Kummer variety of A.

Facts.

- K is a projective variety.
- K can be embedded into $\mathbb{P}^{2^g-1}$.

Heights

- Suppose we can construct an explicit embedding $K \hookrightarrow \mathbb{P}^{2^g-1}$.
- Let $\kappa : A \twoheadrightarrow K \hookrightarrow \mathbb{P}^{2^g-1}$.

Definition.
The naive height h on A is defined by $h(P) := h(\kappa(P))$, where the latter is the usual height on $\mathbb{P}^{2^g-1}$.

Fact.
The naive height is quadratic up to a bounded function.

Definition.
The canonical (or Néron-Tate) height $\hat{h}$ on A is defined by

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

Properties

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

Properties.

(a) $\hat{h}$ is a positive definite quadratic form on Λ and $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

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

(c) $\{P \in A(\mathbb{Q}) : \hat{h}(P) \leq B\}$ is finite for any $B \in \mathbb{R}$.

(c) $(\Lambda, \hat{h})$ defines a lattice in $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

Question.
Given A and $P \in A(\mathbb{Q})$, can we compute $\hat{h}(P)$ in practice?

Applications I

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

- a bound on $\sup_{P\in A(\mathbb{Q})} |\hat{h}(P) - h(P)|$,
- an algorithm for the computation of $\hat{h}$,
- a method for computing $\{P \in A(\mathbb{Q}) : h(P) \leq B\}$ for a given bound B.

Applications II

- $P_1, \ldots, P_r$: generators of Λ,
- $m_{ij} := \frac{\hat{h}(P_i+P_j)-\hat{h}(P_i)-\hat{h}(P_j)}{2}$ for $1 \leq i,j \leq r$,
- $R = \det\left((m_{ij})_{1\leq i,j\leq r}\right)$ is called the regulator of A.

R 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.

Using the Kummer variety

Idea.
Decompose $\hat{h}(P) = h(P) + \sum_v \mu_v(P)$, where the μ_v are certain bounded local error functions (due to Néron) that vanish for almost all v. Then compute $h(P)$ and each $\mu_v(P)$.

This strategy works for

- $g = 1$ (Néron, Tate, Silverman, Bost-Mestre)
- $g = 2$ (Flynn-Smart, Stoll, Uchida, M.)

For the computation of $h(P)$ and $\mu_v(P)$ we need

- an explicit embedding $K \hookrightarrow \mathbb{P}^{2^g-1}$,
- defining equations for the image of K,
- an explicit duplication map on the image of K.

Problems with the Kummer variety

Problem.
The explicit arithmetic of K becomes increasingly complicated for larger g.

For $g = 3$, $A = \mathrm{Jac}(C)$, C hyperelliptic, we have

- an explicit embedding $K \hookrightarrow \mathbb{P}^{2^g-1}$ (Stubbs),
- defining equations for the image of K (Stubbs, M.),
- a map δ on the image of K (Duquesne, M.) that is conjectured to be the duplication map.

We currently cannot prove the correctness of δ due to the complexity of the algebra involved.

Curves

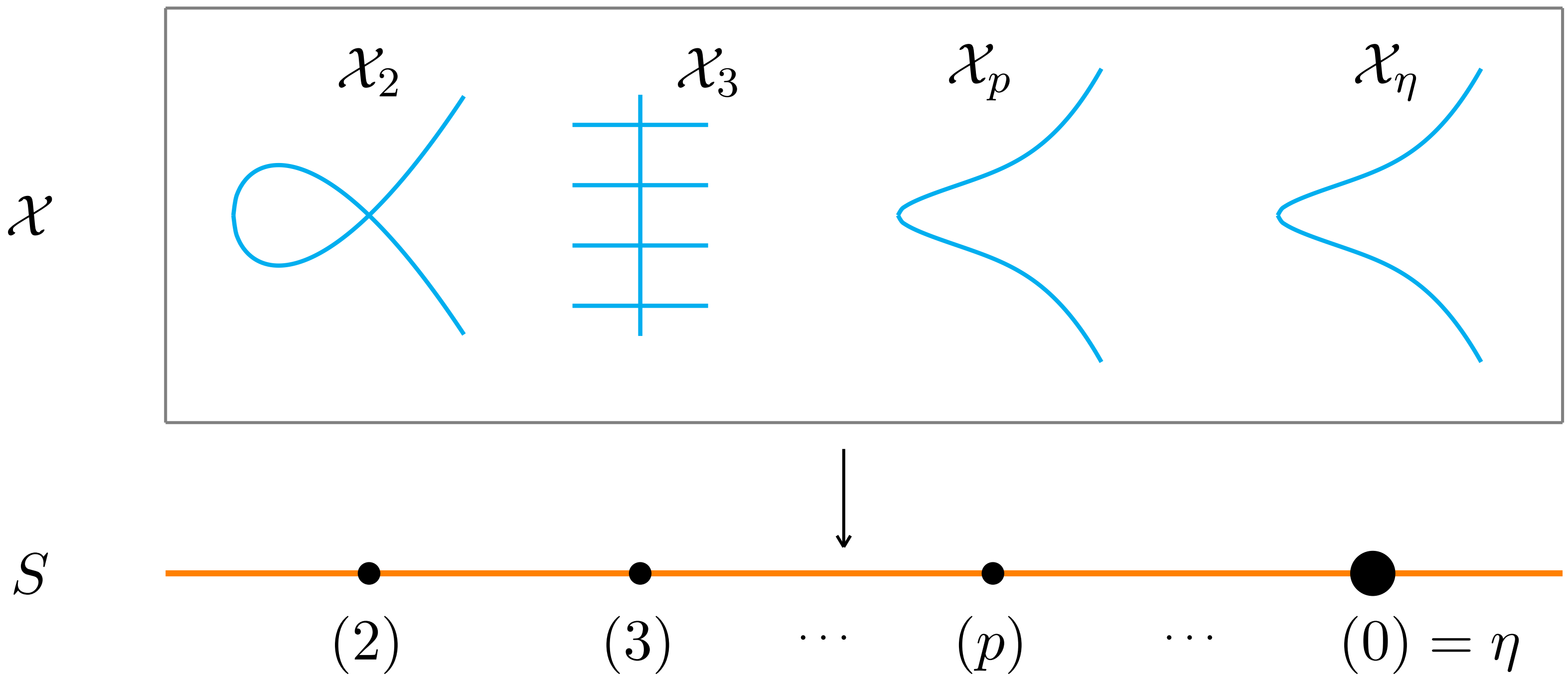
- $C/\mathbb{Q}$: smooth projective geometrically irreducible curve of genus $g > 0$,
- $A = \mathrm{Jac}(C)$.

Idea.
Instead of working on A or K, try to pull the computation of $\hat{h}$ back to C.

- Can compute $\hat{h}$ using arithmetic intersection theory.
- Conjectured by Arakelov,
- proved by Hriljac and Faltings.

Models

Definition. A model $\pi : \mathcal{X} \to S$ of C over $S = \mathrm{Spec}(\mathbb{Z})$ is a 2-dimensional flat S-scheme whose generic fiber is isomorphic to C.



Intersections I

Suppose $\mathcal{X}$ is a proper regular model.

On such models, we have an intersection multiplicity as follows:

- $\mathcal{D}, \mathcal{E}$: effective $\mathbb{Q}$-rational divisors on $\mathcal{X}$ without common component.
- For $x \in \mathcal{X}$ let $I_{\mathcal{D},x}, I_{\mathcal{E},x}$ be defining ideals of $\mathcal{D}, \mathcal{E}$ in x.
- $(\mathcal{D} \cdot \mathcal{E})_x := \ell_{\mathcal{O}_{\mathcal{X},x}}(\mathcal{O}_{\mathcal{X},x}/I_{\mathcal{D},x} + I_{\mathcal{E},x})$.
- $(\mathcal{D} \cdot \mathcal{E})_p := \sum_{x \in \mathcal{X}_p} (\mathcal{D} \cdot \mathcal{E})_x [k(x) : \mathbb{F}_p]$ is called the intersection multiplicity of $\mathcal{D}$ and $\mathcal{E}$ above p.
- $(\mathcal{D} \cdot \mathcal{E})_{\mathrm{fin}} := \sum_p (\mathcal{D} \cdot \mathcal{E})_p \log p$ is called the (finite) intersection multiplicity of $\mathcal{D}$ and $\mathcal{E}$.
- Can extend the pairings above by linearity (to arbitrary $\mathbb{Q}$-rational divisors without common component).

Intersections II

- A divisor $\mathcal{D} \in \mathrm{Div}(\mathcal{X})$ is called horizontal if $\pi(\mathcal{D}) = S$ and vertical if $\pi(\mathcal{D})$ is a finite union of points.
- For $D \in \mathrm{Div}(C)(\mathbb{Q})$ we write $D_{\mathcal{X}}$ for the Zariski closure of D on $\mathcal{X}$ (with multiplicities).

Lemma (Hriljac).
Suppose $D \in \mathrm{Div}(C)(\mathbb{Q})$ has degree zero. Then there exists a vertical $\mathbb{Q}$-divisor $\Phi(D) = \sum_p \Phi_p(D)$ on $\mathcal{X}$ such that

$$(D_{\mathcal{X}} + \Phi(D) \cdot \mathcal{F})_{\mathrm{fin}} = 0$$

for any vertical divisor $\mathcal{F}$ on $\mathcal{X}$.

Intersections III

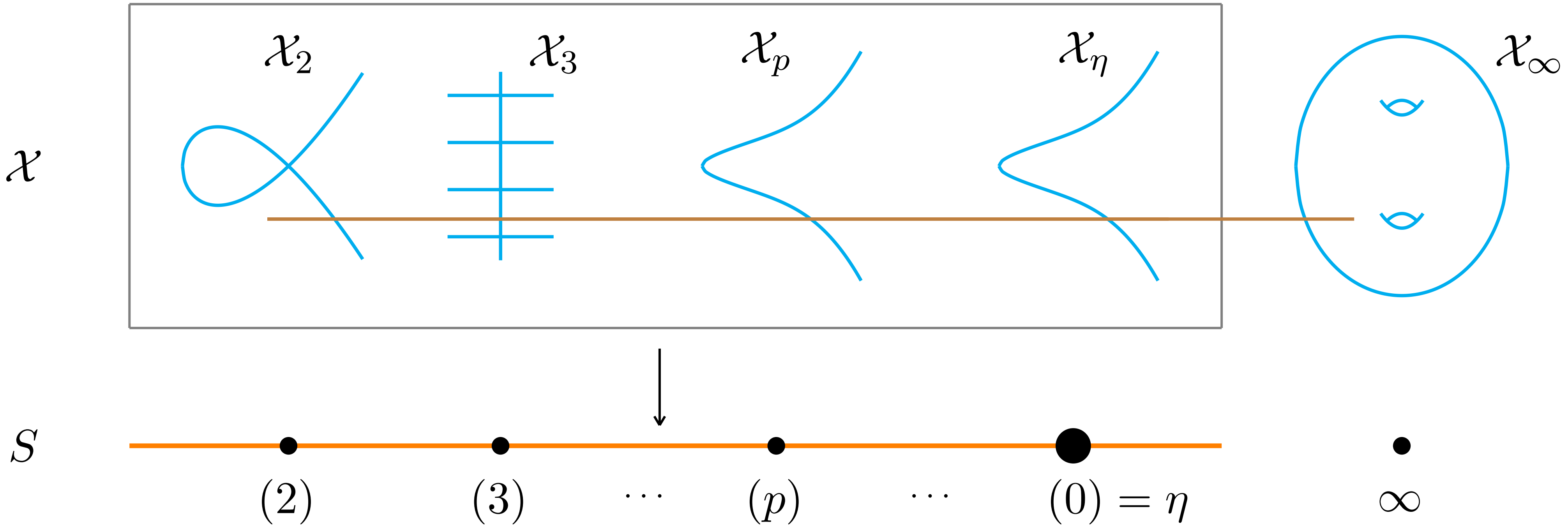
Problem.
The intersection multiplicity on $\mathcal{X}$ as defined above does not respect linear equivalence.

Reason (among others).
The base curve S is not complete.

Idea (Arakelov).

- "Complete" S by adding a point ∞ to S.
- Add a formal fiber $\mathcal{X}_\infty$, corresponding to the Riemann surface $C(\mathbb{C})$.
- Amend the intersection multiplicity using information on $\mathcal{X}_\infty$.

Completed regular model



Green's functions

- X: compact Riemann surface,
- $D \in \mathrm{Div}(X)$,
- μ: volume form on X such that $\int_X \mu = 1$.

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

- g_D has a logarithmic singularity along $\mathrm{supp}(D)$,
- $dd^c g_D = \deg(D)\mu$ outside of $\mathrm{supp}(D)$,
- $\int_X g_D \mu = 0$.

Archimedean intersections

- $\mathcal{X}$: proper regular model of C over S
- $\mathcal{D}, \mathcal{E}$: $\mathbb{Q}$-rational divisors on $\mathcal{X}$ without common component,
- $g_{\mathcal{D}}$: Green's function on $C(\mathbb{C})$ with respect to $\mathcal{D} \otimes \mathbb{C}$ and any volume form normalized as above,
- $\mathcal{E} \otimes \mathbb{C} = \sum_i n_i(Q_i)$.

Definition (Arakelov).
Let

$$(\mathcal{D} \cdot \mathcal{E})_\infty := g_{\mathcal{D}}(\mathcal{E}) := \sum_i n_i g_{\mathcal{D}}(Q_i).$$

Then

$$(\mathcal{D} \cdot \mathcal{E}) := (\mathcal{D} \cdot \mathcal{E})_{\mathrm{fin}} + (\mathcal{D} \cdot \mathcal{E})_\infty$$

is called the arithmetic intersection multiplicity of $\mathcal{D}$ and $\mathcal{E}$.

Faltings-Hriljac

Proposition (Arakelov).
$(- \cdot -)$ respects linear equivalence.

Now we can finally state the connection to canonical heights.

- $D, E \in \mathrm{Div}(C)(\mathbb{Q})$: linearly equivalent and of degree zero,
- $P \in A$: corresponding to the class of D and E.

Theorem 1 (Faltings, Hriljac).
We have

$$\hat{h}(P) = -(D_{\mathcal{X}} + \Phi(D) \cdot E_{\mathcal{X}}).$$

Strategy

Suppose we are given $P \in A(\mathbb{Q})$ and D, E of degree zero and relatively prime, both representing P.

In order to use Theorem 1 to compute $\hat{h}(P)$, we need to be able to perform the following steps:

(i) Compute $g_D(E)$.

(ii) Compute a proper regular model $\mathcal{X}$ of C over S.

(iii) For each p such that $\mathcal{X}_p$ is reducible, find $(\Phi_p(D) \cdot E_{\mathcal{X}})_p$.

(iv) Determine a finite set of primes U containing $\{p : (D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p \neq 0\}$.

(v) For each $p \in U$ compute $(D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p$.

Computing archimedean intersections I

Since we only deal with divisors of degree zero, we only need a Green's function up to an additive constant. Moreover, the value $g_D(E)$ does not depend on the volume form.

Green's functions up to additive constants can be obtained by pulling back theta functions with respect to the analytic Jacobian (conjectured by Arakelov, proved by Hriljac).

Let

- $\iota : C(\mathbb{C}) \hookrightarrow A(\mathbb{C})$: any embedding,
- $\tau \in \mathfrak{h}_g$ such that $A(\mathbb{C}) \cong \mathbb{C}^g/\mathbb{Z}^g \oplus \tau\mathbb{Z}^g$,
- $a = (\frac{1}{2}, \ldots, \frac{1}{2}), b = (\frac{g}{2}, \frac{g-1}{2} \ldots, 1, \frac{1}{2}) \in \frac{1}{2}\mathbb{Z}^g$,
- For $z \in \mathbb{C}^g$ let

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

Computing archimedean intersections II

Suppose that $E = E_1 - E_2$, where $E_1, E_2 \in \mathrm{Div}(C)$ are non-special divisors with disjoint support.

Let $D_1 = \sum_{i=1}^d (P_i)$ and $D_2 = \sum_{i=1}^d (Q_i)$ be two effective divisors such that $\mathrm{supp}(E_i) \cap \mathrm{supp}(D_j) = \emptyset$ for $i, j \in \{1, 2\}$.

Proposition.
If $D = D_1 - D_2$, then $g_D(E)$ is equal to

$$
\begin{aligned}
&-\log \prod_{i=1}^{d} \frac{|\theta_{a,b}(z(\iota(P_i)) - z(\iota(E_1))) \cdot \theta_{a,b}(z(\iota(Q_i)) - z(\iota(E_2)))|}{|\theta_{a,b}(z(\iota(P_i)) - z(\iota(E_2))) \cdot \theta_{a,b}(z(\iota(Q_i)) - z(\iota(E_1)))|} \\
&\quad - 2\pi \sum_{i=1}^{d} \mathrm{Im}(z(\iota(E_1) - \iota(E_2)))^T \,\mathrm{Im}(\tau)^{-1}\,\mathrm{Im}(z(\iota(P_i)) - z(\iota(Q_i))),
\end{aligned}
$$

where for any $Q \in A$ the tuple $z(Q) \in \mathbb{C}^g$ is any complex uniformiser for Q.

Computing archimedean intersections III

So we need to be able to compute

- $\tau \in \mathfrak{h}_g$ given C,
- $\iota(P)$ given $P \in C(\mathbb{C})$,
- $\theta_{a,b}(z)$ given $z \in \mathbb{C}^g$.

All of this is implemented in Magma (due to van Wamelen) in the hyperelliptic case.

The necessary algorithms work in greater generality and are currently being implemented in Sage by Deconinck et al.

Computing a proper regular model

Since 2009, Magma can compute a desingularization $\mathcal{X}$ of the closure of C over S in the strong sense (due to Donnelly).

The implementation only uses blow-ups, avoiding the need to perform explicit normalizations.

This can be shown to always terminate using recent work of Cossart, Jannsen and Saito.

In fact, Magma computes (an affine cover of) a proper regular model of $C \times \mathrm{Spec}(\mathbb{Q}_p)$ over $\mathrm{Spec}(\mathbb{Z}_p)$ for each bad prime p separately. This is sufficient for our purposes.

Computing the correction term

To compute $(\Phi_p(D) \cdot E_{\mathcal{X}})_p$ for a prime p such that $\mathcal{X}_p$ is reducible, we need

- the Moore-Penrose inverse of the intersection matrix M_p of $\mathcal{X}_p$,
- $(D_{\mathcal{X}} \cdot \Gamma)$ and $(E_{\mathcal{X}} \cdot \Gamma)$ for each irreducible componenent Γ of $\mathcal{X}_p$.

Since M_p and defining ideals for all Γ are returned by Magma, (1) and (2) can be computed quite easily, assuming that we have local defining ideals for $D_{\mathcal{X}}$ and $E_{\mathcal{X}}$.

Notation

- $C = \bigcup_i C^i$ affine cover, where
- $C^i = \mathrm{Spec}(\mathbb{Q}[\underline{x}]/I_{C^i})$, I_{C^i} ideal in $\mathbb{Z}[\underline{x}]$.
- $D, E \in \mathrm{Div}(C)(\mathbb{Q})$ effective and with disjoint support.
- For each i, let $I_{D,i},\ I_{E,i} \subset \mathbb{Z}[\underline{x}]$ be defining ideals of D, E on C^i, respectively.
- For each i, let $I_i := I_{C^i} + I_{D,i} + I_{E,i}$.

Primes yielding nontrivial intersection

Lemma.
If p is a prime such that $(D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p \neq 0$, then we have

$$1 \notin \widetilde{I}_i \subset \mathbb{F}_p[\underline{x}]$$

for some i.

We can find all such p by computing

- a Gröbner bases B_i of I_i over $\mathbb{Z}$ for each i,
- the factorization of the unique integer $q_i \in B_i$.

Even more notation

- p: prime such that $(D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p \neq 0$ is possible.
- $\mathcal{X} \times \mathrm{Spec}(\mathbb{Z}_p) = \bigcup_j \mathcal{X}^j$: affine cover, where
- $\mathcal{X}^j = \mathrm{Spec}(\mathbb{Z}_p[\underline{x}]/I_{X^j})$.

We make the following assumptions:

- $D_{\mathcal{X}} \cap E_{\mathcal{X}} \cap \mathcal{X}_p \subset \mathcal{X}^j$ for some j.
- We have defining ideals $I_{D_{\mathcal{X}},j}, I_{E_{\mathcal{X}},j} \subset \mathbb{Z}_p[\underline{x}]$ on $\mathcal{X}^j$ of $D_{\mathcal{X}}, E_{\mathcal{X}}$, respectively.

Computing non-archimedean intersections

Proposition.
We have

$$(D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p = \log |\mathbb{Z}_p[\underline{x}]/(I_{\mathcal{X}^j} + I_{D_{\mathcal{X}},j} + I_{E_{\mathcal{X}},j})|.$$

- The right hand side can be computed at once if we can find a Gröbner basis of $I_{\mathcal{X}^j} + I_{D_{\mathcal{X}},j} + I_{E_{\mathcal{X}},j}$ over $\mathbb{Z}_p$.
- Strategy: We find suitable defining ideals $I_{D,i}, I_{E,i}$ of D, E, respectively, and lift them through the blow-up process.
- But to satisfy our assumptions, we might have to decompose D and E into prime divisors over $\mathbb{Z}_p$ or even $\mathbb{Z}_p^{\mathrm{nr}}$.

Example 1

Suppose C is the smooth projective model of $C^1 : y^2 = f(x)$, $f \in \mathbb{Z}[x]$ separable.

Example 1

- $D = ((x_1, y_1)),\ E = ((x_2, y_2))$,
- p: good prime,
- $\mathcal{X} \times \operatorname{Spec}(\mathbb{Z}_p)$: Zariski closure of C over $\operatorname{Spec}(\mathbb{Z}_p)$.

Then we have

$$(D_{\mathcal{X}} \cdot E_{\mathcal{X}})_p = \min\{\operatorname{ord}_p(x_1 - x_2),\ \operatorname{ord}_p(y_1 - y_2)\} \log p.$$

Example 2

- C as above,
- $D = \sum_j ((x_j, y_j))$, $\mathrm{ord}_p(x_j) \geq 0$ for all j,
- $a(x) = \prod_j (x - x_j)$,
- $b(x) \in \mathbb{Z}_p[x]$ such that $y_j = b(x_j)$ for all j.

Then we can use the defining ideal

$$I_{D,1} = (a(x),\ y - b(x)).$$

In general need to decompose D into prime divisors.

For hyperelliptic curves, this is possible using univariate factorization (of $a(x)$) over $\mathbb{Z}_p$ or $\mathbb{Z}_p^{\mathrm{nr}}$).

Complexity

We have a complete implementation in Magma for hyperelliptic curves over number fields, to be included in the next Magma distribution (December 2011).

A similar algorithm was found independently by D. Holmes.

A formal complexity analysis is difficult, since the algorithm uses external subroutines whose complexity has not been analyzed yet.

- The algorithm to compute the θ-function is exponential in g, but ok for $g \leq 10$.
- We only need Gröbner bases of zero-dimensional ideals with at most 5 generators in at most 3 variables. This is polynomial in D^3, where D is the maximal degree of the generators (Hashemi-Lazard).
- If the divisors are represented by ideals whose generators have very large coefficients, the computation might break down because of the integer factorization required.

Timings I

- C_d: smooth projective model of $y^2 = x^d + 3x^2 + 1$,
- $P = [(0,1) - (0,-1)] \in \mathrm{Jac}(C_d)$.
- The computations were done using a 3.00 GHz Xeon processor.

d	genus	$\hat{h}(P)$	arch. time	nonarch. time
5	2	1.2091089488394304549154848 6513	3.51s	0.33s
7	3	1.319353532098735151587742 24282	6.70s	0.34s
9	4	1.392372556781794225405948 53290	12.65s	0.87s
11	5	1.441873081167141031296676 04112	32.30s	1.67s
13	6	1.476796088419312452293964 57463	120.51s	2.99s
15	7	1.502657019791286715440057 08236	791.14s	5.17s
17	8	1.522540763524838385321488 27258	4729.03s	8.95s
19	9	1.538298826834028486665028 18888	62535.55s	14.20s
21	10	1.551091270847683786375492 92754	280731.59s	21.35s

Timings II

- Now consider multiples of $P = [(0,1) - (0,-1)] \in \mathrm{Jac}(C_5)$.
- The computation does not terminate for $n = 10$ because of the integer factorization.

n	$\hat{h}(nP)$	arch. time	nonarch. time
1	1.20910894883943045491548486513	3.00s	0.31s
2	4.83643579535772181966193946057	3.15s	0.01s
3	10.8819805395548740942393637862	2.93s	0.21s
4	19.3457431814308872786477578421	3.28s	0.02s
5	30.2277237209857613728871216281	3.11s	0.31s
6	43.5279221582194963769574551447	3.29s	0.11s
7	59.2463384931320922908587583915	3.47s	0.34s
8	77.3829727257235491145910313685	3.90s	0.45s
9	97.9378248559938668481542740752	4.31s	1.02s

p-adic heights

Suppose $A/\mathbb{Q}$ is a modular Jacobian and p is a prime of good ordinary reduction.

Combined with an algorithm for explicit Coleman integration due to J. Balakrishnan, the non-archimedean part of our algorithm can be used to compute p-adic heights (due to Néron, Mazur-Tate, Schneider, Coleman-Gross,...) on A.

Current project (joint with J. Balakrishnan and W. Stein):

- Formulate and gather empirical evidence for a generalization of the p-adic Birch and Swinnerton-Dyer-type conjecture for elliptic curves due to Mazur-Tate-Teitelbaum to general modular abelian varieties.
- Need to compute p-adic regulators for this.

Outlook

A generalization of the canonical heights algorithm to other types of curves needs

(a) implementations of the (existing) algorithms to compute the archimedean data;

(b) a method to decompose divisors over local fields.

Note that (b) is not an issue if the divisors in question are pointwise $\mathbb{Q}$-rational (or pointwise $\mathbb{Q}_p$-rational for all relevant p).