p-adic heights and integral points on hyperelliptic curves

Steffen Müller
Universität Hamburg
joint with Jennifer Balakrishnan and Amnon Besser

Rational Points – Geometric, Analytic and Explicit Approaches
University of Warwick

Tuesday, May 28, 2013

Notation

- $f \in \mathbb{Z}[x]$: monic and separable of degree $2g+1 \geq 3$.
- $X/\mathbb{Q}$: hyperelliptic curve of genus g, given by

$$y^2 = f(x)$$

- $\infty \in X(\mathbb{Q})$: point at infinity
- $\mathrm{Div}^0(X)$: divisors on X of degree 0
- $J/\mathbb{Q}$: Jacobian of X
- p: prime of good ordinary reduction for X
- $\log_p$: branch of the p-adic logarithm

Coleman-Gross p-adic height pairing

The Coleman-Gross p-adic height pairing is a symmetric bilinear pairing

$$h : \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbb{Q}_p, \quad \text{where}$$

- h can be decomposed into a sum of local height pairings $h = \sum_v h_v$ over all finite places v of $\mathbb{Q}$.
- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_v)$ with disjoint support.
- We have $h(D, \mathrm{div}(\beta)) = 0$ for $\beta \in k(X)^\times$, so h is well-defined on $J \times J$.
- The local pairings h_v can be extended (non-uniquely) such that $h(D) := h(D, D) = \sum_v h_v(D, D)$ for all $D \in \mathrm{Div}^0(X)$.
- We fix a certain extension and write $h_v(D) := h_v(D, D)$.

Local heights away from p

Consider

- $v \neq p$ prime,
- $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_v)$ with disjoint support,
- $\mathcal{X} \,/\, \mathrm{Spec}(\mathbb{Z}_v)$: proper regular model of X,
- $(\,.\,)_v$: intersection pairing on $\mathcal{X}$,
- $\mathcal{D}, \mathcal{E} \in \mathrm{Div}(\mathcal{X}) \otimes \mathbb{Q}$: extensions of D, E to $\mathcal{X}$ such that $(\mathcal{D}\,.\,F)_v = (\mathcal{E}\,.\,F)_v = 0$ for all vertical divisors $F \in \mathrm{Div}(\mathcal{X})$.

Then we have

$$h_v(D, E) = -(\mathcal{D}\,.\,\mathcal{E})_v \cdot \log_p(v).$$

- Cf. the decomposition of the Néron-Tate height due to Faltings and Hriljac.

Local heights at p

- $X_p := X \times \mathbb{Q}_p$:
- Fix a decomposition

$$H^1_{\mathrm{dR}}(X_p) = \Omega^1(X_p) \oplus W, \tag{1}$$

  where W is isotropic with respect to the cup product pairing.
- ω_D: differential of the third kind on X_p such that
  - $\mathrm{Res}(\omega_D) = D$,
  - ω_D is normalized with respect to (1).
- If D and E have disjoint support, $h_p(D, E)$ is the Coleman integral

$$h_p(D, E) = \int_E \omega_D.$$

Theorem 1

- $\omega_i := \frac{x^i dx}{2y}$ for $i = 0, \dots, g-1$
- $\{\bar{\omega}_0, \dots, \bar{\omega}_{g-1}\}$: basis of W dual to $\{\omega_0, \dots, \omega_{g-1}\}$ with respect to the cup product pairing.
- $\tau(P) := h_p(P - \infty)$ for $P \in X(\mathbb{Q}_p)$

Theorem 1 (Balakrishnan–Besser–M.)
We have

$$\tau(P) = -2 \int_{\infty}^{P} \sum_{i=0}^{g-1} \omega_i \bar{\omega}_i$$

- The integral is an iterated Coleman integral, normalized to have constant term 0 with respect to a certain choice of tangent vector at ∞.
- The proof uses Besser's p-adic Arakelov theory.

A result of Kim

Our second theorem is a generalization of the following result due to M. Kim:

Theorem (Kim).

Let $X = E$ have genus 1 and rank 1 over $\mathbb{Q}$ such that the given model is minimal and all Tamagawa numbers are 1. Then

$$\frac{\int_\infty^P \omega_0\, x\omega_0}{(\int_\infty^P \omega_0)^2},$$

normalized as above, is constant on non-torsion $P \in E(\mathbb{Z})$.

Balakrishnan and Besser have given a simple proof of this result:

- By Theorem 1 we have $-2\int_\infty^P \omega_0\ x\omega_0 = \tau(P)$.
- One can show that $h(P-\infty) = \tau(P)$ for non-torsion $P \in E(\mathbb{Z})$.
- Both $h(P-\infty)$ and $(\int_\infty^P \omega_0)^2$ are quadratic forms on $E(\mathbb{Q}) \otimes \mathbb{Q}$.

Theorem 2

- For $i \in \{0, \dots, g-1\}$ let $f_i(P) = \int_\infty^P \omega_i$.

Theorem 2 (Balakrishnan–Besser–M.)
Suppose that the Mordell-Weil rank of $J/\mathbb{Q}$ is g and that the f_i induce linearly independent $\mathbb{Q}_p$-valued functionals on $J(\mathbb{Q}) \otimes \mathbb{Q}$. Then we have:

(i) There exist constants $\alpha_{ij} \in \mathbb{Q}_p,\ i,j \in \{0, \dots, g-1\}$ such that

$$\rho := \tau - \sum_{i \le j} \alpha_{ij} f_i f_j$$

only takes values on $X(\mathbb{Z}[1/p])$ in an effectively computable finite set T.

(ii) If $P \in X(\mathbb{Z}[1/p])$ reduces to a nonsingular point modulo every $v \neq p$, then $\rho(P) = 0$.

(iii) On each residue disk, ρ is given by a convergent power series.

Proof of Theorem 2

Sketch of proof.

Set $\rho(P) := -\sum_{v\neq p} h_v(P-\infty)$, so we have

$$h(P-\infty) = h_p(P-\infty) + \sum_{v\neq p} h_v(P-\infty) = \tau(P) - \rho(P)$$

If the f_i induce linearly independent functionals on $J(\mathbb{Q})\otimes\mathbb{Q}$, then the set $\{f_i f_j\}_{0\leq i\leq j\leq g-1}$ is a basis of the space of $\mathbb{Q}_p$-valued quadratic forms on $J(\mathbb{Q})\otimes\mathbb{Q}$. Since $h(P-\infty)$ is also quadratic in P, we can write

$$h(P-\infty) = \sum_{i\leq j} \alpha_{ij} f_i(P) f_j(P), \quad \alpha_{ij}\in\mathbb{Q}_p$$

and conclude

$$\rho(P) = \tau(P) - \sum_{i\leq j} \alpha_{ij} f_i(P) f_j(P).$$

Proof of Theorem 2 continued

To prove (i) and (ii), we show that there is a global choice of a proper regular model $\mathcal{X}$ of X such that for all $v \neq p$ and $P \in X(\mathbb{Q}) \setminus \{\infty\}$ we have

$$h_v(P - \infty) = (P_{\mathcal{X}} \,.\, \infty_{\mathcal{X}})_v + \delta_v(P),$$

where

- $P_{\mathcal{X}}$ is the section in $\mathcal{X}(\mathbb{Z})$ corresponding to P,
- $\infty_{\mathcal{X}}$ is the section in $\mathcal{X}(\mathbb{Z})$ corresponding to ∞,
- $\delta_v(P)$ only depends on which component $P_{\mathcal{X}}$ intersects on $\mathcal{X}_v$,
- $\delta_v(P) = 0$ whenever $P_{\mathcal{X}}$ intersects the same component as $\infty_{\mathcal{X}}$.

Now if $P \in X(\mathbb{Z}[1/p])$, then we have $(P_{\mathcal{X}} \,.\, \infty_{\mathcal{X}})_v = 0$, which finishes the proof.

Algorithms

We have Sage-code for the computation of the following objects:

- single and double Coleman-integrals
- $h_p(D, E)$

The main tool is Kedlaya's algorithm for the matrix of Frobenius.

We also have Magma-code for the computation of:

- $h_v(D, E)$ for $v \neq p$
- the set T

The algorithms rely on Gröbner bases and linear algebra.

Example 1.

- $X : y^2 = x^3 - 3024x + 70416$: non-minimal model of "57a1"
- $X(\mathbb{Q})$ has rank 1 and trivial torsion.
- $p = 7$ is a good ordinary prime.
- $Q = (60, -324) \in X(\mathbb{Q})$
- Compute

$$\alpha_{00} = \frac{h(Q - \infty)}{\left(\int_{\infty}^{Q} w_0\right)^2}.$$

- Compute

$$T = \{i \cdot \log_7(2) + j \cdot \log_7(3) \ : \ i \in \{0, 2\}, \ j \in \{0, 2, 5/2\}\}.$$

Example 1 continued

- $X : y^2 = x^3 - 3024x + 70416$
- $T = \{i \cdot \log_7(2) + j \cdot \log_7(3) \, : \, i \in \{0, 2\}, \, j \in \{0, 2, 5/2\}\}$

There are 16 integral points on X; we have

P	$\rho(P)$
$(-48, \pm 324)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(-12, \pm 324)$	$2\log_7(2) + 2\log_7(3)$
$(24, \pm 108)$	$2\log_7(2) + 2\log_7(3)$
$(33, \pm 81)$	$\frac{5}{2}\log_7(3)$
$(40, \pm 116)$	$2\log_7(2)$
$(60, \pm 324)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$
$(132, \pm 1404)$	$2\log_7(2) + 2\log_7(3)$
$(384, \pm 7452)$	$2\log_7(2) + \frac{5}{2}\log_7(3)$

Example 2.

- $X : y^2 = x^3(x-1)^2 + 1$
- $J(\mathbb{Q})$ has rank 2 and trivial torsion.
- $Q_1 = (2, -3), Q_2 = (1, -1), Q_3 = (0, 1) \in X(\mathbb{Q})$ are the only integral points on X up to involution (computed by M. Stoll).
- Set $D_1 = Q_1 - \infty$, $D_2 = Q_2 - Q_3$, then
- $[D_1]$ and $[D_2]$ are independent.
- $p = 11$ is a good, ordinary prime.
- Goal: Recover the integral points and prove that there are no others up to a prescribed height bound.

Example 2 continued

- Compute
$$T = \{0,\ 1/2 \cdot \log_{11}(2),\ 2/3 \cdot \log_{11}(2)\}.$$
- Compute the height pairings $h(D_i, D_j)$ and the Coleman integrals $\int_{D_i} \omega_k \int_{D_j} \omega_l$ and deduce the α_{ij} from $(\alpha_{00}, \alpha_{01}, \alpha_{11})^t =$
$$\begin{pmatrix} \int_{D_1}\omega_0 \int_{D_1}\omega_0 & \int_{D_1}\omega_0 \int_{D_1}\omega_1 & \int_{D_1}\omega_1 \int_{D_1}\omega_1 \\ \int_{D_1}\omega_0 \int_{D_2}\omega_0 & \int_{D_1}\omega_0 \int_{D_2}\omega_1 & \int_{D_1}\omega_1 \int_{D_2}\omega_1 \\ \int_{D_2}\omega_0 \int_{D_2}\omega_0 & \int_{D_2}\omega_0 \int_{D_2}\omega_1 & \int_{D_2}\omega_1 \int_{D_2}\omega_1 \end{pmatrix}^{-1} \begin{pmatrix} h(D_1, D_1) \\ h(D_1, D_2) \\ h(D_2, D_2) \end{pmatrix}$$
- Use power series expansions of τ and of the double and single Coleman integrals to give a power series describing ρ in each residue disk.

Example 2 continued

How can we express τ as a power series on a residue disk $\mathcal{D}$?

- Construct the dual basis $\{\bar{\omega}_0, \bar{\omega}_1\}$ of W.
- Fix a point $P_0 \in \mathcal{D}$.
- Compute $\tau(P_0) = h_p(P_0 - \infty, P_0 - \infty)$ and use

$$\tau(P) = \tau(P_0) - 2\sum_{i=0}^{g-1} \left(\int_{P_0}^{P} \omega_i \bar{\omega}_i + \int_{P_0}^{P} \omega_i \int_{\infty}^{P_0} \bar{\omega}_i \right)$$

  to give a power series describing τ in the residue disk.
- The integral points $P \in \mathcal{D}$ are solutions to

$$\rho(P) = \tau(P) - \sum \alpha_{ij} f_i(P) f_j(P) \in T.$$

Example 2 continued

For example, on the residue disk containing $(0,1)$, the only solutions to $\rho(P) \in T$ modulo $O(11^{11})$ have x-coordinate $O(11^{11})$ or

$$4\cdot 11+7\cdot 11^2+9\cdot 11^3+7\cdot 11^4+9\cdot 11^6+8\cdot 11^7+11^8+4\cdot 11^9+10\cdot 11^{10}+O(11^{11})$$

Here are the recovered integral points and their corresponding ρ values:

P	$\rho(P)$
$(2,\pm 3)$	$\frac{2}{3}\log_{11}(2)$
$(1,\pm 1)$	$\frac{1}{2}\log_{11}(2)$
$(0,\pm 1)$	$\frac{2}{3}\log_{11}(2)$

Outlook

What next?

- Further explore the connection with Kim's nonabelian Chabauty.
- Theorem 2 also yields a bound on the number of integral points on X, but the bound needs computations of certain Coleman integrals. Improve on this to get a Coleman-like bound which only depends on simpler numerical data.
- Try to come up with an efficient algorithm to compute all integral points on X.
- Extend Theorems 1 and 2 to more general classes of curves, e. g. general hyperelliptic curves or superelliptic curves.