p-adic heights and integral points on hyperelliptic curves

Steffen Müller
Universität Hamburg
joint with Jennifer Balakrishnan and Amnon Besser

Heights and Moduli Spaces
Lorentz Center, Leiden University

Tuesday, June 11, 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

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

- $O \in X(\mathbb{Q})$: point at infinity
- $\mathcal{U} = \mathrm{Spec}\left(\mathbb{Z}[x,y]/(y^2 - f(x))\right)$
- $\mathrm{Div}^0(X)$: divisors on X of degree 0
- $J/\mathbb{Q}$: Jacobian of X
- $r = \mathrm{rank}(J/\mathbb{Q})$

Chabauty

- p: prime of good ordinary reduction for X
- $\omega_i = \frac{x^i dx}{2y}$ for $i = 0, \ldots, g-1$
- $f_i(P) = \int_O^P \omega_i$ for $P \in X(\overline{\mathbb{Q}_p})$

Theorem (Chabauty, 1941).
Suppose that $g \geq 2$ and $r < g$. Then there exist $\alpha_0, \ldots, \alpha_{g-1} \in \mathbb{Q}_p$, not all equal to 0, such that

$$\rho(P) = \sum_{i=0}^{g-1} \alpha_i f_i(P)$$

satisfies

- $\rho(P) = 0$ for all $P \in X(\mathbb{Q})$;
- for every $\tilde{P}_0 \in \widetilde{X}(\overline{\mathbb{F}_p})$, the function ρ is given by a convergent power series on the residue disk $\mathrm{red}^{-1}(\tilde{P}_0) \subset X(\overline{\mathbb{Q}_p})$.

A result of Kim

- An explicit version of Chabauty's Theorem due to Coleman can often be used to find $X(\mathbb{Q})$ in practice.

Question. Can we remove or weaken the condition $r < g$?

Theorem (Kim, 2010). Let X have genus 1 and rank 1 over $\mathbb{Q}$ such that the given equation is minimal and all Tamagawa numbers are 1. Then there is a function $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ such that

- $\rho(P) = 0$ for all non-torsion $P \in \mathcal{U}(\mathbb{Z})$;
- on each residue disk of $X/\mathbb{Q}_p$, ρ is given by a convergent power series.

Theorem I

- The following result generalizes Kim's theorem.

Theorem I (Balakrishnan–Besser–M.)
Suppose that $r = g$ 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 a function $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ which only takes values on $\mathcal{U}(\mathbb{Z}[1/p])$ in an effectively computable finite set T.

(ii) If $P \in \mathcal{U}(\mathbb{Z}[1/p])$ 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.

For the proof, we use p-adic heights.

Coleman-Gross p-adic height pairing

For every finite place v of $\mathbb{Q}$ and $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_v)$ with disjoint support, one can define a symmetric bilinear $\mathbb{Q}_p$-valued pairing $h_v(D, E)$, the local height pairing at v, such that if $D, E \in \mathrm{Div}^0(X)$ have disjoint support, then

- $h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) \neq 0$ for only finitely many v;

such that if $D, E \in \mathrm{Div}^0(X)$ have disjoint support, then

- $h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) \neq 0$ for only finitely many v;

- we have $\sum_v h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) = 0$ if $E = \mathrm{div}(\beta)$ for some $\beta \in k(X)^*$.

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

$$\begin{aligned} h : \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) &\to \mathbb{Q}_p \\ (D, E) &\mapsto \sum_v h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v). \end{aligned}$$

Coleman-Gross p-adic height pairing

For every finite place v of $\mathbb{Q}$ and $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_v)$ with disjoint support, one can define a symmetric bilinear $\mathbb{Q}_p$-valued pairing $h_v(D, E)$, the local height pairing at v, such that if $D, E \in \mathrm{Div}^0(X)$ have disjoint support, then

- $h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) \neq 0$ for only finitely many v;

such that if $D, E \in \mathrm{Div}^0(X)$ have disjoint support, then

- $h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) \neq 0$ for only finitely many v;

- we have $\sum_v h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v) = 0$ if $E = \mathrm{div}(\beta)$ for some $\beta \in k(X)^*$.

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

$$\begin{aligned} h : J(\mathbb{Q}) \times J(\mathbb{Q}) &\to \mathbb{Q}_p \\ (D, E) &\mapsto \sum_v h_v(D \times \mathbb{Q}_v, E \times \mathbb{Q}_v). \end{aligned}$$

Local heights away from p

- $v \neq p$ finite place of $\mathbb{Q}$,
- $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_v)$ 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

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

where $\log_p$ is a fixed branch of the p-adic logarithm.

Local heights at p

- $D, E \in \mathrm{Div}^0(X \times \mathbb{Q}_p)$ with disjoint support,
- ω_D: differential of the third kind on $X \times \mathbb{Q}_p$ such that $\mathrm{Res}(\omega_D) = D$ (+ a normalization condition).

Then $h_p(D, E)$ is defined as the Coleman integral

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

Improper intersections

- $v \neq p$: prime number
- $\mathcal{X}/\operatorname{Spec}(\mathbb{Z}_v)$: desingularization in the strong sense of $\overline{X \times \mathbb{Q}_v}^{\mathrm{Zar}}$
- $P \in X(\mathbb{Q}_v)$ with corresponding section $\mathcal{P} \in \mathcal{X}(\mathbb{Z}_v)$
- t_P: tangent vector at P
- z: local parameter at P, normalized such that $\partial_{t_P} z = 1$
- $\beta \in k(X)^*$ such that $P - \mathrm{div}_X(\beta) \cap P = \emptyset$

Gross has defined

$$\mathcal{P}_v^2 = (\mathcal{P} - \mathrm{div}_{\mathcal{X}}(\beta) \,.\, \mathcal{P})_v - \log \left| \frac{\beta}{z^{\mathrm{ord}_P \beta}}(P) \right|_v .$$

Fact. This does not depend on the choice of β.

Extending h_v

- $v \neq p$: prime number
- $\Phi_v(P)$: vertical $\mathbb{Q}$-divisor on $\mathcal{X}$ such that $(\mathcal{P} - \mathcal{O} + \Phi_v(P) \,.\, F)_v = 0$ for all vertical $F \in \mathrm{Div}(\mathcal{X})$
- Depending on the choice of t_P, we can define

$$h_v(P - O) := -\left((\mathcal{P} - \mathcal{O})_v^2 + \Phi_v(P)^2\right) \log_p(v).$$

- Using Besser's p-adic Arakelov theory, can also extend h_p to divisors with common support, depending on the choice of a tangent vector for $P \in X(\mathbb{Q}_p)$.
- $\tau(P) := h_p(P - O)$ for $P \in X(\mathbb{Q}_p)$

Two propositions

Proposition 1.
We can make a certain choice of tangent vectors for every point $P \in X$ such that

- $\mathcal{O}_v^2 = 0$ for all $v \neq p$,
- $\mathcal{P}_v^2 = -\left(\mathcal{P} \,.\, \mathrm{div}_{\mathcal{X}}\left(\omega_0\right)\right)_v$ for all $v \neq p$ and $P \in X(\mathbb{Q}_v) \setminus \{O\}$,
- $\sum_v h_v(P - O) = h(P - O, P - O) =: h(P - O)$ for all $P \in X(\mathbb{Q})$.

Proposition 2.
The function $\tau(P) = h_p(P - O)$ can be written as a convergent power series on every residue disk of $X \times \mathbb{Q}_p$.

- In fact, $\tau(P)$ is an iterated Coleman integral.

Quadratic Chabauty

- Recall that $f_i(P) = \int_O^P \omega_i$ for $i \in \{0, \dots, g-1\}$.

Theorem I (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 $\alpha_{ij} \in \mathbb{Q}_p$, $0 \le i \le j \le g-1$ such that

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

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

(ii) If $P \in \mathcal{U}(\mathbb{Z}[1/p])$ 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 I

Sketch of proof.
For $P \in X(\mathbb{Q})$, we set $\rho(P) := -\sum_{v \neq p} h_v(P - O)$, so we have

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

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 is also quadratic, we can write

$$h(P - O) = \sum_{i \leq j} \alpha_{ij} f_i(P) f_j(P) \quad \text{for some } \alpha_{ij} \in \mathbb{Q}_p$$

and conclude

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

Proof of Theorem I continued

Recall that for $v \neq p$, we have
$$h_v(P-O) = -((\mathcal{P}-\mathcal{O})_v^2 + \Phi_v(P)^2)\log_p(v),$$

where $\Phi_v(P)^2$ is effectively computable and depends only on the component of the special fiber of $\mathcal{X}$ that $\mathcal{P}$ intersects.
When $\mathcal{P}$ and $\mathcal{O}$ intersect the same component, we have $\Phi_v(P)^2 = 0$.

So we have to show that $\sum_{v \neq p}(\mathcal{P}-\mathcal{O})_v^2$ takes only a finite number of values on $\mathcal{U}(\mathbb{Z}[1/p])$.
But for $v \neq p$ and $P \in \mathcal{U}(\mathbb{Z}[1/p])$ we have

$$(\mathcal{P}-\mathcal{O})_v^2 = \mathcal{P}_v^2 - 2(\mathcal{P}\,.\,\mathcal{O})_v + \mathcal{O}_v^2 = \mathcal{P}_v^2 = -(\mathcal{P}\,.\,\mathrm{div}_{\mathcal{X}}(\omega_0))_v$$

by Proposition 1.

Note that $\mathrm{div}_{\mathcal{X}}(\omega_0) = (2g-2)\mathcal{O} + F$, where F is vertical, proving (i).
Moreover, we have $(\mathcal{O}\,.\,F)_v = 0$, so $\mathcal{P}_v^2 = 0$ if P reduces to a nonsingular point modulo v. This proves (ii).

Algorithms

We have `Sage`-code for the computation of:

- 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

Example 1.

- $X : y^2 = x^3(x-1)^2 + 1$
- $J(\mathbb{Q})$ 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 $D_1 = Q_1 - O$, $D_2 = Q_2 - Q_3$, 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 1 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 $(\alpha_{00}, \alpha_{01}, \alpha_{11})^t =$
$$\begin{pmatrix} \int_{D_1} \omega_0 \int_{D_1} \omega_0 & \int_{D_1} \omega_0 \int_{D_1} \omega_1 & \int_{D_1} \omega_1 \int_{D_1} \omega_1 \\ \int_{D_1} \omega_0 \int_{D_2} \omega_0 & \int_{D_1} \omega_0 \int_{D_2} \omega_1 & \int_{D_1} \omega_1 \int_{D_2} \omega_1 \\ \int_{D_2} \omega_0 \int_{D_2} \omega_0 & \int_{D_2} \omega_0 \int_{D_2} \omega_1 & \int_{D_2} \omega_1 \int_{D_2} \omega_1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} h(D_1, D_1) \\ h(D_1, D_2) \\ h(D_2, D_2) \end{pmatrix}$$

- Use power series expansions of τ and of the Coleman integrals f_i to give a power series describing ρ in each residue disk.

Example 1 continued

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

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

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.
- Try to come up with an efficient algorithm to compute all integral points on X.
- Theorem I 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 bound which only depends on simpler numerical data.
- Extend Theorem I to more general classes of curves, e. g. general hyperelliptic curves or superelliptic curves.