$p$-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
- $\text{Div}^0(X)$: 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
The Coleman-Gross $p$-adic height pairing is a symmetric bilinear pairing

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

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 $D, E \in \text{Div}^0(X \times \mathbb{Q}_v)$ with disjoint support.
- We have $h(D, \text{div}(\beta)) = 0$ 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 $D \in \text{Div}^0(X)$.
- We fix a certain extension and write $h_v(D) := h_v(D, D)$. 
Consider

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

Then we have

\[
\hat{h}_v(D, E) = -(\mathcal{D} \cdot \mathcal{E})_v \cdot \log_p(v).
\]

- Cf. the decomposition of the Néron-Tate height due to Faltings and Hriljac.
$X_p := X \times \mathbb{Q}_p$:

- Fix a decomposition

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

where $W$ is isotropic with respect to the cup product pairing.

- $\omega_D$: differential of the third kind on $X_p$ such that
  - $\text{Res}(\omega_D) = D$,
  - $\omega_D$ 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

\[ \omega_i := \frac{x^i}{2y} \, dx \quad \text{for } i = 0, \ldots, g - 1 \]

\[ \{\bar{\omega}_0, \ldots, \bar{\omega}_{g-1}\} : \text{basis of } W \text{ dual to } \{\omega_0, \ldots, \omega_{g-1}\} \text{ with respect to the cup product pairing.} \]

\[ \tau(P) := h_p(P - \infty) \quad \text{for } P \in X(\mathbb{Q}_p) \]

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 \( \infty \).
- The proof uses Besser’s \( p \)-adic Arakelov theory.
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 \( E(\mathbb{Q}) \otimes \mathbb{Q} \).
For \( i \in \{0, \ldots, g - 1\} \) 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 \( \alpha_{ij} \in \mathbb{Q}_p, \ i, j \in \{0, \ldots, g - 1\} \) such that

\[
\rho := \tau - \sum_{i \leq j} \alpha_{ij} f_i f_j
\]

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, \( \rho \) is given by a convergent **power series**.
Proof of Theorem 2

$p$-adic heights  Results  Examples

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

\[
h(P - \infty) = \sum_{i \leq j} \alpha_{ij} f_i(P) f_j(P), \quad \alpha_{ij} \in Q_p
\]

and conclude

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

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

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 $\infty$,
- $\delta_v(P)$ 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 $(P_{\mathcal{X}} \cdot \infty_{\mathcal{X}})_v = 0$, which finishes the proof.
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

$p$-adic heights

Examples

- $X : y^2 = x^3 - 3024x + 70416$

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

There are 16 integral points on $X$; we have

<table>
<thead>
<tr>
<th>$P$</th>
<th>$\rho(P)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(-48, \pm 324)$</td>
<td>$2 \log_7(2) + \frac{3}{2} \log_7(3)$</td>
</tr>
<tr>
<td>$(-12, \pm 324)$</td>
<td>$2 \log_7(2) + 2 \log_7(3)$</td>
</tr>
<tr>
<td>$(24, \pm 108)$</td>
<td>$2 \log_7(2) + 2 \log_7(3)$</td>
</tr>
<tr>
<td>$(33, \pm 81)$</td>
<td>$\frac{5}{2} \log_7(3)$</td>
</tr>
<tr>
<td>$(40, \pm 116)$</td>
<td>$2 \log_7(2)$</td>
</tr>
<tr>
<td>$(60, \pm 324)$</td>
<td>$2 \log_7(2) + \frac{5}{2} \log_7(3)$</td>
</tr>
<tr>
<td>$(132, \pm 1404)$</td>
<td>$2 \log_7(2) + 2 \log_7(3)$</td>
</tr>
<tr>
<td>$(384, \pm 7452)$</td>
<td>$2 \log_7(2) + \frac{5}{2} \log_7(3)$</td>
</tr>
</tbody>
</table>
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 \( \alpha_{ij} \) from \( (\alpha_{00}, \alpha_{01}, \alpha_{11})^t = \left( \begin{array}{ccc} \int_{D_1} \omega_0 \int_{D_1} \omega_0 & \int_{D_1} \omega_0 \int_{D_1} \omega_1 & \int_{D_1} \omega_1 \int_{D_1} \omega_1 \\ \int_{D_1} \omega_0 \int_{D_2} \omega_0 & \int_{D_1} \omega_0 \int_{D_2} \omega_1 & \int_{D_1} \omega_1 \int_{D_2} \omega_1 \\ \int_{D_2} \omega_0 \int_{D_2} \omega_0 & \int_{D_2} \omega_0 \int_{D_2} \omega_1 & \int_{D_2} \omega_1 \int_{D_2} \omega_1 \end{array} \right)^{-1} \left( \begin{array}{c} h(D_1, D_1) \\ h(D_1, D_2) \\ h(D_2, D_2) \end{array} \right) \)

- Use power series expansions of \( \tau \) and of the double and single Coleman integrals to give a power series describing \( \rho \) in each residue disk.
How can we express $\tau$ 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 $\tau$ in the residue disk.

- The integral points $P \in \mathcal{D}$ are solutions to

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

<table>
<thead>
<tr>
<th>(P)</th>
<th>(\rho(P))</th>
</tr>
</thead>
<tbody>
<tr>
<td>((2, \pm 3))</td>
<td>(2 \log_{11}(2))</td>
</tr>
<tr>
<td>((1, \pm 1))</td>
<td>(1 \log_{11}(2))</td>
</tr>
<tr>
<td>((0, \pm 1))</td>
<td>(3 \log_{11}(2))</td>
</tr>
</tbody>
</table>
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.