A p-adic Birch and Swinnerton-Dyer conjecture for modular abelian varieties

Steffen Müller
Universität Hamburg

joint with Jennifer Balakrishnan (Harvard)
and William Stein (U Washington)

Forschungsseminar Arithmetische Geometrie
Humboldt-Universität zu Berlin

Tuesday, November 27, 2012

Elliptic Curves

- Let $N \geq 1$ be an integer and let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$.
- Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_2(\Gamma_0(N))$ be a newform such that all $a_n \in \mathbb{Q}$.
- Let $\mathrm{Ann}_{\mathbb{T}}(f)$ be the annihilator of f in the Hecke algebra $\mathbb{T} = \mathbb{Z}[\ldots, T_n, \ldots]$ generated by the Hecke operators on $J_0(N)$.
- Then $A_f = J_0(N)/\mathrm{Ann}_{\mathbb{T}}(f)J_0(N)$ is an elliptic curve defined over $\mathbb{Q}$.
- Wiles et al. have shown: Every elliptic curve A_f over $\mathbb{Q}$ arises in this way.
- Consequence: The L-function $L(A_f, s) = L(f, s)$ of A_f can be continued analytically to $\mathbb{C}$.

- $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_2(\Gamma_0(N))$: newform
- Then $K_f = \mathbb{Q}(\dots, a_n, \dots)$ is totally real.
- $A_f = J_0(N)/\mathrm{Ann}_{\mathbb{T}}(f)J_0(N)$: abelian variety $/\mathbb{Q}$ associated to f,
- $g = [K_f : \mathbb{Q}]$: dimension of A_f,
- $G_f = \{\sigma : K_f \hookrightarrow \mathbb{R}\}$,
- $f^\sigma(z) = \sum_{n=1}^{\infty} \sigma(a_n) e^{2\pi i n z}$ for $\sigma \in G_f$,
- $L(A_f, s) = \prod_{\sigma \in G_f} L(f^\sigma, s)$: L-function of A_f, can be continued analytically to $\mathbb{C}$,

Let $\mathcal{A}$ denote the Néron model of A_f over $\mathrm{Spec}(\mathbb{Z})$.
A Néron differential on A_f is a generator of the global relative differential g-forms on $\mathcal{A}$, pulled back to A_f.

Example. If A_f is an elliptic curve in minimal Weierstraß form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

then $\frac{dx}{2y+a_1x+a_3}$ is a Néron differential.

We define the real period (resp. the minus period) of A_f by

$$\Omega^{\pm}_{A_f} := \int_{A_f(\mathbb{C})^{\pm}} |\omega_{A_f}|,$$

where ω_{A_f} is a Néron differential and $A_f(\mathbb{C})^{\pm}$ is the set of elements of $A_f(\mathbb{C})$ fixed by $\pm$ complex conjugation.

Tamagawa numbers and regulators

- Let v be a prime number,
- Let $\mathcal{A}_v$ be the special fiber of $\mathcal{A}$ above v and let $\mathcal{A}_v^0$ denote its connected component.
- Then $\Phi_v = \mathcal{A}_v/\mathcal{A}_v^0$ is a finite group scheme defined over $\mathbb{F}_v$.
- The Tamagawa number $c_v(A_f)$ is the number of $\mathbb{F}_v$-rational points on Φ_v.

- Let $\langle\, ,\, \rangle_{\mathrm{NT}}$ denote the Néron-Tate (or canonical) height pairing on A_f.
- The regulator $\mathrm{Reg}(A_f/\mathbb{Q})$ is defined by

$$\mathrm{Reg}(A_f/\mathbb{Q}) := \det\left(\langle P_i, P_j\rangle_{\mathrm{NT}}\right)_{i,j},$$

where $P_1, \ldots, P_r$ generate the free part of $A_f(\mathbb{Q})$.

BSD conjecture

- The Shafarevich-Tate group $Ш(A_f/\mathbb{Q})$ is defined using Galois cohomology We will assume that it is finite throughout this talk.
- Let $L^*(A_f, 1)$ be the leading term of the series expansion of $L(A_f, s)$ in $s = 1$.
- Let $A_f(\mathbb{Q})_{\text{tors}}$ denote the group of rational points on A_f of finite order, likewise for the dual abelian variety $A_f^\vee$ of A_f.

Conjecture (Birch-Swinnerton-Dyer, Tate)
We have $\mathrm{rk}(A_f(\mathbb{Q})) = \mathrm{ord}_{s=1} L(A_f, s)$ and

$$\frac{L^*(A_f, 1)}{\Omega^+_{A_f}} = \frac{\mathrm{Reg}(A_f/\mathbb{Q}) \cdot |Ш(A_f/\mathbb{Q})| \cdot \prod_v c_v(A_f)}{|A_f(\mathbb{Q})_{\text{tors}}| \cdot |A_f^\vee(\mathbb{Q})_{\text{tors}}|}.$$

p-adic analogues?

- Let $p > 2$ be a prime such that A_f has good ordinary reduction at p, that is, $p \nmid a_p$.

  Question. Is there a p-adic analogue of the BSD conjecture?

  Idea. Define a p-adic analytic L-function associated to A_f which interpolates $L(A_f, s)$ p-adically at special values (e.g. at $s = 1$).

  Problem: Need to make $L(A_f, 1)$ algebraic.

p-adic analogues?

- Let $p > 2$ be a prime such that A_f has good ordinary reduction at p, that is, $p \nmid a_p$.

  Question. Is there a p-adic analogue of the BSD conjecture?

  Idea. Define a p-adic analytic L-function associated to A_f which interpolates $L(A_f, s)$ p-adically at special values (e.g. at $s = 1$).

  Problem: Need to make $L(A_f, 1)$ algebraic.

p-adic analogues?

- Let $p > 2$ be a prime such that A_f has good ordinary reduction at p, that is, $p \nmid a_p$.

  Question. Is there a p-adic analogue of the BSD conjecture?

  Idea. Define a p-adic analytic L-function associated to A_f which interpolates $L(A_f, s)$ p-adically at special values (e.g. at $s = 1$).

  Problem: Need to make $L(A_f, 1)$ algebraic.

p-adic analogues?

- Let $p > 2$ be a prime such that A_f has good ordinary reduction at p, that is, $p \nmid a_p$.

  Question. Is there a p-adic analogue of the BSD conjecture?

  Idea. Define a p-adic analytic L-function associated to f which interpolates $L(f, s)$ p-adically at special values (e.g. at $s = 1$).

  Problem: Need to make $L(f, 1)$ algebraic.

p-adic analogues?

- Let $p > 2$ be a prime such that A_f has good ordinary reduction at p, that is, $p \nmid a_p$.

  Question. Is there a p-adic analogue of the BSD conjecture?

  Idea. Define a p-adic analytic L-function associated to f which interpolates $L(f, s)$ p-adically at special values (e.g. at $s = 1$).

  Problem: Need to make $L(f, 1)$ algebraic.

  In fact, we need to look at $L(f^\sigma, 1)$ for all $\sigma \in G_f$.

Dirichlet characters

If $\psi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod k, we use the following notation:

- $\bar{\psi}$ is the conjugate character to ψ.
- $f_\psi(z) = \sum_{n=1}^{\infty} \psi(n) \cdot a_n \cdot e^{2\pi i n z}$,
- K_ψ is the field generated over $\mathbb{Q}$ by the values of ψ,
- $\tau(\psi)$ is the Gauß sum of ψ.

Theorem. (Shimura) For all $\sigma \in G_f$ there exist $\Omega^+_{f^\sigma} \in \mathbb{R}$ and $\Omega^-_{f^\sigma} \in i \cdot \mathbb{R}$ such that the following properties are satisfied:

(i) We have

$$\frac{\pi i}{\Omega^\pm_{f^\sigma}} \left(\int_r^{i\infty} f^\sigma(z)dz \pm \int_{-r}^{i\infty} f^\sigma(z)dz \right) \in K_f$$

for all $r \in \mathbb{Q}$.

(ii) If ψ is a Dirichlet character of sign $\pm$, then

$$\frac{L(f_{\bar{\psi}}, 1)}{\tau(\psi) \cdot \Omega^\pm_f} \in K_f K_\psi.$$

In particular,

$$\frac{L(f, 1)}{\Omega^+_f} \in K_f.$$

Shimura periods cont'd

Theorem. (Shimura) For all $\sigma \in G_f$ there exist $\Omega^+_{f^\sigma} \in \mathbb{R}$ and $\Omega^-_{f^\sigma} \in i \cdot \mathbb{R}$ such that the following properties are satisfied:

(iii) If ψ is a Dirichlet character of sign $\pm$, then

$$\sigma\left(\frac{L(f_{\bar{\psi}}, 1)}{\tau(\psi) \cdot \Omega^\pm_f}\right) = \frac{L(f^\sigma_{\bar{\psi}^\sigma}, 1)}{\tau(\psi^\sigma) \cdot \Omega^\pm_{f^\sigma}}.$$

- We call a set $\{\Omega^\pm_{f^\sigma}\}_{\sigma \in G_f}$ as in the theorem a set of Shimura periods for f.
- Shimura periods are not uniquely determined by the theorem.
- There is always a Dirichlet character ψ such that $L(f_{\bar{\psi}}, 1) \neq 0$.

Modular symbols

- Fix a set of Shimura periods $\{\Omega^{\pm}_{f^\sigma}\}_{\sigma\in G_f}$.
- Fix a prime $\mathfrak{p}$ of K_f such that $\mathfrak{p} \mid p$.
- Let α be the unit root of $x^2 - a_p x + p \in (K_f)_{\mathfrak{p}}[x]$.
- The plus (resp. minus) modular symbol map associated to f (and α) maps $r \in \mathbb{Q}$ to

$$[r]^{\pm}_f := -\frac{\pi i}{\Omega^{+}_f}\left(\int_r^{i\infty} f(z)dz + \int_{-r}^{i\infty} f(z)dz\right) \in K_f.$$

- In particular, we have $[0]^{+}_f = \frac{L(f,1)}{\Omega^{+}_f}$.

- Define measures on $\mathbb{Z}_p^\times$:

$$\mu_f^\pm(a + p^n\mathbb{Z}_p) = \frac{1}{\alpha^n}\left[\frac{a}{p^n}\right]_f^\pm - \frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n-1}}\right]_f^\pm$$

- We can integrate continuous characters $\chi : \mathbb{Z}_p^\times \to \mathbb{C}_p$ against $\mu_f^\pm$.
- Write $x \in \mathbb{Z}_p^\times$ as $\omega(x) \cdot \langle x \rangle$ where $\omega(x)^{p-1} = 1$ and $\langle x \rangle \in 1 + p\mathbb{Z}_p$.
- This yields two continuous characters $\mathbb{Z}_p^\times \to \mathbb{C}_p$.
- Define

$$L_p(f, s) := \int_{\mathbb{Z}_p^\times} \langle x \rangle^{s-1}\, d\mu_f^+(x) \quad \text{for all } s \in \mathbb{Z}_p,$$

where $\langle x \rangle^{s-1} = \exp_p((s-1) \cdot \log_p(\langle x \rangle))$.

Interpolation

- Fix a topological generator γ of $1 + p\mathbb{Z}_p$.
- Convert $L_p(f, s)$ into a p-adic power series $\mathcal{L}_p(f, T)$ in terms of $T = \gamma^{s-1} - 1$.
- Let $\epsilon_p(f) := (1 - \alpha^{-1})^2$ be the p-adic multiplier.

Then we have the following interpolation property (due to Mazur-Tate-Teitelbaum):

$$\frac{\mathcal{L}_p(f,0)}{\epsilon_p(f)} = \frac{L_p(f,1)}{\epsilon_p(f)} = [0]_f^+ = \frac{L(f,1)}{\Omega_f^+}.$$

The case of elliptic curves

- All of this depends on the choice of Ω_f^+!
- If $A_f = E$ is an elliptic curve, then the real period Ω_E^+ satisfies the assertions of Shimura's theorem, so we can take $\Omega_f^+ = \Omega_E^+$.
- This gives a canonical p-adic L-function $L_p(E, s)$ associated to E.
- Let $\mathcal{L}_p(E, T)$ be the corresponding p-adic power series.
- By the interpolation property, the classical BSD conjecture in rank 0 is equivalent to

$$\frac{\mathcal{L}_p(E,0)}{\epsilon_p(f)} = \frac{|\text{Ш}(E/\mathbb{Q})| \cdot \prod_v c_v(E)}{|E(\mathbb{Q})_{\text{tors}}|^2}.$$

Mazur-Tate-Teitelbaum conjecture

Conjecture. (Mazur-Tate-Teitelbaum) If $A_f = E$ is an elliptic curve such that $\mathrm{rk}(E/\mathbb{Q}) = 0$, then $\mathrm{ord}_{T=0}(\mathcal{L}_p(f,T)) = 0$ and

$$\frac{\mathcal{L}_p^*(E,0)}{\epsilon_p(f)} = \frac{|Ш(E/\mathbb{Q})| \cdot \prod_v c_v(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2},$$

where $\mathcal{L}_p^*(E,0)$ is the leading coefficient of $\mathcal{L}_p(E,T)$.

Question. How can this be extended to higher rank?

Mazur-Tate-Teitelbaum conjecture

Conjecture. (Mazur-Tate-Teitelbaum) If $A_f = E$ is an elliptic curve, then we have $r := \mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{T=0}(\mathcal{L}_p(f,T))$ and

$$\frac{\mathcal{L}_p^*(E,0)}{\epsilon_p(f)} = \frac{\mathrm{Reg}(E/\mathbb{Q}) \cdot |\text{Ш}(E/\mathbb{Q})| \cdot \prod_v c_v(E)}{|E(\mathbb{Q})_{\mathsf{tors}}|^2},$$

where $\mathcal{L}_p^*(E,0)$ is the leading coefficient of $\mathcal{L}_p(E,T)$.

Can this be correct?

Mazur-Tate-Teitelbaum conjecture

Conjecture. (Mazur-Tate-Teitelbaum) If $A_f = E$ is an elliptic curve, then we have $r := \mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{T=0}(\mathcal{L}_p(f,T))$ and

$$\frac{\mathcal{L}_p^*(E,0)}{\epsilon_p(f)} = \frac{\mathrm{Reg}(E/\mathbb{Q}) \cdot |\text{Ш}(E/\mathbb{Q})| \cdot \prod_v c_v(E)}{|E(\mathbb{Q})_{\mathsf{tors}}|^2},$$

where $\mathcal{L}_p^*(E,0)$ is the leading coefficient of $\mathcal{L}_p(E,T)$.

Problem: The left hand side is p-adic, the right hand side is real!.
We will modify the right hand side.

Conjecture. (Mazur-Tate-Teitelbaum) If $A_f = E$ is an elliptic curve, then we have $r := \mathrm{rk}(E/\mathbb{Q}) = \mathrm{ord}_{T=0}(\mathcal{L}_p(f,T))$ and

$$\frac{\mathcal{L}_p^*(E,0)}{\epsilon_p(f)} = \frac{\mathrm{Reg}_\gamma(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_v c_v(E)}{|E(\mathbb{Q})_{\text{tors}}|^2},$$

where $\mathcal{L}_p^*(E,0)$ is the leading coefficient of $\mathcal{L}_p(E,T)$.

Here

$$\mathrm{Reg}_\gamma(E/\mathbb{Q}) = \mathrm{Reg}_p(E/\mathbb{Q})/\log_p(\gamma)^r,$$

where $\mathrm{Reg}_p(E/\mathbb{Q})$ is the p-adic regulator, defined using the p-adic height pairing (more on this later), a p-adic analogue of the real-valued Néron-Tate height pairing.

Extending Mazur-Tate-Teitelbaum

An extension of the Mazur-Tate-Teitelbaum conjecture to arbitrary dimension $g > 1$ should

- be equivalent to BSD in rank 0,
- reduce to Mazur-Tate-Teitelbaum if $g = 1$,
- be consistent with the main conjecture of Iwasawa theory for abelian varieties.

Problem. Need to construct a p-adic L-function for A_f!

- Idea: Define $L_p(A_f, s) := \prod_{\sigma \in G_f} L_p(f^\sigma, s)$ (similar to $L(A_f, s)$).
- But to pin down $L_p(f^\sigma, s)$, first need to fix a set $\{\Omega^{\pm}_{f^\sigma}\}_{\sigma \in G_f}$ of Shimura periods.

Theorem. (Balakrishnan, Stein, M.) If $\{\Omega^{\pm}_{f^\sigma}\}_{\sigma\in G_f}$ are Shimura periods, then there exist $c \in \mathbb{Q}^\times$ such that

$$\Omega^{\pm}_{A_f} = c \cdot \prod_{\sigma\in G_f} \Omega^{\pm}_{f^\sigma}.$$

- For the proof, we compare volumes of certain related complex tori.
- By the theorem, we can fix Shimura periods $\{\Omega^{\pm}_{f^\sigma}\}_{\sigma\in G_f}$ such that

$$\Omega^{\pm}_{A_f} = \prod_{\sigma\in G_f} \Omega^{\pm}_{f^\sigma}. \tag{1}$$

- With this choice, define $L_p(A_f, s) := \prod_{\sigma\in G_f} L_p(f^\sigma, s)$.
- Then $L_p(A_f, s)$ does not depend on the choice of Shimura periods, as long as (1) holds.

Interpolation

- Convert $L_p(A_f, s)$ into a p-adic power series $\mathcal{L}_p(A_f, T)$ in terms of $T = \gamma^{s-1} - 1$.
- Let $\epsilon_p(A_f) := \prod_\sigma \epsilon_p(f^\sigma)$ be the p-adic multiplier.
- Then we have the following interpolation property

$$\frac{\mathcal{L}_p(A_f, 0)}{\epsilon_p(A_f)} = \frac{L(A_f, 1)}{\Omega^+_{A_f}}.$$

p-adic heights

Let $A_f^\vee$ be the dual abelian variety of A_f. The p-adic height pairing

$$h : A_f(\mathbb{Q}) \times A_f^\vee(\mathbb{Q}) \to \mathbb{Q}_p$$

is a bilinear pairing with some additional properties (more on this later).

Conjecture. (Schneider) The p-adic height pairing is nondegenerate.

- There are several different constructions of h, due to Néron, Bernardi, Perrin-Riou, Schneider, Mazur-Tate, Nekovář.
- Can define h for arbitrary abelian varieties over number fields and other types of reduction at p.
- For p good ordinary, the constructions are all known to be equivalent (due to Mazur-Tate, Nekovář, Besser).
- If A_f is principally polarized, get a pairing $h : A_f(\mathbb{Q}) \times A_f(\mathbb{Q}) \to \mathbb{Q}_p$.

- $\varphi : A_f \to A_f^\vee$: polarization.
- $P_1, \dots, P_r$: generators of the free part of $A_f(\mathbb{Q})$.

We define

$$\mathrm{Reg}_p(A_f/\mathbb{Q}) := \frac{1}{[A_f^\vee(\mathbb{Q}) : \varphi(A_f(\mathbb{Q}))]} \left(\det\left(h(P_i, \varphi(P_j))\right)_{i,j}\right).$$

- This is independent of the choice of φ.
- Using this, define $\mathrm{Reg}_\gamma(A_f/\mathbb{Q}) := \mathrm{Reg}_p(A_f/\mathbb{Q})/\log_p(\gamma)^r$.

The conjecture

We make the following p-adic BSD conjecture:

Conjecture. (Balakrishnan, Stein, M.) The Mordell-Weil rank r of $A_f/\mathbb{Q}$ equals $\mathrm{ord}_{T=0}(\mathcal{L}_p(A_f, T))$ and

$$\frac{\mathcal{L}_p^*(A_f, 0)}{\epsilon_p(A_f)} = \frac{\mathrm{Reg}_\gamma(A_f/\mathbb{Q}) \cdot |\text{Ш}(A_f/\mathbb{Q})| \cdot \prod_v c_v(A_f)}{|A_f(\mathbb{Q})_{\mathrm{tors}}| \cdot |A_f^\vee(\mathbb{Q})_{\mathrm{tors}}|}.$$

This conjecture

- is equivalent to BSD in rank 0,
- reduces to Mazur-Tate-Teitelbaum if $g = 1$,
- is consistent with the main conjecture of Iwasawa theory for abelian varieties, via work of Perrin-Riou and Schneider.

Computing the p-adic L-function

To test our conjecture in examples, we need an algorithm to compute $\mathcal{L}_p(A_f, T)$.

- The modular symbols $[r]^{+}_{f^\sigma}$ can be computed efficiently in a purely algebraic way – up to a rational factor (Cremona, Stein),
- To compute $\mathcal{L}_p(A_f, T)$ to n digits of accuracy, can use
  (i) approximation using Riemann sums (similar to Stein-Wuthrich) – exponential in n or
  (ii) overconvergent modular symbols (due to Pollack-Stevens) – polynomial in n.
- Both methods are now implemented in Sage.

Normalization

To find the correct normalization of the modular symbols, can use the interpolation property $\prod_\sigma [0]^+_{f^\sigma} = \frac{L(A,1)}{\Omega^+_A}$.

- Find a Dirichlet character ψ associated to a quadratic number field $\mathbb{Q}(\sqrt{D})$ such that $D > 0$ and
  - $L(B,1) \neq 0$, where B is A_f twisted by ψ,
  - $\gcd(N,D) = 1$.
- Can express $[r]^+_B := \prod_\sigma [r]^+_{f^\sigma_\psi}$ in terms of modular symbols $[r]^+_{f^\sigma}$.
- We have $\Omega^+_B \cdot \eta_\psi = D^{g/2} \cdot \Omega^+_{A_f}$ for some $\eta_\psi \in \mathbb{Q}^\times$.

$\Rightarrow$ The correct normalization factor is

$$\frac{L(B,1)}{\Omega^+_B \cdot [0]^+_B} = \frac{\eta_\psi \cdot L(B,1)}{D^{g/2} \cdot \Omega^+_{A_f} \cdot [0]^+_B}.$$

Computing the p-adic regulator if $g = 1$

Question. How can we compute p-adic heights?

- The construction of Mazur-Tate relies on the p-adic σ-function.
- If $g = 1$, then this leads to a practical algorithm (Mazur-Stein-Tate), which was heavily optimized in the PhD thesis of Harvey.

Problem. It's not clear how to generalize this algorithm to $g > 1$.

- Instead, we use a different, but equivalent construction of p-adic heights due to Coleman-Gross.
- From now on, suppose that $A_f = \mathrm{Jac}(C)$, where $C/\mathbb{Q}$ is a curve of genus g.

Coleman-Gross height pairing

The Coleman-Gross height pairing is a symmetric bilinear pairing

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

- h can be written as a sum of local height pairings $h = \sum_v h_v$ over all finite places v of $\mathbb{Q}$.
- We have $h(D, \mathrm{div}(\beta)) = 0$ for $\beta \in k(C)^\times$, so h is well-defined on $A_f \times A_f$.
- The construction of h_v depends on whether $v = p$ or $v \neq p$.
- All h_v are invariant under changes of models of $C \times \mathbb{Q}_v$.

Local heights away from p

- Let $D, E \in \mathrm{Div}^0(C)$ with disjoint support.
- Suppose $v \neq p$,
- $\mathcal{X} \,/\, \mathrm{Spec}(\mathbb{Z}_v)$: proper regular model of C,
- $(\,.\,)_v$: intersection pairing on $\mathcal{X}$,
- $\mathcal{D}$, $\mathcal{E} \in \mathrm{Div}(\mathcal{X})$: 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

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

- This is completely analogous to the decomposition of the Néron-Tate height on A_f in terms of arithmetic intersection theory on $\mathcal{X}$ due to Faltings and Hriljac.

Computing local heights away from p

- Proper regular models can be computed in practice in many cases using `Magma`.
- If C is hyperelliptic, divisors on C and extensions to $\mathcal{X}$ can be represented using Mumford representation.
- Intersection multiplicities of divisors on $\mathcal{X}$ can be computed algorithmically using linear algebra and Gröbner bases (M.) or resultants (Holmes).
- All of this is implemented in `Magma`.

Local heights at p

- $h_p(D, E)$ is defined in terms of Coleman integration on $X := C \times \mathbb{Q}_p$.
- Suppose X is hyperelliptic, given by a model $y^2 = g(x)$, where $\deg(g)$ is odd.
- Let ω_D denote a differential of the third kind on X such that
  - $\mathrm{Res}(\omega_D) = D$,
  - ω_D is normalized with respect to a certain splitting $H^1_{\mathrm{dR}}(X) = H^{1,0}_{\mathrm{dR}}(X) \oplus W$, where $H^{1,0}_{\mathrm{dR}}(X)$ is the set of holomorphic 1-forms on X.

The local height pairing at p is given by the Coleman integral

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

Coleman integration

- If $P, Q \in X(\mathbb{Q}_p)$ such that $P \equiv Q \pmod p$ and ω is a holomorphic 1-form, then it is easy to define and compute $\int_P^Q \omega$.
- Coleman extended this to the rigid analytic space $X^{\mathrm{an}}_{\mathbb{C}_p}$.
- We get a well-defined integral $\int_P^Q \omega$ whenever $P, Q \in X(\mathbb{Q}_p)$ and ω is a meromorphic 1-form which is holomorphic in P and Q.

Properties of the Coleman-integral include

- $\int_P^Q (a_1\omega_1 + a_2\omega_2) = a_1 \int_P^Q \omega_1 + a_2 \int_P^Q \omega_2$,
- $\int_P^R \omega = \int_P^Q \omega = \int_Q^R \omega$,
- $\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$ if ϕ is a rigid analytic map,
- $\int_P^Q df = f(Q) - f(P)$.

Computing local heights at p

- The work of Balakrishnan-Besser makes Coleman integration on hyperelliptic curves practical. Write $\omega_D = \eta - \omega$, where η is holomorphic. We only discuss the computation of $\int_E \eta$.
  - Suppose $P \not\equiv Q \pmod p$, but P and Q are fixed by Frobenius.
  - Then we can compute $\int_P^Q \eta$ using a system of linear equations if we know the action of Frobenius on basis differentials $\frac{x^i dx}{2y}$, $i = 0, \ldots, 2g-1$.
  - The latter can be computed using Kedlaya's algorithm.
  - Using properties of Coleman integrals, can compute $\int_P^Q \eta$ for arbitrary P, Q.
- This has been implemented by Balakrishnan in Sage.
- Further computational tricks (due to Balakrishnan-Besser) can be used to compute $\int_E \omega$.

Computing the p-adic regulator

- Suppose $P_1, \ldots, P_r \in A_f(\mathbb{Q})$ are generators of $A_f(\mathbb{Q})$ mod torsion.
- Suppose $P_i = [D_i]$, $D_i \in \mathrm{Div}(C)^0$ pairwise relatively prime and with pointwise $\mathbb{Q}_p$-rational support.
- Recall that $\mathrm{Reg}_p(A_f/\mathbb{Q}) = \det((m_{ij})_{i,j})$, where $m_{ij} = h(D_i, D_j)$.

Problem. Given a subgroup H of $A_f(\mathbb{Q})$ mod torsion of finite index, need to saturate it.

- Currently only possible for $g = 1, 2$ ($g = 3$ work in progress due to Stoll), so in general only get $\mathrm{Reg}_p(A_f/\mathbb{Q})$ up to a $\mathbb{Q}$-rational square.
- See also recent work of Holmes.
- For $g = 2$, can use generators of H and compute the index using Néron-Tate regulators to get $\mathrm{Reg}_p(A_f/\mathbb{Q})$ exactly.

Empirical evidence for $g = r = 2$

- From "Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves" (Flynn, Leprevost, Schaefer, Stein, Stoll, Wetherell '01), we considered 16 genus 2 curves C_N whose Jacobians A_N are optimal quotients of $J_0(N)$.
- Each A_N has Mordell-Weil rank 2 over $\mathbb{Q}$.

N	Equation of C_N
67	$y^2 + (x^3 + x + 1)y = x^5 - x$
73	$y^2 + (x^3 + x^2 + 1)y = -x^5 - 2x^3 + x$
85	$y^2 + (x^3 + x^2 + x)y = x^4 + x^3 + 3x^2 - 2x + 1$
93	$y^2 + (x^3 + x^2 + 1)y = -2x^5 + x^4 + x^3$
103	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4$
107	$y^2 + (x^3 + x^2 + 1)y = x^4 - x^2 - x - 1$
115	$y^2 + (x^3 + x^2 + 1)y = 2x^3 + x^2 + x$
125	$y^2 + (x^3 + x + 1)y = x^5 + 2x^4 + 2x^3 + x^2 - x - 1$
133	$y^2 + (x^3 + x^2 + 1)y = -x^5 + x^4 - 2x^3 + 2x^2 - 2x$
147	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + x^3 + x^2 + 1$
161	$y^2 + (x^3 + x + 1)y = x^3 + 4x^2 + 4x + 1$
165	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + 3x^3 + x^2 - 3x$
167	$y^2 + (x^3 + x + 1)y = -x^5 - x^3 - x^2 - 1$
177	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3$
188	$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$
191	$y^2 + (x^3 + x + 1)y = -x^3 + x^2 + x$

Empirical evidence for $g = r = 2$, cont'd

- Tamagawa numbers, $|A_N(\mathbb{Q})_{\mathrm{tors}}|$ and $|\text{Ш}(A_N/\mathbb{Q})[2]|$ were already computed by Flynn et al.
- To numerically verify p-adic BSD, need to compute p-adic regulators $\mathrm{Reg}_p(A_N/\mathbb{Q})$ and p-adic special values $\mathcal{L}_p^*(A_N, 0)$.
- We first used Riemann sums for the p-adic special values, leading to very few digits of precision.
- We recomputed the special values later using overconvergent modular symbols.
- All regulators were computed to precision at least p^{12}.

Summary of evidence

Theorem. (Balakrishnan, Stein, M.) Assume that for all A_N the Shafarevich-Tate group over $\mathbb{Q}$ is 2-torsion. Then our conjecture is satisfied up to least 4 digits of precision at all good ordinary primes $5 < p < 100$ such that $C_N \times \mathbb{Q}_p$ has an odd degree model over $\mathbb{Q}_p$.

- Typically, we have at least 6 digits of precision.
- The assertion $Ш(A_N/\mathbb{Q}) = Ш(A_N/\mathbb{Q})[2]$ is equivalent to classical BSD (Flynn et al.).
- For all $N \neq 167$ the differences of $\mathbb{Q}$-rational points on C_N generate $A_N(\mathbb{Q})$.
- For $N = 167$, the divisors we used generate finite index subgroups, depending on p.

For example, for $N = 188$, we have:

p-adic regulator $\mathrm{Reg}_p(A_N/\mathbb{Q})$	p-adic L-value	p-adic multiplier $\epsilon_p(A_N)$
$5623044 + O(7^8)$	$1259 + O(7^4)$	$507488 + O(7^8)$
$4478725 + O(11^7)$	$150222285 + O(11^8)$	$143254320 + O(11^8)$
$775568547 + O(13^8)$	$237088204 + O(13^8)$	$523887415 + O(13^8)$
$1129909080 + O(17^8)$	$6922098082 + O(17^8)$	$4494443586 + O(17^8)$
$14409374565 + O(19^8)$	$15793371104 + O(19^8)$	$4742010391 + O(19^8)$
$31414366115 + O(23^8)$	$210465118 + O(23^8)$	$45043095109 + O(23^8)$
$2114154456754 + O(37^8)$	$1652087821140 + O(37^8)$	$1881820314237 + O(37^8)$
$6279643012659 + O(41^8)$	$2066767021277 + O(41^8)$	$4367414685819 + O(41^8)$
$9585122287133 + O(43^8)$	$3309737400961 + O(43^8)$	$85925017348 + O(43^8)$
$3328142761956 + O(53^8)$	$5143002859 + O(53^6)$	$6112104707558 + O(53^8)$
$17411023818285 + O(59^8)$	$7961878705 + O(59^6)$	$98405729721193 + O(59^8)$
$102563258757138 + O(61^8)$	$216695090848 + O(61^7)$	$137187998566490 + O(61^8)$
$26014679325501 + O(67^8)$	$7767410995 + O(67^6)$	$38320151289262 + O(67^8)$
$490864897182147 + O(71^8)$	$16754252742 + O(71^6)$	$530974572239623 + O(71^8)$
$689452389265311 + O(73^8)$	$193236387 + O(73^5)$	$162807895476311 + O(73^8)$
$878760549863821 + O(79^8)$	$1745712500 + O(79^5)$	$1063642669147985 + O(79^8)$
$2070648686579466 + O(83^8)$	$2888081539 + O(83^5)$	$1103760059074178 + O(83^8)$
$3431343284115672 + O(89^8)$	$1591745960 + O(89^5)$	$1012791564080640 + O(89^8)$
$4259144286293285 + O(97^8)$	$21828881 + O(97^4)$	$6376229493766338 + O(97^8)$

$N = 188$ – normalization

The additional BSD quantities for $N = 188$ are

$$|\text{Ш}(A_N)[2]| = 1,\ |A_N(\mathbb{Q})_{\mathrm{tors}}|^2 = 1,\ c_2 = 9,\ c_{47} = 1.$$

We find that for the quadratic character ψ associated to $\mathbb{Q}(\sqrt{233})$, the twist B of A_N by ψ has rank 0 over $\mathbb{Q}$.

- Algebraic computation yields $[0]_B^+ = 144$,
- $\eta_\psi = 1$, computed by comparing bases for the integral 1-forms on the curve C_N and its twist by ψ.
- $\frac{\eta_\psi \cdot L(B,1)}{233 \cdot \Omega_{A_N}^+} = 36$.
- So the normalization factor for the modular symbol is $1/4$.

Rank 4 evidence

- The Jacobian A of the twist C of $X_0(31)$ by the Dirichlet character associated to $\mathbb{Q}(\sqrt{-47})$ has rank 4 over $\mathbb{Q}$.
- We checked our conjecture for $p = 29, 61, 79$ to 8 digits of precision under the assumption that $\text{Ш}(A/\mathbb{Q})$ is 2-torsion.
- Since the twist is odd, we had to use the minus modular symbol associated to $J_0(31)$.
- For the normalization of the minus modular symbol, we used the twist of $X_0(31)$ by the Dirichlet character associated to $\mathbb{Q}(\sqrt{-19})$, whose Jacobian has rank 0 over $\mathbb{Q}$.
- For the regulator computations, we needed to work with generators of subgroups of finite index, depending on p.

Supersingular reduction

Suppose A_f has supersingular reduction at p.

- For elliptic curves, an analogue of the conjecture of Mazur-Tate-Teitelbaum is due to Bernardi-Perrin-Riou.
- Computation of p-adic special values works analogously.
- To extend Coleman-Gross, we would need a canonical splitting of $H^1_{dR}(C \times \mathbb{Q}_p)$.
- It's not known how to do this!
- Other constructions of the p-adic height don't seem suitable for computations.

Toric reduction

Suppose A_f has purely toric reduction at p.

- If $g = 1$ and the reduction is nonsplit multiplicative, Mazur-Tate-Teitelbaum is analogous to the good ordinary case.
- If $g = 1$ and the reduction is split multiplicative, Mazur-Tate-Teitelbaum becomes more interesting.
- Computation of p-adic special values works similarly.
- An extension of Coleman-Gross to this case is work in progress of Besser.
- Work of Werner provides formulas for the p-adic height pairing if the rigid uniformisation of A_f is known.