p-adic heights and rational points on curves

Jennifer Balakrishnan

Boston University

Journées Algophantiennes Bordelaises 2017
June 8, 2017

Rational points on higher genus curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus $g \geqslant 2$. The set $X(\mathbf{Q})$ is finite.

Rational points on higher genus curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus $g \geqslant 2$. The set $X(\mathbf{Q})$ is finite.

Rational points on higher genus curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus $g \geqslant 2$. The set $X(\mathbf{Q})$ is finite.

One strategy for computing $X(\mathbf{Q})$:

- Given a curve X of genus $g \geqslant 2$, embed it inside its *Jacobian* J. Mordell-Weil tells us that $J(\mathbf{Q}) = \mathbf{Z}^r \oplus T$.

Rational points on higher genus curves

Theorem (Faltings, 1983)

Let X be a smooth projective curve over $\mathbf{Q}$ of genus $g \geqslant 2$. The set $X(\mathbf{Q})$ is finite.

One strategy for computing $X(\mathbf{Q})$:

- Given a curve X of genus $g \geqslant 2$, embed it inside its *Jacobian* J. Mordell-Weil tells us that $J(\mathbf{Q}) = \mathbf{Z}^r \oplus T$.
- If the rank r is *less than* g, can use the Chabauty-Coleman method to compute $X(\mathbf{Q})$.

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- Coleman also used this to give the bound (for good $p > 2g$)

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- Coleman also used this to give the bound (for good $p > 2g$)

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

- This bound can be sharp in practice.

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- Coleman also used this to give the bound (for good $p > 2g$)

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

- This bound can be sharp in practice.
- Even when the bound is not sharp, we can often combine Chabauty–Coleman data at multiple primes (Mordell–Weil sieve) to extract $X(\mathbf{Q})$.

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- Coleman also used this to give the bound (for good $p > 2g$)

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

- This bound can be sharp in practice.
- Even when the bound is not sharp, we can often combine Chabauty–Coleman data at multiple primes (Mordell–Weil sieve) to extract $X(\mathbf{Q})$.

Chabauty-Coleman method

- The method gives us a regular 1-form whose p-adic (Coleman) integral vanishes on rational points.
- Coleman also used this to give the bound (for good $p > 2g$)

$$\#X(\mathbf{Q}) \leqslant \#X(\mathbf{F}_p) + 2g - 2.$$

- This bound can be sharp in practice.
- Even when the bound is not sharp, we can often combine Chabauty–Coleman data at multiple primes (Mordell–Weil sieve) to extract $X(\mathbf{Q})$.

Main question: Can we say anything in *higher* rank?

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

We have* $\operatorname{rk} J(\mathbf{Q}) = 1$, and the *Chabauty-Coleman bound* gives

$$|X(\mathbf{Q})| \leqslant 10.$$

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

We have* $\operatorname{rk} J(\mathbf{Q}) = 1$, and the *Chabauty-Coleman bound* gives

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

We have* $\operatorname{rk} J(\mathbf{Q}) = 1$, and the *Chabauty-Coleman bound* gives

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0),(1,0),(2,0),(5,0),(6,0),\infty$$

and

$$(3,\pm 6),(10,\pm 120)$$

in $X(\mathbf{Q})$.

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

We have* $\operatorname{rk} J(\mathbf{Q}) = 1$, and the *Chabauty-Coleman bound* gives

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

and

$$(3, \pm 6), (10, \pm 120)$$

in $X(\mathbf{Q})$.

We've found 10 points!

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

We have* $\operatorname{rk} J(\mathbf{Q}) = 1$, and the *Chabauty-Coleman bound* gives

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

and

$$(3, \pm 6), (10, \pm 120)$$

in $X(\mathbf{Q})$.

We've found 10 points!

Hence we have provably determined

$$X(\mathbf{Q}) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 120), \infty\}.$$

*Descent calculation first done by Gordon and Grant, 1993

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

It has at least **642** rational points*, with x-coordinates:

0, -1, 1/3, 4, -4, -3/5, -5/3, 5, 6, 2/7, 7/4, 1/8, -9/5, 7/10, 5/11, 11/5, -5/12, 11/12, 5/12, 13/10, 14/9, -15/2, -3/16, 16/15, 11/18, -19/12, 19/5, -19/11, -18/19, 20/3, -20/21, 24/7, -7/24, -17/28, 15/32, 5/32, 33/8, -23/33, -35/12, -35/18, 12/35, -37/14, 38/11, 40/17, -17/40, 34/41, 5/41, 41/16, 43/9, -47/4, -47/54, -9/55, -55/4, 21/55, -11/57, -59/15, 59/9, 61/27, -61/37, 62/21, 63/2, 65/18, -1/67, -60/67, 71/44, 71/3, -73/41, 3/74, -58/81, -41/81, 29/83, 19/83, 36/83, 11/84, 65/84, -86/45, -84/89, 5/89, -91/27, 92/21, 99/37, 100/19, -40/101, -32/101, -104/45, -13/105, 50/111, -113/57, 115/98, -115/44, 116/15, 123/34, 124/63, 125/36, 131/5, -64/133, 135/133, 35/136, -139/88, -145/7, 101/147, 149/12, -149/80, 75/157, -161/102, 97/171, 173/132, -65/173, -189/83, 190/63, 196/103, -195/196, -193/198, 201/28, 210/101, 227/81, 131/240, -259/3, 265/24, 193/267, 19/270, -279/281, 283/33, -229/298, -310/309, 174/335, 31/337, 400/129, -198/401, 384/401, 409/20, -422/199, -424/33, 434/43, -415/446, 106/453, 465/316, -25/489, 490/157, 500/317, -501/317, -404/513, -491/516, 137/581, 597/139, -612/359, 617/335, -620/383, -232/623, 653/129, 663/4, 583/695, 707/353, -772/447, 835/597, -680/843, 853/48, 860/697, 515/869, -733/921, -1049/33, -263/1059, -1060/439, 1075/21, -1111/30, 329/1123, -193/1231, 1336/1033, 321/1340, 1077/1348, -1355/389, 1400/11, -1432/359, -1505/909, 1541/180, -1340/1639, -1651/731, -1705/1761, -1757/1788, -1456/1893, -235/1983, -1990/2103, -2125/84, -2343/635, -2355/779, 2631/1393, -2639/2631, 396/2657, 2691/1301, 2707/948, -164/2777, -2831/508, 2988/43, 3124/395, -3137/3145, -3374/303, 3505/1148, 3589/907, 3131/3655, 3679/384, 535/3698, 3725/1583, 3940/939, 1442/3981, 865/4023, 2601/4124, -2778/4135, 1096/4153, 4365/557, -4552/2061, -197/4620, 4857/1871, 1337/5116, 5245/2133, 1007/5534, 1616/5553, 5965/2646, 6085/1563, 6101/1858, -5266/6303, -4565/6429, 6535/1377, -6613/6636, 6354/6697, -6908/2715, -3335/7211, 7363/3644, -4271/7399, -2872/8193, 2483/8301, -8671/3096, -6975/8941, 9107/6924, -9343/1951, -9589/3212, 10400/373, -8829/10420, 10511/2205, 1129/10836, 675/11932, 8045/12057, 12945/4627, -13680/8543, 14336/243, -100/14949, -15175/8919, 1745/15367, 16610/16683, 17287/16983, 2129/18279, -19138/1865, 19710/4649, -18799/20047, -20148/1141, -20873/9580, 21949/6896, 21985/6999, 235/25197, 16070/26739, 22991/28031, -33555/19603, -37091/14317, -2470/39207, 40645/6896, 46055/19518, -46925/11181, -9455/47584, 55904/8007, 39946/56827, -44323/57516, 15920/59083, 62569/39635, 73132/13509, 82315/67051, -82975/34943, 95393/22735, 14355/98437, 15121/102391, 130190/93793, -141665/55186, 39628/153245, 30145/169333, -140047/169734, 61203/171017, 148451/182305, 86648/195399, -199301/54169, 11795/225434, -84639/266663, 283567/143436, -291415/171792, -314333/195860, 289902/322289, 405523/327188, -342731/523857, 24960/630287, -665281/83977, -688283/82436, 199504/771597, 233305/795263, -799843/183558, -867313/1008993, 1142044/157607, 1399240/322953, -1418023/463891, 1584712/90191, 726821/2137953, 2224780/807321, -2849969/629081, -3198658/3291555, 675911/3302518, -5666740/2779443, 1526015/5872096, 13402625/4101272, 12027943/13799424, -71658936/86391295, 148596731/35675865, 58018579/158830656, 208346440/37486601, -1455780835/761431834, -3898675687/2462651894

Is this list complete?

*Computed by Stoll in 2008.

Reframing Chabauty–Coleman

For a curve $X/\mathbf{Q}$ with rank $J(\mathbf{Q}) < g$, we can find a finite set

$$X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\} \supset X(\mathbf{Q})$$

for some $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$, by pulling back an ω_J that comes from J.

Reframing Chabauty–Coleman

For a curve $X/\mathbf{Q}$ with rank $J(\mathbf{Q}) < g$, we can find a finite set

$$X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\} \supset X(\mathbf{Q})$$

for some $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$, by pulling back an ω_J that comes from J.

Indeed, the Jacobian is a natural geometric source of these p-adic integrals for $r < g$.

Reframing Chabauty–Coleman

For a curve $X/\mathbf{Q}$ with rank $J(\mathbf{Q}) < g$, we can find a finite set

$$X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\} \supset X(\mathbf{Q})$$

for some $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$, by pulling back an ω_J that comes from J.

Indeed, the Jacobian is a natural geometric source of these p-adic integrals for $r < g$.

Are there other geometric objects which can give us further p-adic integrals for $r \geqslant g$?

Nonabelian Chabauty: Explicit Faltings for $r \geqslant g$?

Kim (2005): there are further *iterated* p-adic integrals arising from *Selmer varieties*, cutting out sets of p-adic points

$$X(\mathbf{Q}_p)_1 \supset X(\mathbf{Q}_p)_2 \supset \cdots \supset X(\mathbf{Q}_p)_n \supset \cdots \supset X(\mathbf{Q})$$

where $X(\mathbf{Q}_p)_1$ is the Chabauty–Coleman set and $X(\mathbf{Q}_p)_n$ is a (finite?) set of p-adic points that can be computed in terms of n-fold iterated Coleman integrals.

Conjecture (Kim)

For sufficiently large n,

$$X(\mathbf{Q}_p)_n = X(\mathbf{Q}).$$

Challenge: Explicitly compute $X(\mathbf{Q}_p)_2, X(\mathbf{Q}_p)_3, \ldots$ for curves $X/\mathbf{Q}$ with $r \geqslant g$.

Computing nonabelian Chabauty sets

Kim's theory tells us that the first nonabelian Chabauty set, $X(\mathbf{Q}_p)_2$, should be given in terms of double Coleman integrals

$$\int_P^Q \omega_i \omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j.$$

- These integrals satisfy nice formal properties like $\int_P^Q \omega_i \omega_j + \int_P^Q \omega_j \omega_i = \left(\int_P^Q \omega_i\right)\left(\int_P^Q \omega_j\right).$

Computing nonabelian Chabauty sets

Kim's theory tells us that the first nonabelian Chabauty set, $X(\mathbf{Q}_p)_2$, should be given in terms of double Coleman integrals

$$\int_P^Q \omega_i\omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j.$$

- These integrals satisfy nice formal properties like $\int_P^Q \omega_i\omega_j + \int_P^Q \omega_j\omega_i = \left(\int_P^Q \omega_i\right)\left(\int_P^Q \omega_j\right)$.
- These integrals are very closely related to natural *quadratic* forms on $J(\mathbf{Q})$.

Computing nonabelian Chabauty sets

Kim's theory tells us that the first nonabelian Chabauty set, $X(\mathbf{Q}_p)_2$, should be given in terms of double Coleman integrals

$$\int_P^Q \omega_i \omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j.$$

- These integrals satisfy nice formal properties like $\int_P^Q \omega_i\omega_j + \int_P^Q \omega_j\omega_i = \left(\int_P^Q \omega_i\right)\left(\int_P^Q \omega_j\right)$.
- These integrals are very closely related to natural *quadratic* forms on $J(\mathbf{Q})$.
- Do we know any quadratic forms on $J(\mathbf{Q})$?

Quadratic Chabauty: computing $X(\mathbf{Q}_p)_2$

Strategy: use *p-adic heights* to write down explicit p-adic double integrals vanishing on rational or integral points on curves:

- Genus g hyperelliptic $X/\mathbf{Q}$ with Mordell-Weil rank $\mathrm{rk}(J(\mathbf{Q})) = g$: integral points

Quadratic Chabauty: computing $X(\mathbf{Q}_p)_2$

Strategy: use *p-adic heights* to write down explicit p-adic double integrals vanishing on rational or integral points on curves:

- Genus g hyperelliptic $X/\mathbf{Q}$ with Mordell-Weil rank $\mathrm{rk}(J(\mathbf{Q})) = g$: integral points
- Certain $g = 2$ curves $X/\mathbf{Q}$ with extra structure (bielliptic, real multiplication): rational points

p-adic heights on elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$, p a good, ordinary prime for E, and $P \in E(\mathbf{Q})$ non-torsion point

- that reduces to $\mathcal{O} \in E(\mathbf{F}_p)$

p-adic heights on elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$, p a good, ordinary prime for E, and $P \in E(\mathbf{Q})$ non-torsion point

- that reduces to $\mathcal{O} \in E(\mathbf{F}_p)$
- and to a nonsingular point in $E(\mathbf{F}_\ell)$ at bad primes ℓ.

p-adic heights on elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$, p a good, ordinary prime for E, and $P \in E(\mathbf{Q})$ non-torsion point

- that reduces to $\mathcal{O} \in E(\mathbf{F}_p)$
- and to a nonsingular point in $E(\mathbf{F}_\ell)$ at bad primes ℓ.

p-adic heights on elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$, p a good, ordinary prime for E, and $P \in E(\mathbf{Q})$ non-torsion point

- that reduces to $\mathcal{O} \in E(\mathbf{F}_p)$
- and to a nonsingular point in $E(\mathbf{F}_\ell)$ at bad primes ℓ.

Mazur-Stein-Tate ('06) gives us a fast way to compute the p-adic height h of such P:

$$h(P) = \frac{1}{p} \log_p \left(\frac{\sigma_p(P)}{D(P)} \right).$$

$\sigma_p(P), d(P)$

Two ingredients:

- Denominator function $D(P)$: if $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$, then $D(P) = d$.

$\sigma_p(P), d(P)$

Two ingredients:

- Denominator function $D(P)$: if $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$, then $D(P) = d$.
- p-adic σ function σ_p: the unique odd function $\sigma_p(t) = t + \cdots \in t\mathbf{Z}_p[[t]]$ satisfying

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma_p}\frac{d\sigma_p}{\omega}\right)$$

(with ω the invariant differential $\frac{dx}{2y+a_1x+a_3}$ and $c \in \mathbf{Z}_p$, which can be computed by Kedlaya's algorithm).

The height pairing

We use $h(nP) = n^2 h(P)$ to extend the height to the full Mordell-Weil group.

Question: How can we interpret the p-adic sigma function and denominator – what do they tell us?

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.
- For simplicity, assume p is a prime of ordinary reduction for J.

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.
- For simplicity, assume p is a prime of ordinary reduction for J.

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.
- For simplicity, assume p is a prime of ordinary reduction for J.

The p-adic height

$$h : J(\mathbf{Q}) \to \mathbf{Q}_p$$

- is a quadratic form

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.
- For simplicity, assume p is a prime of ordinary reduction for J.

The p-adic height

$$h : J(\mathbf{Q}) \to \mathbf{Q}_p$$

- is a quadratic form
- decomposes as a finite sum of local heights $h = \sum_v h_v$ over primes v

p-adic heights on Jacobians of curves

- Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $O \in X(\mathbf{Q})$.
- Let $\iota : X \hookrightarrow J$, sending $P \mapsto [P - O]$.
- For simplicity, assume p is a prime of ordinary reduction for J.

The p-adic height

$$h : J(\mathbf{Q}) \to \mathbf{Q}_p$$

- is a quadratic form
- decomposes as a finite sum of local heights $h = \sum_v h_v$ over primes v
- work of Bernardi, Néron, Perrin-Riou, Schneider, Mazur-Tate, Coleman-Gross, Nekovář, Besser

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Construction of h_v depends on whether $v = p$ or $v \neq p$.

- $v \neq p$: intersection theory

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Construction of h_v depends on whether $v = p$ or $v \neq p$.

- $v \neq p$: intersection theory
- $v = p$: normalized differentials, Coleman integration

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Construction of h_v depends on whether $v = p$ or $v \neq p$.

- $v \neq p$: intersection theory
- $v = p$: normalized differentials, Coleman integration

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Construction of h_v depends on whether $v = p$ or $v \neq p$.

- $v \neq p$: intersection theory
- $v = p$: normalized differentials, Coleman integration

Note: 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 $D \in \mathrm{Div}^0(X)$.

Local height pairings

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

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

with $h = \sum_v h_v$, where

- $h_v(D, E)$ is defined for $D, E \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support.
- We have $h(D, \mathrm{div}(g)) = 0$ for $g \in \mathbf{Q}(X)^\times$, so h is well-defined on $J \times J$.

Construction of h_v depends on whether $v = p$ or $v \neq p$.

- $v \neq p$: intersection theory
- $v = p$: normalized differentials, Coleman integration

Note: 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 choice of extension and write $h_v(D) := h_v(D, D)$.

More on h_p, local height at p

- Fix a decomposition

$$H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) = H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}}) \oplus W, \tag{1}$$

where W is a complementary subspace.

More on h_p, local height at p

- Fix a decomposition
$$H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) = H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}}) \oplus W, \tag{1}$$
where W is a complementary subspace.
- ω_D: differential of the third kind on $X_{\mathbf{Q}_p}$ such that

More on h_p, local height at p

- Fix a decomposition

$$H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) = H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}}) \oplus W, \tag{1}$$

  where W is a complementary subspace.
- ω_D: differential of the third kind on $X_{\mathbf{Q}_p}$ such that
  - $\mathrm{Res}(\omega_D) = D$,

More on h_p, local height at p

- Fix a decomposition

$$H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) = H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}}) \oplus W, \tag{1}$$

  where W is a complementary subspace.
- ω_D: differential of the third kind on $X_{\mathbf{Q}_p}$ such that
  - $\mathrm{Res}(\omega_D) = D$,
  - ω_D is normalized with respect to (1).

More on h_p, local height at p

- Fix a decomposition

$$H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) = H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}}) \oplus W, \tag{1}$$

  where W is a complementary subspace.
- ω_D: differential of the third kind on $X_{\mathbf{Q}_p}$ 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

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

Quadratic Chabauty

Given a global p-adic height pairing h, we want to study it on integral points:

$$\underbrace{h}_{\substack{\text{quadratic form, rewrite as a}\\ p\text{-adic analytic function}\\ \text{using Coleman integrals}}} = \underbrace{h_p}_{\substack{p\text{-adic analytic function}\\ \text{via double Coleman integral}}} + \underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite}\\ \text{number of values}\\ \text{on integral points}}}$$

Local height at p

The local height h_p is given in terms of Coleman integration (Coleman-Gross); for a hyperelliptic curve X, we can show:

Theorem (B.-Besser-Müller)

If $P \in X(\mathbf{Q}_p)$, then $h_p(P - \infty)$ is equal to a double Coleman integral

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

where $\{\bar{\omega}_0, \ldots, \bar{\omega}_{g-1}\}$ forms a dual basis to the g regular 1-forms $\{\omega_0, \ldots, \omega_{g-1}\}$ with respect to the cup product pairing on $H^1_{dR}(X_{\mathbf{Q}_p})$.

Local heights away from p

If $q \neq p$ then h_q is defined in terms of arithmetic intersection theory on a regular model of X over $\mathrm{Spec}(\mathbf{Z})$.
There is an explicitly computable finite set $T \subset \mathbf{Q}_p$ such that

$$-\sum_{q \neq p} h_q(P - \infty) \in T$$

for integral points $P \in X(\mathbf{Q})$.

Strategy of Quadratic Chabauty

Consider the $\mathbf{Q}_p$-valued functionals $f_i = \int_O \omega_i$ for $0 \leqslant i \leqslant g-1$ on $J(\mathbf{Q})$.

Idea when $r = g$:

- Suppose the f_i are linearly independent functionals on $J(\mathbf{Q})$.

Strategy of Quadratic Chabauty

Consider the $\mathbf{Q}_p$-valued functionals $f_i = \int_O \omega_i$ for $0 \leqslant i \leqslant g-1$ on $J(\mathbf{Q})$.

Idea when $r = g$:

- Suppose the f_i are linearly independent functionals on $J(\mathbf{Q})$.
- Then $\{f_i f_j\}_{i \leqslant j \leqslant g-1}$ is a natural basis of the space of $\mathbf{Q}_p$-valued quadratic forms on $J(\mathbf{Q})$.

Strategy of Quadratic Chabauty

Consider the $\mathbf{Q}_p$-valued functionals $f_i = \int_O \omega_i$ for $0 \leqslant i \leqslant g-1$ on $J(\mathbf{Q})$.

Idea when $r = g$:

- Suppose the f_i are linearly independent functionals on $J(\mathbf{Q})$.
- Then $\{f_i f_j\}_{i \leqslant j \leqslant g-1}$ is a natural basis of the space of $\mathbf{Q}_p$-valued quadratic forms on $J(\mathbf{Q})$.
- The p-adic height h is also a quadratic form, so there must exist $\alpha_{ij} \in \mathbf{Q}_p$ such that

$$h = \sum_{i \leqslant j \leqslant g-1} \alpha_{ij} f_i f_j$$

Strategy of Quadratic Chabauty

Consider the $\mathbf{Q}_p$-valued functionals $f_i = \int_O \omega_i$ for $0 \leqslant i \leqslant g-1$ on $J(\mathbf{Q})$.

Idea when $r = g$:

- Suppose the f_i are linearly independent functionals on $J(\mathbf{Q})$.
- Then $\{f_i f_j\}_{i \leqslant j \leqslant g-1}$ is a natural basis of the space of $\mathbf{Q}_p$-valued quadratic forms on $J(\mathbf{Q})$.
- The p-adic height h is also a quadratic form, so there must exist $\alpha_{ij} \in \mathbf{Q}_p$ such that

$$h = \sum_{i \leqslant j \leqslant g-1} \alpha_{ij} f_i f_j$$

- Linear algebra gives us the global p-adic height in terms of products of Coleman integrals.

Quadratic Chabauty

We use these double and single Coleman integrals to rewrite the global p-adic height pairing h and to study it on integral points:

$$\underbrace{h}_{\substack{\text{quadratic form, rewrite as a}\\ p\text{-adic analytic function}\\ \text{using Coleman integrals}}} = \underbrace{h_p}_{\substack{p\text{-adic analytic function}\\ \text{via double Coleman integral}}} + \underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite}\\ \text{number of values}\\ \text{on integral points}}}$$

Quadratic Chabauty

We use these double and single Coleman integrals to rewrite the global p-adic height pairing h and to study it on integral points:

$$\underbrace{h_p}_{\substack{p\text{-adic analytic function}\\ \text{via double Coleman integral}}} - \underbrace{h}_{\substack{\text{quadratic form, rewrite as a}\\ p\text{-adic analytic function}\\ \text{using Coleman integrals}}} = -\underbrace{\sum_{v \neq p} h_v}_{\substack{\text{takes on finite}\\ \text{number of values}\\ \text{on integral points}}}$$

Quadratic Chabauty

Theorem (B.-Besser-Müller)

If $r = g \geqslant 1$ and the f_i are independent, then there is an explicitly computable finite set $T \subset \mathbf{Q}_p$ and explicitly computable constants $\alpha_{ij} \in \mathbf{Q}_p$ such that

$$\rho(P) := \sum_{i=0}^{g-1} \int_\infty^P \omega_i \bar{\omega}_i - \sum_{0 \leqslant i \leqslant j \leqslant g-1} \alpha_{ij} f_i f_j(P)$$

takes values in T on integral points.

The case of rank 1 elliptic curves

In the case of $g = r = 1$, quadratic Chabauty says that there is an explicitly computable finite set $T \subset \mathbf{Q}_p$ and explicitly computable constant $\alpha \in \mathbf{Q}_p$ such that

$$\rho(P) = \int_O^P \omega_0 \bar{\omega}_0 - \alpha \left(\int_O^P \omega_0 \right)^2$$

takes values in T on integral points.

Example 1: rank 1 elliptic curve, integral points

We consider the elliptic curve "37a1", given by $y^2 + y = x^3 - x$. We use quadratic Chabauty to compute $X(\mathbf{Z}_p)_2$, up to hyperelliptic involution:

$X(\mathbf{F}_7)$	recovered $x(z)$ in residue disk	$z \in X(\mathbf{Q})$
$\overline{(1,0)}$	$1 + 3 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3 + O(7^6)$	??
	$1 + O(7^6)$	$(1,0)$
$\overline{(0,0)}$	$3 \cdot 7 + 7^2 + 3 \cdot 7^3 + 7^4 + 4 \cdot 7^5 + O(7^6)$	??
	$O(7^6)$	$(0,0)$
$\overline{(2,2)}$	$2 + 3 \cdot 7 + 7^2 + 5 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + O(7^6)$	??
	$2 + O(7^6)$	$(2,2)$
$\overline{(6,0)}$	$6 + O(7^6)$	$(6,14)$
	$6 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + O(7^6)$	$(-1,0)$

Integral points in rank 1

This does not seem unusual; in most computed examples, it appears that $X(\mathbf{Z}_p)_2$ is not enough to precisely cut out integral points on rank 1 elliptic curves.

Integral points in rank 1

This does not seem unusual; in most computed examples, it appears that $X(\mathbf{Z}_p)_2$ is not enough to precisely cut out integral points on rank 1 elliptic curves.

What about $X(\mathbf{Z}_p)_3$, which is given in terms of triple integrals?

Integral points in rank 1

This does not seem unusual; in most computed examples, it appears that $X(\mathbf{Z}_p)_2$ is not enough to precisely cut out integral points on rank 1 elliptic curves.

What about $X(\mathbf{Z}_p)_3$, which is given in terms of triple integrals?

To say something about this, we revisit the work of Goncharov-Levin.

Goncharov-Levin

Let E be an elliptic curve over $\mathbf{Q}$.

- Let $L(E, s)$ denote its L-function

Goncharov-Levin

Let E be an elliptic curve over $\mathbf{Q}$.

- Let $L(E, s)$ denote its L-function
- Let $\mathcal{L}_{2,E}(z)$ denote the elliptic dilogarithm.

Goncharov-Levin

Let E be an elliptic curve over $\mathbf{Q}$.

- Let $L(E, s)$ denote its L-function
- Let $\mathcal{L}_{2,E}(z)$ denote the elliptic dilogarithm.

Goncharov-Levin

Let E be an elliptic curve over $\mathbf{Q}$.

- Let $L(E, s)$ denote its L-function
- Let $\mathcal{L}_{2,E}(z)$ denote the elliptic dilogarithm.

In proving a conjecture of Zagier, Goncharov and Levin showed

Theorem (Goncharov-Levin '98)

Let E be an elliptic curve over $\mathbf{Q}$. Then there exists a $\mathbf{Q}$-rational divisor P (satisfying certain technical conditions) such that

$$L(E, 2) \sim_{\mathbf{Q}^*} \pi \cdot \mathcal{L}_{2,E}(P).$$

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model ″37a1″).

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model "37a1").

- The Mordell-Weil group is generated by $P = (0, 4)$.

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model "37a1").

- The Mordell-Weil group is generated by $P = (0, 4)$.
- Consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model "37a1").

- The Mordell-Weil group is generated by $P = (0, 4)$.
- Consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model "37a1").

- The Mordell-Weil group is generated by $P = (0, 4)$.
- Consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

Goncharov and Levin do numerical calculations to show that

$$\frac{8\pi \cdot \mathcal{L}_{2,q}(P_3)}{37 \cdot L(E,2)} = -8.0000\ldots, \qquad \frac{8\pi \cdot \mathcal{L}_{2,q}(P_6)}{37 \cdot L(E,2)} = -90.0000\ldots$$

Goncharov-Levin

Example

Let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (with minimal model ”37a1”).

- The Mordell-Weil group is generated by $P = (0, 4)$.
- Consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

Goncharov and Levin do numerical calculations to show that

$$\frac{8\pi \cdot \mathcal{L}_{2,q}(P_3)}{37 \cdot L(E,2)} = -8.0000\ldots, \qquad \frac{8\pi \cdot \mathcal{L}_{2,q}(P_6)}{37 \cdot L(E,2)} = -90.0000\ldots$$

In particular, it seems that

$$\frac{\mathcal{L}_{2,q}(P_3)}{\mathcal{L}_{2,q}(P_6)} = \frac{4}{45}.$$

p-adic Goncharov-Levin (B.–Dogra)

We are studying *triple* Coleman integrals and a p-adic analogue of Goncharov-Levin:

Example

As before, let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (minimal model "37a1") and consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

p-adic Goncharov-Levin (B.–Dogra)

We are studying *triple* Coleman integrals and a p-adic analogue of Goncharov-Levin:

Example

As before, let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (minimal model "37a1") and consider the divisor $P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.

p-adic Goncharov-Levin (B.–Dogra)

We are studying *triple* Coleman integrals and a p-adic analogue of Goncharov-Levin:

Example

As before, let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (minimal model "37a1") and consider the divisor
$P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.
Let $\omega_0 = \frac{dx}{2y}$ and $\omega_1 = \frac{xdx}{2y}$. We seem to have

$$\frac{\int_{P_3} \omega_0\omega_1\omega_1 - \frac{1}{2}\int_{P_3} \omega_1}{\int_{P_6} \omega_0\omega_1\omega_1 - \frac{1}{2}\int_{P_6} \omega_1} = \frac{4}{45}.$$

p-adic Goncharov-Levin (B.–Dogra)

We are studying *triple* Coleman integrals and a p-adic analogue of Goncharov-Levin:

Example

As before, let E be the elliptic curve given by $y^2 = x^3 - 16x + 16$ (minimal model "37a1") and consider the divisor
$P_k = (kP) - k(P) - \frac{k^3-k}{6}((2P) - 2(P))$.
Let $\omega_0 = \frac{dx}{2y}$ and $\omega_1 = \frac{xdx}{2y}$. We seem to have

$$\frac{\int_{P_3} \omega_0\omega_1\omega_1 - \frac{1}{2}\int_{P_3}\omega_1}{\int_{P_6} \omega_0\omega_1\omega_1 - \frac{1}{2}\int_{P_6}\omega_1} = \frac{4}{45}.$$

We also seem to have

$$\frac{\int_{P_3} \omega_0\omega_0\omega_1}{\int_{P_6} \omega_0\omega_0\omega_1} = \frac{4}{45}.$$

Example 2: integral points on rank 1 elliptic curves, Kim's conjecture (B.-Dogra)

We can use these triple Coleman integrals to construct a function F_3 vanishing on integral points:

$$X(\mathbf{Z}_p)_3 := \{z : F_3(z) = 0\} \cap X(\mathbf{Z}_p)_2,$$

where

$$X(\mathbf{Z}_p)_2 = \{z : D_2(z) - \alpha \log^2(z) = 0\}.$$

Instead of directly computing $X(\mathbf{Z}_p)_3$, we take $z \in X(\mathbf{Z}_p)_2$ and compute the value of $F_3(z)$.

Example 2: integral points on rank 1 elliptic curves, Kim's conjecture (B.-Dogra)

For example, for $X : y^2 + y = x^3 - x$ ("37a1"), in $X(\mathbf{Z}_7)_2$, we recovered a point

$$z = (1{+}3{\cdot}7{+}6{\cdot}7^2{+}4{\cdot}7^3{+}O(7^6), 6{\cdot}7{+}3{\cdot}7^2{+}2{\cdot}7^3{+}2{\cdot}7^4{+}5{\cdot}7^5{+}O(7^6))$$

(not an integral point). We find

Example 2: integral points on rank 1 elliptic curves, Kim's conjecture (B.-Dogra)

For example, for $X : y^2 + y = x^3 - x$ ("37a1"), in $X(\mathbf{Z}_7)_2$, we recovered a point

$$z = (1+3\cdot7+6\cdot7^2+4\cdot7^3+O(7^6), 6\cdot7+3\cdot7^2+2\cdot7^3+2\cdot7^4+5\cdot7^5+O(7^6))$$

(not an integral point). We find

$$F_3(z) = 6 \cdot 7^3 + 3 \cdot 7^4 + 4 \cdot 7^5 + O(7^6) \neq 0.$$

Example 2: integral points on rank 1 elliptic curves, Kim's conjecture (B.-Dogra)

For example, for $X : y^2 + y = x^3 - x$ ("37a1"), in $X(\mathbf{Z}_7)_2$, we recovered a point

$z = (1+3\cdot 7+6\cdot 7^2+4\cdot 7^3+O(7^6), 6\cdot 7+3\cdot 7^2+2\cdot 7^3+2\cdot 7^4+5\cdot 7^5+O(7^6))$

(not an integral point). We find

$$F_3(z) = 6 \cdot 7^3 + 3 \cdot 7^4 + 4 \cdot 7^5 + O(7^6) \neq 0.$$

In the same residue disk, we recovered $z = (1, 0)$. We find

Example 2: integral points on rank 1 elliptic curves, Kim's conjecture (B.-Dogra)

For example, for $X : y^2 + y = x^3 - x$ ("37a1"), in $X(\mathbf{Z}_7)_2$, we recovered a point

$$z = (1+3\cdot7+6\cdot7^2+4\cdot7^3+O(7^6), 6\cdot7+3\cdot7^2+2\cdot7^3+2\cdot7^4+5\cdot7^5+O(7^6))$$

(not an integral point). We find

$$F_3(z) = 6 \cdot 7^3 + 3 \cdot 7^4 + 4 \cdot 7^5 + O(7^6) \neq 0.$$

In the same residue disk, we recovered $z = (1, 0)$. We find

$$F_3(z) = O(7^{11}).$$

Example 2: integral points, rank 1 elliptic curves

Continuing in this way, we complete the table

$X(\mathbf{F}_7)$	recovered $x(z)$	$z \in X(\mathbf{Q})$	$F_3(z)$
$\overline{(1,0)}$	$1 + 3\cdot 7 + 6\cdot 7^2 + 4\cdot 7^3 + O(7^6)$	??	$6\cdot 7^3 + 3\cdot 7^4 + 4\cdot 7^5 + O(7^6)$
	$1 + O(7^{11})$	$(1,0)$	$O(7^{11})$
$\overline{(0,0)}$	$3\cdot 7 + 7^2 + 3\cdot 7^3 + 7^4 + 4\cdot 7^5 + O(7^6)$	??	$3\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + O(7^6)$
	$O(7^{11})$	$(0,0)$	$O(7^{11})$
$\overline{(2,2)}$	$2 + 3\cdot 7 + 7^2 + 5\cdot 7^3 + 5\cdot 7^4 + 4\cdot 7^5 + O(7^6)$	??	$5\cdot 7^3 + 6\cdot 7^4 + 5\cdot 7^5 + O(7^6)$
	$2 + O(7^{11})$	$(2,2)$	$O(7^{11})$
$\overline{(6,0)}$	$6 + O(7^{11})$	$(6,14)$	$O(7^{11})$
	$6 + 6\cdot 7 + 6\cdot 7^2 + 6\cdot 7^3 + 6\cdot 7^4 + 6\cdot 7^5 + O(7^6)$	$(-1,0)$	$O(7^{11})$

Indeed, it seems that $X(\mathbf{Z}_7)_3$ precisely cut out integral points on this rank 1 elliptic curve!

Rational points for bielliptic genus 2 curves

Let K be $\mathbf{Q}$ or a quadratic imaginary number field, X/K be given by

$$y^2 = x^6 + ax^4 + bx^2 + c$$

and let

$$E_1 : y^2 = x^3 + ax^2 + bx + c \qquad\qquad E_2 : y^2 = x^3 + bx^2 + acx + c^2,$$

with maps

$$\begin{array}{rccc} f_1 : & X & \longrightarrow & E_1 \\ & (x,y) & \mapsto & (x^2, y) \end{array} \qquad \begin{array}{rccc} f_2 : & X & \longrightarrow & E_2 \\ & (x,y) & \mapsto & (cx^{-2}, cyx^{-3}). \end{array}$$

Theorem (B.-Dogra)

Let X/K be as above and suppose E_1 and E_2 each have rank 1. We can carry out quadratic Chabauty to compute a finite set of p-adic points containing $X(K)$.

Details (*all* the p-adic heights)

Theorem (B.–Dogra '16)

Then X/K be a genus 2 bielliptic curve as before. Then $X(K)$ is contained in the finite set of z in $X(K_{\mathfrak{p}})$ satisfying

$$\begin{aligned}\rho(z) &= 2h_{E_2,\mathfrak{p}}(f_2(z)) - h_{E_1,\mathfrak{p}}(f_1(z) + (0, \sqrt{c})) - h_{E_1,\mathfrak{p}}(f_1(z) + (0, -\sqrt{c})) \\ &\quad - 2\alpha_2 \log_{E_2}(f_2(z))^2 + 2\alpha_1(\log_{E_1}(f_1(z))^2 + \log_{E_1}((0, \sqrt{c}))^2) \\ &\in \Omega,\end{aligned}$$

where Ω is the finite set of values

$$\left\{ \sum_{v \nmid p} \left(h_{E_1,v}(f_1(z) + (0, \sqrt{c})) + h_{E_1,v}(f_1(z) + (0, -\sqrt{c})) - 2h_{E_2,v}(f_2(z)) \right) \right\},$$

for (z_v) in $\prod_{v \nmid p} X(K_v)$, and where $\alpha_i = \frac{h_{E_i}(P_i)}{[K:\mathbf{Q}] \log_{E_i}(P_i)^2}$.

Example 3: Computing $X_0(37)(\mathbf{Q}(i))$

[joint work with Dogra and Müller]

Consider

$$X_0(37) : y^2 = -x^6 - 9x^4 - 11x^2 + 37.$$

We have $\mathrm{rk}(J_0(37)(\mathbf{Q}(i))) = 2$.

Change models and use

$$X : y^2 = x^6 - 9x^4 + 11x^2 + 37,$$

which is isomorphic to $X_0(37)$ over $K = \mathbf{Q}(i)$; we have $\mathrm{rk}(J(\mathbf{Q})) = \mathrm{rk}(J(\mathbf{Q}(i))) = 2$.

Define

$$E_1 : y^2 = x^3 - 16x + 16 \qquad\qquad E_2 : y^2 = x^3 - x^2 - 373x + 2813$$

and maps from X

$$\begin{array}{cccc} f_1 : & X & \longrightarrow & E_1 \\ & (x,y) & \mapsto & (x^2-3, y) \end{array} \qquad \begin{array}{cccc} f_2 : & X & \longrightarrow & E_2 \\ & (x,y) & \mapsto & (37x^{-2}+4, 37yx^{-3}). \end{array}$$

Take P_1 and P_2 to be points of infinite order in $E_1(\mathbf{Q})$ and $E_2(\mathbf{Q})$.

$X_0(37)(\mathbf{Q}(i))$, continued

We compute

$$\begin{aligned}\rho(z) = 2h_{E_2,\mathfrak{p}}(f_2(z)) - h_{E_1,\mathfrak{p}}(f_1(z) + (-3, \sqrt{37}))\\ - h_{E_1,\mathfrak{p}}(f_1(z) + (-3, -\sqrt{37}))\\ - 2\alpha_2 h_{E_2}(f_2(z)) + 2\alpha_1(h_{E_1}(f_1(z)) + \log_{E_1}((-3, \sqrt{37}))^2)\end{aligned}$$

and find that points $z \in X(\mathbf{Q}(i))$ satisfy

$$\rho(z) = \frac{4}{3}\log_p(37).$$

Taking $p = 41, 73, 101$, we use ρ to produce points in $X(\mathbf{Q}_{41}), X(\mathbf{Q}_{73}), X(\mathbf{Q}_{101})$.

Recovered points in $X(\mathbf{Q}_{41})$

$X(\mathbf{F}_{41})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$\overline{(1,9)}$	$1 + 16\cdot 41 + 23\cdot 41^2 + 5\cdot 41^3 + 23\cdot 41^4 + O(41^5)$	
	$1 + 6\cdot 41 + 23\cdot 41^2 + 30\cdot 41^3 + 14\cdot 41^4 + O(41^5)$	
$\overline{(2,1)}$	$2 + O(41^5)$	$(2,1)$
	$2 + 19\cdot 41 + 36\cdot 41^2 + 15\cdot 41^3 + 26\cdot 41^4 + O(41^5)$	
$\overline{(4,18)}$		
$\overline{(5,12)}$	$5 + 25\cdot 41 + 26\cdot 41^2 + 26\cdot 41^3 + 31\cdot 41^4 + O(41^5)$	
	$5 + 14\cdot 41 + 12\cdot 41^3 + 33\cdot 41^4 + O(41^5)$	
$\overline{(6,1)}$	$6 + 18\cdot 41^2 + 31\cdot 41^3 + 6\cdot 41^4 + O(41^5)$	
	$6 + 30\cdot 41 + 35\cdot 41^2 + 11\cdot 41^3 + O(41^5)$	
$\overline{(7,15)}$		
$\overline{(9,4)}$	$9 + 9\cdot 41 + 34\cdot 41^2 + 22\cdot 41^3 + 24\cdot 41^4 + O(41^5)$	$(i,4)$
	$9 + 39\cdot 41 + 14\cdot 41^2 + 6\cdot 41^3 + 17\cdot 41^4 + O(41^5)$	
$\overline{(12,5)}$		
$\overline{(13,19)}$	$13 + 10\cdot 41 + 2\cdot 41^2 + 15\cdot 41^3 + 29\cdot 41^4 + O(41^5)$	
	$13 + 7\cdot 41 + 8\cdot 41^2 + 32\cdot 41^3 + 14\cdot 41^4 + O(41^5)$	
$\overline{(16,1)}$	$16 + 13\cdot 41 + 6\cdot 41^3 + 18\cdot 41^4 + O(41^5)$	
	$16 + 12\cdot 41 + 8\cdot 41^2 + 9\cdot 41^3 + 32\cdot 41^4 + O(41^5)$	
$\overline{(17,20)}$	$17 + 24\cdot 41 + 37\cdot 41^2 + 16\cdot 41^3 + 28\cdot 41^4 + O(41^5)$	
	$17 + 19\cdot 41 + 20\cdot 41^2 + 7\cdot 41^3 + 7\cdot 41^4 + O(41^5)$	
$\overline{(18,20)}$	$18 + 3\cdot 41 + 7\cdot 41^2 + 9\cdot 41^3 + 38\cdot 41^4 + O(41^5)$	
	$18 + 41 + 34\cdot 41^2 + 3\cdot 41^3 + 32\cdot 41^4 + O(41^5)$	
$\overline{(19,3)}$		
$\overline{(20,6)}$	$20 + 7\cdot 41 + 40\cdot 41^2 + 22\cdot 41^3 + 7\cdot 41^4 + O(41^5)$	
	$20 + 23\cdot 41 + 26\cdot 41^2 + 17\cdot 41^3 + 22\cdot 41^4 + O(41^5)$	
$\overline{\infty^+}$	∞^+	∞^+
$\overline{(0,18)}$	$32\cdot 41 + 13\cdot 41^2 + 16\cdot 41^3 + 8\cdot 41^4 + O(41^5)$	
	$9\cdot 41 + 27\cdot 41^2 + 24\cdot 41^3 + 32\cdot 41^4 + O(41^5)$	

Recovered points in $X(\mathbf{Q}_{73})$

$X(\mathbf{F}_{73})$	recovered $x(z)$ in residue disk	$z \in X(K)$ (or $X(\mathbf{Q}(\sqrt{3}))$)
$\overline{(2,1)}$	$2 + 61 \cdot 73 + 50 \cdot 73^2 + 71 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$	
	$2 + O(73^5)$	$(2,1)$
$\overline{(5,26)}$	$5 + 63 \cdot 73 + 4 \cdot 73^2 + 42 \cdot 73^3 + 25 \cdot 73^4 + O(73^5)$	
	$5 + 39 \cdot 73 + 65 \cdot 73^2 + 33 \cdot 73^3 + 60 \cdot 73^4 + O(73^5)$	
$\overline{(7,16)}$	$7 + 62 \cdot 73 + 31 \cdot 73^2 + 33 \cdot 73^3 + 44 \cdot 73^4 + O(73^5)$	
	$7 + 29 \cdot 73 + 67 \cdot 73^2 + 69 \cdot 73^3 + 17 \cdot 73^4 + O(73^5)$	
$\overline{(9,34)}$		
$\overline{(10,30)}$	$10 + 53 \cdot 73 + 35 \cdot 73^2 + 21 \cdot 73^3 + 67 \cdot 73^4 + O(73^5)$	
	$10 + 39 \cdot 73 + 40 \cdot 73^2 + 17 \cdot 73^3 + 59 \cdot 73^4 + O(73^5)$	
$\overline{(18,17)}$		
$\overline{(19,2)}$		
$\overline{(20,15)}$		
$\overline{(21,4)}$	$21 + 17 \cdot 73 + 70 \cdot 73^2 + 42 \cdot 73^3 + 18 \cdot 73^4 + O(73^5)$	
	$21 + 52 \cdot 73 + 67 \cdot 73^2 + 20 \cdot 73^3 + 27 \cdot 73^4 + O(73^5)$	$(\sqrt{3},4)$
$\overline{(23,31)}$	$23 + 18 \cdot 73 + 59 \cdot 73^2 + 23 \cdot 73^3 + 2 \cdot 73^4 + O(73^5)$	
	$23 + 70 \cdot 73 + 53 \cdot 73^2 + 21 \cdot 73^3 + 50 \cdot 73^4 + O(73^5)$	
$\overline{(25,25)}$		
$\overline{(27,4)}$	$27 + 62 \cdot 73 + 28 \cdot 73^2 + 56 \cdot 73^3 + 58 \cdot 73^4 + O(73^5)$	$(i,4)$
	$27 + 24 \cdot 73 + 30 \cdot 73^2 + 20 \cdot 73^3 + 65 \cdot 73^4 + O(73^5)$	
$\overline{(29,8)}$	$29 + 70 \cdot 73 + 21 \cdot 73^2 + 56 \cdot 73^3 + 5 \cdot 73^4 + O(73^5)$	
	$29 + 34 \cdot 73 + 42 \cdot 73^2 + 19 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$	
$\overline{(30,20)}$		
$\overline{(36,17)}$	$36 + 70 \cdot 73 + 19 \cdot 73^2 + 11 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$	
	$36 + 32 \cdot 73 + 23 \cdot 73^2 + 23 \cdot 73^3 + 28 \cdot 73^4 + O(73^5)$	
$\overline{\infty^+}$	∞^+	∞^+
$\overline{(0,16)}$	$61 \cdot 73 + 63 \cdot 73^2 + 51 \cdot 73^3 + 16 \cdot 73^4 + O(73^5)$	
	$12 \cdot 73 + 9 \cdot 73^2 + 21 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$	

Recovered points in $X(\mathbf{Q}_{101})$

$X(\mathbf{F}_{101})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$\overline{(2,1)}$	$2 + O(101^7)$	$(2,1)$
	$2 + 38 \cdot 101 + 11 \cdot 101^2 + 99 \cdot 101^3 + 26 \cdot 101^4 + O(101^5)$	
$\overline{(8,36)}$	$8 + 90 \cdot 101 + 39 \cdot 101^2 + 80 \cdot 101^3 + 70 \cdot 101^4 + O(101^5)$	
	$8 + 40 \cdot 101 + 84 \cdot 101^2 + 74 \cdot 101^3 + 15 \cdot 101^4 + O(101^5)$	
$\overline{(10,4)}$	$10 + 5 \cdot 101 + 29 \cdot 101^2 + 66 \cdot 101^3 + 10 \cdot 101^4 + O(101^5)$	$(i,4)$
	$10 + 49 \cdot 101 + 80 \cdot 101^2 + 74 \cdot 101^3 + 8 \cdot 101^4 + O(101^5)$	
$\overline{(12,7)}$	$12 + 12 \cdot 101 + 95 \cdot 101^2 + 55 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
	$12 + 36 \cdot 101 + 62 \cdot 101^2 + 97 \cdot 101^3 + 27 \cdot 101^4 + O(101^5)$	
$\overline{(14,21)}$	$14 + 62 \cdot 101 + 62 \cdot 101^2 + 41 \cdot 101^3 + 51 \cdot 101^4 + O(101^5)$	
	$14 + 80 \cdot 101 + 72 \cdot 101^2 + 32 \cdot 101^3 + 75 \cdot 101^4 + O(101^5)$	
$\overline{(15,11)}$		
$\overline{(17,18)}$	$17 + 65 \cdot 101 + 37 \cdot 101^2 + 80 \cdot 101^3 + 45 \cdot 101^4 + O(101^5)$	
	$17 + 50 \cdot 101 + 61 \cdot 101^2 + 89 \cdot 101^3 + 61 \cdot 101^4 + O(101^5)$	
$\overline{(18,45)}$		
$\overline{(20,47)}$		
$\overline{(22,3)}$	$22 + 59 \cdot 101 + 78 \cdot 101^2 + 43 \cdot 101^3 + 53 \cdot 101^4 + O(101^5)$	
	$22 + 96 \cdot 101 + 29 \cdot 101^2 + 43 \cdot 101^3 + 86 \cdot 101^4 + O(101^5)$	
$\overline{(24,19)}$		
$\overline{(27,39)}$		
$\overline{(28,37)}$	$28 + 30 \cdot 101 + 83 \cdot 101^2 + 5 \cdot 101^3 + 23 \cdot 101^4 + O(101^5)$	
	$28 + 37 \cdot 101 + 24 \cdot 101^2 + 78 \cdot 101^3 + 35 \cdot 101^4 + O(101^5)$	

Recovered points in $X(\mathbf{Q}_{101})$, continued

$X(\mathbf{F}_{101})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$\overline{(30,46)}$		
$\overline{(31,23)}$	$31 + 23 \cdot 101 + 11 \cdot 101^2 + 67 \cdot 101^3 + 39 \cdot 101^4 + O(101^5)$	
	$31 + 29 \cdot 101 + 68 \cdot 101^2 + 29 \cdot 101^3 + 24 \cdot 101^4 + O(101^5)$	
$\overline{(34,45)}$	$34 + 91 \cdot 101 + 46 \cdot 101^2 + 28 \cdot 101^3 + 34 \cdot 101^4 + O(101^5)$	
	$34 + 51 \cdot 101 + 73 \cdot 101^2 + 34 \cdot 101^3 + 14 \cdot 101^4 + O(101^5)$	
$\overline{(37,22)}$		
$\overline{(38,28)}$		
$\overline{(39,46)}$	$39 + 76 \cdot 101 + 86 \cdot 101^2 + 18 \cdot 101^3 + 64 \cdot 101^4 + O(101^5)$	
	$39 + 31 \cdot 101 + 43 \cdot 101^2 + 10 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
$\overline{(46,6)}$		
$\overline{(47,32)}$		
$\overline{(48,27)}$	$48 + 43 \cdot 101 + 100 \cdot 101^2 + 47 \cdot 101^3 + 19 \cdot 101^4 + O(101^5)$	
	$48 + 21 \cdot 101 + 38 \cdot 101^2 + 80 \cdot 101^3 + 95 \cdot 101^4 + O(101^5)$	
$\overline{(50,5)}$	$50 + 59 \cdot 101 + 19 \cdot 101^2 + 64 \cdot 101^3 + 36 \cdot 101^4 + O(101^5)$	
	$50 + 74 \cdot 101 + 69 \cdot 101^2 + 80 \cdot 101^3 + 21 \cdot 101^4 + O(101^5)$	
$\overline{\infty^+}$	∞^+	∞^+
$\overline{(0,21)}$		

Putting it together and computing $X_0(37)(\mathbf{Q}(i))$

Carry out the Mordell-Weil sieve on the sets of points found in $X(\mathbf{Q}_{41}), X(\mathbf{Q}_{73})$, and $X(\mathbf{Q}_{101})$; conclude that

$$X(\mathbf{Q}(i)) = \{(\pm 2 : \pm 1 : 1), (\pm i : \pm 4 : 1), (1 : \pm 1 : 0)\},$$

or in other words,

$$X_0(37)(\mathbf{Q}(i)) = \{(\pm 2i : \pm 1 : 1), (\pm 1 : \pm 4 : 1), (i : \pm 1 : 0)\}.$$

Putting it together and computing $X_0(37)(\mathbf{Q}(i))$

Carry out the Mordell-Weil sieve on the sets of points found in $X(\mathbf{Q}_{41}), X(\mathbf{Q}_{73})$, and $X(\mathbf{Q}_{101})$; conclude that

$$X(\mathbf{Q}(i)) = \{(\pm 2 : \pm 1 : 1), (\pm i : \pm 4 : 1), (1 : \pm 1 : 0)\},$$

or in other words,

$$X_0(37)(\mathbf{Q}(i)) = \{(\pm 2i : \pm 1 : 1), (\pm 1 : \pm 4 : 1), (i : \pm 1 : 0)\}.$$

Note: the computation of points in $X(\mathbf{Q}_{73})$ recovered the points $(\pm\sqrt{-3}, \pm 4) \in X_0(37)(\mathbf{Q}(\sqrt{-3}))$ as well!

Future directions

Francesca Bianchi has recently given an algorithm to compute p-adic heights for *families* of elliptic curves; she can use this to show that there are infinitely many elliptic curves over $\mathbf{Q}$ of rank 2 with nonzero p-adic regulator.

Future directions

Francesca Bianchi has recently given an algorithm to compute p-adic heights for *families* of elliptic curves; she can use this to show that there are infinitely many elliptic curves over $\mathbf{Q}$ of rank 2 with nonzero p-adic regulator.

Up next: Steffen Müller will discuss the latest in computing p-adic heights (and rational points!) for curves whose Jacobians admit real multiplication.