Rational points via p-adic L-functions

Sachi Hashimoto

Brown University

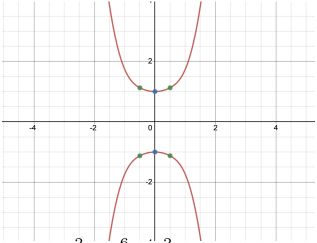
Problem (Diophantus, 3rd century AD)

Find three squares which when added give a square, and such that the first one is the side [the square root] of the second, and the second is the side of the third

In algebra, this translates to finding x, y satisfying $y^2 = x^8 + x^4 + x^2$. If we remove the solution $(0,0)$, we are asked to find rational points on the curve

$$X : y^2 = x^6 + x^2 + 1.$$

Diophantus gave the solution $(1/2, 9/16)$.



A plot of the curve $y^2 = x^6 + x^2 + 1$ and its rational solutions

In 1990, Wetherell showed that the complete set of rational points $X(\mathbf{Q})$ is $\{(0, \pm 1), (\pm 1/2, \pm 9/16), \pm\infty\})$.

An example of Elkies and Stoll

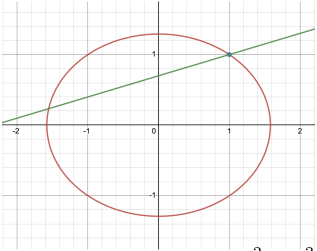
$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

has at least 642 rational solutions 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?

Consider the curve $X : 2x^2 + 3y^2 = 5$. This has the solution $(1, 1)$.



parametrizing rational points on $2x^2 + 3y^2 = 5$

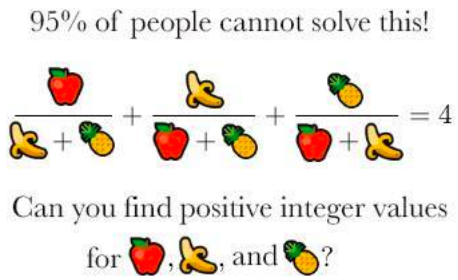
To obtain all other rational solutions (x, y) we can draw a line

$$\ell : y - 1 = m(x - 1)$$

through $(1, 1)$ with rational slope $m \in \mathbf{Q}$.
The second point of intersection $X \cap \ell$ is also rational, and for every rational point on X, the line ℓ will have rational slope.

An example of Bremner and MacLeod

Diophantine equations made a comeback on the internet between 2016 - 2019.[1]



Letting $a =$  , $b =$ , $c =$ 

$$x = \frac{-28(a+b+2c)}{6a+6b-c}, \quad y = \frac{364(a-b)}{6a+6b-c}$$

This equation translates to finding the integer solutions on the elliptic curve

$$y^2 = x^3 + 109x^2 + 224x$$

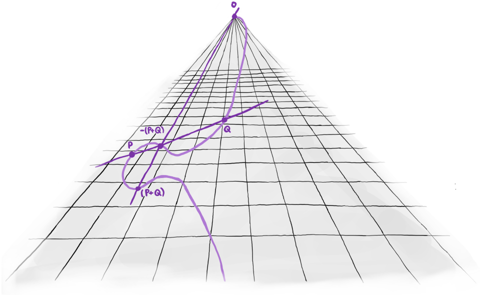
[1] Source: KnowYourMeme, `https://knowyourmeme.com/memes/fruit-math-math-with-fruit`

An example of Bremner and MacLeod

We have the small point $P = (-100, 260)$ ($\leftrightarrow a = 2/7, b = -1/14, c = 11/14$) on

$$y^2 = x^3 + 109x^2 + 224x$$

Generate more solutions by addition. $E(\mathbf{Q}) \simeq \mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$



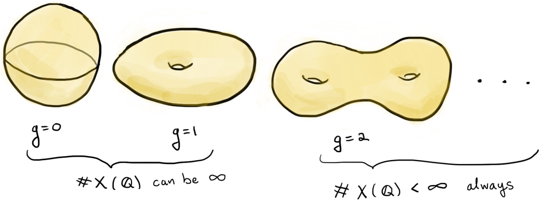
$9P$ gives the smallest positive answer

$$\begin{aligned} a &= 154476802108746166441951315019919837485664325669565431700026634898253202035277999, \\ b &= 36875131794129999827197811565225474825492979968971970996283137471637224634055579, \\ c &= 4373612677928697257861252602371390152816537558161613618621437993378423467772036 \end{aligned}$$

While there are infinitely many rational triples (a, b, c) there are only finitely many integer solutions (a, b, c) (but this slide is too small to list them all).

Set-up

Let X be a nice (smooth projective geometrically integral) curve over $\mathbf{Q}$.
Curves are classified by their genus:



Faltings's theorem (1983) states that a nice curve X of genus $g \geq 2$ has finitely many rational points; however, it does not give an explicit recipe to compute $X(\mathbf{Q})$.

Corollary: while an elliptic curve (of genus 1) can have infinitely many rational points, an affine genus 1 curve has finitely many integer points.

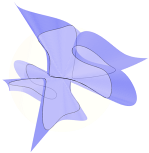
Problem (Motivating question)

Let $X/\mathbf{Q}$ be a nice curve of genus $g \geq 2$. (How) can we provably determine $X(\mathbf{Q})$? If X is modular, can we determine $X(\mathbf{Q})$ from the data of the modular forms associated to X?

Study p-adic methods for $p > 2$ a good prime, focusing on Chabauty's method.

Basic idea: Chabauty's method says that $X(\mathbf{Q})$ is contained in a finite computable set of p-adic points. We compute this set, and hope we can rule out any non-rational points.

Test case that leads to the general case: how can we provably determine the integer points of an affine elliptic curve E of rank 1? Can we do it directly from the modular form f associated to E?



Let $X/\mathbf{Q}_p$.
The p-adic points of X decompose into residue disks

$$X(\mathbf{Q}_p) = \sqcup_{P \in X(\mathbf{F}_p)} X(\mathbf{Q}_p)_P$$

grouped by which $\mathbf{F}_p$-point they reduce to.
The coordinate ring of disk $X(\mathbf{Q}_p)_P$ is a DVR, we can choose a uniformizing parameter t_P.

Theorem (roots of power series)

Let $\ell(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbf{Q}_p[[t]]$ *such that* $a_n \to 0$ *as* $n \to \infty$ *in the p-adic topology. (So* ℓ *converges on* $\mathbf{Z}_p$*.) Let* $v_0 = \max\{|a_n|_p : n \geq 0\}$ *and* $N = \max\{n \geq 0 : |a_n|_p = v_0\}$*. Then*

$$\#\{r \in \mathbf{Z}_p : \ell(r) = 0\} < N.$$

A *locally analytic function* ρ is a function such that on each residue disk $X(\mathbf{Q}_p)_P$, $P \in X(\mathbf{F}_p)$, the function $\rho|_{X(\mathbf{Q}_p)_P} = \sum_{n \geq 1} a_n t^n$ is a convergent power series.
Such a $\rho \neq 0$ has only finitely many zeros.

Example: QC for elliptic curves of rank 1

An elliptic curve (of genus 1) E can have infinitely many rational points, an affine genus 1 curve has finitely many integer points. Quadratic Chabauty computes $E(\mathbf{Z})$ for rank 1 affine genus 1 curves.

The global p-adic height is a symmetric bilinear pairing

$$h : E(\mathbf{Q}) \times E(\mathbf{Q}) \to \mathbf{Q}_p.$$

It decomposes as a sum of local pairings $h = \sum_{v \text{ prime}} h_v$.
There is also the p-adic logarithm $\log : E(\mathbf{Q}_p) \to \mathbf{Q}_p$.

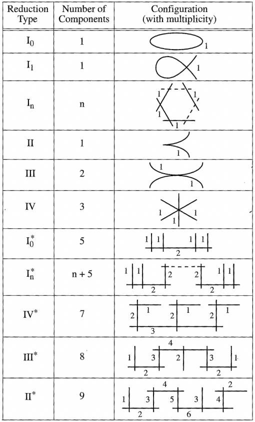
When E is rank 1, $E(\mathbf{Q}) \otimes \mathbf{Z}_p$ is 1-dimensional: it has only a 1-dimensional space of quadratic forms. This implies there exists $\gamma \in \mathbf{Q}_p$ such that

$$h(z) = \gamma \log^2(z)$$

for all $z \in E(\mathbf{Q})$.

There exists $\gamma \in \mathbf{Q}_p$ such that for all $z \in E(\mathbf{Q})$, $h(z) = \gamma \log(z)^2$.

- For primes $v \neq p$, if E has bad reduction at v, $h_v(z)$ takes values in a finite set W_v determined by the Kodaira type of E. Let $W = \prod_v W_v$ and for $w \in W$, let $\|w\|$ be the sum of its elements.
- For $v = p$, for $z \in E(\mathbf{Z})$, $h_p(z)$ is locally analytic.



Reduction Type	Number of Components	Configuration (with multiplicity)
I_0	1	
I_1	1	
I_n	n	
II	1	
III	2	
IV	3	
I_0^*	5	
I_n^*	n + 5	
IV^*	7	
III^*	8	
II^*	9	

The Kodaira-Néron Classification of Special Fibers

Theorem (Balakrishnan–Kedlaya–Kim, Bianchi)

We have

$$E(\mathbf{Z}) \subseteq \bigcup_{w \in W} \{z \in E(\mathbf{Z}_p) : h_p(z) + \|w\| = \gamma \log(z)^2\}.$$

Decomposing the height

Question

How do we compute the constant γ, such that $\forall z \in E(\mathbf{Q})$, $\gamma \log(z)^2 = h(z)$?

If we know any $y \in E(\mathbf{Q})$ of infinite order, this can be done.

$E(\mathbf{Q})$ has a natural generator: the trace of a *Heegner point*. Heegner points are points y_K are attached to an imaginary quadratic fields K.
We assume

- "Heegner hypothesis": every prime q dividing the conductor N of E splits in K; (existence)
- p splits in K and coprime to N and the discriminant D of K is odd and less than -3 (for construction of a p-adic L-function);
- K has class number 1. (for simplicity)

Goal

Compute $\log(z)^2$ and $h(z)$ when z is the trace of the Heegner point for $E(\mathbf{Z})$.

Main theorem: integral points on affine elliptic curves

Theorem (H.)

Let $E/\mathbf{Z}$ be an affine elliptic curve of rank 1. Let f/K be the modular form associated to E. Assume $p > 2$ is a good ordinary prime.
Then γ is equal the ratio of the two p-adic L-values

$$\gamma := C_f \frac{\mathcal{L}'_{p,\mathrm{PR}}(f/K, 1)}{L_{p,\mathrm{BDP}}(f/K, 1)}$$

that appear in the p-adic Gross–Zagier formulas of Perrin-Riou and Bertolini, Darmon and Prasanna times an explicit constant C_f depending only on f/K.
Furthermore, we give an algorithm to compute γ.

The analogue of this theorem holds for rational points on higher genus quotients of modular curves $X_0(N)/W$. The global height can be written as a linear combination of logarithm functions, where the coefficients are special values of p-adic L-functions.

Let K is an imaginary quadratic field of class number 1 satisfying the Heegner hypothesis.

Remark

Heegner points are special points on $J_0(N)(K)$ corresponding to CM elliptic curves whose traces generate the rank one part of the Mordell–Weil group of $J_0(N)(\mathbf{Q})$.

- The Heegner hypothesis implies $N = \mathfrak{n}\overline{\mathfrak{n}}$ over K.
- The elliptic curve $P_K := (\mathbf{C}/\overline{\mathfrak{n}}^{-1}, 1/N)$ has CM by $\mathcal{O}_K$, and defines a CM point on $X_0(N)(K)$.
- We define $y_K := [P_K - \infty] \in J_0(N)(K)$ to be the Heegner point.

Gross and Zagier show that, for some choice of K, the image of y_K under the modular parametrization $\pi : X_0(N) \to E$ generates $E(\mathbf{Q})$ up to finite index.

Gross–Zagier formula

Consider the vector space $V = J_0(N)(K) \otimes \overline{\mathbf{Q}}$. We have a decomposition

$$V = \bigoplus_f V^f$$

into Hecke eigenspaces, summing over eigenforms f of weight 2 and level N. Write $y_{K,f}$ for component of y_K in V^f.

Gross and Zagier show that for any newform f of weight 2 and level N

$$h_{\mathrm{NT}}(y_{K,f}) \doteq L'(f/K, 1).$$

When f has analytic rank 1, Waldspurger's theorem guarantees the existence of infinitely many fields K such that the right hand side does not vanish.

Shimura defines an isogengy factor A_f of $J_0(N)$ attached to f. Gross and Zagier show that if $h_{\mathrm{NT}}(y_{K,f}) \neq 0$ then (the image of) $y_{K,f}$ generates $A_f(\mathbf{Q})$ up to finite index (under the action of Hecke).

p-adic Gross–Zagier

There are p-adic Gross–Zagier formulas that relate $h(z)$ and $\log(z)^2$ of a Heegner point to analytic quantities, i.e. special values of p-adic L-functions. These p-adic L-functions interpolate classical L-values of Rankin L-functions for different sets of Hecke characters.

Let f be a modular form of level N, weight 2 and analytic rank 1.

Theorem (Perrin-Riou)

There is a p-adic L-function whose derivative in the cyclotomic direction is

$$\mathcal{L}_p'(f/K, 1) \doteq h(y_{K,f})$$

Theorem (Bertolini–Darmon–Prasanna)

There is an anticyclotomic p-adic L-function whose value at 1 *is*

$$L_p(f, 1, 1) \doteq (\log_{f dq/q} y_K)^2.$$

An example

Let E be the elliptic curve $X_0(43)^+$ with LMFDB label `43.a1` and $p = 11$. Choose the class number 1 field $K = \mathbf{Q}(\sqrt{-7})$, where p and $N = 43$ split. Fix an equation for $E/\mathbf{Q}$ on for we want to compute integer points

$$E : y^2 + y = x^3 + x^2.$$

We can compute γ:

$$\gamma = \frac{h(\pi(y_K))}{\log(\pi(y_K))^2} = \frac{\mathcal{L}_p'(f, \mathbf{1})\left(\frac{1}{2}\right)\left(1 - \frac{1}{\alpha_p}\right)^{-4} \deg \pi}{L_p(f, 1, 1)\left(\frac{1-a_p(f)+p}{p}\right)^{-2}}$$

$$= \frac{9 \cdot 11 + 5 \cdot 11^2 + 5 \cdot 11^3 + 3 \cdot 11^4 + 7 \cdot 11^6 + 4 \cdot 11^7 + 4 \cdot 11^8 + O(11^9)}{11^2 + 8 \cdot 11^3 + 9 \cdot 11^4 + 6 \cdot 11^5 + 8 \cdot 11^6 + 6 \cdot 11^7 + 4 \cdot 11^8 + 4 \cdot 11^9 + O(11^{10})}.$$

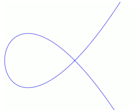
Example, cont.

$$E : y^2 + y = x^3 + x^2$$

Recall that $h(z) = h_p + \sum_v h_v(z) = \gamma \log(z)^2$ and therefore

$$E(\mathbf{Z}) \subseteq \bigcup_{w \in W} \{z \in E(\mathbf{Z}_p) : h_p(z) + \|w\| = \gamma \log(z)^2\}.$$

These W come from the local heights at primes of bad reduction. The only prime of bad reduction is $v = 43$, this has Kodaira type I1



so there will be no local height contributions at 43.

Example, cont.

We have

$$E(\mathbf{Z}) \subseteq \{z \in E(\mathbf{Z}_p) : h_p(z) = \gamma \log(z)^2\}.$$

Then by plugging

$$\gamma = 9 \cdot 11^{-1} + 10 + 2 \cdot 11 + 4 \cdot 11^2 + 5 \cdot 11^4 + 8 \cdot 11^5 + 10 \cdot 11^6 + O(11^7)$$

into these equations we can solve for the zeros of the p-adic power series in each residue disk. We obtain

$$\begin{aligned} E(\mathbf{Z}) \subseteq &\{(-1,-1),(0,-1),(1,-2),(2,-4),(21,-99),\\ &(10 \cdot 11 + 7 \cdot 11^2 + O(11^3), 10 + 10 \cdot 11 + 9 \cdot 11^2 + 5 \cdot 11^3 + O(11^3)),\\ &(1 + 6 \cdot 11 + 2 \cdot 11^2 + O(11^3), 9 + 3 \cdot 11^2 + O(11^3)),\\ &(2 + 9 \cdot 11 + 7 \cdot 11^2 + O(11^3), 3 + 8 \cdot 11 + 11^2 + O(11^3))\} \end{aligned}$$

and their conjugates under the hyperelliptic involution.

The anticyclotomic p-adic L-function

Let $f = \sum_{n \geq 0} a_n z^n$ be a weight 2 newform for $\Gamma_0(N)$ and K an imaginary quadratic field of class number 1 satisfying the Heegner hypothesis for N. Let p be split in K and coprime to N.

Theorem (Bertolini–Darmon–Prasanna)

There is an anticyclotomic p-adic L-function whose value at 1 *is*

$$L_p(f, 1, 1) \doteq (\log_{f dq/q} y_K)^2.$$

How do we compute $L_p(f, 1, 1)$? What even is this p-adic L-function?
The Shimura–Maass derivative is a derivative operator

$$\delta_k = \frac{1}{2\pi i} \left(\frac{\partial}{\partial z} + \frac{k}{2iy} \right)$$

sending a nearly holomorphic modular form of weight k to one of weight $k + 2$. We write δ^j for the composition $\delta_{k+2j-2} \circ \cdots \circ \delta_k$.
After normalizing by a period, the values of $\delta^j f$ at a CM point are algebraic and belong to the compositum of the CM field and the coefficient field of f.

Computing the anticyclotomic p-adic L-function

For example, let f be the modular form of the elliptic curve `89.a1`, $N = 89$, $p = 3$. Let $\tau_N = \frac{-73+\sqrt{-11}}{178}$, so $P_K = (\mathbf{C}/(\mathbf{Z}+\mathbf{Z}\tau_N), 1/N)$ is the Heegner point for $K = \mathbf{Q}(\sqrt{-11})$ on $X_0(89)$.
Then the values of $(1 - a_p\mathfrak{p}^{r-1}\bar{\mathfrak{p}}^{-1-r} + \mathfrak{p}^{2r-1}\bar{\mathfrak{p}}^{-2r-1})^2(\delta^{r-1}f(\tau_N))^2/\Omega_K^{4r}$ are algebraic numbers in K whose value in $\mathbf{Q}_p \simeq K_\mathfrak{p}$ are

$$
\begin{aligned}
r = 3^1: &\quad 1 + 3 + 2\cdot 3^2 + 2\cdot 3^4 + 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + 2\cdot 3^8 + O(3^{10})\\
r = 3^2: &\quad 1 + 3 + 2\cdot 3^2 + 3^3 + 3^4 + 3^7 + 3^9 + O(3^{10})\\
r = 3^3: &\quad 1 + 3 + 2\cdot 3^2 + 3^3 + 2\cdot 3^4 + 2\cdot 3^6 + 2\cdot 3^9 + O(3^{10})\\
r = 3^4: &\quad 1 + 3 + 2\cdot 3^2 + 3^3 + 2\cdot 3^4 + 3^5 + 2\cdot 3^6 + 2\cdot 3^8 + 2\cdot 3^9 + O(3^{10}).
\end{aligned}
$$

The anticyclotomic p-adic L-function $L_p(f)$ interpolates the square of the values of the Shimura–Maass derivative δ^{r-1} of f evaluated at τ_N, for $r \geq 1$:

$$L_p(f, K, 1+r, 1-r)/\Omega_p^{4r} = (1 - a_p\mathfrak{p}^{r-1}\bar{\mathfrak{p}}^{-1-r} + \mathfrak{p}^{2r-1}\bar{\mathfrak{p}}^{-2r-1})^2(\delta^{r-1}f(\tau_N))^2/\Omega_K^{4r}$$

The special value $L_p(f, 1, 1)$ occurs at $r = 0$. This is *not* a value in the range of interpolation!

We can still recover this value, using the continuity of $L_p(f, 1, 1)$ with inspiration from a paper of Rubin.

Computing in the range of interpolation

To compute $L_p(f, 1+r, 1-r)$ in the range of interpolation we need to compute $\delta^{r-1}(f(\tau_N))$.

Zagier shows the values $\{\delta^j f(\tau)\}_{j \geq 0}$ satisfy a recurrence relation when τ is a CM point due to the large amount of structure on $M_*(\Gamma_0(N))$.

There is an iterative relation that allows us to obtain $\delta^{r+1} f(\tau_N)$ from $\delta^r f(\tau_N)$ and $\delta^{r-1} f(\tau_N)$ for $r \geq 1$.

Computing outside the range of interpolation

Let $r \geq 1$.

$$\ell(r) := L_p(f, 1+r, 1-r) \cdot \Omega_p^{-4r} =$$
$$(1 - a_p \mathfrak{p}^{r-1}\bar{\mathfrak{p}}^{-1-r} + \mathfrak{p}^{2r-1}\bar{\mathfrak{p}}^{-2r-1})^2(\delta^{r-1} f(\tau_N))^2/\Omega_K^{4r}$$

We want to compute $\ell(0) = L_p(f, 1, 1) = \left(\frac{1-a_p(f)+p}{p}\right)^2 \log_{f\,dq/q}(y_K)^2$.
Instead, we compute auxiliary values $\ell((p-1)), \ell(2(p-1)), \ldots, \ell(B(p-1))$ in the range of interpolation and recover $\ell(0)$ modulo $\mathfrak{p}^B$ from the following.

Proposition (H.)

$$\ell(0)^{(p-1)/2} \equiv \sum_{j=1}^{B} \left(\sum_{i=j}^{B} (-1)^{j-1} \binom{i-1}{j-1} \right) \ell(j(p-1))^{(p-1)/2} \mod \mathfrak{p}^B.$$

Furthermore, $\ell(0) \equiv \ell((p-1)^2/2) \mod \mathfrak{p}$.

Example of the logarithm

When E is the elliptic curve $y^2 + y = x^3 - x$ with label 37.a1, $K = \mathbf{Q}(\sqrt{-11})$, and $p = 5$, we have the values

r	$\ell(r) \mod \mathfrak{p}^{10}$
4	-2341944
8	830906
12	-3933069
16	-35494
20	1760756
24	1706556
28	1972781
32	-3662194
36	3734381
40	4015256

So the proposition implies that

$$\ell(0)^2 = L_p(f,1,1)^2 \equiv 2502536 \mod \mathfrak{p}^{10}$$

$$L_p(f,1,1) \equiv \ell(8) \equiv 830906 \mod \mathfrak{p}$$

$$L_p(f,1,1) \equiv 4635631 \mod \mathfrak{p}^{10}.$$

The height

Recall $\pi : X_0(N) \to E$ the modular parametrization.
Perrin-Riou's p-adic Gross–Zagier theorem says

$$\mathcal{L}_p'(f/K, \mathbf{1}) = \left(1 - \frac{1}{\alpha_p}\right)^4 \frac{2h(\pi(y_K))}{\deg \pi}.$$

We can relate this to the p-adic L-function of an elliptic curve of Amice–Velú $L_{p,\mathrm{MTT}}$ using the following formula

$$\mathcal{L}_p'(f, \mathbf{1}) = L_{p,\mathrm{MTT}}'(E, 1) \left(1 - \frac{1}{\alpha_p}\right)^2 \frac{L(E^D, 1)}{\Omega_{E^D}^+} \Omega_{E^D}^+ \left(\frac{\sqrt{|D|}}{8\pi^2 \|f\|}\right)$$

where E^D is the quadratic twist of E by the discriminant of K.

Question

Let X be curve of genus $g \geq 2$ with Jacobian J_X. Can we extend this method to compute $X(\mathbf{Q})$?

Given a nontrivial $Z \in \ker(\mathrm{NS}(J_X) \to \mathrm{NS}(X))$, one can define a height h on $X(\mathbf{Q})$ using Nekovář's theory of p-adic heights on Galois representations, as well as local heights h_v on $X(\mathbf{Q}_v)$. This decomposes

$$h = h_p + \sum_v h_v$$

where h_p is locally analytic and h_v for $v \neq p$ have finite image.

The analogue of $h(z) = \gamma \log^2(z)$ is to write $h(z)$ in terms of a basis of symmetric bilinear pairings on J_X. Let $\omega_1, \ldots, \omega_g$ be a basis for $H^0(X_{\mathbf{Q}_p}, \Omega^1)$. A basis is given by

$$g_{ij}(D_1, D_2) := \frac{1}{2}(\log_{\omega_i}(D_1)\log_{\omega_j}(D_2) + \log_{\omega_i}(D_2)\log_{\omega_j}(D_1)),$$

$i = 1, \ldots, g$.

If $\mathrm{rk} J_X(\mathbf{Q}) = g$ and we knew a basis $y_1, \ldots, y_g$ for $J_X(\mathbf{Q})$, we could determine γ_{ij} such that $h(z) = \sum \gamma_{ij} g_{ij}$.

Definition

Let $\phi : X_0(N) \to X$ dominant and X genus g. Suppose J_X is simple. Then we have an associated f modular form of level M unique up to Galois conjugacy satisfying

$$\prod_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} L(f^\sigma, s) = L(J_X, s).$$

We say X is a *simple new* $\Gamma_0(N)$*-modular* curve if X satisfies these assumptions and furthermore f is newform of level N.

For our approach to quadratic Chabauty to succeed, we needed $\mathrm{rk} J_X(\mathbf{Q}) = g$ and $\mathrm{rk}\, NS(J_X) > 1$.
When f is analytic rank 1, these simple new simple new $\Gamma_0(N)$-modular curves satisfy $\mathrm{rk} J_X(\mathbf{Q}) = g = \mathrm{rk}\, NS(J_X) > 1$.

Theorem (H.)

Let $\phi : X_0(N) \to X$ *be a simple new* $\Gamma_0(N)$*-modular curve with associated newform* f *of analytic rank* 1*. Let* E_f *be the coefficient field of* f*. Let* K *be an imaginary quadratic field of class number* 1 *with odd discriminant* $D < -3$*. Let* p *be a good ordinary prime and assume* p *is split in the imaginary quadratic field* K*.*
Then

$$\gamma_\sigma := \frac{C_f \deg(\phi) \mathcal{L}'_{p,\mathrm{PR}}(f^\sigma, 1)}{L_{p,\mathrm{BDP}}(f^\sigma, 1, 1)}$$

for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$ *where* C_f *is a constant depending only on* f*.*
The γ_σ *are computable and for* $z \in X(\mathbf{Q})$ *we have*

$$\sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \gamma_\sigma (\log_{f^\sigma dq/q}(z))^2 = h(z).$$

This allows us to compute a finite set of p-adic points containing $X(\mathbf{Q})$.

q-expansion of the height

Let α denote the endomorphism associated to Z. Since X is modular, we assume that α is the sum of Hecke operators and the identity. Then $\alpha(f^\sigma) = \lambda_\sigma f^\sigma$ for some scalar λ_{f^σ}.
We can decompose the q-expansion of (the Nekovář height) as

$$h(q) = \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \gamma_\sigma \int_0^q f^\sigma \frac{dq}{q} \left(c_{f^\sigma, Z} + \lambda_\sigma \int_0^q f^\sigma \frac{dq}{q} \right)$$

The term $c_{f^\sigma, Z}$ appears in the literature as

$$\log_{f^\sigma dq/q}(\Pi_Z(\Delta_{\mathrm{GKS},b}))$$

where $\Pi_Z(\Delta_{\mathrm{GKS},b})$ is the Chow–Heegner point with respect to b.

Genus 2 example: quadratic Chabauty

Consider $X_0(67)^+$, let f be the Hecke eigenform of weight 2 level 67. The coefficient field of f is $\mathbf{Q}(\nu)$ where ν is a root of $z^2 - z - 1$. Let $p = 11$. Fix the embedding $\mathbf{Q}(\nu) \to \mathbf{Q}_p$ sending $\nu \mapsto 4 + 3 \cdot 11 + O(11^3)$. Let $K := \mathbf{Q}(\sqrt{-7})$.

The q-expansion of the global height in disc is

$$O(11^7) - (571863 + O(11^6))q - (8833444 \cdot 11^{-1} + O(11^6))q^2 + \dots$$

with basepoint ∞ and Z the correspondence $-4T_{11}$.

$$\gamma_f := \frac{\frac{1}{2} h(\phi_*(y_{K,f}), \phi_*(y_{K,f}))}{(\log_{f\,dq/q} \phi_*(y_K))^2} = 8 \cdot 11^{-1} + 7 + 6 \cdot 11 + 9 \cdot 11^2 + 10 \cdot 11^3 + O(11^4)$$

$$\gamma_{f^\sigma} := \frac{\frac{1}{2} h(\phi_*(y_{K,f^\sigma}), \phi_*(y_{K,f^\sigma}))}{(\log_{f^\sigma dq/q} \phi_*(y_K))^2} = 5 \cdot 11^{-1} + 5 \cdot 11 + 4 \cdot 11^2 + 4 \cdot 11^3 + O(11^4).$$

Note that we can also compute

$$c_{f,Z} = 193046 \cdot 11 + O(11^7), \quad c_{Z,f^\sigma} = 255850 \cdot 11 + O(11^7).$$

We can solve for a finite set of p-adic points containing the rational points.
Other examples: $X_0(73)^+$, $X_0(107)^+$, $X_0(85)^*$.

Summary

1. Quadratic Chabauty methods rely on explicit equations to determine rational points. A dream would be to determine rational points on modular curves directly from modular forms and their data, for example in Mazur's method for determining rational points on the family $X_0(p)$.
2. Theorems of Gross and Zagier, and their p-adic analogues, offer analytic techniques that allow us to compute arithmetic invariants from the modular form f.
3. This is the first step in the direction towards a more moduli-friendly quadratic Chabauty – there is a lot more work to be done!