

NEXT UP ON “WHAT IF IT WERE p -ADIC”? THE BIRCH-SWINNERTON-DYER CONJECTURE

BENEDIKT ARNARSSON

♣♣♣ Angus: [First of all, love the title.]

♣♣♣ Jacksyn: [Nice work, this was a tough one!]

These notes give an overview of the p -adic analogue of the Birch-Swinnerton-Dyer conjecture, following lectures by John and Professor Balakrishnan. The main reference is [BM86]. All errors are my own.

CONTENTS

1. Intro to Classical BSD	1
2. Some p -adic analysis	3
3. Modular Symbols	5
4. More integrals	6
5. Interpolation of special values	7
6. Greenberg-Stevens	9
7. Experimental stuff	11
8. Further readings	12
References	13

1. INTRO TO CLASSICAL BSD

Just as with the previous write-up on p -adic families of modular forms, we will be taking something over \mathbb{Q} and “upgrading” to objects over \mathbb{Q}_p . As is often the case, the local theory is easier, so we can often say a lot more, but first we need to review the “classical” theory.

We’ve already had a quick overview of elliptic curves when we covered Elkies paper, so we will skip that and jump right into the main question: What is the Birch-Swinnerton-Dyer Conjecture? (From now on we will call it the BSD conjecture.)

Let E/\mathbb{Q} be an elliptic curve. Then, by Mordell’s Theorem, we have

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{tors}(\mathbb{Q})$$

and we call $r = \text{rk}(E(\mathbb{Q}))$ the *rank* of E . Due to work of Mazur [BMT77], the torsion points, $E_{\text{tors}}(\mathbb{Q})$, are completely understood – a nice review of this by Andrew Snowden is [here](#).

So, the rank $\text{rk}(E(\mathbb{Q}))$ is the main difficulty. The problem is that no general method guarantees the computation of $\text{rk}(E(\mathbb{Q}))$ for any elliptic curve E/\mathbb{Q} .

Are there other possible ways to understand the rank? What about other invariants of E/\mathbb{Q} that we could use? In the 1960s, Birch and Swinnerton-Dyer conjectured (based on computational experiments) that $\text{rk}(E(\mathbb{Q}))$ could be computed using data from $\tilde{E}(\mathbb{F}_p)$ – this is where the L -function, $L(E/\mathbb{Q}, s)$, comes in (due to the Euler product).

Let Δ_E be the minimal discriminant of E/\mathbb{Q} . Let $p \nmid \Delta_E$ be prime. Then $\tilde{E}_{(\mathbb{F}_p)}$ is an elliptic curve. Let $N_p := \#\tilde{E}(\mathbb{F}_p)$. Idea: large $\text{rk}(E(\mathbb{Q}))$ should imply lots of \mathbb{Q} -rational points, which in turn should imply that you have lots of \mathbb{F}_p -rational points (and thus large N_p , which is much more computationally tractable – Weil Conjectures, finitude, etc.) Birch and Swinnerton-Dyer looked at $\prod_{p < X} N_p/p$ for large X and conjectured:

Conjecture 1.1. There exists a constant c_E depending on E such that as $X \rightarrow \infty$, we have

$$\prod_{p < X} \frac{N_p}{p} \sim c_E (\log X)^{\text{rk}(E(\mathbb{Q}))}.$$

These days, we package the N_p in a slightly different way: let $a_p := p + 1 - N_p$ and

$$L(E/\mathbb{Q}, s) \simeq \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \left(\prod_{p \mid \Delta_E} \frac{1}{1 - a_p p^{-s}} \right).$$

This is a complex analytic function which converges for $\text{Re}(s) > \frac{3}{2}$. Now, let's do something that is a little illegal: pretend to evaluate at $s = 1$.

$$L(E/\mathbb{Q}, 1) \approx \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p - a_p + 1} = \prod_p \frac{p}{N_p}$$

so, assuming that we can make sense of $L(E/\mathbb{Q}, 1)$, then the L -function should tell us about $\text{rk}(E(\mathbb{Q}))$.

Conjecture 1.2 (BSD1). The L -function $L(E/\mathbb{Q}, s)$ extends to an analytic function on all of \mathbb{C} , and $L(E/\mathbb{Q}, 1) \neq 0$ if and only if $|E(\mathbb{Q})| < \infty$ (so we only have torsion points). Moreover, $\text{rk } E(\mathbb{Q}) = \text{ord}_{s=1} L(E/\mathbb{Q}, s)$. We call the left-hand side the “algebraic rank” and the right-hand side the “analytic rank”.

We know that analytic continuation holds due to ([Wil95], [TW95], [BCDT01]), and so we have a new conjecture

Conjecture 1.3 (BSD2). Let E/\mathbb{Q} ♣♣♣ Kate: [It feels like something is missing here? Maybe, "Let E/\mathbb{Q} be an elliptic curve. Then:"]

$$\lim_{s \rightarrow 1} \frac{L(E/\mathbb{Q}, s)}{(s-1)^{\text{rk } E(\mathbb{Q})}} = \frac{|\text{III}(E/\mathbb{Q})| \cdot \text{Reg}(E/\mathbb{Q}) \cdot \Omega_{\mathbb{R}} \cdot (\prod_{\ell} c_{\ell})}{|E_{\text{tors}}(\mathbb{Q})|^2}$$

where

- $\text{III}(E/\mathbb{Q})$ is the Shafarevich-Tate group (is it finite?); ♣♣♣ Kate: [I have in my notes that for the purpose of this conjecture we assume that it is.]
- $\text{Reg}(E/\mathbb{Q})$ is the *regulator*, defined as $\det(\langle P_i, P_j \rangle)$, where $\langle -, - \rangle$ is the Neron-Tate height pairing and $\{P_1, \dots, P_r\}$ is a basis for the free part of $E(\mathbb{Q})$; ♣♣♣ Kate: [I believe you want a little up accent on the e, like Néron]
- c_ℓ is the Tamagawa number at ℓ , $c_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$ ♣♣♣ John: [added a closing parenthesis you forgot] where $E_0(\mathbb{Q}_\ell) = \{p \in E(\mathbb{Q}_\ell) : p \text{ reduces to a nonsingular point in } E(\mathbb{F}_\ell)\}$ – if E is good at ℓ , then $c_\ell = 1$;
- $\Omega_{\mathbb{R}} = \int_{E(\mathbb{R})} \frac{dx}{|2y+a_1x+a_3|}$ (the a_i s from the Weierstrass equation);

What is known?

Theorem 1.4 ([Kol89], [GZ86]). *If $r_{an}(E) \leq 1$, then $\text{rk } E(\mathbb{Q}) = r_{an}$, and $\text{III}(E/\mathbb{Q})$ is finite*

Theorem 1.5 ([SU14], [Ski14], [Zha14]). *Under tehcnical ♣♣♣ Jacksyn: [technical] hypotheses, we have converse of K, G-Z. If $\text{rk } E(\mathbb{Q}) \leq 1$, then $\text{rk } E(\mathbb{Q}) = r_{an}(E)$ (and so $\text{III}(E/\mathbb{Q})$ is finite).*

♣♣♣ Angus: [You could mention the recent paper by Kim here if you like (I know you mention it at the end).]

Remark 1.6. What more can be said?

Generalization to abelian varieties was done (statement of BSD in this context) by Tate.

What about over different base fields? Over function fields, we have ([YZ17]). In our case, we will be working with elliptic curves over number fields, but constructing p -adic analytic functions (instead of complex analytic functions), so let's get right into that.

♣♣♣ Angus: [This was a little unclear to me in this p -adic BSD story. Are we considering elliptic curves over p -adic fields, or elliptic curves over \mathbb{Q} ? My understanding is that we still consider the curves over \mathbb{Q} , but just attach this funny invariant, the p -adic L -function, and use p -adic methods to talk about that. Someone correct me if I've got this wrong!] ♣♣♣ Kate: [I think this is correct. In Chapter 2 Section 10 (pages 37-38), the p -adic analogue of the conjecture, stated at the top of p.38, doesn't change the definition of E specified at the start of the section.] ♣♣♣ John: [My understanding is that you take an elliptic curve over \mathbb{Q} . The p -adic setting is just a place to do analysis that replaces \mathbb{C} , but the ultimate goal is to detect the arithmetic of a rational elliptic curve.]

2. SOME p -ADIC ANALYSIS

Time for a notation dump. ♣♣♣ Angus: [This certainly isn't on you, Ben, but man it would be nice for this somehow to develop naturally. Is there a way to see why all these definitions and notations are motivated based on our goal to understand L -functions?] ♣♣♣ John:

[I think the best one can do is write a book on complex L-functions and then notice that these are exact analogues in the p -adic case. I was hoping to come up with a nice way of making these things natural, but I think the best I could do was to shove the naturality to the complex setting.] Let $\mathcal{C}(N, \epsilon, k)$ denote the set of cuspforms of level N , character ϵ , and weight k . Let $\mathcal{P}_k(R) := \{\text{polynomials with } R \text{ coefficients of degree } \leq k-2\}$. For $A \in \text{GL}_2(\mathbb{Q})^+$ (positive determinant) define for $f \in \mathcal{C}(N, \epsilon, k)$



$$(f|A)(z) = \left(\frac{\sqrt{\det(A)}}{cz + d} \right)^k \cdot f(Az)$$

and $p \in \mathcal{P}_k(\mathbb{C})$

$$(p|A)(z) = \left(\frac{\sqrt{\det(A)}}{cz + d} \right)^{k-2} \cdot p(Az)$$

Let's start by looking at the L -function of cusp forms: $L(f, s)$ for $f \in \mathcal{C}(N, \epsilon, k)$. One “natural” way of going about this is by the Mellin transform

$$\begin{aligned} q_f(s) &= \int_{t=0}^{\infty} f(it) t^s \frac{dt}{t} \\ &= (2\pi)^{-s} \Gamma(s) L(f, s) \end{aligned}$$

where we can think of t^s as a character (see Tate's thesis, found in [?]), so we can naturally bring twists of L -functions into the picture by putting new characters in place of t^s .  Angus: [I asked about this point during John's talk. It is true Tate's thesis thinks of these convolution integrals with characters, but I think the type of character we twist with are Dirichlet characters, so they live on a different group.]  John: [I think I finally understand your question now, Angus. The Dirichlet characters actually still show up in the character space because our characters are defined in $\mathbb{Z}_{p,M}^\times$ instead of just \mathbb{Z}_p^\times . You can think about the M -part as the discrete part (and virtually all constructions project to the p -part). So I guess you would functionally take M to be divisible by the conductor of any Dirichlet character you want to twist by or take the inverse limit if you want to work with all possible Dirichlet characters.]

$$\begin{aligned} \omega : \mathbb{C} &\rightarrow \mathbb{C}^\times \\ \omega(x) &= |x|^s \end{aligned}$$

Plan:

- (1) Define integration $\mathbb{Z}_p^\times \rightarrow \mathbb{C}_p$;
- (2) Integrate characters to get p -adic L -functions.

Essentially, we need some p -adic distribution to define the object on rigid analytic disks and then we can add it up using the integration.

Definition 2.1 (Modular integrals). Let

$$\Phi : \mathcal{C}_k \times \mathcal{P}_k \times \mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{C}$$

such that

- (1) Φ bilinear on $\mathcal{C}_k \times \mathcal{P}_k(\mathbb{C})$;
- (2) $\Phi(f|A, P|A, r) = \Phi(f, P, A(r)) - \Phi(f, P, A(\infty))$

The only modular integral we will be using is

$$\phi(f, P, r) = 2\pi i \int_{\infty}^r f(z)P(z)dz = 2\pi \int_0^{\infty} f(r+it)P(r+it)dt$$

so just think of this whenever you see modular integral or Φ .

Definition 2.2. Let $f \in \mathcal{C}_k$ and Φ_f the corresponding modular integral. Define the *module of values* L_f to be the image of $\mathcal{P}(\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Q})$ under the modular integral Φ_f , i.e. for $A_i \in \mathrm{SL}_2(\mathbb{Z})$ representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$

$$L_f := \Phi(f, \mathcal{P}_k(\mathbb{Z}), \mathbb{P}^1(\mathbb{Q}))$$

Proposition 2.3. If $f \in \mathcal{C}(N, \epsilon, k)$, then L_f is a $\mathbb{Z}[\epsilon]$ -module generated by $\Phi(f, z^i, A_j(\infty)) - \Phi(f, z^i, A_j(0))$ for $0 \leq i \leq k-2$ and all A_j .

Proof. See page 6 in [BM86]. □

3. MODULAR SYMBOLS

Definition 3.1. Let $\lambda : \mathcal{C}_k \times \mathcal{P}_k(\mathbb{C}) \times \mathbb{Q} \times \mathbb{Q}^+ \rightarrow \mathbb{C}$ and define

$$\lambda(f, P; a, m) := \Phi\left(f, P(mz+a), -\frac{a}{m}\right) = m^{\frac{k}{2}-1} \cdot \Phi\left(f \left| \begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix} \right., P, 0\right)$$

♣♣♣ **Angus:** [You can use `pmatrix` instead of `array` for matrices]

Recall: Hecke Operators. For ℓ a prime, let

$$f|T_{\ell} := \ell^{\frac{k}{2}-1} \left[\sum_{u=0}^{\ell-1} f \left| \begin{pmatrix} 1 & u \\ 0 & \ell \end{pmatrix} \right. + \epsilon(\ell) \cdot f \left| \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \right. \right]$$

♣♣♣ **Jacksyn:** [You might have a parenthesis in a wrong spot here.] How do Hecke operators interact with modular symbols?

Proposition 3.2.

$$\lambda(f | T_{\ell}, P; a, m) = \sum_{u=0}^{\ell-1} \lambda(f, P; a - um, \ell m) + \epsilon(\ell) \cdot \ell^{k-2} \lambda(f, P; a, m\ell)$$

So, on the complex side of things (over \mathbb{C}), modular symbols allow us to calculate special values of L -functions

Proposition 3.3.

$$\lambda(f, z^n; 0, 1) = i^n \frac{n}{(2\pi)^n} \cdot L(f, n+1)$$

for $0 \leq n \leq k-2$

Definition 3.4 (*p*-adic Distribution). Fix $f \in \mathcal{C}(N, \epsilon, k)$. Choose α , a root of $X^2 - a_p C + \epsilon(p)p^{k-1}$, where a_p is the p th Fourier coefficient of f . α is called *allowable* if $\text{ord}_p(\alpha) < k-1$.

♣♣♣ **Angus:** [This was a strict inequality, right?] Define

$$\mu : \mathcal{C}(N, \epsilon, k) \times \{\alpha\} \times \mathcal{P}_k(\mathbb{C}) \times \mathbb{Q} \times \mathbb{Q}^+ \rightarrow \mathbb{C}$$

$$\mu(f, \alpha, P; a, m) = \frac{1}{\alpha^{\text{ord}_p(m)}} \lambda(f, P; a, m) - \frac{\epsilon(p)p^{k-2}}{\alpha^{\text{ord}_p(m)+1}} \lambda(f, P; a, m/p)$$

For $(p, m) = 1$ let $\mathbb{Z}_{p,M} = \varprojlim_{r \rightarrow \infty} (\mathbb{Z}/p^r M \mathbb{Z}) = \mathbb{Z}_p^\times \times (\mathbb{Z}/M \mathbb{Z})^\times$

Let $D(a, v) :=$ open disk centered at a of radius p^{-v} .

A p -adic measure is a p -adic distribution that is p -adically bounded.

4. MORE INTEGRALS

More notation: Let

$$\Omega_f := L_f \otimes_{\mathbb{Z}} \mathcal{O}_p$$

and

$$V_f := \Omega_f \otimes_{\mathcal{O}} \mathbb{C}_p$$

for

$$U \subseteq \mathbb{Z}_{p,M}^\times, \quad \text{open and compact}$$

think of U as the open disks

$$D(a, v) = \{x \in \mathbb{Z}_{p,M}^\times : |x - a|_p < p^v\}$$

Notation: ♣♣♣ **Kate:** [I don't think you need to specify it's notation again since you're still kind of under the "More Notation" block at the start of the section] for all $x \in \mathbb{Z}_{p,M}^\times$, let x_p denote the \mathbb{Z}_p^\times -component

Theorem 4.1 (Vishik, Amice-Vélu). Let $f \in \mathcal{C}(N, \epsilon, k)$. Let $0 \leq h \leq k-1$ be an integer and $\alpha \in \mathbb{C}_p$ be a root fo $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $\text{ord}_p \alpha < h$. Then there exists a unique V_f -valued integral at all $a \in \mathbb{Z}$, $r \geq 1$, denoted $\int_U F d\mu_{f,\alpha}$, such that ♣♣♣ **Angus:** [Maybe this should be $d\mu_{f,\alpha}$ to agree with later notation.]

- (1) The integral is \mathbb{C}_p -linear on F (the integrand) and finitely additive on the domain U (compact open);
- (2) For $0 \leq j \leq k-2$, $\int_{D(a,v)} x_p^j = \mu_{f,\alpha}(z^j, a, p^v M)$;
- (3) (Divisibility) for all $n \geq 0$, $\int_{D(a,v)} (x-a)_p^n \in \left(\frac{p^n}{\alpha}\right)^v \alpha^{-1} \Omega_f$;

(4) If $F(x) = \sum_{n \geq 0} c_n (x - a)_p^n$ is convergent on $D(a, v)$ then

$$\int_{D(a, v)} F = \sum_{n \geq 0} \int_{D(a, v)} (x - a)_p^n$$

(For proof see page 13 in [BM86].)

Integrands: in order to build our p -adic L -functions, there are two types of characters that we’re going to integrate:

(1) Special characters of the form

$$\chi(x) = x_p^j \cdot \Psi(x)$$

for $0 \leq j \leq k - 2$ and Ψ a finite character;

(2) For $s \in \mathbb{Z}_p$,

$$\begin{aligned} \chi_s &:= \langle x \rangle^s := \exp(s \log_p(x)) \\ &= \sum_{r=0}^{\infty} \frac{s^r}{r!} (\log_p \langle x \rangle)^r \end{aligned}$$

think of the projection

$$\langle x \rangle : \mathbb{Z}_p^\times \rightarrow 1 + p\mathbb{Z}_p$$

Definition 4.2. Finally, we can define our L -function

$$L_p(f, \alpha, \chi) = \int_{\mathbb{Z}_{p, M}^\times} \chi d\mu_{f, \alpha}$$

(for χ a special character). and, the twist,

$$L_p(f, \alpha, \chi, s) := L_p(f, \alpha, \chi \cdot \chi_s)$$

Proposition 4.3. $L_p(F, \alpha, \chi, s)$ is locally analytic on \mathbb{Z}_p and for a Dirichlet character Ψ , we have

$$L_p(f, \alpha, \Psi, s) = \sum_{r \geq 0} \frac{s^r}{r!} \sum_{a \pmod{p^r M}} \Psi(a) \int_{D(a, v)} \log_p(x_p)^r$$

5. INTERPOLATION OF SPECIAL VALUES

Definition 5.1. Let Ψ be a Dirichlet character with conductor $p^v M$ and set $\chi = \Psi \cdot \chi_j$. The p -adic multiplier is defined to be

$$e_p(\alpha, \chi) = \frac{1}{\alpha^v} \left(1 - \frac{\overline{\Psi}(p) \epsilon(p) p^{k-2-j}}{\alpha} \right) \left(1 - \frac{\Psi(p) p^j}{\alpha} \right)$$

We care about the p -adic multiplier because it captures the difference between p -adic L -functions and our usual complex L -functions. Let’s make this precise:

Proposition 5.2. (For a proof see p.20 of [BM86].) If χ is a special character

$$L_p(f, \alpha, \chi) = e_p(\alpha, \chi) \frac{(p^v M)^{j+1}}{\tau(\overline{\Psi})} \lambda(f_{\overline{\Psi}}, z^j, 0, 1) = e_p(\alpha, \chi) \frac{(p^v M)^{j+1}}{\tau(\overline{\Psi})} \frac{j!}{(-2\pi i)^j} L(f_{\overline{\Psi}}, j+1)$$

We can see that if the p -adic multiplier is zero, then the p -adic L -function is zero, even if the complex L -function isn't zero – a case of extra zeros, which we call *exceptional zeros*.

Proposition 5.3. $L_p(f, \alpha, \chi)$ is nonzero if and only if $e_p(\alpha, \chi)$ and $L(f_{\overline{\chi}}, j+1)$ are nonzero

Proposition 5.4. There exists Ψ such that $e_p(\alpha, \Psi, j) = e_p(\alpha, \Psi \cdot \chi_j) = 0$ only if

- (1) k is even, $p \parallel N$, $\tilde{\epsilon}(p) \neq 0$, $j = \frac{k-2}{2}$ (the “central point”), or; ♣♣♣ John: [Not to add another bit of notation, but I think it'd worth stating $p \parallel N$ denotes p exactly divides N .]
- (2) k is odd and:
 - (a) $p \nmid N$, $\alpha = \zeta p^{(k-1)/2}$, where ζ is a root of unity and $j = (k-1)/2$ or $(k-3)/2$ (the “near central points”), or;
 - (b) $\text{ord}_p(N) = \text{ord}_p(\text{cond } \tilde{\epsilon}) > 0$, $a_p = \zeta p^{(k-1)/2}$, where ζ is a root of unity, and $j = (k-1)/2$

(Proof of proposition on p22 of [BM86].)

In the elliptic curve case, (1) corresponds to E/\mathbb{Q} having split multiplicative reduction at p – in this case we can prove a lot more (which we do below). Here is a start: we want to find some geometric manner of approaching the p -adic multiplier. This is done with the L -invariant.

Definition 5.5. Let E/K be an elliptic curve (with non-integer j -invariant) for K/\mathbb{Q}_p a finite extension. Then, by Tate uniformization, for any finite extension L/K

$$E(L) \cong L^\times / q^\mathbb{Z}$$

so, we have a p -adic number attached to E :

$$q(E) = j^{-1} + 744j^{-2} + 750420j^{-3} + \dots$$

Then, we define the L -invariant as

$$\mathcal{L}(E) = \frac{\log_p(N_{K/\mathbb{Q}_p}(q(E)))}{\text{ord}_p(q(E))}.$$

Let

$$L_p^{(k)}(E) := \left(\frac{1}{k!} \right) \cdot \frac{d^k}{ds^k} L_p(E, s)|_{s=1}$$

Conjecture 5.6 (p -adic BSD). Let E be an elliptic curve over \mathbb{Q} . If (α, χ) doesn't give an exceptional zero, then

- (1) $L_p^{(k)}(E) = 0$ if $k < r = \text{rk}(E(\mathbb{Q}))$;

- (2) $L_p^{(r)}(E) = (1 - \frac{1}{\alpha}) |\text{III}(E)| \cdot \text{Reg}_p(E) (\prod m_\ell) \Omega^+$ with $b = 2$ if good reduction and 1 otherwise.

If (α, χ) is exceptional, take same but replace r with $r + 1$ and $b = 0$. (See p38 of [BM86].)

♣♣♣ Angus: [Along with my earlier comment, it might clarify things at this stage if we re-define all the terms here. Say something like "let E/\mathbb{Q} be an elliptic curve" etc.]

Conjecture 5.7 (The p -adic exceptional zero conjecture). For $r = 0$, $M = \text{cond}(\Psi)$, and if we are in the exceptional case, then

$$\lim_{n \rightarrow \infty} \sum_{a \in \mathbb{Z}/p^n M \mathbb{Z}} \Psi(a) \log_p(A) \lambda_E(a, p^n M) = \mathcal{L}_p(E) \cdot \sum_{a \in \mathbb{Z}/M \mathbb{Z}} \Psi(a) \lambda_p(a, M)$$

6. GREENBERG-STEVENSONS

Now we will prove the exceptional zeros conjecture for elliptic curves with split multiplicative reduction at p (following Greenberg-Stevens in [MS94]) – note that this doesn't give us notion of p -adic BSD unless E is of rank 0.

Theorem 6.1. *Let $p \geq 5$, E/\mathbb{Q} a modular elliptic curve with split multiplicative reduction at p . Then*

$$L'_p(E, 1) = \mathcal{L}_p(E) \cdot \frac{L_\infty(E, 1)}{\Omega_E^+}$$

Definition 6.2. In the case of E/\mathbb{Q} , we can simplify our L -invariant to

$$\mathcal{L}_p(E) = \frac{\log_p(q_E)}{\text{ord}_p(q_E)}$$

where $q_E \neq 1$ is in $\ker(\lambda_E: \overline{\mathbb{Q}}_p^\times \rightarrow E(\overline{\mathbb{Q}}_p^\times))$ (Tate uniformization), $q_E \in \mathbb{Q}_p^\times$.

In addition, we have the functional equation:

$$L_p(E, 2 - s) = \epsilon_p \langle N \rangle^{s-1} L_p(E, s)$$

Where $\epsilon_p = \pm 1$ is the p -adic sign, and N is the conductor of E , and the brackets denote the projection to $1 + p\mathbb{Z}_p$.

If ϵ_∞ is sign of $L_\infty(E, s)$, then

$$\epsilon_\infty = \begin{cases} \epsilon_p & \text{good or nonsplit reduction at } p \\ -\epsilon_p & \text{split multiplicative reduction at } p \end{cases}$$

Case 1: $\epsilon_\infty = 1$ and $\epsilon_p = 1$, then take derivative of functional equation

$$L'_p(E, 2 - s) = \epsilon_p \langle N \rangle^{s-2} L'_p(E, s)$$

so, both sides vanish.

Case 2: $\epsilon_\infty = 1$ and $\epsilon_p = -1$. In this case we want to use 2-variable p -adic L -functions. Now we will state a theorem and spend a little bit explaining what everything means (but not proving the theorem). Then we will apply this theorem to prove our desired conjecture.

Theorem 6.3. *Let $\alpha_p = h_E(T_p) \in \Lambda$ and $\alpha_p(k) = \sigma_{k-2}(\alpha_p)$ for $k \in \mathbb{Z}_p$. Then there exists $L_p(k, s)$ for $k, s \in \mathbb{Z}_p$, $L_p^*(k, 1)$ such that*

- (1) $L_p(2, s) = L_p(E, s)$ for all $s \in \mathbb{Z}_p$;
- (2) $L_p(k, s) = \epsilon_p \cdot \langle N \rangle^{\frac{k}{2}-s} L_p(k, k-s)$;
- (3) $L_p(k, 1) = 1 - \alpha_p(k)^{-1} \cdot L_p^*(k, 1)$;
- (4) $L_p^*(2, 1) = \left(1 - \frac{\beta}{p}\right) \frac{L_\infty(E, 1)}{\Omega_E^+}$

Now, let's define everything we need to understand this:

Definition 6.4. Let $\Lambda = \mathbb{Z}_p[[\mathbb{Z}_p^\times]] = \varprojlim_n \mathbb{Z}_p[[\mathbb{Z}/p^n\mathbb{Z}]^\times]$ – this is the *Iwasawa algebra* (in some cases we would need a finite algebra over the Iwasawa algebra, but it's fine to think of this simple version since we are only working over \mathbb{Q}). The map $h_E : \mathbf{T} \rightarrow \Lambda$ gives us how the Hecke operators act on families of p -adic modular forms (specifically, think of the Hida family).

For $g \in \mathbb{Z}_p^\times$, define $\sigma_{k-2}(g) = \chi_{\text{cyclo}}(g)^{k-2}$ (where χ_{cyclo} is the cyclotomic character).

Finally, β is the non-unit root of $X^2 - a_p X + p = (x - \alpha)(x - \beta)$ (the characteristic polynomial of Frobenius, also called the Hecke polynomial), since we already used the unit root in the construction of the L -function. We can think of α_p as encoding the contribution of the unit root α , since if we take $k = 2$ we get the image of α in the Iwasawa algebra (or just α , double check).

Theorem 6.5. *Let $\alpha_p(k)$ be the p -adic analytic function attached to the p -th coefficient of Hida's Λ -adic modular form. Then, $\alpha_p(2) = 1$, and $\alpha_p'(2) = -\frac{1}{2} \mathcal{L}_p(E)$.*

Remark 6.6. Heuristically, we can think of the Hida family as the power series

$$f = \sum \alpha_n(k) \cdot q^n \in \mathcal{A}_U[[q]]$$

for $2 \in U \subseteq \mathbb{Z}_p$ a compact open. Then, if we take $k \in \mathbb{Z}$ we get classical modular forms, with $k = 2$ being the eigenform associated to our elliptic curve E .

Sketch of Greenberg-Stevens. $L(k, s)$ vanishes along $s = k/2$. Let's try to write our L -function as a power series, noting that because of the p -adic sign our constant term is zero:

$$L(k, s) = c \left(\frac{k}{2} - s \right) \pmod{\deg 2}$$

Then, we look at

$$\frac{\partial}{\partial s} L(k, s)|_{(k,s)=(2,1)} = -c = \frac{d}{ds} L_p(E, s)|_{s=1}$$

and

$$\frac{\partial}{\partial k} L(k, s)|_{(k,s)=(2,1)} = \frac{c}{2} = \frac{d}{dk} L_p(k, 1)$$

so

$$\begin{aligned} L'_p(E, 1) &= \frac{d}{dk} (1 - \alpha_p(k)^{-1}) L_p^*(k, 1)|_{k=2} \\ &= (1 - \alpha_p(k)^{-2} \alpha'_p(k)) \cdot L_p^*(k, 1) + (1 - \alpha_p(k)^{-1}) L_p^*(k, 1) \\ &= (1 + \frac{1}{2} \mathcal{L}_p(E)) L_p^*(k, 1) \end{aligned}$$

□

7. EXPERIMENTAL STUFF

For $p > 2$, good and ordinary for E/\mathbb{Q} an elliptic curve, the p -adic multiplier is $\epsilon_p = (1 - \frac{1}{\alpha})^2$ (the unit root α again), then p -adic BSD is

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

where

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

and γ is something like $1 + p$ (for details, see [SW13]) and $r = \text{rk}(E(\mathbb{Q}))$. Rohrlich proved that $\mathcal{L}(E, T)$ is not identically 0 ([Roh84]). So, can use this plus the work of Kato to get

$$\text{ord}_{T=0} \mathcal{L}_p(E, T) \geq r$$

so, using p -adic L -functions we can get bounds on the rank of E . References for p -adic heights, regulators for elliptic curves E/\mathbb{Q} : [MST06], [MT91], or [SW13] (for other types of reduction).

Recall that

$$\text{Reg}_p(E/\mathbb{Q}) = \det \langle P_i, P_j \rangle$$

where P_i, P_j are generators for of the free part of $E(\mathbb{Q})$ and $\langle -, - \rangle$ is the p -adic height pairing defined as

$$\langle P_i, P_j \rangle = h(P_i) + h(P_j) - h(P_i + P_j)$$

where h is a p -adic height function

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

where for $P = (\frac{a}{d^2}, \frac{b}{d^3})$ then $D(p) = d$ (the denominator) and where $\sigma(P)$ is the p -adic sigma function and for

$$P \equiv 0 \in E(\mathbb{F}_p)$$

and P reduces to nonsingular point in $E(\mathbb{F}_\ell)$ for bad ℓ . The sigma function is $\sigma(t) = t + \cdot \in t \mathbb{Z}_p[[t]]$ defined as a solution to the p -adic differential equation

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

where

$$c = \frac{a_1^2 + 4a_2 - E_2(E, \omega)}{12}$$

and

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

is the invariant differential.

So, we can conjecturally¹ (based on p -adic BSD), rank of $|\text{III}(E/\mathbb{Q})(p)|$, the p -primary part of III. On CoCalc, we have code in which we calculate some of these ranks.

8. FURTHER READINGS

A recent paper has a modified proof of the converse to Kolyvagin, Gross-Zagier, by a previous Boston University student: [Kim21]. For more on the Heegner point approach of Gross-Zagier, a nice survey is [Zha13]. For more Iwasawa theory, I don't know of good references (so please contribute). For extensions of this material to the realm of abelian varieties, see [BMS14].

♣♣♣ Sachi: [I took the liberty of commenting out some commands that loaded the packages ulem, biblatex, and the one specifying the biblio file in the preamble then added the bibliography style and file commands at the end here. The ulem package just styles the titles with underlines rather than italics so you can uncomment it if you prefer, but the other two are not working compatibly with the rest of your packages. There are a few “typos” in the bibliography that could be fixed: e.g. the Stein–Wuthrich paper needs lowercase names and uppercase Iwasawa and the Zhang papers are missing a lot of info. To get bibliographic information, I often go to MathSciNet, which you can access through BU by going to this link <https://ezproxy.bu.edu/login?url=https://mathscinet.ams.org/mathscinet>. It's a great resource for looking up papers, citations in bibtex format, and reading short summaries of papers.] ♣♣♣ Angus: [I'll second mathscinet as a great resource. You can also get BibTeX information from Google scholar or arXiv if it is a preprint or something else not listed on mathscinet.] ♣♣♣ Jacksyn: [Pointless aside: does anyone know the history of why math doesn't have (or at least widely follow) a standard bibliographic style like they do in history or psychology? Or is there one?] ♣♣♣ Angus: [I seem to recall that all instances in which I searched for information on bibliographic conventions just returned "Here's how to use BibTeX"]

¹actually, using Iwasawa theory, this isn't conjectural, but we won't get into that here...

♣♣♣ John: [For a reference on Iwasawa Theory, I like the first few chapters of “Cyclotomic Fields and Zeta Values” by Coates and Sujatha. It’s a very dense book, but it approaches Iwasawa theory from the lens of cyclotomic fields which (imo) is easier to play around with. Washington also has a book called “Introduction to Cyclotomic Fields” which does the same thing but actually writes out all the details. Lang’s “Cyclotomic Fields I & II” are also good since Lang really emphasizes the idea of distributions, but ofc it’s riddled with typos. I believe there is also an AWS notes on Iwasawa theory, but I’d suggest first reading the cyclotomic case bc I like number fields.]

REFERENCES

- [BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over q : Wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, May 2001.
- [BM86] J. Teitelbaum B. Mazur, J. Tate. On p -adic analogues of the conjectures of birch and swinnerton-dyer. *Inventiones mathematicae*, 84:1–48, 1986.
- [BMS14] Jennifer S. Balakrishnan, J. Steffen Müller, and William A. Stein. A p -adic analogue of the conjecture of birch and swinnerton-dyer for modular abelian varieties, 2014.
- [BMT77] J. Tate B. Mazur and J. Teitelbaum. Modular curves and the eisenstein ideal. *Publications Mathématiques de l’IHÉS*, 47:33–186, 1977.
- [GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L -series. *Inventiones Mathematicae*, 84(2):225–320, Jun 1986.
- [Kim21] Chan-Ho Kim. On the p -converse to a theorem of gross-zagier and kolyvagin, 2021.
- [Kol89] V A Kolyvagin. On the mordell-weil and shafarevich-tate groups for weil elliptic curves. *Mathematics of the USSR-Izvestiya*, 33(3):473–499, Jun 1989.
- [MS94] Barry Mazur and Glenn Stevens. *p -Adic Monodromy and the Birch and Swinnerton-Dyer Conjecture*. American Mathematical Society, 1994.
- [MST06] Barry C. Mazur, William Stein, and John Torrence Tate. Computation of p -adic heights and log convergence. *Documenta Mathematica*, pages 577–614, 2006.
- [MT91] B. Mazur and J. Tate. The p -adic sigma function. *Duke Mathematical Journal*, 62(3), Apr 1991.
- [Roh84] David E. Rohrlich. On L -functions of elliptic curves and cyclotomic towers. *Inventiones mathematicae*, 75:409–424, 1984.
- [Ski14] Christopher Skinner. A converse to a theorem of gross, zagier, and kolyvagin, 2014.
- [SU14] Christopher Skinner and Eric Urban. The iwasawa main conjectures for gl_2 . *Inventiones mathematicae*, 195(1):1–277, Jan 2014.
- [SW13] WILLIAM STEIN and CHRISTIAN WUTHRICH. Algorithms for the arithmetic of elliptic curves using iwasawa theory. *Mathematics of Computation*, 82(283):1757–1792, 2013.
- [TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain hecke algebras. *The Annals of Mathematics*, 141(3):553, May 1995.
- [Wil95] Andrew Wiles. Modular elliptic curves and fermat’s last theorem. *The Annals of Mathematics*, 141(3):443, May 1995.
- [YZ17] Zhiwei Yun and Wei Zhang. Shtukas and the taylor expansion of L -functions, 2017.
- [Zha13] Wei Zhang. The birch-swinerton-dyer conjecture and heegner points: A survey. *Current Developments in Mathematics*, 2013(1):169–203, 2013.
- [Zha14] Wei Zhang. Selmer groups and the indivisibility of heegner points. 2014.