CONGRUENCES BETWEEN LOGARITHMS OF HEEGNER POINTS

DANIEL KRIZ, ERIC SHEN, KEVIN WU

Abstract. Elliptic curves are an important class of Diophantine equations. We study certain special solutions of elliptic curves called Heegner points, which are the traces of images under modular parametrizations of complex multiplication points in the complex upper half-plane. We prove, for pairs of elliptic curves with isomorphic Galois representations, a general congruence of stabilized formal logarithms. This is done by first showing that the isomorphism of Galois representations implies a congruence of stabilized modular forms and then translating these to the congruence of formal logarithms using Honda's theorem relating formal groups of elliptic curves to L-series and the modular parametrization. We use this congruence to show that examples of elliptic curves with analytic and algebraic rank 1 propagate in quadratic twist families.

Keywords: elliptic curves, BSD, heegner points, formal logarithm, quadratic twists.

Contents

1. Introduction

An elliptic curve is a projective, nonsingular curve given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We will consider elliptic curves E over $\mathbb{Q}$. Over rationals, we can reduce to a Weierstrass equation of the form

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

Recall that the rational points on E form a group $E(\mathbb{Q})$. Mordell's theorem states that this group is finitely generated, i.e. $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, where $r \geq 0$. We call r the *rank* of the elliptic curve.

There is also an *analytic rank* associated to each elliptic curve. Let $a_p = p + 1 - |E(\mathbb{F}_p)|$, where $E(\mathbb{F}_p)$ denotes the elliptic curve reduced mod p. Define

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p \cdot p^{-2s}) & E \text{ has good reduction at } p \\ 1 - p^{-s} & E \text{ has split multiplicative reduction at } p \\ 1 + p^s & E \text{ has nonsplit multiplicative reduction at } v \\ 1 & E \text{ has additive reduction at } v \end{cases}. \tag{1.1}$$

Then, the L-series of the curve is given by the Euler product $\prod_p L_p(E,s)$. We define the analytic rank of the curve to be the order of the pole of the L-function at $s = 1$, i.e.

$$r_{an} = \text{ord}_{s=1} L(E,s).$$

From its Euler product definition, $L(E, s)$ can be viewed as a generating function of E encoding information on the number of $\mathbb{F}_p$ (or mod p) points on E. In analogy with Dirichlet L-series, $L(E, s)$ is known to have a functional equation relating $L(E, s)$ and $\epsilon \cdot L(E, 2-s)$ for some $\epsilon \in \{\pm 1\}$; this is a consequence of the modularity theorem of Wiles [22], Taylor-Wiles [21] and Breuil-Conrad-Diamond-Taylor [3]. Thus, in the same philosophy of the Dirichlet class number formula [4] for $L(\chi, 1)$ describing the unit group of the number field cut out by the Dirichlet character χ, the Birch and Swinnerton-Dyer (BSD) conjecture predicts that the behavior of $L(E, s)$ at the central point $s = 1$ reveals information about the rank r of $E(\mathbb{Q})$.

Conjecture 1.1 (BSD Conjecture)**.** The Mordell-Weil rank and analytic rank are equal, i.e. $r = r_{an}(E)$.

The original conjecture from Birch and Swinnerton-Dyer's paper ([1]) was the following asymptotic

$$f(P) \sim C(\log P)^{r(E)},$$

where $P = \prod_p \frac{p}{\#E(\mathbb{F}_p)}$ and as $P \to \infty$.

Mazur's torsion theorem [18, p. 242] tells us the possible torsion subgroups of $E(\mathbb{Q})$, and that the maximal order of a point is at most 12. Additionally, Nagell-Lutz [18, p. 240] tells us that all torsion points must be integral, and that the y-coordinate of a torsion point must divide the discriminant, so the torsion subgroup is computable by a finite case check. Therefore knowing r "ineffectively" solves the Diophantine equation. It turns out that r is difficult but $r_{an}(E)$ is much simpler to compute, so if this conjecture were true it would ineffectively solve elliptic curves.

In practice however the only known ways to find r are in the $r = 0, 1$ case and involve producing explicit rational points coming from *Heegner points* (see [9], [13, Section 3.6]). For an imaginary quadratic field $K/\mathbb{Q}$ (called the *Heegner field*) satisfying the so-called Heegner hypothesis with respect to E:

$$\text{for every prime } \ell \text{ dividing the conductor of } N, \ \ell \text{ is split in } K$$

the Heegner point is a specific point in $E(K)$. When this point is nontorsion, then we can say $r = 0$ or 1 (precisely, $r = \frac{1-\epsilon}{2}$ where ϵ is the sign appearing in the functional equation of $L(E, s)$).

In our paper, we prove this conjecture over a wide class of elliptic curves by considering the formal logarithm and the Heegner point.

Given an elliptic curve, we can construct the formal group by using the change of variables $z = \frac{-x}{y}$, $w = -\frac{1}{y}$, so that the point at infinity $O \in E$ becomes $(z, w) = (0, 0)$. We can then write the neighborhood of the group about O as a formal group in z. From the formal group we can then construct a differential form

$$\omega = F_X(0, T)^{-1} dT$$

satisfying the equation

$$\omega \circ F(T, S) = \omega(T).$$

Integrating this form gives the formal logarithm, which is a power series in z that is also a homomorphism from the formal group of the elliptic curve to the additive formal group:

$$\log_E : \hat{E} \to \hat{\mathbb{G}}_a.$$

The formal logarithm has the special property that its value at a point is nonzero if and only if the point is nontorsion. Thus to show the Heegner point is nontorsion, it suffices to show its formal logarithm is nonzero, which then (by the work of Gross-Zagier and Kolyvagin) implies the curve has analytic rank 1 and thus satisfies the BSD conjecture.

We examine elliptic curves which have isomorphic mod p^r Galois forms. In Section 2, we show that mod p^r Galois representations being isomorphic implies the stabilized modular forms are congruent mod p^r. In Sections 3 and 4 we show this congruence translates to the congruence of formal logarithms. To show this, we use Honda's theorem and the modular parametrization from the modularity theorem to use the coordinate q on the modular curve. Plugging in Heegner points, the stabilizations produce Euler-like factors in the congruence.

One application of our congruence is the following:

Theorem 1.2. *Let N be the conductor of E. Suppose $E' = E^d$ (the quadratic twist of E by d) where $(N, d) = 1$. Let $L_p(E, 1)$ be as in (1.1) and let $\tilde{L}_p(E, 1)$ be as in the statement of Theorem 4.6. Then*

$$\tilde{L}_2(E,1) \cdot \left(\prod_{\ell | d} L_\ell(E,1) \right) \cdot \log_{\hat{E}}(P_E) \equiv \tilde{L}_2(E^d,1) \cdot \log_{\hat{E}^d}(P_{E^d}) \pmod 2. \tag{1.2}$$

Proof. Recall that $E[2] \cong E^d[2]$, and $L_\ell(E^d, 1) = 1$ for $\ell \mid d$. Then, applying 4.5 to E, E^d gives the theorem. □

Remark 1.3. This is a generalization of [13, Theorem 1.16], which handles the 2 split in K (i.e. $D_K \equiv 1 \bmod 8$) case (where $D_K < 0$ is the fundamental discriminant of the Heegner imaginary quadratic field K).

We can use this theorem to show that the formal logarithm of Heegner points are nonzero by showing that both sides are congruent to 1 mod 2. By the work of Kolyvagin [12] and Gross-Zagier [10] this is enough to show that the curve has rank 0 or 1 and satisfies BSD.

2. Galois representations and modular forms of elliptic curves

Let $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ be an elliptic curve. In this section, we will recall some crucial facts on the Galois representations attached to E as well as properties of the modular form attached to E. Recall $E[p^n] \cong (\mathbb{Z}/p^n)^{\oplus 2}$. Let $T_pE = \varprojlim_n E[p^n] \cong \mathbb{Z}_p^{\oplus 2}$ be the p-adic Galois representation of E. This means that $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on T_pE gives a group homomorphism

$$\rho_E : G_\mathbb{Q} \to \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

The point $[+]_E$ is given by polynomials in (x, y) over $\mathbb{Q}$, and $G_\mathbb{Q}$ commutes with polynomial over $\mathbb{Q}$ operations, so $\sigma(P_1[+]_E P_2) = \sigma(P_1)[+]_E \sigma(P_2)$ for all $\sigma \in G_\mathbb{Q}$, where $[+]_E$ is the group law of E (i.e. the action is linear, so ρ_E is linear). Note that

$$\rho_{E,r} \coloneqq \rho_E \bmod p^r : G_\mathbb{Q} \to \mathrm{Aut}(E[p^r]) \cong GL_2(\mathbb{Z}/p^r).$$

Let N be the conductor of E throughout. Let

$$f_E(q) = \sum_{n=1}^{\infty} a_n q^n \in \mathbb{Z}[\![q]\!],$$

where for a prime ℓ,

$$a_{\ell^r} = \begin{cases} 1 + \ell^r - \#\tilde{E}(\mathbb{F}_{\ell^r}) & \ell \nmid N \\ 1 & \ell || N, \text{ split multiplicative reduction} \\ (-1)^r & \ell || N \text{ nonsplit multiplicative reduction} \\ 0 & \ell^2 | N \end{cases}. \tag{2.1}$$

Let $n = \prod_{i=1}^s \ell_i^{e_i}$ denote the prime factorization of n, $a_n = \prod_{i=1}^s a_{\ell_i^{e_i}}$. When we wish to emphasize the dependence of a_n on the elliptic curve E, we will write $a_n(E)$ instead of a_n.

Definition 2.1. We define the N-stabilization of the modular form f_E attached E (by [22], [21], and [3]) to be

$$f_E^{(N)}(q) = \sum_{n=1,(n,N)=1}^{\infty} a_n q^n.$$

Definition 2.2. For any $f = \sum_{n=1}^\infty b_n q^n \in \mathbb{Z}[\![q]\!]$, define the "$\ell$-depletion operator" as

$$f^{(\ell)}(q) := \sum_{n=1,(\ell,n)=1}^{\infty} b_n q^n,$$

which in the case of elliptic curves is

$$f(q) - b_\ell f(q^\ell) + \ell f(q^{\ell^2}),$$

and let $f^{(\ell^t)}(q) = f^{(\ell)}(q)$ for any $t \geq 1$.

Proposition 2.3. *If $\prod_{i=1}^s \ell_i$ is the squarefree radical of N, then*

$$f_E^{(N)}(q) = \left(\left(\dots\left(f_E^{(\ell_1)}\right)^{(\ell_2)}\dots\right)^{(\ell_{s-1})}\right)^{(\ell_s)}(q).$$

Proof. This follows from Definition 2.1 above and Equation 2.3) below. □

Definition 2.4. Let ℓ be a good prime of E (i.e. $\ell \nmid N$), and let α_ℓ, β_ℓ be the roots of the characteristic polynomial of Frob_ℓ

$$T^2 - a_\ell T + \ell.$$

Also define

$$f_E^{(\ell^+)}(q) = f_E(q) - \alpha_\ell f_E(q^\ell), \qquad f_E^{(\ell^-)}(q) = f_E(q) - \beta_\ell f_E(q^\ell).$$

Recall the definition of semisimplification V^{ss} of a representation V: Taking a Jordan-Holder series

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

where each V_i is a subrepresentation and V_i/V_{i-1} is simple then

$$V^{\mathrm{ss}} = \bigoplus_{i=1}^n V_i/V_{i-1}.$$

Theorem 2.5. *Let E, E' be two elliptic curves over $\mathbb{Q}$ with conductors N, N' and let $r \in \mathbb{Z}_{\geq 0}$ such that*

$$\rho_{E,r}^{\mathrm{ss}} \cong \rho_{E',r}^{\mathrm{ss}} \iff f_E^{(NN')}(q) \equiv f_{E'}^{(NN')}(q) \pmod{p^r\mathbb{Z}[\![q]\!]}. \tag{2.2}$$

The key for the proof is first to reduce to the following statement.

Proposition 2.6. *For all primes $\ell \nmid NN'$,*

$$f_E^{(NN')}(q) \equiv f_{E'}^{(NN')}(q) \pmod{p^r\mathbb{Z}[\![q]\!]} \iff a_\ell(E) \equiv a_\ell(E') \pmod{p^r}$$

Proof. The left hand side implies the right hand side because if the functions are congruent the coefficients must be the same. The converse is harder. We use the following fact.

Let N, N' be the conductors of E, E'. For $\ell \nmid NN'$ ("good ℓ"), we have

$$a_{\ell^r} = a_\ell \cdot a_{\ell^{r-1}} - \ell a_{\ell^{r-2}}. \tag{2.3}$$

This recursion follows from the Weil conjectures for elliptic curves over $\mathbb{F}_\ell$. From this recursion it is clear that

$$a_\ell(E) \equiv a_\ell(E') \pmod{p^r} \implies a_{\ell^k}(E) \equiv a_{\ell^k}(E') \pmod{p^r}$$

for all good primes ℓ, so then all of the coefficients of the stabilized modular forms are congruent as desired. □

We now need another key result, which is the essential link between ρ_E and $f_E(q)$. Suppose E is an elliptic curve over any field of characteristic prime to p. For every $r \in \mathbb{Z}_{\geq 0}$, we have an alternating bilinear pairing

$$\langle \cdot, \cdot \rangle : E[p^r] \times E[p^r] \to \mu_{p^r},$$

satisfying the following "Galois equivariance property": for all $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\langle \sigma(P), \sigma(Q) \rangle = \sigma(\langle P, Q \rangle).$$

Moreover, the Weil pairing is nondegenerate: suppose $P \in E[p^r]$. Then

$$\langle P, Q \rangle = 0, \quad \forall Q \in E[p^r] \implies P = [0],$$

where $[0] \in E[p^r]$ is the identity element.

Note if $\rho : G \to GL_2(\mathbb{Z}/p^r)$ is our representation, then

$$\langle \sigma(P), \sigma(Q) \rangle = \langle \rho(\sigma)(P), \rho(\sigma)(Q) \rangle = \langle P, Q \rangle^{\det(\rho(\sigma))}.$$

Proposition 2.7. *Recall the $G_{\mathbb{Q}}$-representation $\rho_{E,r}$. Then for all ℓ not dividing the conductor of E,*

$$\det(\rho_E(\mathrm{Frob}_\ell)) = \ell.$$

Proof. Take e_1, e_2 to be a basis of $E[p^r] \cong (\mathbb{Z}/p^r)^{\oplus 2}$. We then have

$$\langle e_1, e_2 \rangle^{\det(\rho_E(\sigma))} = \langle \sigma(e_1), \sigma(e_2) \rangle = \sigma(\langle e_1, e_2 \rangle).$$

Plugging in $\sigma = \mathrm{Frob}_\ell$ gives

$$\langle e_1, e_2 \rangle^{\det(\rho_E(\sigma))} = \langle e_1, e_2 \rangle^{\ell}.$$

Therefore $\ell = \det(\rho_E(\mathrm{Frob}_\ell))$.

□

We now cite the following results to establish Theorem 2.5.

Theorem 2.8 (Eichler-Shimura, [17])**.** *For all $\ell \nmid NN'$, there are elements $\mathrm{Frob}_\ell \in G_{\mathbb{Q}}$ ("Frobenius at ℓ") such that*

$$\mathrm{Trace}(\rho_E(\mathrm{Frob}_\ell)) = a_\ell.$$

Theorem 2.9 (Brauer-Nesbitt Theorem, [2])**.** *Let G be a group, let R be any ring, and let $\rho, \rho' : G \to GL_n(R)$ be two representations of G. Then*

$$\rho^{\mathrm{ss}} \cong \rho'^{\mathrm{ss}} \iff \mathrm{char}_\rho(T) = \mathrm{char}_{\rho'}(T).$$

Here

$$\mathrm{char}_\rho : G \to R[T]$$

is defined element-wise.

Proof of Theorem 2.5. For the $\implies$ direction, recall that since $\rho \cong \rho'$ we have $\mathrm{Trace}(\rho) = \mathrm{Trace}(\rho')$. Now, we are done by Theorem 2.8 and Proposition 2.6.

For the $\impliedby$ direction, by Theorem 2.8 and Proposition 2.7, we have

$$\begin{aligned} \mathrm{char}_\rho(\mathrm{Frob}_\ell)(T) &= T^2 - \mathrm{Trace}(\mathrm{Frob}_\ell)T + \det(\mathrm{Frob}_\ell) \\ &= T^2 - a_\ell(E)T + \ell \equiv T^2 - a_\ell(E')T + \ell \pmod{p^r}. \end{aligned}$$

However, by the Chebotarev density theorem and the continuity of char_ρ, we have

$$\mathrm{char}_\rho(g) \equiv \mathrm{char}_{\rho'}(g) \pmod{p^r} \quad \forall g \in G_{\mathbb{Q}}.$$

So by Theorem 2.9, we are done. □

3. Congruences of modular forms

We have already seen what happens when the Galois representations of two elliptic curves are congruent modulo p^r. In general, Galois representations $\rho_{E,r}$ are irreducible (i.e. have no nontrivial subrepresentation). It is known that $\rho_{E,\infty}$ is always irreducible. In this section, we will further study consequences of congruences of modular forms, in particular what happens when the Galois representation $\rho_E : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p)$ is reducible modulo p^r, i.e. $\rho_{E,r}$ is reducible. Recall this means

$$\rho_{E,r} = \begin{pmatrix} \chi_1 & \bullet \\ 0 & \chi_2 \end{pmatrix},$$

where

$$\chi_i : G_{\mathbb{Q}} \to (\mathbb{Z}/p^r)^\times$$

are Galois characters. (Characters on a Galois group.)

Remark 3.1. Here the χ_i are characters on $G_{\mathbb{Q}}$, but we want to view them as Dirichlet characters $\chi_i : (\mathbb{Z}/N_i)^\times \to \overline{\mathbb{Q}}^\times$ below. For this, note that

$$\chi_i : G_{\mathbb{Q}} \to (\mathbb{Z}/p^r)^\times,$$

so χ_i factors through a finite abelian quotient of $G_{\mathbb{Q}}$, i.e. $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q})$ for some finite extension $F/\mathbb{Q}$ such that $\mathrm{Gal}(F/\mathbb{Q})$ is abelian. (In other words, F is an "abelian extension of $\mathbb{Q}$".)

Recall that the Kronecker-Weber theorem gives that all abelian extensions $F/\mathbb{Q}$ are contained in $\mathbb{Q}(\mu_M)$ for some M where μ_M denotes the group of Mth roots of unity.

In summary, we can view

$$\chi_i : (\mathbb{Z}/N_i)^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_{N_i})/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q}) \to (\mathbb{Z}/p^r)^\times$$

for some minimal N_i (i.e. the minimal N_i such that $F \subset \mathbb{Q}(\mu_{N_i})$). Thus we can view χ_i as a Dirichlet character of conductor N_i.

Under the projection

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{N_i})/\mathbb{Q}) \cong (\mathbb{Z}/N_i)^\times,$$

the element Frob_ℓ is sent to $\ell \pmod{N_i}$ (for $(\ell, N_i) = 1$). Thus $\chi_i(\mathrm{Frob}_\ell) = \chi_i(\ell)$.

Definition 3.2. Define the *mod p^r Teichmüller character*

$$\omega_r : G_{\mathbb{Q}} \to (\mathbb{Z}/p^r)^\times$$

by

$$\sigma(\zeta) = \zeta^{\omega_r(\sigma)} \ \forall \zeta \in \mu_{p^r}.$$

Note that ω_r is defined for every r, and the ω_r satisfy the following compatibility for all $r \le r'$:

$$\omega_r \equiv \omega_{r'} \pmod{p^r}.$$

The *cyclotomic character* $\chi : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is defined by

$$\chi(\sigma) = (\omega_1(\sigma), \omega_2(\sigma), \ldots, \omega_r(\sigma), \omega_{r+1}(\sigma), \ldots) \in \varprojlim_{r \ge 0} (\mathbb{Z}/p^r)^\times = \mathbb{Z}_p^\times.$$

By Remark 3.1 applied to the character ω_r, we have

$$\zeta^{\omega_r(\mathrm{Frob}_\ell)} = \mathrm{Frob}_\ell(\zeta) = \zeta^\ell,$$

and thus

$$\omega_r(\mathrm{Frob}_\ell) = \omega_r(\ell), \tag{3.1}$$

where the left-hand side is viewed as a Galois character, and the right-hand side as a Dirichlet character.

Proposition 3.3. *Let N be the conductor of E. We have $N_1 N_2 \mid N$.*

Reducible also means

$$\rho_{E,r}^{\mathrm{ss}} = \chi_1 \oplus \chi_2, \tag{3.2}$$

is a direct sum of characters. We will see that analogously to Theorem 2.5, this "essentially" implies

$$f_E(q) \equiv E_2^{\chi_1, \chi_2} \pmod{p^r \mathbb{Z}[\![q]\!]}$$

where $E_2^{\chi_1,\chi_2}$ is some *Eisenstein series*.

Remark 3.4. $f_E(q)$ can be thought of as the generating function of the representation ρ_E by (2.1). Similarly, $E_2^{\chi_1,\chi_2}$ can be thought of as the generating function of the representation $\chi_1 \oplus \chi_2$. Essentially, we are showing that congruences of representations imply congruences of their associated generating functions.

Proposition 3.5. *We have that*

$$\chi_1 \chi_2 \equiv \omega_r \pmod{p^r}.$$

Proof. Note that in the setting of this section (i.e. $\rho_{E,r}^{\mathrm{ss}} = \chi_1 \oplus \chi_2$), $\det(\rho_{E,r}) = \chi_1\chi_2$.

Recall

$$\rho_{E,r} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/p^r).$$

From the Weil pairing, $\det(\rho_{E,r}) = \omega_r$. Let us give some details: Recall $E[p^r] = (\mathbb{Z}/p^r)^{\oplus 2}$. Fix a $(\mathbb{Z}/p^r)$-basis e_1, e_2 of $E[p^r]$, without loss of . Write $\zeta = \langle e_1, e_2\rangle \in \mu_{p^r}$. (One can check that ζ has to be primitive, since the Weil pairing is surjective.) For all $\sigma \in G_{\mathbb{Q}}$, we have

$$\langle \rho_{E,r}(\sigma)(e_1), \rho_{E,r}(\sigma)(e_2)\rangle = \langle \sigma(e_1), \sigma(e_2)\rangle = \sigma(\langle e_1, e_2\rangle)$$

where the first equality follows from the definition of $\rho_{E,r}$ and the second follows from the Galois equivariance property of the Weil pairing $\langle\cdot,\cdot\rangle : E[p^r] \times E[p^r] \to \mu_{p^r}$. But the right-hand side is

$$\sigma(\langle e_1, e_2\rangle) = \sigma(\zeta) = \zeta^{\omega_r(\sigma)}.$$

Now using the bilinearity of the Weil pairing, the left-hand side of the above displayed equation is equal to $\zeta^{\det(\rho_{E,r}(\sigma)}$. Write

$$\rho_{E,r}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/p^r).$$

Then

$$\rho_{E,r}(\sigma)(e_1) = ae_1 + ce_2, \qquad \rho_{E,r}(\sigma)(e_2) = be_1 + de_2.$$

So

$$\langle \rho_{E,r}(\sigma)(e_1), \rho_{E,r}(\sigma)(e_2)\rangle = \langle ae_1 + ce_2, be_1 + de_2\rangle = \langle e_1, e_2\rangle^{ad-bc} = \zeta^{\det(\rho_{E,r}(\sigma))}.$$

So we get the determinant identity involving ω_r.

Now equating the two identities, we get the proposition. □

Definition 3.6. Define a differential operator acting on q-series $\theta = \frac{qd}{dq} = q \cdot \frac{d}{dq}$, i.e.

$$\theta\left(\sum_{n=0}^{\infty} c_n q^n\right) = \sum_{n=0} n c_n q^n.$$

Note that θ kills the constant term.

Corollary 3.7. *For all $j \geq 1$, we have*

$$\theta^j f_E^{(Np)}(q) \equiv \theta^j (E_2^{\chi_1,\chi_1^{-1}})^{(Np)}(q) \pmod{p^r}.$$

If moreover $b_0 \equiv 0 \pmod{p^r}$, then the above congruence holds for $j = 0$ as well.

Definition 3.8 (p-adic uniform topology)**.** Suppose $F/\mathbb{Q}_p$ is a finite extension and $R = F[\![q]\!]$ is the the usual power series ring. Then we define a metric on R as follows: given $f = \sum_{n=0}^{\infty} a_n q^n, g(q) = \sum_{n=0}^{\infty} b_n q^n$

$$|f(q) - g(q)| = \sup_n |a_n - b_n|_p$$

where $|\cdot|_p$ is the p-adic absolute value on F. The topology on R induced by this metric is called the p-adic uniform topology (because convergence in this topology is the p-adic notion of "uniform convergence", i.e. uniform coefficient-wise convergence).

If $\mathcal{O}_F/\mathbb{Z}_p$ is the valuation ring of F (i.e. the elements with $|x|_p \leq 1$), then $\mathfrak{p} = \{|x|_p < 1\}$ is a prime ideal which contains p. Then

$$\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_{p^n}$$

for some integer $n \geq 1$. This is called the residue field.

Proposition 3.9. *For any finite extension $F/\mathbb{Q}_p$, the residue field $\mathcal{O}_F/\mathfrak{p}$ is finite.*

Proof. $\mathbb{Z}_p$ is compact with respect to the p-adic topology. If $\mathcal{O}_F/\mathbb{Z}_p$ is finite, then as a $\mathbb{Z}_p$-module, $\mathcal{O}_F$ is isomorphic (and homeomorphic, i.e. the isomorphism and its inverse are both continuous) to $\mathbb{Z}_p^{\oplus n}$ for some $n \geq 1$. This latter space is a compact by Tychonoff's theorem, so $\mathcal{O}_F$ is compact with respect to its p-adic topology.

Choose a set of representatives S in $\mathcal{O}_F$ of $\mathcal{O}_F/\mathfrak{p}$. Then $\{a+\mathfrak{p}\}_{a\in S}$ is an open cover of $\mathcal{O}_F$. So by compactness, there is a finite subcover, i.e. a finite subset $S_0 \subset S$ such that $\{a+\mathfrak{p}\}_{a\in S_0}$ covers $\mathcal{O}_F$. This means that $S_0 \pmod p = \mathcal{O}_F/\mathfrak{p}$, which implies the latter is finite. □

Fermat's little theorem for $\mathbb{F}_p$ involves the order $\#\mathbb{F}_{p^n} = p^n - 1$; this is divisible by numbers other than p and $p-1$ in general.

Any field k has a ring homomorphism $\mathbb{Z} \to k$. This has some kernel I, which gives an injection $\mathbb{Z}/I \hookrightarrow k$. Since k is a field, then $\mathbb{Z}/I$ is a field, then I is a prime ideal, and so is either (0) or (p) for some prime p. If the former, we say k has characteristic 0, and if the latter, characteristic p.

(The exponent below in the limit would be $p^m(p^n-1)$ instead as $m \to \infty$.)

Proposition 3.10. *Given a q-series $F(q) = \sum_{n=0}^{\infty} c_n q^n \in \mathbb{Z}_p[\![q]\!]$ with coefficients in some finite extension $F/\mathbb{Q}_p$, if the order of the residue field $\mathcal{O}_F$ is p^n then (in the p-adic uniform topology)*

$$\lim_{m\to\infty} \theta^{p^m(p^n-1)}(F(q)) = F^{(p)}(q).$$

Here $F^{(p)}$ is p-stabilization as in Proposition 2.3.

Proof. Note that

$$\theta^{p^m(p^n-1)}(F(q)) = \sum_{i=0}^{\infty} i^{p^m(p^n-1)} c_i q^i = \sum_{i=0}^{\infty} (i^{p^n-1})^{p^m} c_i q^i.$$

Clearly, if $p \mid i$, then $\lim_{m\to\infty}(i^{p^n-1})^{p^m} = 0$. If $p \nmid i$, then by Lagrange's theorem applied to the multiplicative group of $\mathcal{O}_F$ we have $i^{p^n-1} \equiv 1 \pmod{\mathfrak{p}}$. Then the lifting the exponent lemma tells us that $(i^{p^n-1})^{p^m} \equiv 1 \pmod{p^m}$ so we have that $\lim_{m\to\infty}(i^{p^n-1})^{p^m} = 1$.

Therefore

$$\lim_{m\to\infty} \theta^{p^m(p^n-1)}(F(q)) = \sum_{i\geq 0, p\nmid i} c_n q^n = F^{(p)}(q).$$

□

Recall $q = \exp(2\pi i\tau)$ where τ is coordinate on the upper half plane $\mathcal{H}^+ = \{\mathrm{Im}(\tau) > 0\}$. $q = \exp(2\pi i \,\mathrm{Re}(\tau)) \cdot \exp(-2\pi \,\mathrm{Im}(\tau)) \implies |q| = \exp(-2\pi \,\mathrm{Im}(\tau))$. Thus $\mathcal{H}^+ = \{|q| < 1\}$. Note that $\tau = \infty \iff q = 0$, so q can be viewed as the "coordinate at ∞".

We will show q can be taken as a natural coordinate on the formal $\hat{E}$ (over $\mathbb{Z}_p$) of E. Recall that $\mathcal{H}^+$ has a left action by $SL_2(\mathbb{R})$, and $\Gamma_0(N) \subset SL_2(\mathbb{Z})$ given by matrices with bottom left entry congruent to 0 mod N. Let $Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H}^+$, and there is way to add finitely points ("compactify"), including the point at infinity ∞, to get $X_0(N)(\mathbb{C})$.

Recall Shimura's theorem ([17]): there is an algebraic curve $X_0(N)$ over $\mathbb{Q}$ such that $X_0(N)(\mathbb{C})$ is equal to the set in the previous paragraph.

Recall the modularity theorem due to Wiles ([22]), Taylor-Wiles ([21]) and Breuil-Conrad-Diamond-Taylor ([3]): there is a nonconstant (and thus surjective) morphism of algebraic curves over $\mathbb{Q}$

$$\pi_E : X_0(N) \twoheadrightarrow E \tag{3.3}$$

mapping ∞ to the point at infinity ∞_E on E (which is the identity element in the group law).

Assume now that $p \nmid N$, so that E has good reduction at p and thus a minimal good integral model E_+ at p. Moreover, $X_0(N)$ has a model $X_0(N)_+$ over $\mathbb{Z}_p$ due to Morita ([14]). From the Néron mapping property, (3.3) extends to a map of algebraic curves over $\mathbb{Z}_p$

$$\pi_E : X_0(N)_+ \to E_+. \tag{3.4}$$

Let $X_0(N)_\infty$ denote the formal completion of $X_0(N)_+$ at the point at infinity $\infty \in X_0(N)_+(\mathbb{F}_p)$. Recall coordinate q from the Tate curve $\mathbb{G}_m/q^{\mathbb{Z}}$ over $\mathbb{Z}_p[\![q]\!]$ can be viewed as a coordinate on

$X_0(N)_\infty$. Let $\hat{E}$ denote the formal group of E_+/ZZ_p. Then (3.4) gives a map of formal neighborhoods

$$\pi_E : X_0(N)_\infty \to \hat{E} \tag{3.5}$$

where $\hat{E}$ is the usual formal group. If this map is an isomorphism, then the coordinate q on the left-hand side gives a coordinate on the right-hand side $\hat{E}$. We will in fact show that (3.5) is an isomorphism in Theorem 4.1.

4. Congruences of formal logarithms

In this section, we will use the results of the previous sections in order to prove our main theorem (Theorem 4.6) on congruences between formal logarithms of Heegner points. Once again let N be the conductor of the elliptic curve E. By the modularity theorem ([22], [21], [3]), we have a nonconstant morphism of curves $\pi_E : X_0(N) \to E$ over $\mathbb{Q}$. Here $X_0(N)$ is the canonical model of the modular curve attached to the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Then E has a "Néron model" E^+ over $\mathbb{Z}[1/N]$; this means E^+ satisfies

$$E^+ \times_{\mathrm{Spec}(\mathbb{Z}[1/N])} \mathrm{Spec}(\mathbb{Q}) = E.$$

Also, $X_0(N)$ has a model $X_0(N)^+$ over $\mathbb{Z}[1/N]$ by theorems on representability of moduli problems. Then analogously,

$$X_0(N)^+ \times_{\mathrm{Spec}(\mathbb{Z}[1/N])} \mathrm{Spec}(\mathbb{Q}) = X_0(N).$$

By smoothness over $\mathbb{Z}_p$, the morphism $\pi_E : X_0(N) \to E$ extends to a morphism

$$\pi_E^+ : X_0(N)^+ \to E^+,$$

in other words, the polynomials defining π_E which a priori had coefficients in $\mathbb{Q}$, actually have coefficients in $\mathbb{Z}[1/N]$.

Now assume $p \nmid N$ (p is "good reduction for E"). Then the p-adic completion of $\mathbb{Z}[1/N]$ is $\varprojlim_n \mathbb{Z}[1/N]/p^n = \varprojlim_n \mathbb{Z}/p^n = \mathbb{Z}_p$. So p-adically completing π_E^+ (i.e. extending scalars along $\mathbb{Z}[1/N] \subset \mathbb{Z}_p$), we get a nonconstant morphism

$$\pi_{E,p}^+ : X_0(N)_p^+ \to E_p^+,$$

where $X_0(N)_p^+$ is the p-adic completion of $X_0(N)^+$, E_p^+ is the p-adic completion of E^+.

Additionally the point at infinity $\infty \in X_0(N)$ is mapped to the point at infinity in E by π_E. (Recall the point at infinity in E is the identity element in the group law of E.)

By taking the formal completion at ∞ on both sides of $\pi_{E,p}^+ : X_0(N)_p^+ \to E_p^+$, then we get a map

$$\pi_E^+ : (X_0(N)_p^+)_\infty \to \hat{E}_p^+ \tag{4.1}$$

where the right-hand side is the usual p-adic formal group of E, and $(X_0(N)_p^+)_\infty$ is the "formal completion at ∞", which is a formal scheme of dimension 1 (we can think of it informally as an infinitesimal neighborhood of ∞). In fact, one can show

$$(X_0(N)_p^+)_\infty \cong \mathrm{Spf}(\mathbb{Z}_p[\![q]\!])$$

where q is the same q appearing in q-expansions of modular forms. We we will "push forward" this coordinate q to E along (4.1).

Theorem 4.1. *For any E with good reduction at p, the map (4.1) is an isomorphism of formal schemes over* $\mathrm{Spf}(\mathbb{Z}_p[\![q]\!])$.

Proof. Let f_E be the normalized newform of level N and weight 2 attached to E by modularity ([22], [21], [3]), and let $f_E(q) = \sum_{n=1}^{\infty} a_n q^n$ be its q-expansion. Let $\omega_E = f(q)\frac{dq}{q}$ be the 1-form attached to f_E. It suffices to show that the ramification index of π_E^+ at the point at infinity $\infty \in X_0(N)^+(\mathbb{Z}_p)$ is 1, which is equivalent to showing that ω_E does not vanish at ∞. However, we have $\omega_E = f_E(q)\frac{dq}{q} = \left(q + a_2q^2 + \cdots\right)\frac{dq}{q} = (1 + a_2q + \cdots)\,dq$. Since q takes the value 0 at ∞, we see that $\omega_E(\infty) = dq(\infty)$; since dq is a generator of the sheaf of differentials at ∞ we have $dq(\infty) \neq 0$, which gives the desired nonvanishing.

□

The consequence is that the coordinate q on the LHS of (4.1) induces a coordinate on the RHS. In other words, we get a coordinate q on the p-adic formal group $\hat{E}_p^+$. We can apply Honda's theorem with respect to this coordinate.

Recall given two elliptic curves E, E' over $\mathbb{Q}$ with good reduction at p, and isomorphic Galois representations $E[p^r] \cong E'[p^r]$, we proved $f_E^{(NN')}(q) \equiv f_{E'}^{(NN')}(q) \pmod{p^r}$. Recall $\theta = qd/dq$. This implies

$$\theta^j(f_E^{(NN')}(q)) \equiv \theta^j(f_{E'}^{(NN')}(q)) \pmod{p^r}$$

for every $j \in \mathbb{Z}_{\geq 0}$. (Here, θ^j is the j-fold composition of θ.) Letting $j = -1 + p^m(p-1)$ and taking the limit $m \to \infty$, then the above congruence tends to a congruence

$$\sum_{n=1,(n,pNN')=1} \frac{a_n}{n} q^n \equiv \sum_{n=1,(n,pNN')=1} \frac{b_n}{n} q^n \pmod{p^r},$$

where $f_E(q) = \sum_{n=1}^{\infty} a_n q^n$, $f_{E'}(q) = \sum_{n=1}^{\infty} b_n q^n$.

We know from above that q can be used as a coordinate on $\hat{E}_p^+$. What does Honda's theorem say: It says that (modulo certain assumptions on E) $\sum_{n=1}^{\infty} a_n q^n$ is the logarithm of some formal group isomorphic to $\hat{E}_p^+$. In other words, rewriting $\hat{E}_p^+$ in terms of the coordinate q, the formal logarithm $\log_{\hat{E}_p^+}$ is $\sum_{n=1}^{\infty} a_n q^n$.

Note that Theorem 4.1 gives an isomorphism of formal schemes

$$(X_0(N)_p^+)_\infty \cong \hat{E}_p^+, \qquad (X_0(N')_p^+)_\infty \cong \hat{E'}_p^+.$$

However, there is a modular curve $X_0(NN')$, and we can check that there are natural maps

$$X_0(NN')^+ \to X_0(N)^+, \qquad X_0(NN')^+ \to X_0(N')^+ \tag{4.2}$$

over $\mathbb{Z}[1/NN']$.

Lemma 4.2. *The induced maps of formal schemes $(X_0(NN')_p^+)_\infty \to (X_0(N)_p^+)_\infty$ and $(X_0(NN')_p^+)_\infty \to (X_0(N')_p^+)_\infty$ over $\mathbb{Z}_p$ are isomorphisms.*

Proof. From the modular interpretations of $X_0(N)^+$, $X_0(N')$ and $X_0(NN')^+$, we have that $X_0(NN')^+ \to X_0(N)^+$ and $X_0(NN')^+ \to X_0(N')^+$ are finite étale maps of curves over $\mathbb{Z}_p$. Now the statements immediately follow from the fact that the residue fields of $X_0(N)^+$, $X_0(N')^+$ and $X_0(NN')^+$ at ∞ are all $\mathbb{F}_p$.

□

As a consequence of Theorem 4.1 and Lemma 4.2, we get an isomorphism of formal schemes over $\mathbb{Z}_p$

$$\hat{E}_p^+ \cong \hat{E'}_p^+.$$

For simplicity now, let $\log_E := \log_{\hat{E}_p^+}$. From the above discussion, we have

Theorem 4.3. *We have the following congruence of functions on $\hat{E}_p^+ \cong \hat{E'}_p^+$*

$$\log_E^{(pNN')}(q) \equiv \log_{E'}^{(pNN')}(q) \pmod{p^r}. \tag{4.3}$$

Proof. Given two curves E, E' with isomorphic Galois representations, we have that their stabilized modular forms are congruent by Equation 2.2. Thus, we can apply Proposition 2.15 to get that

$$\sum_{n\geq 1,(n,pNN')=1} \frac{a_n}{n} q^n \equiv \sum_{n\geq 1,(n,pNN')=1} \frac{b_n}{n} q^n \pmod{p^r},$$

where the coordinate q is from $X_0(N)_p^+$. Because of 4.1, we can parameterize the group $\hat{E}_p^+$ using this coordinate. Write both sides in terms of $\sum_{n=1}^{\infty} \frac{a_n}{n} q^n$ and $\sum_{n=1}^{\infty} \frac{b_n}{n} q^n$ (meaning we can also make a change of variables $q \mapsto q^{\ell^i}$ for various ℓ, etc.).

Now, in the context of Honda's Theorem 5: E, our elliptic curve over $\mathbb{Q}$, gives us two formal groups: $F = F(x, y)$ from $\hat{E}$ and G some formal group defined by $L(E, s)$. Honda says that G really is a formal group (nontrivial), and there is an isomorphism: by definition

$$\xi : F \xrightarrow{\sim} G, \qquad \xi \in \mathbb{Z}_S[\![q]\!], \qquad F(\xi(x), \xi(y)) = \xi(G(x, y))$$

which has an inverse $\xi^{-1} \in \mathbb{Z}[\![t]\!]$ such that

$$G(\xi^{-1}(x), \xi^{-1}(y)) = \xi^{-1}(F(x, y)).$$

Let F', G' be the corresponding objects for E' in place of E above.

In our setting, $\log_F = \log_{\hat{E}}$, so we have

$$\sum_{n=1}^{\infty} \frac{a_n}{n} q^n = \log_G = \log_F \circ \xi = \log_{\hat{E}} \circ \xi \tag{4.4}$$

in $\mathbb{Q}[\![q]\!]$.

Corollary 4.4. *We have the following formula in terms of* $\log_{\hat{E}} \circ \xi(q) = \log_G$. *Define* $\log_{\hat{E}}^{(pNN')}$ *by*

$$\log_{\hat{E}}^{(pNN')} \circ \xi(q) = \log_G^{(pNN')},$$

or equivalently,

$$\log_{\hat{E}}^{(pNN')} = \log_G^{(pNN')} \circ \xi^{-1}.$$

Then

$$\log_{\hat{E}}^{(pNN')} \equiv \log_{\hat{E}'}^{(pNN')} \pmod{p^r}.$$

Proof. From the isomorphism $E[p^r] \cong E'[p^r]$, we have $a_n \equiv b_n \pmod{p^r}$ for all $(n, pNN') = 1$, which formally implies

$$\log_G^{(pNN')}(q) \equiv \log_{G'}^{(pNN')}(q) \pmod{p^r \mathbb{Z}_p[\![q]\!]}.$$

By (4.4) and the formulas for stabilization, we have $\log_F^{(pNN')} = \log_G^{(pNN')}$, and thus

$$\log_F^{(pNN')}(\xi(q)) \equiv \log_{F'}^{(pNN')}(\xi(q)) \pmod{p^r \mathbb{Z}[\![q]\!]}.$$

□

□

Let $b_n = \frac{a_n}{n}$. Note that b_n is also multiplicative since a_n, n are. From 2.3 then

$$b_{\ell^r} = \frac{a_{\ell^r}}{\ell^r} = \frac{a_\ell}{\ell} \cdot \frac{a_{\ell^{r-1}}}{\ell^{r-1}} - \frac{a_{\ell^{r-2}}}{\ell^{r-2} \cdot \ell} = b_\ell \cdot b_{\ell^{r-1}} - \frac{b_{\ell^{r-2}}}{\ell}.$$

We then see that

$$\begin{aligned}\log_E(q) - \frac{a_\ell}{\ell}\log_E(q^\ell) + \frac{1}{\ell}\log_E(q^{\ell^2}) &= \sum_{i=1}^{\infty} b_n\left(q^n - q^{n\ell} + \frac{1}{\ell}q^{n\ell^2}\right)\\ &= \sum_{i\geq 1,\ell\nmid i} b_i q^i + b_{i\ell}q^{i\ell} - b_i b_\ell q^{i\ell} + \sum_{i\geq 1}\left(b_{i\ell^2} - b_\ell b_{i\ell} + \frac{b_i}{\ell}\right)q_{i\ell^2}\\ &= \sum_{i\geq 1,l\nmid i} b_i q^i + \sum_{i\geq 1} 0\cdot q_{i\ell^2} = \log_E^{(\ell)}(q).\end{aligned}$$

Notice that if q is a Heegner point of conductor 1 ([13, Sections 3.4 and 3.6]), and ℓ splits in K, then $\log_E(q^\ell) = \log_E(q)$, so we get

$$\log_E^{(\ell)}(q) = \log_E(q)\cdot\left(1 - \frac{a_\ell}{\ell} + \frac{1}{\ell}\right).$$

If q is a Heegner point of conductor p or p^2 ([9]), then a similar calculation as in loc. cit. implies

$$\log_E^{(p)}(q) = \log(q)\cdot\tilde{L}_p(E,1).$$

Definition 4.5. Recall the definition of the Euler factor of $L(E,1)$ at ℓ:

$$L_\ell(E,1) := \begin{cases} 1 - a_\ell(E)/\ell + 1/\ell & \ell\nmid N\\ 1 - 1/\ell & \ell||N, \ell \text{ split multiplicative reduction}\\ 1 + 1/\ell & \ell||N, \ell \text{ nonsplit multiplicative reduction}\\ 1 & \ell^2|N\end{cases}.$$

Define a modified Euler factor at p

$$\tilde{L}_p(E,1) := \begin{cases} L_p(E,1) & p \text{ split in } K\\ 1 - a_p(E)^2\frac{p-1}{p^2(p+1)} - \frac{1}{p^2} & p \text{ inert in } K\\ 1 - a_p(E)\frac{p-1}{p^2} - \frac{1}{p^2} & p \text{ ramified in } K\end{cases}.$$

Theorem 4.6. *Let E, E' be elliptic curves over $\mathbb{Q}$ with conductors N, N'. Suppose $E[p^r] \cong E'[p^r]$. Letting P be the Heegner point of conductor 1 when p is split in K, conductor p^2 when p is inert in K and conductor p when p is ramified in K ([9]), we have*

(4.5)

$$\left(\tilde{L}_p(E,1)\prod_{\ell|NN'/M} L_\ell(E,1)\right)\cdot\log_{\hat{E}}(P_E) \equiv \pm\left(\tilde{L}_p(E,1)\prod_{\ell|NN'/M} L_\ell(E',1)\right)\cdot\log_{\hat{E}'}(P_{E'}) \pmod{p^r}$$

where

$$M = \prod_{\ell|NN', a_\ell(E)\equiv a_\ell(E)' \bmod p^r} \ell^{\mathrm{ord}_\ell(NN')}.$$

Remark 4.7. Here, $P_E = \pi_E(y)$ where y is the H/K trace of the Heegner point on the modular curve $X_0(N)$ defined over the Hilbert class field H of $K = \mathbb{Q}(\sqrt{D})$ ($D < 0$), and $\pi_E : X_0(N) \to E$ is the modular parametrization.

Remark 4.8. Note that P does not necessarily lie in the analytic radius of convergence for $\log_{\hat{E}}$, and so $\log_{\hat{E}}(P)$ is not necessarily p-adically integral. However, $\log_{\hat{E}}([p\cdot L_p(E,1)]_E(P))$ converges if

$$p\nmid N.$$

This is because (from Silverman)

$$p\cdot L_p(E,1) = 1 + p - a_p(E) = \#E(\mathbb{F}_p),$$

and also from Silverman, we have

$$[E(\mathbb{Q}_p) : \hat{E}(p\mathbb{Z}_p)] = \#E(\mathbb{F}_p).$$

This last fact follows from the reduction modulo p exact sequence

$$0 \to \hat{E}(p\mathbb{Z}_p) \to E(\mathbb{Q}_p) \xrightarrow{\text{red}} E(\mathbb{F}_p) \to 0.$$

We always know that $P \in E(\mathbb{Q}_p)$, so

$$[p \cdot L_p(E,1)]_E(P) \in \hat{E}(p\mathbb{Z}_p),$$

and thus $\log_{\hat{E}}([p \cdot L_p(E,1)]_E(P)) \in p\mathcal{O}_{\mathbb{C}_p}$ makes sense. In the p split in K case of (4.5), we are thus comparing two elements of $\mathcal{O}_{\mathbb{C}_p}$: $\frac{1}{p}\log_{\hat{E}}([p \cdot L_p(E,1)]_E(P)) \cdots$ and $\frac{1}{p}\log_{\hat{E}'}([p \cdot L_p(E',1)]_{E'}(P)) \cdots$. When p is inert or ramified in K, similar reasoning combined with (2.3) also shows that both sides of (4.5) are elements of $\mathcal{O}_{\mathbb{C}_p}$.

Remark 4.9. Here is a nice observation for computationally verifying Theorem 1.2. Recall that $p = 2$ in this setting. By Honda's theorem, we can substitute $\log_{\hat{E}}(q)$ for $\sum_{n=1}^{\infty}\frac{a_n}{n}q^n$. Now note that if $q \in 2 \cdot \mathcal{O}_{\mathbb{C}_2}$ (which will be the case when we plug in $q = -x/y$ where (x,y) are the coordinates of $[2 \cdot L_2(E,1)]_E(P)$ where P is the Heegner point), then

$$\frac{1}{2}\sum_{n=1}^{\infty}\frac{a_n(E)}{n}q^n \equiv \frac{a_1(E)}{2}q + \frac{a_2(E)}{2^2}q^2 = \frac{1}{2}q + \frac{a_2(E)}{4}q^2 \pmod{2\mathcal{O}_{\mathbb{C}_2}}.$$

The same is true for E^d.

Remark 4.10. The sign $\pm$ in (4.5) appears because there is some sign ambiguity in defining the Heegner point on a given elliptic curve. In particular, the sign might be different for E and E'.

Remark 4.11. A heuristic for the identity (4.5) is that "log" is a p-adic substitute for the BSD L-value $L(E,1)$. $\rho_E \cong \rho_{E'} \pmod{p^r}$ (this means $E[p^r] \cong E'[p^r]$ as a $\mathrm{Gal}(\mathbb{Q})$-module), then we expect $L(E,1) \equiv L(E',1)$, because the Euler factors away from pNN' are congruent. I.e., pretend that $L(E,1)$ is a product of Euler factors $\left(1 - a_\ell(E)\ell^{-s} + \ell^{1-2s}\right)$ (the Euler factor of $L(E,s)$ at ℓ if $\ell \nmid N$). If $\ell || N$, then the Euler factor is $1 \mp \ell^{-s}$ for split/nonsplit multiplicative reduction, and is 1 if $\ell^2 | N$ i.e. additive reduction. Recall $\rho_E \equiv \rho_{E'} \pmod{p^r}$ implies $a_\ell(E) := \mathrm{Trace}_{\rho_E}(\mathrm{Frob}_\ell) \equiv \mathrm{Trace}_{\rho_{E'}}(\mathrm{Frob}_\ell) =: a_\ell(E') \pmod{p^r}$ if $\ell \nmid pNN'$. This congruence implies that the Euler factors of $L(E,1)$ and $L(E',1)$ at ℓ are congruent. However, the Euler product formula does not hold at $s = 1$.

Modularity (Wiles, Taylor-Wiles, et al.): Given $E/\mathbb{Q}$, the generating function $f_E(q)$ is actually a modular form (holomorphic function on $\mathcal{H}^+ = \{\mathrm{Im}(\tau) > 0\}$ with a $\Gamma_0(N)$-transformation property) of weight 2 and $L(E,s) = L(f_E,s)$.

Here, "(pNN')" is the stabilization operator we defined in Definition 2.1. Note: the actual $\log_E$ does not quite appear in the above Theorem. But when we plug in certain special points ("Heegner points") y into the above congruence, we will get a relation like

$$\log_E^{(pNN')}(y) = (\text{some "Euler-like factor"}) \cdot \log_E(y).$$

Another caveat is that in order to plug in y, we need y to belong to $\hat{E}_p^+$ and $\hat{E'}_p^+$, which by [18, Chapter VII] means that $y \pmod{p} = 0$. This might not always happen with Heegner points. Heegner points in general always belong to $E(\overline{\mathbb{Q}_p})$. Recall however, that if E has good reduction at p, we have an exact sequence ([18, Chapter VII])

$$0 \to \hat{E}_p^+(\mathbb{C}_p) \to E(\mathbb{C}_p) \xrightarrow{\text{red}} \tilde{E}(\overline{\mathbb{F}_p}) \to 0,$$

where $\tilde{E}$ is $E \pmod{p}$, third arrow is reduction map.

Remark 4.12. Note that by the above exact sequence, multiplying anything in $E(\mathbb{C}_p)$ by $[\#\tilde{E}(\overline{\mathbb{F}_p})]_E$ (in the group law on E) results in something in $\hat{E}_p^+(\mathbb{C}_p)$. So precomposing both sides of (4.3) with $[\#\tilde{E}(\overline{\mathbb{F}_p})]_E$, we do get a congruence of functions $E(\mathbb{C}_p)$.

5. Appendix: Chebotarev density

For a finite Galois group G, we give G the discrete topology (every element is an open set).

Recall that for almost all ℓ (i.e. those primes which are unramified), the Frobenius element $\mathrm{Frob}_\ell \in G$ (more precisely, a conjugacy class) is well-defined. We have the following extremely important theorem.

Theorem 5.1 (Chebotarev)**.** *Let $X \subset G$ be a conjugation-invariant subset. Then the density of primes ℓ such that $\mathrm{Frob}_\ell \in X$ is equal to $\#X/\#G$.*

Corollary 5.2. *$\{\mathrm{Frob}_\ell\}_\ell \subset G$ is dense.*

Proof. From the fact that $\{\mathrm{Frob}_\ell\}_\ell$ is conjugation-invariant, which along with the Chebotarev density theorem implies that every element of G is Frob_ℓ for some ℓ, we can deduce that $\{Frob_\ell\}_\ell$ is dense. □

6. Example of Thereom 1.2

We consider the elliptic curve

$$E = 37a2 : y^2 + y = x^3 - x.$$

The curve is rank one, with conductor $N = 37$. The field

$$K = \mathbb{Q}(\sqrt{-7})$$

satisfies the Heegner hypothesis.

This gives a Heegner point of $P = (0, 0)$ with $|E(\mathbb{F}_2)| = 5$ and $5P = (1/4, -5/8)$ giving $t = \frac{-x(5P)}{y(5P)} = \frac{2}{5}$.

Consider a quadratic twist by $d = 53$. We use the following code to compute the left-hand side of 1.3:

```
y = E.heegner_point(D)
p1 = y.point_exact() * E.base_extend(GF(2)).cardinality()
z = -p1[0]/p1[1]
L_2 = (E.reduction(2).cardinality())/2
Ll = 1
for l in range(1, d+1):
    if ZZ(l).is_prime() and d%l == 0:
      Ll *= (E.reduction(l).cardinality())/l
logMod2 = 0
modular_form = E.anlist(10)
for i in range(1, 9):
  logMod2 += modular_form[i] * z**i/ (i)
print(L_2 *Ll * logMod2)
```

This returns that

$$L_2(E, 1) \cdot \prod_{l|d} L_\ell(E, 1) \cdot \log_{\hat{E}}(P_E) \equiv 1 \pmod 2.$$

For the right hand side, we can compute

```
Ed = EllipticCurve('37a1').quadratic_twist(53)
D = -7
y = Ed.heegner_point(D)
p1 = y.point_exact(150) * Ed.base_extend(GF(2)).cardinality()
z = -p1[0]/p1[1]
L_2 = (Ed.reduction(2).cardinality())/2
logMod2 = 0
modular_form = Ed.anlist(10)
for i in range(1, 9):
  logMod2 += modular_form[i] * z**i/ (i)
print(L_2 * logMod2 % 2)
```

As expected, both sides are congruent to 1 (mod 2), so we conclude that P_E and P_{E^d} are both nontorsion, and thus E, E^d both have analytic and arithmtic rank 1.

7. Acknowledgments

We would like to thank the MIT PRIMES-USA program for making this paper possible.

References

[1] B. Birch, P. Swinnerton-Dyer, *Notes on Elliptic Curves (II)*, J. Reine Angew. Math. 165 (218): 79-108.
[2] R. Brauer, C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2) 42, (1941). 556-590.
[3] C. Breuil; B. Conrad; F. Diamond; R. Taylor (2001), *On the modularity of elliptic curves over Q: wild 3-adic exercises*, Journal of the American Mathematical Society, 14 (4): 843–939
[4] H. Davenport, *Multiplicative Number Theory*. Springer New York, 2000.
[5] F. Diamond and J. M. Shurman, *A first course in modular forms*. New York: Springer, 2005.
[6] F. Brunault, *On the ramification of modular parametrizations at the cusps*. Journal de Théorie des Nombres de Bordeaux 28 (2016), 773–790.
[7] A. Corbett, A. Saha, *On the order of vanishing of newforms at cusps*. Math. Res. Lett. Volume 25, Number 6, 1771–1804, 2018
[8] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, II. Proc. Roy. Soc. London Ser. A, 322(1551):405 420, 1971.
[9] B. Gross, *Heegner points on X0(N)*, In Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87 105. Horwood, Chichester, 1984.
[10] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., 84(2): 225-320, 1986.
[11] T. Honda, *Formal groups and zeta functions*. Osaka J. Math., 5 (1968), 199–213.
[12] V. Kolyvagin, *Euler systems*, in: The Grothendieck Festschift (Vol. II), P. Cartier et al., eds., Prog. in Math 87, Boston: Birkhäuser (1990) 435-483.
[13] D. Kriz, C. Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum of Mathematics, Sigma, Volume 7, 2019, e15.
[14] Y. Morita, *On potential good reduction of abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. I A Math. 22 (1975), no. 3, pp. 437-447.
[15] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc., 104(1):20 24, 1988.
[16] E. Shen and K. Wu, *Eisenstein congruences between logarithms of Heegner points*, in preparation.
[17] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo.
[18] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2nd edition, 2009.
[19] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, Cham, 2nd edition, 2015.
[20] H. Taya, *Iwasawa invariants and class numbers of quadratic fields for the prime 3*, Proc. Amer. Math. Soc., 128(5):1285 1292, 2000.
[21] R. Taylor; A. Wiles (1995), *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics, Second Series, 141 (3): 553–572.
[22] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics, Second Series, 141 (3): 443–551.