THE IWASAWA μ-INVARIANT OF CERTAIN ELLIPTIC CURVES OF ANALYTIC RANK ZERO

ADITHYA CHAKRAVARTHY

ABSTRACT. This paper is about the Iwasawa theory of elliptic curves over the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_{\mathrm{cyc}}$ of $\mathbf{Q}$. We discuss a deep conjecture of Greenberg that if $E/\mathbf{Q}$ is an elliptic curve with good ordinary reduction at p, and $E[p]$ is irreducible as a Galois module, then the Selmer group of E over $\mathbf{Q}_{\mathrm{cyc}}$ has μ-invariant zero. We prove new cases of Greenberg's conjecture for some elliptic curves of analytic rank 0. The proof involves studying the p-adic L-function of E. The crucial input is a new technique using the Rankin-Selberg method.

1. INTRODUCTION

We begin with a fundamental theorem of Iwasawa, which serves as the starting point of Iwasawa theory. Let K be a number field and let K_∞/K be a $\mathbf{Z}_p$-extension: a Galois extension with Galois group isomorphic to the additive group $\mathbf{Z}_p$ of p-adic integers. For each integer $n > 0$ there is a unique subfield K_n of K_∞ of degree p^n over K. Iwasawa proved the following now famous theorem about the growth of class numbers in such towers.

Theorem (Iwasawa). *Let K be a number field and let K_∞/K be a $\mathbf{Z}_p$ extension with layers K_n. Suppose that p^{e_n} is the exact power of p dividing the class number of K_n. Then there exist integers μ, λ, ν such that*

$$e_n = \mu p^n + \lambda n + \nu$$

for all sufficiently large values of n.

The most important example of a $\mathbf{Z}_p$-extension of K is the so-called *cyclotomic $\mathbf{Z}_p$-extension* of K, denoted K^{cyc}/K. It is defined by letting K^{cyc} be the appropriate subfield of $\cup_{n\geq 1} K(\zeta_{p^n})$. Iwasawa has conjectured the following about the cyclotomic $\mathbf{Z}_p$-extension.

Conjecture 1.1 (Iwasawa's $\mu = 0$ Conjecture). *Let K be a number field and let K^{cyc} be the cyclotomic $\mathbf{Z}_p$ extension of K. Then $\mu = 0$.*

This conjecture is probably the deepest open problem from classical Iwasawa theory. The only progress towards this comes from a paper of Ferrero and Washington [FW79], where they prove the conjecture in the case when $K/\mathbf{Q}$ is abelian. Other than this, the conjecture remains wide open and it seems intractable at present.

This paper is about a generalization of Iwasawa's $\mu = 0$ conjecture to the Iwasawa theory of *elliptic curves*. We now briefly outline the main aspects of the Iwasawa theory of elliptic curves and then state the analogue of Iwasawa's $\mu = 0$ conjecture in this context. In a landmark paper [Maz72], Mazur observed that many features of classical Iwasawa theory could be used to study elliptic curves. This initiated the study of what we now call the Iwasawa theory of elliptic curves. If E is an elliptic curve over a number field K, let $\text{Ш}(E/K)[p^\infty]$ denote the p-primary part of the

Tate-Shafarevich group of E over K. We then have the following analogue [Gre99, Theorem 1.10] of Iwasawa's theorem.

Theorem. *Let* $\mathbf{Q}^{cyc} = \cup \mathbf{Q}_n$ *denote the cyclotomic* $\mathbf{Z}_p$ *extension of* $\mathbf{Q}$. *Let* $E/\mathbf{Q}$ *be an elliptic curve, and let* p *be a prime of good ordinary reduction. Assume that* $\text{Ш}(E/\mathbf{Q}_n)[p^\infty]$ *is finite for all* n *and let* p^{e_n} *be the exact power of* p *dividing* $|\text{Ш}(E/\mathbf{Q}_n)[p^\infty]|$. *Then there exist integers* μ, λ, ν *such that*

$$e_n = \mu p^n + \lambda n + \nu$$

for all sufficiently large values of n.

The quantity $\mu_p(E)$ in the above formula is called the μ-*invariant* of E over $\mathbf{Q}^{\text{cyc}}$. (See Section 2 for a more abstract definition of $\mu_p(E)$.) In analogy with Iwasawa's $\mu = 0$ conjecture for class groups, one might expect that $\mu_p(E)$ always vanishes. This turns out to be *false*. Indeed, Mazur [Maz72] discovered that the elliptic curve $X_0(11)$ has a nonzero μ-invariant at the prime $p = 5$. However, in a beautiful paper [Gre99, Conjecture 1.11], Greenberg conjectures that one can rescue Iwasawa's conjecture in the following sense:

Conjecture 1.2. *Let* $E/\mathbf{Q}$ *be an elliptic curve, let* p *be an odd prime of good ordinary reduction. Then there is a* $\mathbf{Q}$-*isogenous curve* E' *such that* $\mu_p(E') = 0$.

That is, Greenberg predicts that μ can be made zero after perhaps shifting by an isogeny. In particular, the above conjecture implies:

Conjecture 1.3 (Greenberg's $\mu = 0$ Conjecture). *Let* $E/\mathbf{Q}$ *be an elliptic curve, and let* p *be an odd prime of good ordinary reduction. If* $E[p]$ *is irreducible as a Galois module, then* $\mu_p(E) = 0$.

Remark 1.4. *It is known by the work of Drinen* [Dri03] *that this conjecture is false over general number fields. So it applies particularly for curves* E *over* $\mathbf{Q}$.

Remark 1.5. *Schneider has given a simple formula for the effect of an isogeny on the* μ-*invariant of* E *for odd* p *(see* [Sch87, Isogeny Formula, Second Form]*). Thus, Greenberg's conjecture effectively predicts the* μ-*invariant of any elliptic curve over* $\mathbf{Q}$.

Greenberg's conjecture bifurcates into two cases, one of which seems to be much harder than the other. First, there is the case where $E[p]$ is reducible as a Galois module (the "reducible case") and second, there is the case where $E[p]$ is irreducible as a Galois module (the "irreducible case"). Most of the progress to date has been in the *reducible* case, where we have the following theorem [GV00, Theorem 1.3] of Greenberg and Vatsal: if $E[p]$ has a $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-submodule which is either ramified at p and even, or unramified at p and odd, then $\mu_p(E) = 0$. This theorem follows from a bootstrapping of the Ferrero-Washington Theorem. This result was furthered by Trifkovic [Tri05], who showed that Greenberg's conjecture was true for infinitely many curves E with $E[p]$ reducible, for $p = 3$ or 5. The core strategy in Trifkovic's paper was an explicit evaluation of the global duality pairing for finite flat group schemes over rings of integers.

There has also been progress in proving that "$\mu = 0$" can be propagated in families of modular forms. In a beautiful paper, Emerton-Pollack-Weston [EPW06], showed that "$\mu = 0$" is invariant in Hida families. That is, if f is a modular form with $\mu = 0$, then that implies that every form in the Hida family passing through f also has $\mu = 0$. On another front, Ray recently [Ray24] showed the following result for $p = 5$: there is a positive proportion of elliptic curves $E/\mathbf{Q}$ for which $\mu_5(E) = \lambda_5(E) = 0$. Ray uses results of Bhargava-Shankar [BS13] on average ranks of Selmer groups. In another paper, Ray [Ray23] also showed that if $E[p]$ is irreducible, if the classical

Iwasawa μ-invariant vanishes for the splitting field $\mathbf{Q}(E[p])$, and a purely Galois theoretic condition on $E[p]$ holds, Greenberg's conjecture should hold.

The irreducible case of Greenberg's conjecture, however, remains unsolved in general. In this paper, we prove new results about the irreducible case of Greenberg's Conjecture, specifically for some elliptic curves with analytic rank 0:

Theorem 1.6. *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N. Let p be a prime of good ordinary reduction. Assume:*

(1) $L(E/K, 1) \neq 0$, where $K = \mathbf{Q}(\sqrt{-N})$ and $L(E/K, s)$ denotes the Hasse-Weil L-series of E over K,

(2) $p > 100\sqrt{N}(\log N + 5)m_E$, where m_E denotes the modular degree of E,

(3) p does not divide the the Manin constant of E,

(4) p is not anomalous for E, i.e: p does not divide $\#E(\mathbf{F}_p)$,

(5) N is a prime congruent to 3 modulo 4.

Then $\mu_p(E) = 0$ and $\lambda_p(E) = 0$.

The following are well-known consequences:

Corollary 1.7. *Keep the notations and assumptions as above. Let $\mathbf{Q}_{cyc}$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ and let $\mathbf{Q}_n$ denote the n-th layer of $\mathbf{Q}_{cyc}$. Then:*

(1) the Mordell-Weil rank of $E(\mathbf{Q}_n)$ is zero for all $n \geq 1$, and

(2) the p-primary part of $\text{Ш}(E/\mathbf{Q})$ vanishes.

1.1. **Examples.** Let $E_1 = \texttt{11a1}$ be the elliptic curve of conductor 11. We show in the final section of the paper that $L(E_1/\mathbf{Q}(\sqrt{-11}), 1) \neq 0$. Theorem 1.6 says that if $p > 100\sqrt{N}(\log N + 5) m_E \approx 2453.604\ldots$ is a good ordinary prime, then $\mu_p(E_1) = \lambda(E_1) = 0$. Furthermore, we have $\text{Ш}(E/\mathbf{Q})[p^\infty] = 0$ and the rank of E over $\mathbf{Q}_n$ is zero for all $n \geq 1$.

As another example, let $E_2 = \texttt{67a1}$ be the elliptic curve of conductor 67. We show in the final section of the paper that $L(E_2/\mathbf{Q}(\sqrt{-67}), 1) \neq 0$. If $p > 100\sqrt{N}(\log N + 5)m_E \approx 37671.828\ldots$ is a good ordinary prime which is not anomalous for E_2, then $\mu_p(E_2) = \lambda_p(E_2) = 0$. Furthermore, we have $\text{Ш}(E_2/\mathbf{Q})[p^\infty] = 0$ and the rank of E_2 over $\mathbf{Q}_n$ is zero for all $n \geq 1$.

However, some lower bound on p is necessary. Indeed, consider the elliptic curve $E_3 = \texttt{24691a1}$ and $p = 5$. From the LMFDB [LMF24], the analytic order of $\text{Ш}(E_3/\mathbf{Q})$ is 25. So the conclusion of Corollary 1.7 is false in this case. That being said, it should definitely be possible to improve the bound $p \geq 100\sqrt{N}(\log N + 5) m_E$ in Theorem 1.6, but we have not attempted to do so here.

1.2. **Strategy.** Using results of Kato on the Iwasawa main conjecture, it is known that in order to prove that $\mu_p(E) = \lambda_p(E) = 0$, it suffices to show that the p-adic L-function of E is a unit. One knows that if p is not anomalous and that p does not divide $L(E, 1)/\Omega_E$, then the p-adic L-function is a unit. So as long as one avoids the finitely many prime divisors of $L(E, 1)/\Omega_E$ (and the anomalous primes), then we have $\mu_p(E) = 0$ and $\lambda_p(E) = 0$. But a priori, one has no idea what primes divide $L(E, 1)/\Omega_E$. The main point of this paper is to give an *explicit upper bound* for which primes divide $L(E, 1)/\Omega_E$. This is roughly the statement of Theorem 2.2. We prove Theorem 2.2 using the Rankin-Selberg method.

Remark 1.8. *In proving Theorem 1.6, we actually show Greenberg's Conjecture both for E and the quadratic twist $E^{(-N)}$ by $-N$.*

1.3. **Outline.** In the first section, we explain the Iwasawa main conjecture. We then reduce Theorem 1.6 to Theorem 2.2, which is purely a statement about L-values of modular forms. In the next section, we explain the Rankin-Selberg method. In the section after that, we prove Theorem 2.2. Finally in the last section, we give numerical examples that use the Rankin-Selberg method to calculate Iwasawa invariants.

1.4. **Acknowledgements.** I would like to thank Kumar Murty and members of the GANITA lab for their constant support. I would also like to thank Debanjana Kundu for teaching me Iwasawa theory, for suggesting this problem to me, and for her mentorship. I would also like to thank Antonio Lei and Robert Pollack for providing helpful comments on a preliminary draft of this paper and for suggesting further applications.

2. Preliminaries

In this section, p will denote an odd prime and $E/\mathbf{Q}$ will be an elliptic curve with good ordinary reduction at p. Let $\mathbf{Q}^{\mathrm{cyc}}$ denote the cyclotomic $\mathbf{Z}_p$ extension of $\mathbf{Q}$.

To fix notation, we briefly summarize some facts about the Iwasawa main conjecture for elliptic curves. We will first summarize the objects on the algebraic side of the main conjecture, then summarize the objects on the analytic side, and then state the Iwasawa main conjecture which bridges these two worlds.

The algebraic side. For any algebraic extension $K/\mathbf{Q}$, the Selmer group of E over K is a certain subgroup of $H^1(G_K, E(\overline{\mathbf{Q}})_{\mathrm{tors}})$, where $G_K = \mathrm{Gal}(\overline{K}/K)$. The Selmer group fits into the fundamental exact sequence

$$0 \to E(K) \otimes \mathbf{Q}/\mathbf{Z} \to \mathrm{Sel}(E/K) \to \mathrm{III}(E/K) \to 0$$

where $\mathrm{III}(E/K)$ denotes the Tate-Shafarevich group of E over K. Let $K = \mathbf{Q}^{\mathrm{cyc}}$. Then we can consider the Selmer group $\mathrm{Sel}(E/\mathbf{Q}^{\mathrm{cyc}})$, and this has an action of $\Gamma = \mathrm{Gal}(\mathbf{Q}^{\mathrm{cyc}}/\mathbf{Q})$. Its p-primary subgroup $\mathrm{Sel}(E/\mathbf{Q}^{\mathrm{cyc}})_p$ can be regarded as a Λ-module, where $\Lambda = \mathbf{Z}_p[\![T]\!]$. This ring Λ is called the *Iwasawa algebra*. It is now known from the deep work of Kato [Kat04] that the Pontryagin dual $X(E/\mathbf{Q}^{\mathrm{cyc}}) = \mathrm{Sel}(E/\mathbf{Q}^{\mathrm{cyc}})_p^\vee$ is a finitely generated *torsion* Λ-module. Therefore the structure theorem of finitely generated Λ-modules (see for example [Was97, Theorem 13.12]) says that one has a pseudo-isomorphism

$$X(E/\mathbf{Q}^{\mathrm{cyc}}) \sim \left(\oplus_{i=1}^n \Lambda/(f_i(T)^{a_i}) \right) \oplus \left(\oplus_{j=1}^m \Lambda/(p^{\mu_j}) \right),$$

where the $f_i(T)$'s are irreducible distinguished polynomials[1] in Λ. One can then define the algebraic Iwasawa invariants by

$$\lambda_E^{\mathrm{alg}} = \sum_{i=1}^n a_i \deg(f_i(T)), \qquad \text{and} \qquad \mu_p^{\mathrm{alg}}(E) = \sum_{j=0}^m \mu_j.$$

The *characteristic ideal* of $X(E/\mathbf{Q}^{\mathrm{cyc}})$ is the ideal of Λ generated by $p^\mu f_1(T)^{a_1} \ldots f_n(T)^{a_n}$.

---

[1]A polynomial $f(T)$ is *distinguished* if when you reduce f modulo p, only the highest degree term remains.

The analytic side. For an elliptic curve $E/\mathbf{Q}$ with good ordinary reduction at a prime p and χ an even Dirichlet character, denote by $L(E, \chi, s)$ the Hasse Weil L-function of E twisted by χ. Let $H_1(E(\mathbf{C}), \mathbf{Z})^{\pm}$ be the eigenspaces under complex conjugation, and let $\Lambda_E^{\pm}$ be the respective generators of these spaces over $\mathbf{Z}$. The periods Ω_E^+ and Ω_E^- are defined by

$$\Omega_E^{\pm} = \int_{\Lambda_E^{\pm}} \omega_E,$$

where ω_E is the invariant differential of E. We may assume that Ω_E^+ and $i\Omega_E^-$ are real positive. It is known by the work of Shimura that $L(E, \chi, 1)/\Omega_E^{\chi(-1)}$, *a priori* a transcendental number, is in fact an *algebraic* number. Mazur and Swinnterton-Dyer have attached to E a p-adic L-function $\mathcal{L}_p(E/\mathbf{Q}, T) \in \Lambda \otimes \mathbf{Q}_p$ satisfying the following interpolation properties. If we write $a_p = (p+1) - \#E(\mathbf{F}_p)$, consider the Hecke polynomial $X^2 - a_p X + p$. Let $\alpha \in \mathbf{Z}_p^{\times}$ denote this unique p-adic unit root of the Hecke polynomial. Then,

$$\tag{1} \mathcal{L}_p(E/\mathbf{Q}, 0) = \left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{L(E, 1)}{\Omega_E^+}.$$

Let χ be an even Dirichlet character of conductor p^n and p-power order. Then,

$$\mathcal{L}_p(E/\mathbf{Q}, \chi(1+p) - 1) = \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{g(\chi^{-1})} \frac{L(E, \chi^{-1}, 1)}{\Omega_E^+}.$$

Using the Weierstrauss preparation theorem [Was97, Theorem 7.3], we can define the analytic invariants $\mu_p^{\mathrm{an}}(E)$ and λ_E^{an} by writing:

$$\mathcal{L}_p(E/\mathbf{Q}, T) = p^{\mu_p^{\mathrm{an}}(E)} \cdot u(T) \cdot f(T)$$

where $f(T)$ is a distinguished polynomial of degree λ_E^{an} and $u(T)$ is a unit in Λ. It is known (see [SW13, Proposition 3.7]) that if $E/\mathbf{Q}$ has good ordinary reduction at an *odd* prime p, and that $E[p]$ is irreducible as a Galois module, then $\mu_p^{\mathrm{an}}(E) \geq 0$. In other words, $\mathcal{L}_p(E/\mathbf{Q}, T) \in \Lambda$.

Iwasawa Main Conjecture. The Iwasawa *main conjecture* relates the Selmer group on the algebraic side to the p-adic L-function on the analytic side. Precisely, suppose that $E/\mathbf{Q}$ is an elliptic curve with good ordinary reduction at an *odd* prime p, and that $E[p]$ is irreducible as a Galois module. Then on the algebraic side, we can look at the characteristic ideal of the p-primary Selmer group $X(E/\mathbf{Q}^{\mathrm{cyc}})$; this is an ideal in Λ. On the analytic side, we can attach to E a p-adic L-function $\mathcal{L}_p(E/\mathbf{Q}, T) \in \Lambda$. The *main conjecture* asserts that the characteristic ideal of the p-primary Selmer group $X(E/\mathbf{Q}^{\mathrm{cyc}})$ is generated by $\mathcal{L}_p(E/\mathbf{Q}, T)$ in Λ. In particular, it implies that $\mu_E^{\mathrm{alg}} = \mu_E^{\mathrm{an}}$ and $\lambda_E^{\mathrm{alg}} = \lambda_E^{\mathrm{an}}$. Kato [Kat04] has proven a deep result on one divisibility of the main conjecture, which is the starting point of our proof.

Theorem 2.1 (Kato). *Let $E/\mathbf{Q}$ be an elliptic curve, and let $p \geq 5$ be a prime of good ordinary reduction. Suppose that the mod p Galois representation $\overline{\rho_{E,p}} : G_{\mathbf{Q}} \to GL_2(\mathbf{F}_p)$ is surjective. Then the characteristic ideal of $X(E/\mathbf{Q}^{cyc})$ divides the ideal generated by $\mathcal{L}_p(E/\mathbf{Q}, T)$ in Λ. In particular, $\mu_E^{alg} \leq \mu_E^{an}$ and $\lambda_E^{alg} \leq \lambda_E^{an}$.*

2.1. **Modular Forms.** For the rest of the paper, fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p}$. Kato's Theorem shows that to prove $\mu_p^{\mathrm{alg}}(E) = \lambda_p^{\mathrm{alg}}(E) = 0$, it suffices to show that $\mu_p^{\mathrm{an}}(E) = \lambda_p^{\mathrm{an}}(E) = 0$. This is equivalent to showing that the constant term of $\mathcal{L}_p(E/\mathbf{Q}, T)$ is nonzero mod p; by (1), this means

$$\left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{L(E, 1)}{\Omega_E^+} \not\equiv 0 \mod p.$$

(Note that we are viewing $L(E, 1)/\Omega_E^+$ as an element of $\overline{\mathbf{Q}_p}$ via our fixed emebedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p}$.) This is really a problem about modular forms, not elliptic curves. To see this, let $f \in S_2(\Gamma_0(N))$ be the newform associated to E by modularity. Then we have an equality of L-functions: $L(E, s) = L(f, s)$. Define the Petersson norm of f as follows:

$$\langle f, f \rangle = \int_{\Gamma_0(N) \backslash \mathbf{H}} |f|^2 dx \, dy.$$

An elliptic curve $E/\mathbf{Q}$ is *optimal* if the map $H_1(X_0(N)(\mathbf{C}), \mathbf{Z}) \to H_1(E(\mathbf{C}), \mathbf{Z})$ is surjective. (See [Ste89]). We will derive Theorem 1.6 from:

Theorem 2.2. *Let N be a prime and let $f \in S_2(\Gamma_0(N))$ be a weight 2 newform with rational Fourier coefficients. Let p be an odd prime. Assume that*

- *(1) N is congruent to 3 modulo 4,*
- *(2) $L(f, 1)L(f, \chi, 1) \neq 0$, where χ is the unique quadratic character mod N, and*
- *(3) $p > 100\sqrt{N}(\log N + 5) \deg \pi_E$, where E is an optimal elliptic curve in the isogeny class corresponding to f.*

Then p does not divide $\dfrac{L(f, 1) \, L(f, \chi, 1)}{\pi^2 \langle f, f \rangle} \dfrac{g(\chi)}{i}$.

Proof of Theorem 2.2 $\implies$ Theorem 1.6. Let $E/\mathbf{Q}$ be an elliptic curve of conductor N as in Theorem 1.6. There exists a modular parametrization $\pi_E : X_0(N) \to E$ that is a surjective morphism over $\mathbf{Q}$. Let c_E be the Manin constant of E, that is, the number such that

$$\pi_E^*(\omega_E) = c_E \cdot 2\pi i f(z) dz,$$

where ω_E is the invariant differential on E and $f \in S_2(\Gamma_0(N))$ is the modular form attached to E. Let $m_E = \deg \pi_E$ denote the modular degree of E. We have

$$(2) \qquad \Omega_E^+ \Omega_E^- = \int_{E(\mathbf{C})} \omega_E \wedge \overline{\omega_E} = \frac{4\pi^2 c_E^2}{m_E} \langle f, f \rangle,$$

where $\Omega_E^\pm$ are the real and imaginary Neron periods of E. Recall that we have assumed in Theorem 1.6 that p does not divide m_E or c_E, and that $p > 100\sqrt{N}(\log N + 5)m_E$. Therefore, the assumptions of Theorem 2.2 are satisfied. We conclude that p does not divide

$$\frac{L(E, 1)}{\Omega_E^+} \cdot \frac{L(E, \chi, 1)}{\Omega_E^-} \frac{g(\chi)}{i}.$$

It follows that p does not divide $L(E, 1)/\Omega_E^+$. By the interpolation property (1) of the p-adic L-function of E, if p is not anomalous for E, we conclude that the constant term of $\mathcal{L}_p(E, T)$ is a p-adic unit and hence the analytic μ and λ-invariants of E vanish. Kato's Theorem implies that the algebraic μ and λ-invariants of E vanish as well. This proves Theorem 1.6. $\qquad \square$

Remark 2.3. *Theorem 2.2 works equally well in the supersingular case and the ordinary case. In the supersingular case, Kurihara [Kur02] has proven an explicit growth formula for the Tate Shafarevich group in the cyclotomic tower, assuming that p does not divide $L(E,1)/\Omega_E$. Theorem 2.2 gives an explicit upper bound for which primes divide $L(E,1)/\Omega_E$, which in turn gives an upper bound for primes p for which where Kurihara's theorem applies. (We thank Robert Pollack for pointing out this application to us.)*

3. Rankin-Selberg Method

The rest of the paper is devoted to proving Theorem 2.2. The proof of Theorem 2.2 was catalyzed by reading Shimura's [Shi76] paper on the Rankin-Selberg method, which we now explain.

Let $N \geq 1$ be an integer and let ω be an odd Dirichlet character modulo N. Put

$$G_\omega(\tau, s) = \frac{N}{-4\pi i g(\omega)} \sum_{(m,n)\in \mathbf{Z}^2\setminus(0,0)} \frac{\omega(n)}{(mN\tau + n)|mN\tau + n|^{2s}},$$

where $g(\omega)$ is the Gauss sum. This function has a meromorphic continuation to all $s \in \mathbf{C}$ (see [Shi76, Page 788] and the references therein) and it is holomorphic at $s = 0$. Thus we can set

$$G_\omega(\tau) := G_\omega(\tau, 0).$$

By [Shi76, Page 788], the function $G_\omega(\tau)$ belongs to $M_1(\Gamma_0(N), \omega)$. If ω is *primitive*, by [Shi76, Equation (3.4)], we have the Fourier expansion[2]

$$(3) \qquad G_\omega(\tau) = \frac{L(0, \omega)}{2} + \sum_{n=1}^{\infty} \left(\sum_{d|n} \omega(d) \right) q^n.$$

Let us now fix an element $f \in S_2(\Gamma_0(N))$ and an element $g \in M_1(\Gamma_0(N), \omega)$, where ω is a Dirichlet character modulo N. Suppose that they have Fourier expansions

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad g(\tau) = \sum_{n=0}^{\infty} b_n q^n.$$

Then we put

$$L(s, f \times g) := L(2s-1, \omega) \sum_{n=1}^{\infty} \frac{a_n b_n}{n^s},$$

where $L(s, \omega)$ is the usual Dirichlet L-function attached to ω. The L-function $L(s, f \times g)$ is called the *Rankin-Selberg convolution L-function*[3] of f and g. For an integer $M \geq 1$ and modular forms $g \in S_k(\Gamma_0(M))$ and $h \in M_k(\Gamma_0(M))$, define the Petersson inner product as

$$\langle g, h \rangle := \int_{\Gamma_0(M)\backslash \mathbf{H}} \overline{g(\tau)} h(\tau) y^{k-2} \, dx \, dy.$$

Then by [Shi76, Equation (2.4)], we have

$$(4) \qquad \langle f, g \cdot G_{\overline{\omega}} \rangle = L(1, f \times g) \frac{g(\overline{\omega})}{8\pi^2 i},$$

where $g(\overline{\omega})$ is the Gauss sum. To determine the form g, we need the following

---

[2]Shimura expresses the constant term of $G_\omega(\tau)$ in terms of the value $L(1, \omega)$, whereas we have applied the functional equation for $L(s, \omega)$ to express the constant term in terms of the value $L(0, \omega)$.

[3]Shimura uses the notation $D(s, f, g)$ instead of the now more standard $L(s, f \times g)$.

Proposition 3.1. *Let χ, ψ be primitive Dirichlet characters modulo M_1 and M_2, respectively, such that $\chi\psi(-1) = -1$. There exists an element $G_{\chi,\psi} = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{E}_1(\Gamma_0(M_1 M_2), \chi\psi)(= \text{space of weight } 1 \text{ Eisenstein series for } \Gamma_0(M_1 M_2) \text{ and nebentypus } \chi\psi) \text{ such that}*

$$a_n = \sum_{d|n} \chi(d)\psi(n/d), \qquad n \geq 1$$

and

$$a_0 = \begin{cases} 0 & \text{if both } \chi, \psi \text{ are non-trivial,} \\ \dfrac{L(0, \chi\psi)}{2} & \text{otherwise.} \end{cases}$$

Proof. See for example [Miy06, Theorem 4.7.1]. $\qquad\square$

Now suppose that $f \in S_2(\Gamma_0(N))$ is a newform. Let χ, ψ be Dirichlet characters such that $\chi\psi(-1) = -1$. By [Shi76, Equation (4.3)], we have

$$(5) \qquad\qquad L(1, f \times G_{\chi,\psi}) = L(f, \chi, 1)L(f, \psi, 1),$$

where $G_{\chi,\psi}$ is the function from Proposition 3.1 above. Combining (4) and (5) and dividing through by $\langle f, f \rangle$, we obtain the main result of this section:

Proposition 3.2. *Let $N \geq 1$ be an integer and let $f \in S_2(\Gamma_0(N))$ be a newform. Let χ, ψ be primitive Dirichlet characters such that $\chi\psi(-1) = -1$. Then:*

$$\frac{\langle f, G_{\chi,\psi} \cdot G_{\overline{\chi\psi}} \rangle}{\langle f, f \rangle} = \frac{L(f, \chi, 1)L(f, \psi, 1)}{\langle f, f \rangle} \cdot \frac{g(\overline{\chi\psi})}{8\pi^2 i},$$

where $g(\overline{\chi\psi})$ denotes the Gauss sum.

4. Proof of Theorem 2.2

We first need two preliminary results.

Proposition 4.1. *Let N be an odd integer. Let χ be an odd primitive quadratic character of conductor N. Then*

$$L(0, \chi) \leq \frac{\sqrt{N}}{2\pi}(\log N + 5).$$

Proof. In [Ram01, Corollary 2], Ramaré proves the following bound for odd primitive characters χ modulo odd N:

$$(6) \qquad\qquad |(1 - \chi(2)/2)L(1, \chi)| \leq \frac{1}{4}(\log N + 5).$$

(Note that Ramaré does not require χ to be quadratic.) The functional equation for $L(s, \chi)$ gives

$$L(0, \chi) = \frac{g(\chi)}{i\pi}L(1, \chi).$$

Since $|g(\chi)| = \sqrt{N}$ for χ quadratic, (6) gives us

$$L(0, \chi) \leq \frac{\sqrt{N}}{2\pi}(\log N + 5 - 2\log(3/2)) \leq \frac{\sqrt{N}}{2\pi}(\log N + 5),$$

which completes the proof. $\qquad\square$

Next we show that algebraic L-values have bounded denominators. An elliptic curve $E/\mathbf{Q}$ is *optimal* if the map $H_1(X_0(N)(\mathbf{C}), \mathbf{Z}) \to H_1(E(\mathbf{C}), \mathbf{Z})$ is surjective.

Proposition 4.2. *Let N be a prime which is 3 mod 4. Let $f \in S_2(\Gamma_0(N))$ be a newform and let χ be an odd quadratic character mod N. Assume that $L(f,1) L(f,\chi,1) \neq 0$. Then the rational number*

$$(7) \qquad \frac{L(f,1) L(f,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} \frac{g(\chi)}{i}$$

has denominator $\leq 576 m_E$, where E is an optimal curve in the isogeny class of f and m_E denotes the modular degree of E.

The proof of Proposition 4.2 has a distinct thread from the rest of the proof so we prove it in the next section.

We are now ready to prove Theorem 2.2. Let N be a prime which is 3 mod 4. Let χ be the unique quadratic character mod N. Since $N \equiv 3$ mod 4, the character χ is odd. From Proposition 3.2, we have the identity:

$$(8) \qquad G_{1,\chi} \cdot G_{\overline{\chi}} = cE + \sum_j \left(\frac{L(f_j,1) L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} \frac{g(\chi)}{i} \right) f_j,$$

where the sum runs over all newforms $f_j \in S_2(\Gamma_0(N))$ and $E = \dfrac{N-1}{12} + q + \cdots \in \mathcal{E}_2(\Gamma_0(N))$ is the unique normalized Eisenstein series and $c \in \mathbf{C}$ is a constant. Looking at the first Fourier coefficient (i.e: the coefficient of q) on each side, we obtain:

$$L(0,\chi) = c + \sum_j \frac{L(f_j,1) L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} \frac{g(\chi)}{i}.$$

It is classical that $g(\chi) = i\sqrt{N}$. Dividing both sides by $g(\chi)/i = \sqrt{N}$ and rearranging, we obtain:

$$(9) \qquad \frac{L(0,\chi) - c}{\sqrt{N}} = \sum_j \frac{L(f_j,1) L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle}.$$

From (8) we deduce that

$$c = \frac{\text{constant term of } G_{1,\chi}^2}{\text{constant term of } E} = \frac{L(0,\chi)^2/4}{(N-1)/12} > 0.$$

Combining this with the estimate $L(0,\chi) < \frac{\sqrt{N}}{2\pi}(\log N + 5)$ from Proposition 4.1, we find that

$$(10) \qquad \frac{L(0,\chi) - c}{\sqrt{N}} < \frac{L(0,\chi)}{\sqrt{N}} < \frac{1}{2\pi}(\log N + 5).$$

Now comes the key step: we appeal to a deep theorem of Guo [Guo96] about non-negativity of L-values.

Theorem 4.3 (Guo). *Let $N \geq 1$ be an integer and let $f \in S_2(\Gamma_0(N))$ be an eigenform. Let χ be a quadratic character. Then $L(f,1) \geq 0$ and $L(f,\chi,1) \geq 0$.*

Theorem 4.3 implies that for each newform $f_j \in S_2(\Gamma_0(N))$, we have

$$\frac{L(f_j,1) L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} \leq \sum_j \frac{L(f_j,1) L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle}.$$

Combining this with (10) and (9), we conclude that

$$\frac{L(f_j,1)\,L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} < \frac{1}{2\pi}(\log N + 5)$$

for each newform $f_j \in S_2(\Gamma_0(N))$. Multiplying through by $g(\chi)/i = \sqrt{N}$, we obtain:

$$(11) \qquad \frac{L(f_j,1)\,L(f_j,\chi,1)}{\pi^2 \langle f_j, f_j \rangle} \frac{g(\chi)}{i} < \frac{\sqrt{N}}{2\pi}(\log N + 5).$$

Now suppose that $f = f_j$ has rational Fourier coefficients. By Proposition 4.2, the LHS of (11) is a rational number with denominator $\leq 576 m_E$, where m_E is the modular degree of E. By assumption, we have $L(f,1)\,L(f,\chi,1) \neq 0$. So we can write the LHS of (11) in the form a/n for some $a > 0$, where $n \leq 576 m_E$. Since $a/n < \frac{\sqrt{N}}{2\pi}(\log N + 5)$ by (11), we conclude that $a < 576 \frac{\sqrt{N}}{2\pi}(\log N + 5)m_E$. So if p is a prime such that

$$p \geq 100\sqrt{N}(\log N + 5)m_E > 576 \cdot \frac{\sqrt{N}}{2\pi}(\log N + 5)m_E,$$

then p cannot divide a. This implies that

$$p \nmid \left(\frac{L(f,1)\,L(f,\chi,1)}{\pi^2 \langle f, f \rangle} \frac{g(\chi)}{i} \right),$$

completing the proof of Theorem 2.2, and thus Theorem 1.6.

5. PROOF OF PROPOSITION 4.2

In this section, we follow closely the template of a paper by Wiersema and Wuthrich [WW20]. Let $E/\mathbf{Q}$ be an elliptic curve of conductor N. Let f be the newform associated to E. For $r \in \mathbf{Q}$, define

$$(12) \qquad \lambda(r) = 2\pi i \int_{i\infty}^{r} f(z)\,dz = \frac{1}{c_E} \int_{\gamma(r)} \omega_E,$$

where $\gamma(r)$ is the image in $E(\mathbf{C})$ of the vertical line in the upper half plane from $i\infty$ to r, and c_E is the Manin constant of E. Let Λ_E be the Neron lattice of E, i.e. the set of all values $\int_{\gamma} \omega_E$ as γ runs through closed loops in $E(\mathbf{C})$. Let c_∞ be the number of connected components of $E(\mathbf{R})$. Then we have (see [WW20, Section 2]):

$$(13) \qquad \{\mathrm{Re}(z) : z \in \Lambda_E\} = \frac{1}{2}\Omega_E^+ \mathbf{Z}$$

and

$$(14) \qquad \{\mathrm{Im}(z)i : z \in \Lambda_E\} = \frac{1}{2}c_\infty \Omega_E^- \mathbf{Z} \subseteq \frac{1}{2}\Omega_E^- \mathbf{Z}.$$

We now define the standard modular symbols $[r]^\pm$ by

$$[r]^+ = \frac{\mathrm{Re}(\lambda(r))}{\Omega_E^+} \qquad \text{and} \qquad [r]^- = \frac{\mathrm{Im}(\lambda(r))}{\Omega_E^-}$$

for any $r \in \mathbf{Q}$. For any Dirichlet character $\chi \bmod m$, we have

$$(15) \qquad \frac{L(E,\chi,1)g(\overline{\chi})}{\Omega_E^{\chi(-1)}} = \sum_{a \bmod m} \chi(a) \left[\frac{a}{m} \right]^{\chi(-1)}.$$

Proof of Proposition 4.2. Let $\pi_E : X_0(N) \to E$ denote the modular parametrization of E. Since N is prime, the elliptic curve E is semistable. Therefore, one can show that for all $r \in \mathbf{Q}$, the point $P_r = \pi_E(r)$ is a torsion point defined over $\mathbf{Q}$ (see [Ste12, Theorem 1.3.1]). By Mazur's theorem on torsion [Maz77], the point P_r must have order dividing $1, \ldots, 10$, or 12. Hence the path γ in the definition of $\lambda(r)$ ends at a point in $E[m]$ for some $m = 1, \ldots, 10, 12$. So $\lambda(r) \in \frac{1}{m}\Lambda$. Now by (13) and (14) we obtain $[r]^{\pm} \in \frac{1}{2m}\mathbf{Z}$. By (15), it follows that for all Dirichlet characters χ, the value $2m \cdot \frac{L(E,\chi,1)g(\overline{\chi})}{\Omega_E^{\chi(-1)}}$ is an algebraic integer for some $m = 1, \ldots, 10, 12$. (The m does not depend on χ.)

By (2), we have

$$(16) \qquad \frac{L(f,1)L(f,\chi,1)}{\pi^2\langle f,f\rangle}\frac{g(\chi)}{i} = \frac{4c_E^2}{\deg\pi_E}\frac{L(E,1)}{\Omega_E^+}\frac{L(E,\chi,1)}{\Omega_E^-}\frac{g(\chi)}{i}.$$

Since E is a optimal curve, there is a conjecture that the Manin constant c_E is equal to 1. And this conjecture is known to be true if E is semistable by [ARS06], so $c_E = 1$. It follows that the denominator of (16) divides $4m^2 \deg\pi_E$ for some $m = 1, \ldots, 10, 12$. Since $m \leq 12$, the denominator of (16) is $\leq 4 \cdot 12^2 \deg\pi_E = 576 \deg\pi_E$. $\qquad\square$

6. EXAMPLES

The Rankin-Selberg method allows us to compute the algebraic parts of L-values, which in turn allows us to calculate Iwasawa invariants. We demonstrate this in two examples.

Example 1. Let $N = 11$ and let χ be the unique (odd) quadratic character of conductor 11. The Eisenstein series $G_{\mathbf{1},\chi}$ is the unique eigenform (normalized so that $a_1 = 1$) in the space $\mathcal{E}_1(\Gamma_0(11), \chi)$:

$$G_{\mathbf{1},\chi} = \frac{1}{2} + q + 2q^3 + q^4 + 2q^5 + \ldots.$$

The space $M_2(\Gamma_0(11))$ is spanned by an Eisenstein series and a cuspidal newform whose q-expansions are:

$$E = \frac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \ldots,$$
$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + \ldots.$$

By examining these q-expansions, we find that

$$G_{\mathbf{1},\chi}^2 = \frac{3}{5}E + \frac{2}{5}f.$$

Proposition 3.2 then says that

$$\frac{L(f,1)L(f,\chi,1)}{\langle f,f\rangle} \cdot \frac{g(\chi)}{8\pi^2 i} = \frac{\langle f, G_{\mathbf{1},\chi}^2\rangle}{\langle f,f\rangle} = \frac{2}{5}.$$

Let $E = X_0(11)$ be the elliptic curve corresponding to f. Let $p \neq 2, 5$ be a prime of good ordinary reduction which is not anomalous for E. Then $2/5$ is a p-adic unit so $\mu_p(E) = \lambda_p(E) = 0$ for all such primes p.

Example 2. Let $N = 67$ and let χ be the unique (odd) quadratic character of conductor 67. The Eisenstein series $G_{\mathbf{1},\chi}$ has q-expansion

$$G_{\mathbf{1},\chi} = \frac{1}{2} + q + q^2 + q^4 + 2q^5 + \ldots$$

The space $M_2(\Gamma_0(67))$ is spanned by an Eisenstein series and five newforms $f_1, f_2, f_2^c, f_3, f_3^c$, where f_i^c denotes the Galois conjugate of f_i:

$$E = \frac{11}{4} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \dots,$$
$$f_1 = q + 2q^2 - 2q^3 + 2q^4 + 2q^5 + \dots.$$
$$f_2 = q + (-\beta - 1)q^2 + (\beta - 2)q^3 + 3\beta q^4 - 3q^5 + \dots.$$
$$f_3 = q - \beta q^2 + (-\beta + 1)q^3 + (\beta - 1)q^4 + (2\beta + 1)q^5 + \dots,$$

where $\beta = \frac{1}{2}(1 + \sqrt{5})$. We have

$$G_{\mathbf{1},\chi}^2 = \frac{1}{11}E + \frac{2}{5}f_1 + 0(f_2 + f_2^c) + \frac{2}{55}(7 - \sqrt{5})f_3 + \frac{2}{55}(7 + \sqrt{5})f_3^c.$$

Proposition 3.2 then says that

$$\frac{L(f_1, 1)L(f_1, \chi, 1)}{\langle f_1, f_1 \rangle} \cdot \frac{g(\chi)}{8\pi^2 i} = \frac{\langle f_1, G_{\mathbf{1},\chi}^2 \rangle}{\langle f_1, f_1 \rangle} = \frac{2}{5}.$$

Let E be the elliptic curve of conductor 67 corresponding to f_1. Let $p \neq 2, 5$ be a prime which is not anomalous for E. Then $2/5$ is a p-adic unit so $\mu_p(E) = \lambda_p(E) = 0$ for all such primes p.

REFERENCES

[ARS06] Amod Agashe, Kenneth Ribet, and William A Stein, *The Manin constant*, Pure and Applied Mathematics Quarterly **2** (2006), no. 2, 617–636.

[BS13]   Manjul Bhargava and Arul Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, arXiv preprint arXiv:1312.7859 (2013).

[Dri03] Michael J Drinen, *Iwasawa μ-invariants of elliptic curves and their symmetric powers*, Journal of Number Theory **102** (2003), no. 2, 191–213.

[EPW06] Matthew Emerton, Robert Pollack, and Tom Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), 523–580.

[FW79]   Bruce Ferrero and Lawrence C Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Annals of Mathematics (1979), 377–395.

[Gre99] R. Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[Guo96] Jiandong Guo, *On the positivity of the central critical values of automorphic L-functions for* GL(2), Duke Math. J **83** (1996), no. 1.

[GV00]   Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Inventiones Mathematicae (2000).

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

[Kur02] Masato Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Inventiones mathematicae **149** (2002), no. 1, 195–224.

[LMF24] The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2024, [Online; accessed 22 April 2024].

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inventiones mathematicae **18** (1972), no. 3, 183–266.

[Maz77] _____, *Modular curves and the Eisenstein Ideal*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **47** (1977), no. 1, 33–186.

[Miy06] Toshitsune Miyake, *Modular Forms*, Springer Science & Business Media, 2006.

[Ram01] Olivier Ramaré, *Approximate formulae for $L(1, \chi)$*, Acta Arithmetica **100** (2001), no. 3, 245–266.

[Ray23] Anwesh Ray, *Remarks on Greenberg's conjecture for Galois representations associated to elliptic curves*, 2023, arXiv:2308.06673.

[Ray24]   ———, *Statistics for Iwasawa invariants of elliptic curves,* III, 2024, arXiv:2404.09009.

[Sch87]   Peter Schneider, *The μ-invariant of isogenies*, J. Indian Math. Soc. (N.S.) **52** (1987), 159–170 (1988). MR 989235

[Shi76]   Goro Shimura, *The Special Values of the Zeta Functions associated with Cusp Forms*, Communications on Pure and Applied Mathematics **29** (1976), no. 6, 783–804.

[Ste89]   Glenn Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Inventiones mathematicae **98** (1989), no. 1, 75–106.

[Ste12]   ———, *Arithmetic on modular curves*, vol. 20, Springer Science & Business Media, 2012.

[SW13]   William Stein and Christian Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Mathematics of Computation **82** (2013), no. 283, 1757–1792.

[Tri05]   Mak Trifković, *On the vanishing of μ-invariants of elliptic curves over $\mathbb{Q}$*, Canadian Journal of Mathematics **57** (2005), no. 4, 812–843.

[Was97]   Lawrence C Washington, *Introduction to cyclotomic fields*, vol. 83, Springer Science & Business Media, 1997.

[WW20]   Hanneke Wiersema and Christian Wuthrich, *Integrality of twisted L-values of elliptic curves*, arXiv preprint arXiv:2004.05492 (2020).