ON A QUESTION IN NON-EQUAL CHARACTERISTIC IWASAWA THEORY FOR ELLIPTIC CURVES

DEBANJANA KUNDU AND ANTONIO LEI

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve. Let p and q be two distinct primes. We study the p-adic Iwasawa theory of E over the cyclotomic $\mathbb{Z}_q$-extension $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$. In particular, we study a conjecture, which predicts the stabilization of the p-primary Selmer groups of E over $\mathbb{Q}_{\mathrm{cyc}}$, and the p-adic valuation of the algebraic L-values of E twisted by finite characters of the Galois group of $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$. We prove the equivalence of this conjecture for elliptic curves with isomorphic residual representations at p. Furthermore, we establish the conjecture in two cases: first, for a class of elliptic curves whose residual Galois representation is reducible, and second, for elliptic curves with complex multiplication.

1. Introduction

Let q be a prime number. Given an algebraic number field $F/\mathbb{Q}$, let F_∞/F denote a Galois extension with Galois group isomorphic to the additive group $\mathbb{Z}_q$ of q-adic integers. For each integer $n \geq 0$, there is a unique subfield F_n/F of degree q^n. Let $h(F_n)$ be the class number of F_n. In the 1950's, K. Iwasawa initiated the study of the q-part of the class number in $\mathbb{Z}_q$-extensions of F. In particular, he showed that if q^{e_n} is the highest power of q dividing $h(F_n)$, then there exist non-negative integers λ, μ and an integer ν that are independent of n, such that $e_n = \mu q^n + \lambda n + \nu$ for $n \gg 0$. For each prime q there is a unique $\mathbb{Z}_q$-extension $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$, called the *cyclotomic* $\mathbb{Z}_q$-extension. This is a totally real subfield of $\bigcup_n \mathbb{Q}(\zeta_{q^n})$ where ζ_{q^n} denotes a primitive q^n-th root of unity. For this extension, Iwasawa calculated $\mu = \lambda = \nu = 0$ for all primes q. He further conjectured that for the cyclotomic $\mathbb{Z}_q$-extension of a number field, the μ-invariant is always 0; this is known to be true for abelian number fields $F/\mathbb{Q}$ [FW79].

In [Was75, Was78], L. C. Washington proved that if $F/\mathbb{Q}$ is an abelian extension and p, q are distinct primes, the p-part of the class number stabilizes in the *cyclotomic* $\mathbb{Z}_q$-extension of F. The proof involves an investigation of the p-adic valuation of the values of Dirichlet L-functions at $s = 0$. Later in [Sin87b], W. Sinnott provided a different proof of Washington's theorem based on the fact that values of L-functions are "generated by rational functions"; he proved a general result applicable to any rational function measure. More recently, Washington's results have been extended to other $\mathbb{Z}_q$-extensions using Sinnott's approach. In particular, J. Lamplugh proved the following in [Lam15]: if p, q are distinct primes ≥ 5 that split in an imaginary quadratic field K of class number 1 and F/K is a prime-to-p abelian extension which is also unramified at p, then the p-class group stabilizes in the $\mathbb{Z}_q$-extension of F which is unramified outside precisely one of the primes above q. In [KL23], we showed that (for the same setup) the p-class group stabilizes in the anticyclotomic $\mathbb{Z}_q$-extension of K. The algebraic techniques developed for studying Iwasawa theory have mostly focused on the case of equal characteristic. Only recently has a systematic framework been developed by A. Bandini–I. Longhi in the non-equal characteristic setting; see [BL26].

In arithmetic geometry, it is *often* observed that class groups of number fields and Selmer groups of elliptic curves have similar growth behaviour. For example, in [Gre99b, Proposition 5.11], R. Greenberg asserts that under certain hypotheses on the mod p representation of an elliptic curve $E/\mathbb{Q}$, the p-torsion of the p-primary Selmer group in the cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}$ is finite. Furthermore, Lamplugh's proof of the growth stabilization of class groups in [Lam15] relies on analyzing the stabilization of Selmer groups of elliptic curves with complex multiplication (CM). However, it is pertinent to point out that the growth behaviour of class groups and Selmer groups is *not* always identical; for example, there exist

2020 *Mathematics Subject Classification.* Primary 11R23, 11G05.
Key words and phrases. $p \neq q$ Iwasawa theory, CM elliptic curves.

examples of elliptic curves $E/\mathbb{Q}$ with good ordinary reduction at q such that the μ-invariant of the q-primary Selmer group over $\mathbb{Q}_{\mathrm{cyc}}$ is positive. However, Greenberg predicts (see [Gre99b, Conjecture 1.11]) that if $E/\mathbb{Q}$ is an elliptic curve with good ordinary reduction at $q \geq 3$, then there exists a $\mathbb{Q}$-isogenous elliptic curve E' whose corresponding μ-invariant is zero. In particular, writing E_q to denote the q-torsion points of E, if E_q is irreducible as an $\mathbb{F}_q$-representation of the absolute Galois group $G_{\mathbb{Q}}$, it is predicted that the μ-invariant of the q-primary Selmer group of E over $\mathbb{Q}_{\mathrm{cyc}}$ should vanish.

The main question under consideration in the present article can be considered as the non-equal characteristic version of the conjecture of Greenberg. Let us first introduce some notation that will be used throughout the article. Let $p \neq q$ be distinct rational primes, both coprime to 6. Let $\mathbb{Q}_{\mathrm{cyc}}$ denote the cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}$ as before. For an integer $n \geq 0$, let $\mathbb{Q}_{(n)}$ denote the unique sub-extension of $\mathbb{Q}_{\mathrm{cyc}}$ such that $[\mathbb{Q}_{(n)} : \mathbb{Q}] = q^n$. Let $E/\mathbb{Q}$ be an elliptic curve. We write Ω_E for the real Néron period of E. In what follows, we use the notation $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})$ to denote the p-primary Selmer group of an elliptic curve E over $\mathbb{Q}_{\mathrm{cyc}}$ and E_{p^∞} is the set of p-power torsions on E; see §2 where we review its definition.

Let Ξ_q denote the set of all Dirichlet characters that factor through $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$. Note that these characters are even since $\mathbb{Q}_{\mathrm{cyc}}$ is totally real. Given a $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$-module M and $\chi \in \Xi_q$, following the notation introduced in [Kat04, p. 235], we write $M^\chi = \{x \in M : I_\chi \cdot x = 0\}$, where $I_\chi \subset \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})]$ is the kernel of the ring homomorphism $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})] \to \overline{\mathbb{Q}}$ induced by χ. Note that if χ and χ' are two characters of order q^n, then $I_\chi = I_{\chi'}$ is the ideal generated by the q^n-th cyclotomic character in γ, where γ is a topological generator of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$. In particular, $M^\chi = M^{\chi'}$.

Throughout, we fix an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. Let ord_p denote the p-adic valuation on $\overline{\mathbb{Q}_p}$ normalized by $\mathrm{ord}_p(p) = 1$. Given $\alpha \in \overline{\mathbb{Q}}$, we write $\mathrm{ord}_p(\alpha)$ instead of $\mathrm{ord}_p(\iota_p(\alpha))$ for simplicity.

We investigate the validity of the following Non-Equal Characteristic Vanishing (NECV) Conjecture.

NECV Conjecture. *Let $E/\mathbb{Q}$ be an elliptic curve, and p, q be two distinct primes coprime to 6. There exists a $\mathbb{Q}$-isogenous elliptic curve $E^\dagger$ (i.e., there is a $\mathbb{Q}$-isogeny from E to $E^\dagger$) such that the following assertions hold.*

(*i*) [Analytic] *We have* $\mathrm{ord}_p\left(\dfrac{L(E^\dagger,\chi,1)}{\Omega_{E^\dagger}}\right) = 0$ *for all but finitely many* $\chi \in \Xi_q$.

(*ii*) [Algebraic] *We have* $\mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^\chi = 0$ *for all but finitely many* $\chi \in \Xi_q$.

In [Roh88], D. Rohrlich proved that for almost all $\chi \in \Xi_q$, we have $L(E,\chi,1) \neq 0$, and so the p-adic valuation of $\dfrac{L(E,\chi,1)}{\Omega_E}$ is finite. Consequently, [Kat04, Corollary 14.3] tells us that $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^\chi$ is finite for almost all $\chi \in \Xi_q$. Thus, the NECV Conjecture may be viewed as a refined description of these arithmetic objects. We make a number of remarks regarding this conjecture.

Remark 1.1. Note that if χ and χ' are two characters in Ξ_q of the same order, then

$$\mathrm{ord}_p\left(\frac{L(E^\dagger,\chi,1)}{\Omega_{E^\dagger}}\right) = \mathrm{ord}_p\left(\frac{L(E^\dagger,\chi',1)}{\Omega_{E^\dagger}}\right) \quad \text{and} \quad \mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^\chi = \mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^{\chi'}$$

since $E^\dagger$ is defined over $\mathbb{Q}$. In other words, both the analytic and algebraic assertions of the NECV Conjecture only depend on the order of χ, rather than χ itself.

Remark 1.2. In the case where E_p is an irreducible representation of $G_{\mathbb{Q}}$, we expect that E itself satisfies the properties asserted. This is because the degree of a $\mathbb{Q}$-isogeny $\phi : E \to E^\dagger$ has to be coprime to p. Consequently,

$$\mathrm{ord}_p\left(\frac{L(E,\chi,1)}{\Omega_E}\right) = \mathrm{ord}_p\left(\frac{L(E^\dagger,\chi,1)}{\Omega_{E^\dagger}}\right) \quad \text{and} \quad \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}}) \simeq \mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}}).$$

Remark 1.3. In [Gre99b, Proposition 5.11], it is stated that the p-primary Selmer group of an elliptic curve $E/\mathbb{Q}$ over the cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}$ is of the form $(\mathbb{Q}_p/\mathbb{Z}_p)^t \times$(a finite group) if it has good ordinary or multiplicative reduction at $p \geq 3$ and E_{p^∞} contains a $G_{\mathbb{Q}}$-invariant subgroup Φ of order p

which is either ramified at p and even or unramified at p and odd. This implies that the algebraic NECV Conjecture holds for such curves. As a detailed proof is not provided in *loc. cit.*, we have included one in this article for the reader's convenience; see Theorem 4.2.

Remark 1.4. Since $p \neq q$, the restriction and corestriction maps on cohomology induce a split short exact sequence

$$0 \longrightarrow \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)}) \longrightarrow \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(m)}) \longrightarrow \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(m)})/\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)}) \longrightarrow 0$$

for all $m \geq n$. In other words, $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$ is a direct summand of $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(m)})$. Furthermore, the restriction map induces an isomorphism $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)}) \simeq \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(m)})^{\mathrm{Gal}(\mathbb{Q}_{(m)}/\mathbb{Q}_{(n)})}$; see [LPP24, Lemma 3.13]. As $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_{(n+1)}/\mathbb{Q})]$-representations, we have the following decomposition

$$\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n+1)}) = \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n+1)})^{\mathrm{Gal}(\mathbb{Q}_{(n+1)}/\mathbb{Q}_{(n)})} \oplus \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n+1)})^{\chi},$$

where χ is any character of Ξ_q of order q^{n+1}. Therefore, the condition that $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^{\chi} = 0$ for all but finitely many $\chi \in \Xi_q$ is equivalent to saying that there exists an integer n_0 such that the restriction map $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n_0)}) \to \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n_0+n)})$ is an isomorphism for all $n \geq 0$. Note that this is also equivalent to $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n_0)}) \simeq \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})$. We show in Lemma 2.4 that the assertion $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^{\chi} = 0$ for all but finitely many $\chi \in \Xi_q$ is equivalent to $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})$ being cofinitely generated over $\mathbb{Z}_p$.

Definition 1.5. *Let $(M_n)_{n\geq 0}$ be a direct system of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$-modules. We say that M_n **stabilizes** if there exists n_0 such that the connecting maps of the direct system induce an isomorphism $M_n \simeq M_{n_0}$ for all $n \geq n_0$.*

In view of this definition and the discussion in Remark 1.4, we may rephrase to say that the algebraic NECV Conjecture predicts that the Selmer group $\mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{(n)})$ stabilizes.

Remark 1.6. It is well-known by the results of K. Kato [Kat04] and D. Rohrlich [Roh88] (see for example [Gre99a, Theorem 1.4]) that for an elliptic curve $E/\mathbb{Q}$, its Mordell–Weil rank is bounded in the cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}$. Therefore, if we assume the finiteness of $Ш(E/\mathbb{Q}_{(n)})[p^\infty]$ for all n, the algebraic NECV Conjecture predicts that there exists a curve in the $\mathbb{Q}$-isogeny class of E such that these groups stabilize as $n \to \infty$.

Furthermore, [DD15, Theorem 1.1] gives an explicit formula that relates the size of the p-primary part of the Shafarevich–Tate groups of $\mathbb{Q}$-isogenous curves in terms of their periods and Tamagawa numbers. More precisely, if E and $E^\dagger$ are $\mathbb{Q}$-isogenous, there exists an integer ν such that

$$\mathrm{ord}_p\left|Ш(E/\mathbb{Q}_{(n)})[p^\infty]\right| - \mathrm{ord}_p\left|Ш(E^\dagger/\mathbb{Q}_{(n)})[p^\infty]\right| = \mathrm{ord}_p\left(\frac{\Omega_{E^\dagger}}{\Omega_E}\right) q^n + \nu \tag{1.1}$$

for $n \gg 0$. Therefore, we expect that the curve $E^\dagger$, for which the stabilization of Shafarevich–Tate groups is predicted to occur, is the minimal curve in the isogeny class (in the sense of G. Stevens [Ste89]). This is in direct analogy with Greenberg's $\mu = 0$ conjecture in the equal-characteristic setting. Furthermore, combined with (1.1), we have

$$\mathrm{ord}_p\left|Ш(E/\mathbb{Q}_{(n)})[p^\infty]\right| = \mathrm{ord}_p\left(\frac{\Omega_{E^\dagger}}{\Omega_E}\right) q^n + \nu$$

for $n \gg 0$.

Remark 1.7. We point out that the algebraic and analytic parts of the NECV Conjecture are intimately related to each other. Indeed, if we assume that p does not divide the Tamagawa number of $E^\dagger/\mathbb{Q}_{(n)}$ and the size of its torsion subgroup, then the equivariant Birch and Swinnerton-Dyer conjecture predicts that $\mathrm{ord}_p\left(\dfrac{L(E^\dagger,\chi,1)}{\Omega_{E^\dagger}}\right) = 0$ if and only if $\mathrm{Sel}(E^\dagger_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^{\chi} = 0$ for $\chi \in \Xi_q$.

If E has good reduction at both p and q, this equivalence follows from the classical Iwasawa Main Conjecture (or from its plus/minus variant when p is supersingular) over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for the modular form associated with E twisted by χ, combined with the control theorem. Under

certain hypotheses on the p-adic representation attached to E, the Iwasawa Main Conjecture is known from the works of [Rub91, Kat04, SU14, PR04, BSTW24, Spr24, CÇSS18].

1.1. **Main Results.** We now discuss the main results of this article and a sketch of their proofs.

1.1.1. *Transferability.* We prove the equivalence of the NECV Conjecture (under mild hypotheses) when there are two elliptic curves E and E' with isomorphic Galois representations modulo p. More precisely,

Theorem A (Theorems 3.2 and 3.3)**.** *Let E and E' be elliptic curves defined over $\mathbb{Q}$ with isomorphic Galois representations modulo p, where p is an odd prime.*

- (*i*) *Suppose that E and E' have semi-stable reduction at p, and that their mod p representations are irreducible. The analytic NECV Conjecture holds for E if and only if it holds for E'.*
- (*ii*) *Suppose that p is a prime of good reduction for E and E'. The algebraic NECV Conjecture holds for E if and only if it holds for E'.*

Let f and g be the modular forms associated with E and E', respectively. Let Σ be a finite set of primes containing the primes of bad reduction of E and E'. To prove the transferability of the analytic NECV Conjecture in Theorem 3.2, we show that it suffices to prove the result for the Σ-depleted modular forms f^Σ, g^Σ, which satisfy the additional property that $f^\Sigma \equiv g^\Sigma \mod p$ under our assumption. We then appeal to results of [Vat99, GV00], which show that $\dfrac{L(f^\Sigma,\chi,1)}{\Omega_E}$ and $\dfrac{L(g^\Sigma,\chi,1)}{\Omega_{E'}}$ are congruent modulo p for $\chi \in \Xi_q$.

The proof of the transferability of the algebraic NECV Conjecture relies on working with certain imprimitive Selmer groups, which satisfy

$$\mathrm{Sel}^\Sigma(E_p, \mathbb{Q}_{(n)}) \simeq \mathrm{Sel}^\Sigma(E'_p, \mathbb{Q}_{(n)})$$

under our hypothesis $E_p \simeq E'_p$. Using Proposition 2.8, we prove that the growth stabilization of $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$ is equivalent to that of $\mathrm{Sel}^\Sigma(E_p, \mathbb{Q}_{(n)})$, and similarly for E'. This allows us to complete the proof of part (ii) of Theorem A.

Theorem A is inspired by the work of R. Greenberg–V. Vatsal [GV00] on μ-invariants when $p = q$. One key difference is that we work with Bloch–Kato Selmer groups (and their imprimitive versions). This provides the flexibility of treating the local conditions at p from a more representation-theoretic viewpoint. One might ask whether the results on λ-invariants in the aforementioned work extend to the non-equal characteristic case. However, the results of [BL26] on the algebraic structure of $\mathbb{Z}_p[\![\mathbb{Z}_q]\!]$ show that no such invariant can exist. Indeed, the characteristic ideals of modules over this ring are given by infinite sequences of powers of p. The NECV Conjecture predicts that, in the context of elliptic curves, the relevant characteristic ideals should correspond to sequences that are eventually constant.

1.1.2. *Reducible case.* In the case where E_p is reducible, we mentioned in Remark 1.3 that the algebraic NECV Conjecture holds under certain hypotheses. We prove the analytic analogue of this result.

Theorem B (Theorem 4.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and p be an odd prime of semi-stable reduction. Suppose that there is an exact sequence of $G_\mathbb{Q}$-modules*

$$0 \longrightarrow \Phi \longrightarrow E_p \longrightarrow \Psi \longrightarrow 0, \tag{1.2}$$

where Φ, Ψ are viewed as sub-quotient of the $G_\mathbb{Q}$-module E_p, as well as characters $\Phi, \Psi : G_\mathbb{Q} \to \mathbb{F}_p^\times$, such that Ψ is odd and unramified at p. If E is optimal in its isogeny class for the modular parametrization $\pi : X_1(N_E) \to E$, then $\mathrm{ord}_p\left(\dfrac{L(E,\chi,1)}{\Omega_E}\right) = 0$ for all but finitely many $\chi \in \Xi_q$.

Here, our approach is once again inspired by the work of [GV00] in the case of equal characteristic. Our assumption on E_p allows us to show that the modified L-function associated with E is congruent to a product of two modified L-functions associated with Dirichlet characters. The non-vanishing modulo p of special values of these L-functions follows from the work of Sinnott [Sin87a].

As alluded to in Remark 1.3, we reproduce a proof of the algebraic NECV Conjecture assuming (1.2). We relate the imprimitive Selmer group of E_p to the imprimitive Selmer groups of Φ and Ψ.

These Selmer groups can be reinterpreted in terms of class groups, whose growth stabilization follows from the work of Washington and Sinnott on class groups. Note that without the hypothesis on Ψ being odd and unramified at p, the Selmer groups do not stabilize. Indeed, we can relate them to certain class groups *and* unit groups of (explicit) number fields. When ψ is an even character, the growth of these unit groups is unbounded in the tower; see Theorem 4.3. This does not violate the NECV Conjecture as there may exist a $\mathbb{Q}$-isogenous curve for which stabilization still holds. In fact, our hypotheses on E_p imply that E is not the minimal curve in its isogeny class. Therefore, it is expected that $|Ш(E/\mathbb{Q}_{(n)})[p^\infty]|$ is unbounded as $n \to \infty$ in light of the discussion in Remark 1.6.

1.1.3. *Elliptic curves with complex multiplication.* Finally, we prove that the NECV Conjecture holds in the case of CM elliptic curves.

Theorem C (Corollary 5.15 and Theorem 5.18)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by the ring of integers of an imaginary quadratic field K. Let p and q be distinct primes ≥ 5 which are both good ordinary primes for E. Let ψ be the Hecke character attached to E and write $\mathfrak{f}$ for the conductor of ψ. Suppose that $p \nmid [\mathscr{R}(\mathfrak{f}) : K]$, where $\mathscr{R}(\mathfrak{m})$ denotes the ray class field of K of conductor $\mathfrak{m}$. Then*

(i) we have $\mathrm{ord}_p\left(\frac{L(E,\chi,1)}{\Omega_E}\right) = 0$ for all but finitely many $\chi \in \Xi_q$.
(ii) we have $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})^\chi = 0$ for all but finitely many $\chi \in \Xi_q$.

The proof of this theorem builds on our previous work [KL25]. We generalize the work of [Lam15] by defining a $\overline{\mathbb{Q}_p}$-valued "elliptic function measure" on $\mathbb{Z}_q^2$, which means that its Fourier transform is given by the values of a rational function of a CM elliptic curve E evaluated at E_{q^∞} (see Definition 5.3). Let K be the CM field of E. We work with a specific choice of measure such that its values when evaluated at finite-order characters of $\mathbb{Z}_q^2$ interpolate the L-values of the elliptic curve twisted by Hecke characters over K of p-power conductor. To prove part (i) of Theorem C, we analyze the p-adic valuations of the measure when the Hecke character factors through the cyclotomic $\mathbb{Z}_q$-extension of K.

Let $\mathfrak{p}$ be one of the primes of K lying above p. To prove part (ii), we make use of the Iwasawa Main Conjecture for E over $\mathbb{Q}_{(n)} \cdot K(\mathfrak{p}^\infty)$, which was proved by K. Rubin [Rub91]. Combining a control theorem and part (i), we establish the stabilization of the Selmer group $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)} \cdot K)$, which in turn gives the stabilization of $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$.

It seems plausible that a comparable line of argument could be used to derive the algebraic NECV Conjecture from the analytic counterpart by appealing to the Iwasawa Main Conjectures for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_{(n)}$ in the non-CM setting. In the reducible case, one might expect that, under suitable hypotheses, Theorem B could be obtained from [Gre99b, Proposition 5.11], and vice versa. Nevertheless, the arguments we develop in this paper rely on quite different methods that bypass any use of Iwasawa Main Conjectures, and may be of independent interest.

1.2. **Outlook.** The questions studied in this paper may be regarded as a first step toward a theory of non-characteristic Iwasawa theory for elliptic curves. We hope that our results will stimulate further investigation. For instance, instead of restricting to the cyclotomic $\mathbb{Z}_q$-extension of $\mathbb{Q}$, one can pose the same questions for more general q-adic Lie extensions such as $\mathbb{Q}(\mu_{q^\infty})$, $\mathrm{GL}(\mathbb{Z}_q)$-extensions, etc. It is reasonable to expect that, at the cost of more involved calculations and heavier notation, many of our results can be generalized to the case of abelian extensions. In the non-abelian setting, however, substantially more sophisticated tools (for example, techniques from algebraic K-theory) may be required even to formulate reasonable analogues of our conjectures, in the spirit of the $\mathfrak{M}_H(G)$-conjecture in the equal characteristic setting. It can also be interesting to study the growth of p-primary Selmer groups in $\prod_{i=1}^t \mathbb{Z}_{q_i}$-extensions, where $p, q_1, \ldots, q_t$ are pairwise distinct prime numbers. One may go even one step further to investigate the extension given by $\bigcup_{p\nmid n} \mathbb{Q}(\mu_n)$, which would involve studying twists by all Dirichlet characters whose conductors are coprime to p.

1.3. **Organization.** Including this introduction, this article consists of five sections. Section 2 is preliminary in nature. We give basic definitions of Selmer groups, record well-known analytic results

required for our main proofs, and prove algebraic results which are used multiple times for the proofs of our main theorems. We then prove Theorems A, B, and C in Sections 3, 4, and 5, respectively.

Acknowledgements. The authors thank Alex Bartel and Laurent Berger for helpful discussions during the preparation of the article. We also thank the anonymous referee for a careful reading of earlier versions of this article, as well as for numerous comments and suggestions that led to many improvements. This project was initiated while DK was visiting AL at the University of Ottawa and was supported by an AWM-NSF Mentorship grant for pre-tenure faculty. This article was completed while DK was in residence at the Lodha Mathematical Sciences Institute (LMSI), Mumbai, in Fall 2025. She acknowledges the support of NSERC Discovery grants RGPIN-2026-07384 and DGECR-2026-00254. AL's research is supported by the NSERC Discovery Grant RGPIN-2026-04351.

2. Preliminaries

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. An algebraic extension of $\mathbb{Q}$ is then regarded as a subfield of this fixed algebraic closure, $\overline{\mathbb{Q}}$. Throughout, p and q denote fixed rational odd primes.

2.1. **Analytic preliminaries.** Let R be any unital commutative ring. We consider the ring of polynomials $R[X;\mathbb{Z}_q]$ whose elements are polynomials in X with exponents in $\mathbb{Z}_q$ and coefficients in R. Therefore, elements of $R[X;\mathbb{Z}_q]$ are expressions of the form

$$P(X) = \sum_{a\in\mathbb{Z}_q} c_a X^a,$$

where $c_a = 0$ for all but finitely many $a \in \mathbb{Z}_q$. There is a projection map

$$\mathbb{Z}[X;\mathbb{Z}_q] \longrightarrow \mathbb{F}_p[X;\mathbb{Z}_q] \text{ given by } P(X) = \sum_{a\in\mathbb{Z}_q} c_a X^a \longmapsto \bar{P}(X) = \sum_{a\in\mathbb{Z}_q} \bar{c}_a X^a,$$

where the bar denotes the reduction modulo p.

We introduce the notation $\mu_{q^\infty}(\overline{\mathbb{F}_p})$ to denote the group of all q-power roots of unity in $\overline{\mathbb{F}_p}$.

Theorem 2.1. *Let $P(X) \in \mathbb{Z}[X;\mathbb{Z}_q]$ be such that $\min\{\mathrm{ord}_p(c_a) \,:\, a \in \mathbb{Z}_q\} = 0$. Then $\bar{P}(X) \in \mathbb{F}_p[X;\mathbb{Z}_q]$ has only finitely many zeros in $\mu_{q^\infty}(\overline{\mathbb{F}_p})$.*

Proof. This follows directly from [Sin87b, Theorem 2.2]. □

2.2. **Algebraic preliminaries.**

2.2.1. *Bloch–Kato Selmer groups and basic properties.* Throughout this subsection, let $T \simeq \mathbb{Z}_p^{\oplus d}$ be a free $\mathbb{Z}_p$-module that is equipped with a continuous $G_{\mathbb{Q}}$-action that is unramified outside a finite set of primes S. Furthermore, we assume that the representation is de Rham at p. We set $V := T \otimes \mathbb{Q}_p$ and $A := V/T$. Furthermore, we write $A_p = \frac{1}{p}T/T \subset A$. All of these modules are equipped with a continuous natural $G_{\mathbb{Q}}$-action. More generally, if M is a $\mathbb{Z}_p$-module, we shall write $M_p = M[p]$ and $M_{p^\infty} = \bigcup_{n\geq 1} M[p^n]$.

For every algebraic extension L of $\mathbb{Q}$, denote by L_S the maximal algebraic extension of L unramified outside S. We write $G_S(L) = \mathrm{Gal}(L_S/L)$, and write $S(L)$ for the set of primes of L above S.

Definition 2.2. *Let L be a finite extension of $\mathbb{Q}$.*

(*i*) *For any place of L and $M \in \{T, V, A\}$, define $H^1_f(L_v, M)$ as the Bloch–Kato subgroup of $H^1(L_v, M)$ from* [BK90, §3].

(*ii*) *Define $H^1_f(L_v, A_p)$ to be the pre-image of $H^1_f(L_v, A)$ under the natural map*

$$H^1(L_v, A_p) \longrightarrow H^1(L_v, A).$$

(*iii*) *For $M \in \{T, V, A, A_p\}$, define the* **Bloch–Kato Selmer group**

$$\mathrm{Sel}(M/L) := \ker\left(H^1(G_S(L), M) \longrightarrow \bigoplus_{v\in S(L)} \frac{H^1(L_v, M)}{H^1_f(L_v, M)} \right).$$

(*iv*) *Let* $\Sigma \subseteq S \setminus \{p\}$. *Define the* **non-primitive Bloch–Kato Selmer group** *as*

$$\mathrm{Sel}^{\Sigma}(M/L) := \ker\left(H^1(G_S(L), M) \longrightarrow \bigoplus_{v \in S(L)\setminus\Sigma(L)} \frac{H^1(L_v, M)}{H^1_f(L_v, M)} \right).$$

Remark 2.3. We recall from [Rub00, Proposition 1.6.8] that $H^1_f(L_v, E_{p^\infty})$ coincides with the image of $E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the Kummer map and the Bloch–Kato Selmer group of E_{p^∞} coincides with the classical definition of the p-primary Selmer group of E.

2.2.2. *Relationship between primitive and non-primitive Selmer groups.* Observe that if $L/\mathbb{Q}$ is an algebraic extension contained in $\mathbb{Q}_S$, then for any $M \in \{T, V, A\}$ there exists an exact sequence

$$0 \longrightarrow \mathrm{Sel}(M/L) \longrightarrow \mathrm{Sel}^{\Sigma}(M/L) \longrightarrow \bigoplus_{v \in \Sigma(L)} \frac{H^1(L_v, M)}{H^1_f(L_v, M)}.$$

The main (algebraic) result we prove in this section is Proposition 2.8, which is the main ingredient of our proofs of Theorems A and B. The proof of the proposition relies on the following lemmas.

Lemma 2.4. *Let* M *be a cofinitely generated* $\mathbb{Z}_p$*-module that is equipped with a continuous* $\mathbb{Z}_p$*-linear action of* $\Gamma \simeq \mathbb{Z}_q$. *If* $\chi \in \Xi_q$, *then* $M^\chi = 0$ *when the order of* χ *is sufficiently large.*

Proof. For an integer $n \geq 1$, we write $\Gamma_n = \Gamma^{q^n}$. Consider the submodules

$$M^\Gamma \subset M^{\Gamma_1} \subset M^{\Gamma_2} \subset \cdots$$

in M. As in the discussion in Remark 1.4, we deduce that M^{Γ_n} is a direct summand of $M^{\Gamma_{n+1}}$, and

$$M^{\Gamma_{n+1}} \simeq M^{\Gamma_n} \oplus M^\chi,$$

where χ is any character of Ξ_q of order q^{n+1}. Suppose $M^\chi \neq 0$ for infinitely many χ. Then, M admits an infinite sequence of submodules

$$N_1 \subsetneq N_1 \oplus N_2 \subsetneq N_1 \oplus N_2 \oplus N_3 \subsetneq \cdots.$$

As M is cofinitely generated over $\mathbb{Z}_p$, the p-rank of M, i.e., $r := \dim_{\mathbb{F}_p} M[p]$, is finite. In particular,

$$\sum_{i=1}^{n} \dim_{\mathbb{F}_p} N_i[p] \leq r$$

for all n. Therefore, when n is sufficiently large, we have $\dim_{\mathbb{F}_p} N_n[p] = 0$, and so $N_n = 0$, which is a contradiction. Thus, $M^\chi = 0$ for all but finitely many χ, as desired. □

We now show that if the p-primary Selmer group stabilizes in the cyclotomic $\mathbb{Z}_q$-extension $\mathbb{Q}_{\mathrm{cyc}}$ of $\mathbb{Q}$, then the non-primitive p-primary Selmer group stabilizes as well.

Lemma 2.5. *Let* p, q *be distinct odd primes. Let* $\Sigma = S \setminus \{p\}$. *For* $n \gg 0$, *the Selmer group* $\mathrm{Sel}(A/\mathbb{Q}_{(n)})$ *stabilizes in* $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$ *if and only if* $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$ *stabilizes in* $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$.

Proof. Since $\mathrm{Sel}(A/\mathbb{Q}_{(n)})$ is a subgroup of $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$, if the latter stabilizes, so does the former.

For the converse, assume that $\mathrm{Sel}(A/\mathbb{Q}_{(n)})$ stabilizes. It is enough to show that for all $v \in \Sigma(\mathbb{Q}_{(n)})$, the quotient $H^1(\mathbb{Q}_{(n),v}, A)/H^1_f(\mathbb{Q}_{(n),v}, A)$ stabilizes since all rational primes are finitely decomposed in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$. Recall from [Rub00, Lemma 1.3.5] that

$$H^1_{\mathrm{ur}}(\mathbb{Q}_{(n),v}, A)/H^1_f(\mathbb{Q}_{(n),v}, A) \simeq \mathcal{W}/(\mathrm{Frob}_v - 1)\mathcal{W},$$

where $\mathcal{W} = A^{I_v}/(A^{I_v})_{\mathrm{div}}$, I_v is the inertia group at v, and Frob_v is the Frobenius. In particular, this is a sub-quotient of A, which is cofinitely generated over $\mathbb{Z}_p$. Hence, it follows from Lemma 2.4 that the quotient $H^1_{\mathrm{ur}}(\mathbb{Q}_{(n),v}, A)/H^1_f(\mathbb{Q}_{(n),v}, A)$ stabilizes as $n \to \infty$. Thus, it suffices to show that $H^1(\mathbb{Q}_{(n),v}, A)/H^1_{\mathrm{ur}}(\mathbb{Q}_{(n),v}, A)$ stabilizes.

It follows from the inflation-restriction exact sequence that there is an injection

$$H^1(\mathbb{Q}_{(n),v}, A)/H^1_{\mathrm{ur}}(\mathbb{Q}_{(n),v}, A) \hookrightarrow H^1(I_v, A).$$

As $v \nmid p$, there exists a unique subgroup J_v of I_v such that $I_v/J_v \simeq \mathbb{Z}_p$, and J_v has profinite order prime to p. Applying the inflation-restriction exact sequence once more, we deduce that

$$H^1(I_v, A) \simeq H^1(I_v/J_v, A^{J_v}).$$

As I_v/J_v is pro-cyclic, we have

$$H^1(I_v/J_v, A^{J_v}) \simeq A^{J_v}/(\gamma_v - 1)A^{J_v},$$

where γ_v is a topological generator of I_v/J_v. As before, Lemma 2.4 tells us that this quotient stabilizes, which concludes the proof. □

Next, we relate the growth of $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$ and its p-torsion part which is denoted by $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})_p$.

Lemma 2.6. *Let p, q be distinct odd primes. Let $\Sigma \subsetneq S$ be defined as before. The non-primitive Selmer group $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$ stabilizes in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$ if and only if $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})_p$ stabilizes in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$.*

Proof. The forward implication is clear. Now, suppose that $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})_p$ stabilizes in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$; equivalently, the p-rank of $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$ stabilizes when $n \gg 0$. Using an argument identical to [KL23, Theorem 5.9], the claim follows. For convenience of the reader, we briefly recall the proof of *loc. cit.* As in Remark 1.4, the restriction map induces an isomorphism

$$\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(m)}) \simeq \mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)}) \oplus \mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(m)})/\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})$$

for all $m \geq n$. We can write $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(k)}) = (\mathbb{Q}_p/\mathbb{Z}_p)^{s_k} \oplus U_k$, where U_k is finite. Let r_k denote the p-rank of U_k. Then the p-rank of $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(k)})$ is $s_k + r_k$. In particular, by assumption s_k stabilizes as k increases. When n is sufficiently large, we have $s_m = s_n$ for all $m \geq n$. When this occurs, we have

$$U_m = U_n \oplus \mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(m)})/\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)}).$$

Furthermore, r_k also stabilizes. When $r_m = r_n$, we have $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(m)})/\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)}) = 0$, as desired. □

The next lemma allows us to compare the p-torsion part of $\mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{\mathrm{cyc}})$ and $\mathrm{Sel}^{\Sigma}(A_p/\mathbb{Q}_{\mathrm{cyc}})$.

Lemma 2.7. *Let p, q be distinct odd primes. For $n \gg 0$, the kernel and cokernel of the following map*

$$\mathrm{Sel}^{\Sigma}(A_p/\mathbb{Q}_{(n)}) \longrightarrow \mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})_p$$

are finite and bounded independently of n.

Proof. To prove the result, we analyze the following diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\Sigma}(A_p/\mathbb{Q}_{(n)}) & \longrightarrow & H^1(G_S(\mathbb{Q}_{(n)}), A_p) & \longrightarrow & \displaystyle\bigoplus_{\mathfrak{p}|p} \frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}}, A_p)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A_p)} \\
 & & \downarrow s_n & & \downarrow f_n & & \downarrow \oplus_{\mathfrak{p}} \gamma_{n,\mathfrak{p}} \\
0 & \longrightarrow & \mathrm{Sel}^{\Sigma}(A/\mathbb{Q}_{(n)})_p & \longrightarrow & H^1(G_S(\mathbb{Q}_{(n)}), A)_p & \longrightarrow & \displaystyle\bigoplus_{\mathfrak{p}|p} \left(\frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}}, A)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A)} \right)_p
\end{array}$$

We start by first considering the short exact sequence

$$0 \longrightarrow A_p \longrightarrow A \xrightarrow{\times p} A \longrightarrow 0.$$

Taking Galois cohomology, we obtain

$$0 \longrightarrow H^0(G_S(\mathbb{Q}_{(n)}), A)/p \longrightarrow H^1(G_S(\mathbb{Q}_{(n)}), A_p) \longrightarrow H^1(G_S(\mathbb{Q}_{(n)}), A)_p \longrightarrow 0.$$

The cardinality of $H^0(G_S(\mathbb{Q}_{(n)}), A)/p$ is at most p^d, where d is the corank of A. Thus, $\ker(f_n)$ and hence $\ker(s_n)$ are finite and bounded independently of n. Further, note that $\mathrm{coker}(f_n) = 0$ from the cohomology sequence above.

To bound the cokernel of s_n, we show that $\ker \gamma_{n,\mathfrak{p}} = 0$. Let $\phi : H^1(\mathbb{Q}_{(n),\mathfrak{p}}, A_p) \to H^1(\mathbb{Q}_{(n),\mathfrak{p}}, A)$ be the natural map. If $\gamma_{n,\mathfrak{p}}(x + H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A_p)) = 0$, then $\phi(x) \in H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A)$, which means that

$x \in H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A_p)$ (as $H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A_p)$ is defined as the pre-image of $H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, A)$ under ϕ). This completes the proof. □

Proposition 2.8. *Let p, q be distinct odd primes. Let $\Sigma = S \setminus \{p\}$. Then stabilization of $\mathrm{Sel}(A/\mathbb{Q}_{(n)})$ in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$ holds if and only if $\mathrm{Sel}^{\Sigma}(A_p/\mathbb{Q}_{(n)})$ stabilizes in $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$.*

Proof. The result is obtained by combining Lemmas 2.5, 2.6, and 2.7. □

3. Transferability of the NECV Conjecture under congruences

3.1. Analytic results.

Lemma 3.1. *Let ℓ be a prime and $\chi \in \Xi_q$. Let $P_\ell(E, \chi, 1)$ denote the Euler factor of $L(E, \chi, 1)$ at ℓ. Then for all but finitely many χ,*

$$\mathrm{ord}_p\left(P_\ell(E, \chi, 1)\right) = 0.$$

Proof. Let us write $Q_\ell(X) \in \mathbb{Z}[X]$ such that the Euler factor of $L(E, s)$ at ℓ is given by $Q_\ell(\ell^{-s})$. Then

$$P_\ell(E, \chi, 1) = Q_\ell(\ell^{-1}\chi(\ell)).$$

Since the polynomial $Q_\ell(\ell^{-1}X) \in \mathbb{Z}_p[X] \setminus p\mathbb{Z}_p[X]$ and $\chi(\ell)$ is a q-power root of unity, it follows from Theorem 2.1 that for all but finitely many χ, we have

$$\mathrm{ord}_p\left(P_\ell(E, \chi, 1)\right) = \mathrm{ord}_p\left(Q_\ell(\ell^{-1}\chi(\ell))\right) = 0.$$ □

Theorem 3.2. *Let E and E' be elliptic curves defined over $\mathbb{Q}$ with semi-stable reduction at $p \geq 3$. Suppose that $E_p \simeq E'_p$ as $G_{\mathbb{Q}}$-representations and that E_p is irreducible. Then the analytic NECV Conjecture holds for E if and only if it holds for E'.*

Proof. Let f and g be the weight-two modular forms associated with E and E', respectively. Let Σ be the set of primes that divide the integer $N_E N_{E'}$. Write f^Σ for the modular form such that $a_n(f^\Sigma) = a_n(f)$ whenever n is coprime to $N_E N_{E'}$ and $a_n(f^\Sigma) = 0$ otherwise. Define g^Σ similarly. The hypothesis $E_p \simeq E'_p$ implies that $f^\Sigma \equiv g^\Sigma \mod p$.

It follows from [Vat99, Proposition 1.7] that for all $\chi \in \Xi_q$

$$\tau(\overline{\chi}) \cdot \frac{L(f^\Sigma, \chi, 1)}{2\pi i \Omega_{f^\Sigma}} \equiv \tau(\overline{\chi}) \cdot \frac{L(g^\Sigma, \chi, 1)}{2\pi i \Omega_{g^\Sigma}} \mod p,$$

where Ω_{f^Σ} and Ω_{g^Σ} are Vatsal's canonical periods for f^Σ and g^Σ, respectively.

Let $E^\dagger$ be a strong Weil curve in the $\mathbb{Q}$-isogeny class of E. Firstly, as explained in [GV00, Remark 3.4], the hypothesis that E_p is irreducible implies that Ω_E and $\Omega_{E^\dagger}$ differ by a p-adic unit. Secondly, it follows from Theorem 3.2 and Proposition 3.3 in *op. cit.* that the Manin constant associated with the strong parametrization $\pi_0 : X_0(N_E) \to E^\dagger$ is a p-adic unit. This in turn implies that $\Omega_{E^\dagger}$ and $2\pi i \Omega_f$, where Ω_f is Vatsal's canonical period for f, differ by a p-adic unit. Furthermore, the proof of Lemma 3.6 in *op. cit.* tells us that Ω_f and Ω_{f^Σ} also differ by a p-adic unit (even though the lemma is stated for ordinary primes, the proof relies on the method developed in [Maz78], which works as long as E is semi-stable at p). Therefore, we deduce that Ω_E and Ω_{f^Σ} differ by a p-adic unit. Analogously, the same can be said about $\Omega_{E'}$ and Ω_{g^Σ}.

Note that the Gauss sum can be eliminated since it is a p-adic unit under the condition that $p \neq q$. Therefore, there exists a p-adic unit u such that

$$\frac{L(f^\Sigma, \chi, 1)}{\Omega_E} \equiv u \cdot \frac{L(g^\Sigma, \chi, 1)}{\Omega_{E'}} \mod p.$$

Suppose that E satisfies the analytic NECV Conjecture. Combined with Lemma 3.1, we have

$$\mathrm{ord}_p\left(\frac{L(f^\Sigma, \chi, 1)}{\Omega_E}\right) = 0$$

for all but finitely many χ. In particular, the same is true if we replace f and E by g and E', respectively. Applying Lemma 3.1 to E' implies that the analytic NECV Conjecture holds for E'. □

3.2. **Algebraic results.**

Theorem 3.3. *Let E and E' be elliptic curves defined over $\mathbb{Q}$ such that $E_p \simeq E'_p$ as $G_{\mathbb{Q}}$-representations and p is an odd prime of good reduction for E and E'. The algebraic NECV Conjecture holds for E if and only if it holds for E'.*

The reason why we assume that p is a prime of good reduction here is that we will appeal to the theory of Fontaine–Laffaille for crystalline representations, which will allow us to compare the Bloch–Kato Selmer local conditions for elliptic curves with isomorphic mod p representations. In what follows, let k be a finite unramified extension of $\mathbb{Q}_p$. Write $T_p(E)$ to denote the p-adic Tate module of E. Recall from Definition 2.2 that $H^1_f(k, E_p)$ is defined as the pre-image of $H^1_f(k, E_{p^\infty})$ under the natural map $H^1(k, E_p) \to H^1(k, E_{p^\infty})$. As $H^1_f(k, E_{p^\infty})$ and $H^1_f(k, T_p(E))$ are exact annihilators of each other under the local Tate pairing on $H^1(k, E_{p^\infty}) \times H^1(k, T_p(E))$ (see [BK90, Proposition 3.8]). We can equally define $H^1_f(k, E_p)$ as the image of $H^1_f(k, T_p(E))$ under the natural map

$$H^1(k, T_p(E)) \to H^1(k, T_p(E)/p) = H^1(k, E_p).$$

Furthermore, it is equal to the image of $E(k)/p$ under the Kummer map.

Lemma 3.4. *Let E and E' be elliptic curves defined over k with good reduction such that $E_p \simeq E'_p$ as G_k-representations. The natural isomorphism $H^1(k, E_p) \simeq H^1(k, E'_p)$ induces an isomorphism $H^1_f(k, E_p) \simeq H^1_f(k, E'_p)$.*

Proof. Since p is assumed to be odd, the G_k-representations $T_p(E)$ and $T_p(E')$ are crystalline with Hodge–Tate weights 0 and 1, and $k/\mathbb{Q}_p$ is a finite unramified extension, the lemma follows from the theory of J.-M. Fontaine–G. Laffaille [FL82]; see [IM15, Corollary 4.1.12]. □

Definition 3.5. *Set $S = \{p, q, \infty\} \cup \{\ell \colon \ell \mid N_E\} \cup \{\ell \colon \ell \mid N_{E'}\}$. For $\Sigma = S \setminus \{p\}$, define*

$$\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}) = \ker\left(H^1(G_S(\mathbb{Q}_{(n)}), E_p) \longrightarrow \bigoplus_{\mathfrak{p}\mid p} \frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}}, E_p)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, E_p)} \right),$$

where $\mathfrak{p}$ runs over all primes above p.

Proof of Theorem 3.3. Assume that the algebraic NECV Conjecture is true for E. By Proposition 2.8, it follows that $\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)})$ stabilizes. Our hypothesis $E_p \simeq E'_p$ and Lemma 3.4 together imply that $\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}) \simeq \mathrm{Sel}^{\Sigma}(E'_p/\mathbb{Q}_{(n)})$. Hence, applying Proposition 2.8 to $A = E'_{p^\infty}$ allows us to conclude that the algebraic NECV Conjecture holds for E'. □

4. The NECV Conjecture in the reducible case

In this section, we assume that E_p is a reducible $G_{\mathbb{Q}}$-representation and $p \geq 5$ is a prime of semi-stable reduction. It follows that p is a prime of good ordinary or multiplicative reduction. We impose the following hypotheses, which originate from the work of Greenberg–Vatsal [GV00]:

- (**red**) There is an exact sequence of $G_{\mathbb{Q}}$-modules
$$0 \longrightarrow \Phi \longrightarrow E_p \longrightarrow \Psi \longrightarrow 0,$$
where $\Phi, \Psi : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ are characters such that Ψ is odd and unramified at p.
- (**opt**) E is optimal in its isogeny class for the modular parametrization $\pi : X_1(N_E) \to E$; see [GV00, p. 50].

We define $\tilde{\Phi}$ and $\tilde{\Psi}$ as the $\mathbb{Z}_p^{\times}$-valued characters of $G_{\mathbb{Q}}$ that are obtained from composing Φ and Ψ with the Teichmüller character. We consider the $G_{\mathbb{Q}}$-modules $C = \mu_{p^\infty} \otimes \tilde{\Psi}^{-1}$ and $D = (\mathbb{Q}_p/\mathbb{Z}_p) \otimes \tilde{\Psi}$. Both C and D are isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a group; further $\Phi = C_p$ and $\Psi = D_p$.

4.1. **Analytic results.** Let $G = \sum b_n q^n$ be the Eisenstein series that satisfies

$$L(G,s) = L^{\Sigma_0}(\tilde{\Psi},s)L^{\Sigma_0}(\tilde{\Psi}^{-1},s-1)$$

given as in [GV00, p. 58], where Σ_0 denotes the set of primes dividing N_E.

Theorem 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying* (**red**) *and* (**opt**). *Then the analytic NECV Conjecture holds in the isogeny class of E.*

Proof. It follows from [Vat99, Theorem 2.10] that for all $\chi \in \Xi_q$, we have

$$\tau(\overline{\chi}) \cdot \frac{L(f^{\Sigma_0},\chi,1)}{2\pi i \Omega_{f^{\Sigma_0}}} \equiv \tau(\overline{\chi}) \cdot \frac{L(G,\chi,1)}{2\pi i \Omega_G} \mod p,$$

where Ω_G is a p-adic unit. Under (**opt**), it follows from [GV00, Proposition 3.1 and Lemma 3.6] that $2\pi i\Omega_{f^{\Sigma_0}}$ and Ω_E differ by a p-adic unit. As before, we can eliminate the Gauss sum $\tau(\overline{\chi})$ since $p \neq q$. Thus, we deduce that there exists a p-adic unit u such that

$$\begin{aligned}\frac{L(f^{\Sigma_0},\chi,1)}{\Omega_E} &\equiv u \cdot \frac{L(G,\chi,1)}{2\pi i} \mod p \\ &= u \cdot \frac{L^{\Sigma_0}(\tilde{\Psi}\chi,1)L^{\Sigma_0}(\tilde{\Psi}^{-1}\chi,0)}{2\pi i} \\ &= \frac{u}{2\tau(\tilde{\Psi}^{-1}\chi^{-1})} \cdot L^{\Sigma_0}(\tilde{\Psi}^{-1}\chi^{-1},0)L^{\Sigma_0}(\tilde{\Psi}^{-1}\chi,0).\end{aligned}$$

As both $\tilde{\Psi}$ and χ are unramified at p, the Gauss sum $\tau(\tilde{\Psi}^{-1}\chi^{-1})$ is a p-adic unit. Furthermore, (**red**) says that $\tilde{\Psi}$ is an odd character. Thus, [Sin87a, Theorem 4.1] implies that

$$\operatorname{ord}_p\left(L^{\Sigma_0}(\tilde{\Psi}^{-1}\chi^{-1},0)L^{\Sigma_0}(\tilde{\Psi}^{-1}\chi,0)\right) = 0$$

for all but finitely many χ. We deduce that $\operatorname{ord}_p\left(\dfrac{L(f^{\Sigma_0},\chi,1)}{\Omega_E}\right) = 0$ for all but finitely many χ. Combined with Lemma 3.1, we conclude that the analytic NECV Conjecture holds for E. □

4.2. **Algebraic results.** In [Gre99b, Proposition 5.11], Greenberg provides a sketch that if $E/\mathbb{Q}$ is an elliptic curve with good ordinary or multiplicative reduction at p satisfying (**red**), then $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}})_p$ is finite, where $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$ is the cyclotomic $\mathbb{Z}_q$-extension. Moreover, $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{\mathrm{cyc}}) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^t \times U$ where $t \geq 0$ and U is a finite group. This implies the algebraic NECV Conjecture holds as discussed in Remark 1.4. We provide a detailed proof here for the reader's convenience.

Theorem 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime of semi-stable reduction such that E_p is a reducible $G_{\mathbb{Q}}$-representation satisfying* (**red**). *Then the algebraic NECV Conjecture holds for the isogeny class of E.*

Proof. Choose $S = S(\mathbb{Q}) = \{p,q,\infty\} \cup \{\ell : \ell \mid N_E\}$. Proposition 2.8 asserts that the theorem follows if we show the stabilization of $\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)})$ in the cyclotomic $\mathbb{Z}_q$-tower where $\Sigma = S \setminus \{p\}$.
Claim: Stabilization of $\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)})$ follows if $\mathrm{Sel}^{\Sigma}(C_p/\mathbb{Q}_{(n)})$ and $\mathrm{Sel}^{\Sigma}(D_p/\mathbb{Q}_{(n)})$ stabilize.
Justification: The short exact sequence (1.2) gives rise to the following commutative diagram

(4.1)

$$\begin{array}{ccccccc} H^0(G_S(\mathbb{Q}_{(n)}),\Psi) & \longrightarrow & H^1(G_S(\mathbb{Q}_{(n)}),\Phi) & \xrightarrow{a_n} & H^1(G_S(\mathbb{Q}_{(n)}),E_p) & \xrightarrow{b_n} & H^1(G_S(\mathbb{Q}_{(n)}),\Psi) \\ & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \gamma_n} \\ & & \displaystyle\bigoplus_{\mathfrak{p}\mid p} \frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}},\Phi)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}},\Phi)} & \xrightarrow{a'_n} & \displaystyle\bigoplus_{\mathfrak{p}\mid p} \frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}},E_p)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}},E_p)} & \longrightarrow & \displaystyle\bigoplus_{\mathfrak{p}\mid p} \frac{H^1(\mathbb{Q}_{(n),\mathfrak{p}},\Psi)}{H^1_f(\mathbb{Q}_{(n),\mathfrak{p}},\Psi)}. \end{array}$$

Clearly, the top row is exact. Since Ψ is an odd character and $\mathbb{Q}_{(n)}$ is totally real, we deduce that $H^0(G_S(\mathbb{Q}_{(n)}), \Psi) = 0$. Moreover, by definition

$$\ker(\alpha_n) = \mathrm{Sel}^{\Sigma}(\Phi/\mathbb{Q}_{(n)}), \quad \ker(\beta_n) = \mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}), \quad \ker(\gamma_n) = \mathrm{Sel}^{\Sigma}(\Psi/\mathbb{Q}_{(n)}).$$

Thus, it suffices to show that both $\mathrm{Im}(a_n) \cap \mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)})$ and $b_n(\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}))$ stabilize. It is clear from (4.1) that $b_n(\mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)})) \subseteq \mathrm{Sel}^{\Sigma}(D_p/\mathbb{Q}_{(n)})$, which we assume stabilizes. Hence, it remains to study $\mathrm{Im}(a_n) \cap \mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}) = \mathrm{Im}(a_n) \cap \ker(\beta_n)$.

Since a_n is injective, we have

$$\mathrm{Im}(a_n) \cap \ker(\beta_n) \simeq \ker(a_n' \circ \alpha_n).$$

Clearly, $\ker(\alpha_n) \subseteq \ker(a_n' \circ \alpha_n)$. Further, we have the isomorphism

$$\ker(a_n' \circ \alpha_n)/\ker(\alpha_n) \simeq \ker(a_n') \cap \mathrm{Im}(\alpha_n).$$

As $\ker(\alpha_n)$ is assumed to stabilize, it is enough to show that $\ker(a_n')$ also stabilizes. The short exact sequence (1.2) gives the long exact sequence

$$H^0(\mathbb{Q}_{(n),\mathfrak{p}}, \Psi) \to H^1(\mathbb{Q}_{(n),\mathfrak{p}}, \Phi) \to H^1(\mathbb{Q}_{(n),\mathfrak{p}}, E_p) \to \cdots$$

As $H^0(\mathbb{Q}_{(n),\mathfrak{p}}, \Psi)$ is bounded independently of n, the kernel of $H^1(\mathbb{Q}_{(n),\mathfrak{p}}, \Phi) \to H^1(\mathbb{Q}_{(n),\mathfrak{p}}, E_p)$ stabilizes.

As the Hodge–Tate weight of $\tilde{\Psi}^{-1}(1)$ is 1, we have

$$H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, \mathbb{Z}_p(\tilde{\Psi}^{-1})(1)) = H^1(\mathbb{Q}_{(n),\mathfrak{p}}, \mathbb{Z}_p(\tilde{\Psi}^{-1})(1)).$$

Therefore, $H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, \Phi)$ is given by the image of $H^1(\mathbb{Q}_{(n),\mathfrak{p}}, \mathbb{Z}_p(\tilde{\Psi}^{-1})(1)) \to H^1(\mathbb{Q}_{(n),\mathfrak{p}}, \Phi)$ induced by the short exact sequence $0 \to \mathbb{Z}_p(\tilde{\Psi}^{-1})(1) \to \mathbb{Z}_p(\tilde{\Psi}^{-1})(1) \to \Phi \to 0$. By the local Euler characteristic formula, we deduce that the cardinality of $H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, \Phi)$ is $p^{q^n} \cdot \delta$, where δ is bounded independently of n. As $H^1_f(\mathbb{Q}_{(n),\mathfrak{p}}, E_p) \simeq E(\mathbb{Q}_{(n),\mathfrak{p}})/p$, its cardinality is also of the form $p^{q^n} \cdot \delta'$, where δ' is bounded independently of n. Thus, we deduce that $\ker(a_n')$ stabilizes, concluding the proof of the claim.

Let L be an abelian extension of $\mathbb{Q}$ through which the character $\tilde{\Psi}$ factors. Once again, in view of Proposition 2.8 we know that when A is 1-dimensional (i.e. A is either C or D), the stabilization of $\mathrm{Sel}^{\Sigma}(A_p/\mathbb{Q}_{(n)})$ will follow once we show that the growth of $\mathrm{Sel}(A/\mathbb{Q}_{(n)})$ can be described by the p-part of the class group of L_n, where L_n is the compositum of $\mathbb{Q}_{(n)}$ and L, and control the size of these class groups in $\mathbb{Z}_q$-towers.

Set $\Delta = \mathrm{Gal}(L_n/\mathbb{Q}_{(n)})$, which has order coprime to p. By [Rub00, Proposition 1.6.1], we have

$$\mathrm{Sel}(D/\mathbb{Q}_{(n)}) \simeq \mathrm{Hom}_{\Delta}(\mathrm{Cl}(L_n), \mathbb{Q}_p/\mathbb{Z}_p \otimes \mathcal{O}^{\times}_{\tilde{\Psi}}).$$

Here, $\mathrm{Cl}(L_n)$ denotes the p-part of the class group of L_n. On the other hand, by [Rub00, Proposition 1.6.4], we have a short exact sequence

$$0 \longrightarrow (\mathcal{O}^{\times}_{L_n} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\tilde{\Psi}} \longrightarrow \mathrm{Sel}(C/\mathbb{Q}_{(n)}) \longrightarrow \mathrm{Cl}(L_n)^{\tilde{\Psi}} \longrightarrow 0.$$

We claim that $(\mathcal{O}^{\times}_{L_n})^{\tilde{\Psi}}$ is finite, and that there is an isomorphism $\mathrm{Sel}(C/\mathbb{Q}_{(n)}) \simeq \mathrm{Cl}(L_n)^{\tilde{\Psi}}$. Indeed, since $\tilde{\Psi}$ is odd, if $x \in \mathcal{O}^{\times}_L$, then $\tilde{\Psi}(x) = x^* = x^{-1}$, where x^* denotes the complex conjugation of x. This implies that $|x| = 1$ under any embeddings of $L \hookrightarrow \mathbb{C}$. Thus, Kronecker's theorem tells us that x is a root of unity. In particular, $(\mathcal{O}^{\times}_{L_n} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\tilde{\Psi}} = 0$. Since $L_n/\mathbb{Q}$ is abelian, the main result of [Was78] says that $\mathrm{Cl}(L_n)$ stabilizes as n varies over the layers of the cyclotomic $\mathbb{Z}_q$ extension. Therefore, both $\mathrm{Sel}(C/\mathbb{Q}_{(n)})$ and $\mathrm{Sel}(D/\mathbb{Q}_{(n)})$ stabilize, as desired. □

Theorem 4.3. *Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime of semi-stable reduction such that E_p admits a short exact sequence of $G_{\mathbb{Q}}$-modules*

$$0 \longrightarrow \Phi \longrightarrow E_p \longrightarrow \Psi \longrightarrow 0,$$

where $\Phi, \Psi : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ are characters such that Ψ is even and unramified at p. Then $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$ does not stabilize. In fact, the p-rank of $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$ is unbounded as $n \to \infty$.

Proof. The commutative diagram (4.1) in the proof of Theorem 4.2 still applies, with the exception that $H^0(G_S(\mathbb{Q}_{(n)}), \Psi)$ is no longer trivial (because now Ψ is an even character), but it is finite and bounded independently of n. Further, just as before

$$\ker(\alpha_n) = \mathrm{Sel}^{\Sigma}(\Phi/\mathbb{Q}_{(n)}), \quad \ker(\beta_n) = \mathrm{Sel}^{\Sigma}(E_p/\mathbb{Q}_{(n)}), \quad \ker(\gamma_n) = \mathrm{Sel}^{\Sigma}(\Psi/\mathbb{Q}_{(n)}).$$

Thus, it suffices to show that $\mathrm{Sel}(C/\mathbb{Q}_{(n)})$ has unbounded growth. Recall that [Rub00, Proposition 1.6.4] gives the short exact sequence

$$0 \longrightarrow (\mathcal{O}_{L_n}^{\times} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\tilde{\Psi}} \longrightarrow \mathrm{Sel}(C/\mathbb{Q}_{(n)}) \longrightarrow \mathrm{Cl}(L_n)^{\tilde{\Psi}} \longrightarrow 0.$$

As a consequence of Artin's Induction Theorem and Dirichlet's Unit Theorem, there is an isomorphism of $\mathrm{Gal}(L_n/\mathbb{Q})$-modules

$$\mathcal{O}_{L_n}^{\times} \otimes \mathbb{Q} \simeq \mathbb{Q}[S_{L_n}]/\mathbb{Q},$$

where S_{L_n} is the set of infinite places of L_n (see [Tat84, Chapter I, §4.3])[1]. Thus,

$$\mathcal{O}_{L_n}^{\times} \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq \bigoplus_{\substack{\mathbf{1} \neq \theta \in \widehat{\mathrm{Gal}(L_n/\mathbb{Q})} \\ \theta \text{ even}}} (\mathbb{Q}_p/\mathbb{Z}_p)(\theta)$$

as $\mathrm{Gal}(L_n/\mathbb{Q})$-modules. Since $\tilde{\Psi}$ is an even character, the corank of $(\mathcal{O}_{L_n}^{\times} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\tilde{\Psi}}$ is unbounded as $n \to \infty$. □

5. The CM case

In this section, we prove Theorem C, that is, the NECV Conjecture for elliptic curves $E/\mathbb{Q}$ with complex multiplication.

Throughout, if $x \in \mathbb{C}$, we write x^* for its complex conjugation. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Note that K has class number one. We assume that $q \geq 5$ and that E has good ordinary reduction at q. In particular, q splits into two distinct primes $\mathfrak{q}$ and $\mathfrak{q}^*$ in $\mathcal{O}_K$. Let ψ be the Hecke character of infinity type $(1,0)$ attached to E. Let $\mathfrak{f}$ denote the conductor of ψ. We use the notation $\mathscr{R}(\mathfrak{m})$ to denote the *ray class field* of K of conductor $\mathfrak{m}$. Throughout this section, we assume that $p \nmid [\mathscr{R}(\mathfrak{f}) : K]$, $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ with $\mathfrak{p} \neq \mathfrak{p}^*$, and $\gcd(p, 6q) = 1$.

5.1. **Preliminaries.** Let K_∞ denote the $\mathbb{Z}_q^2$-extension of K and write $\Gamma_\infty = \mathrm{Gal}(K_\infty/K)$. For $\mathfrak{r} \in \{\mathfrak{q}, \mathfrak{q}^*\}$, let $K_{\mathfrak{r}}$ be the $\mathbb{Z}_q$-extension of K given by $K_\infty \cap \mathscr{R}(\mathfrak{r}^\infty)$, where $\mathscr{R}(\mathfrak{r}^\infty) = \bigcup_{n \geq 0} \mathscr{R}(\mathfrak{r}^n)$. Let $\Gamma_{\mathfrak{r}} = \mathrm{Gal}(K_{\mathfrak{r}}/K)$. We have a canonical decomposition $\Gamma_\infty = \Gamma_{\mathfrak{q}} \times \Gamma_{\mathfrak{q}^*}$. Fix a topological generator $\gamma_{\mathfrak{q}}$ of $\Gamma_{\mathfrak{q}}$ so that the action of the complex conjugation on Γ_∞ sends $\gamma_{\mathfrak{q}}$ to $\gamma_{\mathfrak{q}^*}$. There is an isomorphism

$$\Gamma_\infty = \Gamma_{\mathfrak{q}} \times \Gamma_{\mathfrak{q}^*} \simeq (1 + q\mathbb{Z}_q)^2, \tag{5.1}$$

such that the images of $\gamma_{\mathfrak{q}}$ and $\gamma_{\mathfrak{q}^*}$ are given by $(1+q, 1)$ and $(1, 1+q)$, respectively. Given a character χ of Γ_∞, we shall regard it as a character of $(1 + q\mathbb{Z}_q)^2$.

For the remainder of the article, we fix an isomorphism of the groups $\delta : (\mu_{q^\infty})^2 \xrightarrow{\sim} E_{q^\infty}$. As E is defined over $\mathbb{Q}$, the complex conjugation induces a canonical isomorphism $c : E_{\mathfrak{q}^\infty} \xrightarrow{\sim} E_{\mathfrak{q}^{*\infty}}$. We choose δ so that $\delta(\zeta, 1) \in E_{\mathfrak{q}^\infty}$, $\delta(1, \zeta) \in E_{\mathfrak{q}^{*\infty}}$, and $c \circ \delta(\zeta, 1) = \delta(1, \zeta)$ for all $\zeta \in \mu_{q^\infty}$.

Definition 5.1. *Let $\mathcal{S}_{\mathrm{cyc}}$ be the image of $\{(\zeta, \zeta) : \zeta \in \mu_{q^\infty}\}$ under δ inside E_{q^∞}.*

Note that given any $P \in E_{\mathfrak{q}^n}$, there exists a unique element $P^* \in E_{\mathfrak{q}^{*n}}$ such that $P \oplus_E P^* \in \mathcal{S}_{\mathrm{cyc}}$, where $\oplus_E$ denotes the group operation on E.

We can identify $E(\mathbb{C})$ with $\mathbb{C}/\mathcal{L}$ for some lattice $\mathcal{L}$, which can be chosen to be a fractional ideal of K. Since E is defined over $\mathbb{Q}$, the lattice $\mathcal{L}$ is furthermore invariant under complex conjugation. Let

[1] We thank Alex Bartel for pointing this out to us.

$\mathscr{Q}$ be a generator of $\mathfrak{q}$ (which exists since K has class number one). We have the following explicit description of $\mathcal{S}_{\mathrm{cyc}}$

$$\mathcal{S}_{\mathrm{cyc}} = \left\{a\mathscr{Q}^{-n} + (a\mathscr{Q}^{-n})^* + \mathcal{L} \in \mathbb{C}/\mathcal{L} : a \in \mathcal{L}\right\}.$$

Given any $x \in \mathcal{O}_K$ and $s = a\mathscr{Q}^{-n} + (a\mathscr{Q}^{-n})^* + \mathcal{L} \in \mathcal{S}_{\mathrm{cyc}}$, define

$$x \cdot s := xa\mathscr{Q}^{-n} + (xa\mathscr{Q}^{-n})^* + \mathcal{L}.$$

This defines an inclusion $\mathcal{O}_K \hookrightarrow \mathrm{End}(\mathcal{S}_{\mathrm{cyc}}) \simeq \mathbb{Z}_q$, which we denote by ι_{cyc}. Note that there is a natural inclusion

$$\mathrm{End}(\mathcal{S}_{\mathrm{cyc}}) \subset \mathrm{End}(E_{\mathfrak{q}^\infty}) \times \mathrm{End}(E_{q^*\infty}) \simeq \mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*}.$$

An element η of $\mathrm{End}(\mathcal{S}_{\mathrm{cyc}})$ can be expressed as (x, x^*), where $x \in \mathcal{O}_{K,\mathfrak{q}}$ and $x^* \in \mathcal{O}_{K,\mathfrak{q}^*}$.

Given an ideal $\mathfrak{g}$ of $\mathcal{O}_K$, we say that Q is a *primitive $\mathfrak{g}$-divisible point* on E if $Q \in E[\mathfrak{g}] \setminus E[\mathfrak{h}]$ for any $\mathfrak{h} \supsetneq \mathfrak{g}$. When $\mathfrak{g} = \mathfrak{q}^n\mathfrak{q}^{*n}$, we shall write q^n for the ideal $\mathfrak{q}^n\mathfrak{q}^{*n}$ to simplify the notation. Note that if an element of $\mathcal{S}_{\mathrm{cyc}}$ is of order q^n, then it is a primitive q^n-division point on E.

Lemma 5.2. *Let $Q \in \mathcal{S}_{\mathrm{cyc}}$ be an element of order q^n. The cardinality of the Galois orbit*

$$\left\{Q^\sigma : \sigma \in \mathrm{Gal}(\overline{K}/K)\right\}$$

is $\geq (q-1)^2q^{2(n-1)}/w_K$, where w_K denotes the size of μ_K, i.e., the number of roots of unity in K.

Proof. By definition, Q is a primitive q^n-division point on E. Let Q' be another primitive q^n-division point on E. As elements of $\mathbb{C}/\mathcal{L}$, there exist $\sigma \in \mathrm{Gal}(\mathscr{R}(q^n)/K)$ and $\zeta \in \mu_K$ such that $Q' = \zeta Q^\sigma$ by [KL25, Lemma 6.7]. Since there are $(q-1)^2q^{2(n-1)}$ primitive q^n-division points in E, the lemma follows. □

Let $k/\mathbb{Q}_p$ be a finite unramified extension containing $\mathbb{Q}_p(E_{\mathfrak{f}q})$. Set $J = k(\mu_{q^\infty})$. Let $\mathfrak{O}$ denote the ring of integers of J. Fix a uniformizer π of k and let ord_π denote the normalized valuation map

$$\mathrm{ord}_\pi : J \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

Recall the following definitions from [KL25]:

Definition 5.3. *Let α be a J-valued distribution on $\mathbb{Z}_q^2$, i.e., α is a finitely additive function on the set of compact open subsets of $\mathbb{Z}_q^2$ with values in J.*

(*i*) *Given any $c = (c_1, c_2) \in (\mathbb{Z}_q^\times)^2$, define $\alpha \circ c$ to be the distribution given by $\alpha \circ c(X) = \alpha(cX)$ for all open compact subsets X of $\mathbb{Z}_q^2$.*

(*ii*) *The* **Fourier transform** *of α is defined to be*

$$\hat{\alpha} : \mu_{q^\infty}^2 \longrightarrow J$$
$$(\zeta_1, \zeta_2) \longmapsto \int_{(x,y)\in\mathbb{Z}_q^2} \zeta_1^x\zeta_2^y d\alpha(x,y).$$

(*iii*) *Given a finite character χ on $(\mathbb{Z}_q^\times)^2$ with values in J, define the* **Leopoldt Γ-transform** *as*

$$\Gamma_\alpha(\chi) = \int_{\mathbb{Z}_q^2} \chi d\alpha,$$

where χ is extended to $\mathbb{Z}_q^2$ by sending all elements not inside $(\mathbb{Z}_q^\times)^2$ to zero.

(*iv*) *The distribution α is called a* **measure** *on $\mathbb{Z}_q^2$ if the image of α has bounded values with respect to ord_π.*

(*v*) *A J-valued distribution α on $\mathbb{Z}_q^2$ is an* **elliptic function measure** *with respect to δ for the fixed elliptic curve E if there exists a rational function $R \in J(E)$ such that for almost all $\underline{\zeta} = (\zeta_1, \zeta_2) \in (\mu_{q^\infty})^2$,*

$$\hat{\alpha}(\underline{\zeta}) = R(\delta(\underline{\zeta})).$$

Note that given any $R \in J(E)$, there exists a unique measure α on $\mathbb{Z}_q^2$ such that the Fourier transform $\hat{\alpha}$ coincides with $R \circ \delta$; see [KL25, Lemma 3.7].

(vi) *Given $R \in J(E)$, if $R \neq 0$ and $\mathrm{ord}_\pi(R(Q)) = n$ for almost all $Q \in E_{q^\infty}$, define its* **valuation** $\mathrm{ord}_\pi(R)$ *to be the integer n. If $R = 0$, set $\mathrm{ord}_\pi(R) = \infty$; see* [KL25, Lemma 3.5] *and* [Lam15, Lemma 3.2].

Lemma 5.4. *Let α be a J-valued elliptic function measure on $\mathbb{Z}_q^2$ corresponding to a rational function R. Then $\alpha^\times := \alpha|_{(\mathbb{Z}_q^\times)^2}$ is an elliptic function measure on $\mathbb{Z}_q^2$ corresponding to*

$$R^\times : P \mapsto R(P) - \frac{1}{q}\sum_{Q \in E_{\mathfrak{q}}} R(P \oplus_E Q) - \frac{1}{q}\sum_{Q \in E_{q^*}} R(P \oplus_E Q) + \frac{1}{q^2}\sum_{Q \in E_q} R(P \oplus_E Q).$$

Proof. Let β be the elliptic function measure corresponding to $R^\times$. It is enough to show that $\hat{\alpha}^\times = \hat{\beta}$.

Let $(\zeta_1, \zeta_2) \in \mu_{q^\infty}^2$, $(x, y) \in \mathbb{Z}_q^2$, and $(u, v) \in \mu_q$. Then

$$\zeta_1^x\zeta_2^y - \frac{1}{q}\sum_{u \in \mu_q}(\zeta_1 u)^x\zeta_2^y - \frac{1}{q}\sum_{v \in \mu_q}\zeta_1^x(\zeta_2 v)^y + \frac{1}{q^2}\sum_{u,v \in \mu_q}(\zeta_1 u)^x(\zeta_2 v)^y = \begin{cases}\zeta_1^x\zeta_2^y & \text{if } (x,y) \in (\mathbb{Z}_q^\times)^2,\\ 0 & \text{otherwise.}\end{cases}$$

Let $P = \delta(\zeta_1, \zeta_2)$, where $P \in E_{q^\infty}$. Given any $Q \in E_q$, there exists a unique element $(u, v) \in \mu_q^2$ such that $P \oplus_E Q = \delta(\zeta_1 u, \zeta_2 v)$. Furthermore, $u = 1$ (resp. $v = 1$) if and only if $Q \in E_{\mathfrak{q}^*}$ (resp. $Q \in E_{\mathfrak{q}}$). Thus,

$$\begin{aligned}
\hat{\alpha}^\times(\zeta_1, \zeta_2) &= \int_{(x,y)\in\mathbb{Z}_q^2} \zeta_1^x\zeta_2^y d\alpha^\times(x, y)\\
&= \int_{(x,y)\in(\mathbb{Z}_q^\times)^2} \zeta_1^x\zeta_2^y d\alpha(x, y)\\
&= \int_{(x,y)\in\mathbb{Z}_q^2} \left(\zeta_1^x\zeta_2^y - \frac{1}{q}\sum_{u\in\mu_q}(\zeta_1 u)^x\zeta_2^y - \frac{1}{q}\sum_{v\in\mu_q}\zeta_1^x(\zeta_2 v)^y + \frac{1}{q^2}\sum_{u,v\in\mu_q}(\zeta_1 u)^x(\zeta_2 v)^y\right) d\alpha(x, y)\\
&= R(P) - \frac{1}{q}\sum_{Q\in E_{\mathfrak{q}}} R(P \oplus_E Q) - \frac{1}{q}\sum_{Q\in E_{q^*}} R(P \oplus_E Q) + \frac{1}{q^2}\sum_{Q\in E_q} R(P \oplus_E Q)\\
&= \hat{\beta}(\zeta_1, \zeta_2),
\end{aligned}$$

as desired. □

Definition 5.5. *Let Ξ_{cyc} denote the set of finite-order characters of Γ_∞ that factor through $\mathrm{Gal}(K_{\mathrm{cyc}}/K)$, where K_{cyc} denotes the cyclotomic $\mathbb{Z}_q$-extension of K.*

Note that Ξ_q and Ξ_{cyc} are not equal as sets, but they can be identified with each other since $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) \simeq \mathrm{Gal}(K_{\mathrm{cyc}}/K)$. Under the identification $\Gamma_\infty \simeq (1 + q\mathbb{Z}_q)^2$ given by (5.1), a finite-order character χ of Γ_∞ belongs to Ξ_{cyc} if and only if $\chi(1 + q, 1) = \chi(1, 1 + q)$.

5.2. **Algebraic Independence.** Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_K$. Let $\mathbb{F}$ be the residue field of $\mathcal{O}_K$ modulo $\mathfrak{l}$. Suppose that $\mathbb{F}$ is of characteristic ℓ, with $\ell \neq q$. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, with good reduction at q. Throughout this section, we assume that E has good reduction at ℓ and write $\mathcal{E}$ to denote the base-change of the reduced curve of E modulo ℓ from $\mathbb{F}_\ell$ to $\mathbb{F}$.

Lemma 5.6. *Let $\Phi_1, \ldots, \Phi_s$ be non-trivial morphisms from $\mathcal{E}^n = \mathcal{E} \times \ldots \times \mathcal{E}$ to $\mathcal{E}$ of the form*

$$\Phi_j : (P_i)_{i=1}^n \mapsto \sum_{i=1}^n \alpha_{ij}(P_i),$$

where $\alpha_{ij} \in \mathrm{End}_{\mathbb{F}}(\mathcal{E})$ for all $1 \leq i \leq n$ and $1 \leq j \leq s$. Suppose that the only relation of the kind $x\Phi_t = x'\Phi_{t'}$ for $x, x' \in \mathrm{End}_{\mathbb{F}}(\mathcal{E})$ and $t \neq t'$, is when $x = x' = 0$. If $r_1, \ldots, r_s \in \mathbb{F}(\mathcal{E})$ with $\sum_{j=1}^s r_j \circ \Phi_j = 0$, then each r_j is a constant function.

Proof. See [Lam15, Proposition 4.4]. □

In what follows, we consider $\eta = (c_1, c_2) \in \mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*}$ as a map

$$\begin{aligned} \eta : \mathcal{S}_{\mathrm{cyc}} &\longrightarrow E_{q^\infty}, \\ P \oplus_E P^* &\longmapsto c_1 P \oplus_E c_2 P^*. \end{aligned}$$

We say that $\eta, \eta' \in \mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*}$ are *linearly independent over* K if

$$x\eta = x'\eta',\ x, x' \in K \implies x = x' = 0.$$

Since $\mathrm{char}(\mathbb{F}) \neq q$, there is a natural isomorphism $E_{q^\infty} \simeq \mathcal{E}_{q^\infty}$. In what follows, we shall denote the image of $\mathcal{S}_{\mathrm{cyc}} \subset E_{q^\infty}$ in $\mathcal{E}_{q^\infty}$ by the same notation.

Theorem 5.7. *Let $\mathbb{F}$ be a finite field as above. Let $\mathcal{E}/\mathbb{F}$ be the reduction of E. Suppose that*

$$\eta_i = (c_{i,1}, c_{i,2}) \in \mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*} \text{ for } i = 1, \ldots, s$$

are such that $\eta_t, \eta_{t'}$ are linearly independent over K for all $t \neq t'$. If $r_1, \ldots, r_s \in \mathbb{F}(\mathcal{E})$ satisfy

$$(r_1 \circ \eta_1 + \cdots + r_s \circ \eta_s)(Q) = 0 \quad \forall Q \in \mathcal{S}_{\mathrm{cyc}},$$

then $r_1, \ldots, r_s$ are all constant functions.

Proof. We follow closely the argument given in [Lam15, Theorem 4.5]. Let A be a free $\mathcal{O}_K$-submodule of $\mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*}$ of rank n containing $\eta_1, \ldots, \eta_s$, with the basis $\{\varepsilon_1, \ldots, \varepsilon_n\}$. Write

$$\begin{bmatrix} \eta_1 & \cdots & \eta_s \end{bmatrix} = \begin{bmatrix} \varepsilon_1 & \cdots & \varepsilon_n \end{bmatrix} \mathcal{A},$$

where $\mathcal{A} = [a_{ij}] \in \mathrm{Mat}_{n \times s}(\mathcal{O}_K)$. Define for $j = 1, \ldots, s$ the morphism

$$\begin{aligned} \Phi_j : \mathcal{E}^n &\longrightarrow \mathcal{E} \\ (P_i)_{i=1}^n &\longmapsto \sum_{i=1}^n a_{ij} P_i, \end{aligned}$$

and let $R : \mathcal{E}^n \to \mathbb{F}$ be the map given by $r_1 \circ \Phi_1 + \cdots + r_s \circ \Phi_s$. Furthermore, define

$$\begin{aligned} \Theta : \mathcal{S}_{\mathrm{cyc}} &\longrightarrow \mathcal{E}^n \\ Q &\longmapsto (\varepsilon_i Q)_{i=1}^n. \end{aligned}$$

Then $R \circ \Theta$ coincides with $r_1 \circ \eta_1 + \cdots + r_s \circ \eta_s$. In particular, by assumption, the morphism R vanishes on $\Theta(\mathcal{S}_{\mathrm{cyc}}) \subset \mathcal{E}^n$.

We verify that the morphisms $\Phi_1, \ldots, \Phi_s$ satisfy the hypothesis of Lemma 5.6, from which the theorem follows. Suppose that $x\Phi_t = x'\Phi_{t'}$ for some $x, x' \in \mathrm{End}_{\mathbb{F}}(\mathcal{E}) = \mathcal{O}_K$ and $t \neq t'$. For $i \in \{t, t'\}$ and $Q \in \mathcal{S}_{\mathrm{cyc}}$, we have

$$\Phi_i \circ \Theta(Q) = \eta_i(Q).$$

Therefore, $x\eta_t(Q) = x'\eta_{t'}(Q)$ for all $Q \in \mathcal{S}_{\mathrm{cyc}}$. If we write $Q = P \oplus_E P^*$, where $P \in \mathcal{E}_{\mathfrak{q}^m} \setminus \mathcal{E}_{\mathfrak{q}^{m-1}}$ and $P^* \in \mathcal{E}_{\mathfrak{q}^{*m}} \setminus \mathcal{E}_{\mathfrak{q}^{*m-1}}$. Then

$$\begin{aligned} xc_{t,1}P \oplus_E xc_{t,2}P^* &= x'c_{t',1}P \oplus_E x'c_{t',2}P^* \\ (xc_{t,1} - x'c_{t',1})P &= (x'c_{t'.2} - xc_{t,2})P^*. \end{aligned}$$

As $\mathcal{E}_{q^m} \cap \mathcal{E}_{q^{*m}} = 0$, this forces $\mathfrak{q}^m$ and $\mathfrak{q}^{*m}$ to divide $xc_{t,1} - x'c_{t',1}$ and $xc_{t,2} - x'c_{t',2}$, respectively. As this holds for arbitrarily large m, we have

$$xc_{t,1} - x'c_{t',1} = xc_{t,2} - x'c_{t',2} = 0.$$

In other words, $x\eta_t = x'\eta_{t'}$. As η_t and $\eta_{t'}$ are linearly independent over K, this implies that $x = x' = 0$, as desired. □

We now prove a strengthened version of Theorem 5.7.

Theorem 5.8. *Let $\mathbb{F}$ be a finite field as above. Let $\mathcal{E}/\mathbb{F}$ be the reduction of the curve E. Suppose that $\eta_i = (c_{i,1}, c_{i,2}) \in \mathcal{O}_{K,\mathfrak{q}} \times \mathcal{O}_{K,\mathfrak{q}^*}$, $i = 1, \dots, s$ are such that η_t and $\eta_{t'}$ are linearly independent over K for all $t \neq t'$. Consider the function*

$$R = \sum_{i=1}^{s} r_i \circ \eta_i : \mathcal{S}_{\mathrm{cyc}} \to \overline{\mathbb{F}}$$

where $r_i \in \mathbb{F}(\mathcal{E})$. Then either R has finitely many zeroes or R is identically zero. In the latter case, all r_i's are constant functions.

Proof. Let $d = \max_{1 \leq i \leq s} \deg(r_i)$ and set

$$c = \frac{(q-1)^2}{w_K q^2 s d}.$$

Recall from [KL25, Lemma 4.3] that there exists an integer N such that for all $n \geq N$, there are $b_1, \dots, b_s \in \mathcal{O}_K$ and $(u_1, u_2) \in \mathcal{O}_{K,\mathfrak{q}}^{\times} \times \mathcal{O}_{K,\mathfrak{q}^*}^{\times}$ (depending on n) such that

$$v_{\mathfrak{q}}(u_1 c_{i,1} - b_i) \geq n, \quad v_{\mathfrak{q}^*}(u_2 c_{i,2} - b_i) \geq n, \quad \text{and} \quad N_{K/\mathbb{Q}}(b_i) < c \cdot q^{2n}$$

for all $i \in \{1, \dots, s\}$. Let R_n be the rational function given by $\sum_{i=1}^{s} r_i \circ b_i$. Then

$$\deg(R_n) \leq \sum_{i=1}^{s} d \cdot N_{K/\mathbb{Q}}(b_i) < sdcq^{2n} = (q-1)^2 q^{2(n-1)}/w_K.$$

Suppose that n is large enough so that $R(Q) = 0$ for some $Q \in \mathcal{S}_{\mathrm{cyc}}$ of order q^n. Define

$$\begin{aligned} \mathfrak{u} : \mathcal{S}_{\mathrm{cyc}} &\longrightarrow E_{q^\infty} \\ P \oplus_E P^* &\longmapsto u_1^{-1} P \oplus_E u_2^{-1} P^*, \end{aligned}$$

where $P \in E_{\mathfrak{q}^\infty}$ and $P^* \in E_{\mathfrak{q}^{*\infty}}$. It is clear that $\mathfrak{u}$ is injective. Let $\mathfrak{v} : \mathfrak{u}(\mathcal{S}_{\mathrm{cyc}}) \to \mathcal{S}_{\mathrm{cyc}}$ be the inverse of $\mathfrak{u}$. Then $R \circ \mathfrak{v}$ and R_n agree on all elements of $\mathfrak{u}(\mathcal{S}_{\mathrm{cyc}})$. In particular, we have

$$R_n(\mathfrak{u}(Q)) = R \circ \mathfrak{v}(\mathfrak{u}(Q)) = R(Q) = 0.$$

Since R_n is invariant under the action of $\mathrm{Gal}(\overline{K}/K)$ and $\mathfrak{u}(Q)$ is a primitive q^n-division point on E, Lemma 5.2 implies that R_n possesses at least $(q-1)^2 q^{2(n-1)}/w_K$ roots. Consequently, R_n is identically zero. Therefore, R vanishes for all elements of $\mathcal{S}_{\mathrm{cyc}}$ whose orders are at most q^n. Since n can be arbitrarily large, this implies that R vanishes for all $Q \in \mathcal{S}_{\mathrm{cyc}}$, proving the first assertion of the theorem. The second assertion now follows from Theorem 5.7. □

5.3. **Gamma Transforms.** As before, let $k/\mathbb{Q}_p$ be a finite unramified extension containing $\mathbb{Q}_p(E_{\mathfrak{f}\mathfrak{q}})$. Set $J = k(\mu_{q^\infty})$. The main theorem we prove in this subsection is the following.

Theorem 5.9. *Let α be an elliptic function measure for E/k on $\mathbb{Z}_q^2$, which is supported on $(\mathbb{Z}_q^{\times})^2$, and which satisfies $\alpha \circ \omega = \alpha$ for all $\omega \in \mu_K^2$. Let R denote the corresponding rational function given by Definition 5.3(v) and let $n = \mathrm{ord}_\pi(R)$ be given by Definition 5.3(vi). Then, for almost all finite-order characters χ of Ξ_{cyc},*

$$\mathrm{ord}_\pi(\Gamma_\alpha(\chi)) = n.$$

To prove Theorem 5.9, we will use the following technical lemma.

Lemma 5.10. *Let α be an elliptic function measure as in the statement of Theorem 5.9. Let*

$$\begin{aligned} \iota : \mu_K &\longrightarrow \mu_{q-1}^2 \\ \zeta &\longmapsto (\zeta, \zeta). \end{aligned}$$

Define

$$\beta = \sum_{\eta} (\alpha \circ \eta)\,|_{(1+q\mathbb{Z}_q)^2},$$

where η runs over a set of representatives for $\mu_{q-1}^2/\iota(\mu_K)$ and $\alpha\circ\eta$ is defined as in Definition 5.3(i). For each $y=(y_1,y_2)\in(1+q\mathbb{Z}_q)^2/(1+q^M\mathbb{Z}_q)^2$, write

$$\beta_y=\beta|_{y_1(1+q^M\mathbb{Z}_q)\times y_2(1+q^M\mathbb{Z}_q)},$$

where $M\geq 1$ is the integer such that $\mu_{q^\infty}\cap k=\mu_{q^M}$. Let χ be a finite-order character of Ξ_{cyc}. Suppose that there exist integers $N\geq M$ satisfying

$$\ker\left(\chi|_{(1+q\mathbb{Z}_q)\times 1}\right)=\ker\left(\chi|_{1\times(1+q\mathbb{Z}_q)}\right)=1+q^{N+M}\mathbb{Z}_q.$$

Let $\underline{\zeta}=(\zeta,\zeta)\in\mu_{q^\infty}^2$ such that $\zeta^{q^N}=\chi(1+q^N,1)=\chi(1,1+q^N)$. Then $\Gamma_\beta(\chi)\in\pi\mathfrak{O}$ if and only if $\hat{\beta}_y(\underline{\zeta}^{y^{-1}})\in\pi\mathfrak{O}$ for all $y\in(1+q\mathbb{Z}_q)^2$.

Proof. This is a special case of [KL25, Lemma 5.3], with $\zeta_1=\zeta_2$ and η running over a set of representatives $\mu_{q-1}^2/\iota(\mu_K)$. We remark that there are two typos in *loc. cit.*: $\underline{\zeta}=(\zeta_1,\zeta_2)$ should be an element of $\mu_{q^\infty}^2$, not μ_{q^∞}, and y should be an element of $(1+q\mathbb{Z}_q)^2$, rather than μ_{q-1}^2. □

Proof of Theorem 5.9. Without loss of generality, we assume that $n=\mathrm{ord}_\pi(R)=0$. Let β be as defined in the statement of Lemma 5.10, and w_K denote the number of elements in μ_K (which is coprime to $p>3$). We have

$$\frac{1}{w_K^2}\Gamma_\alpha(\chi)=\Gamma_\beta(\chi).$$

Recall from [KL25, Lemma 3.5] that if $f\in\mathfrak{O}[x,y]$ is such that the image of f in $J(E)$ is non-zero, then there exists a unique integer $m\geq 0$ satisfying

$$\mathrm{ord}_\pi(f(Q))\geq m\ \forall Q\in\mathcal{S}_{\mathrm{cyc}}\setminus\{0\}$$

with equality holding for almost all $Q\in\mathcal{S}_{\mathrm{cyc}}$. Therefore, combined with the fact that $p\nmid w_K$, we have

$$\mathrm{ord}_\pi(\Gamma_\alpha(\chi))=\mathrm{ord}_\pi(\Gamma_\beta(\chi)).$$

Let us write

$$\alpha_{\eta y}=\alpha|_{\eta_1 y_1(1+q^M\mathbb{Z}_q)\times\eta_2 y_2(1+q^M\mathbb{Z}_q)}$$

for $\eta=(\eta_1,\eta_2)\in\mu_{q-1}^2$ and $y=(y_1,y_2)\in(1+q\mathbb{Z}_q)^2$. Note that $\alpha_{\eta y}$ is an elliptic function measure since it is a restriction of α. Now, write $R_{\eta y}$ for the rational function on E attached to $\alpha_{\eta y}$ (meaning that $\hat{\alpha}_{\eta y}=R_{\eta y}\circ\delta$ as functions on $\mu_{q^\infty}^2$). Moreover, $R_{\eta y}$ takes values in $\mathfrak{O}$; see [KL25, proof of Lemma 3.7]. Let $\tilde{R}_{\eta y}$ denote the function $R_{\eta y}$ modulo π.

Suppose (for the sake of contradiction) that the set of characters $\chi\in\Xi_{\mathrm{cyc}}$ with $\mathrm{ord}_\pi(\Gamma_\alpha(\chi))>0$ is infinite. Equivalently, the set of characters χ such that $\Gamma_\beta(\chi)\in\pi\mathfrak{O}$ is infinite. By Lemma 5.10, for each $y=(y_1,y_2)\in(1+q\mathbb{Z}_q)^2$, we have $\hat{\beta}_y(\underline{\zeta}^{y^{-1}})\in\pi\mathfrak{O}$ for infinitely many $\underline{\zeta}=(\zeta,\zeta)\in\mu_{q^\infty}^2$. Consider the cyclotomic line $\mathcal{S}_{\mathrm{cyc}}\subseteq E_{q^\infty}\simeq\mathcal{E}_{q^\infty}$ where the isomorphism follows as $p\neq q$. From the above discussion, we have an infinite set of elements $Q\in\mathcal{S}_{\mathrm{cyc}}$ such that

$$\sum_{\eta\in\mu_{q-1}^2/\iota(\mu_K)}\tilde{R}_{\eta y}\circ\eta^{-1}(Q)=0$$

since β_y decomposes into $\sum_\eta\alpha_{\eta y}\circ\eta$, where $\alpha_{\eta y}=\alpha|_{\eta y(1+q^M\mathbb{Z}_q)^2}$, and we have $\widehat{\alpha_{\eta y}\circ\eta}(\zeta)=\widehat{\alpha_{\eta y}}(\zeta^{\eta^{-1}})$ (see [Lam15, p. 616]).

Applying Theorem 5.8, we conclude that $\tilde{R}_{\eta y}$ is a constant function. Let $c_{\eta y}$ denote a constant in $\mathfrak{O}$ lifting $\tilde{R}_{\eta y}$ and let δ_0 denote the Dirac measure of $\mathbb{Z}_q^2$ concentrated at $(0,0)$. By definition, the Fourier transform $\hat{\delta}_0$ sends all $\underline{\zeta}\in\mu_{q^\infty}^2$ to 1. Therefore, the Fourier transform of the elliptic function measure $\alpha_{\eta y}-c_{\eta y}\delta_0$ takes values in $\pi\mathfrak{O}$. In particular,

$$\mathrm{ord}_\pi(\alpha_{\eta y}-c_{\eta y}\delta_0)>0.$$

However, if we restrict the measure $\alpha_{\eta y}-c_{\eta y}\delta_0$ to $(\mathbb{Z}_q^\times)^2$, it agrees with $\alpha_{\eta y}$. Thus,

$$\mathrm{ord}_\pi(\alpha_{\eta y})=\mathrm{ord}_\pi(\alpha_{\eta y}-c_{\eta y}\delta_0)>0.$$

Now, summing over all coset representatives $\eta y \in (\mathbb{Z}_q^\times)^2/(1+q^M\mathbb{Z}_q)^2$, we have

$$\mathrm{ord}_\pi(\alpha) = \mathrm{ord}_\pi\left(\sum_{\eta y} \alpha_{\eta y}\right) > 0,$$

which is a contradiction to our hypothesis that $\mathrm{ord}_\pi(R) = 0$. □

5.4. **Analytic side.**

5.4.1. *Review on L-functions.* We review basic notions of L-functions attached to Hecke characters.

Definition 5.11. *Let $\mathfrak{h}$ be an integral ideal of K and ϵ a Hecke character of K whose conductor divides $\mathfrak{h}$. The* imprimitive L-function *of ϵ modulo $\mathfrak{h}$ is defined as*

$$L_{\mathfrak{h}}(\epsilon, s) = \sum_{\gcd(\mathfrak{a},\mathfrak{h})=1} \frac{\epsilon(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

The primitive Hecke L-function *of ϵ is defined as*

$$L(\epsilon, s) = \sum_{\mathfrak{a}\trianglelefteq\mathcal{O}_K} \frac{\epsilon(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

The primitive and imprimitive L-functions defined above only converge on some right half-plane. However, they have analytic continuations to the entire complex plane.

Recall that ψ denotes the Hecke character over K attached to E with conductor $\mathfrak{f}$. Suppose that ϵ is of the form $\varphi\overline{\psi}$, where φ is a finite-order character. We define the *primitive algebraic Hecke L-value* of $\varphi\overline{\psi}$ as

$$L^{(\mathrm{alg})}\left(\varphi\overline{\psi}\right) := \frac{L\left(\varphi\overline{\psi}, 1\right)}{\Omega_\infty},$$

where Ω_∞ is the complex period of E satisfying $\mathcal{L} = \Omega_\infty\mathcal{O}_K$.

5.4.2. *Construction of an elliptic function measure.* We review the construction of a rational function on a CM elliptic curve in [Lam15, §6]. This is a special case of the function constructed in [KL25, §6], which captures L-values of a CM character of infinity type $(1,0)$ twisted by a finite-order character of the $\mathbb{Z}_q^2$-extension.

Let $\mathfrak{h}$ be an ideal of $\mathcal{O}_K$. As before, we write $\mathscr{R}(\mathfrak{h})$ to denote the ray class field of K whose conductor is $\mathfrak{h}$. We fix another ideal $\mathfrak{a}$ that is coprime to $6\mathfrak{f}q$. Define the rational function $\zeta_{\mathfrak{a}}$ on E by

$$\zeta_{\mathfrak{a}}(P) = \prod_Q \big(x(P) - x(Q)\big)^{-1},$$

where Q runs over a set of representatives of $E_{\mathfrak{a}} \setminus \{0\} \pmod{\pm 1}$. There exists a constant $c(\mathfrak{a}) \in K^\times$ such that the function

$$\gamma_{\mathfrak{a}}(P) := c(\mathfrak{a})\zeta_{\mathfrak{a}}(P)$$

has the property that for all $\beta \in \mathrm{End}(E)$ with $\gcd(\beta, \mathfrak{a}) = 1$,

$$\gamma_{\mathfrak{a}}(\beta(P)) = \prod_{R\in\ker(\beta)} \gamma_{\mathfrak{a}}(P \oplus_E R).$$

Define the derivative operator on $\mathbb{C}(E)^\times$ by

$$D(f) = \frac{d}{dz}\log f(z).$$

Consider the complex analytic isomorphism of complex Lie groups

$$\xi(z,\mathcal{L}) : \mathbb{C}/\mathcal{L} \xrightarrow{\sim} E(\mathbb{C}) \quad \text{given by} \quad \xi(z,\mathcal{L}) = \big(\wp(z,\mathcal{L}), \wp'(z,\mathcal{L})\big),$$

where $\wp$ is the Weierstrass $\wp$-function and $\wp'$ is the corresponding derivative.

Let $F_n = \mathscr{R}(\mathfrak{f}q^{n+1})$. Then,

$$\mathrm{Gal}(F_n/K) \simeq \mathrm{Gal}(\mathscr{R}(\mathfrak{f})/K) \times \mathrm{Gal}(F_n/\mathscr{R}(\mathfrak{f})).$$

From now on, we fix a character θ of $\mathrm{Gal}(\mathscr{R}(\mathfrak{f})/K)$ and a primitive $\mathfrak{f}$-division point V. For our chosen ideal $\mathfrak{a}$, we define the rational function on E

$$\vartheta^{(\theta)}_{\mathfrak{a},V}(P) := \sum_{\tau \in \mathrm{Gal}(\mathscr{R}(\mathfrak{f})/K)} \theta^{-1}(\tau)(D\gamma_{\mathfrak{a}})(P \oplus_E V^{\tau}).$$

To simplify the notation, we shall write $\vartheta = \vartheta^{(\theta)}_{\mathfrak{a},V}$. We can associate with ϑ an elliptic function measure, α on $\mathbb{Z}_q^2$ via [KL25, Lemma 3.7]. This α depends on the choice of $\mathfrak{a}$, V, and θ (but we suppress it from the notation). We further define $\alpha^{\times} = \alpha|_{(\mathbb{Z}_q^{\times})^2}$ and write $\vartheta^{\times}$ for the rational function corresponding to $\alpha^{\times}$.

Lemma 5.12. *Suppose that $\mathfrak{a} = (\lambda)$ is such that $\lambda \notin \mu_K$, $(\lambda, 6\mathfrak{p}\mathfrak{f}q) = 1$, and $\lambda \equiv 1 \mod \mathfrak{f}$. Then*

$$\mathrm{ord}_{\pi}(\vartheta) = \mathrm{ord}_{\pi}\left(\vartheta^{\times}\right) = 0.$$

Proof. By [Lam15, Lemma 6.7], we have $\mathrm{ord}_{\pi}(\vartheta) = 0$. Furthermore, Lemma 6.8 in *op. cit.* can be adapted to prove that

$$\sum_{Q \in E_{\mathfrak{b}}} \vartheta(P \oplus_E Q) = \theta(\tau_{\mathfrak{b}})\,\psi(\mathfrak{b})\,\vartheta\left(\psi(\mathfrak{b})P\right)$$

for any ideal of $\mathcal{O}_K$ that is coprime to $\mathfrak{a}\mathfrak{f}$. Hence, combined with Lemma 5.4, we deduce

$$\vartheta^{\times}(P) = \vartheta(P) - \frac{1}{q}\theta(\tau_{\mathfrak{q}})\,\psi(\mathfrak{q})\,\vartheta(\psi(\mathfrak{q})P) - \frac{1}{q}\theta(\tau_{\mathfrak{q}^*})\,\psi(\mathfrak{q}^*)\,\vartheta(\psi(\mathfrak{q}^*)P) + \frac{1}{q^2}\theta(\tau_{\mathfrak{q}\mathfrak{q}^*})\,\psi(\mathfrak{q}\mathfrak{q}^*)\,\vartheta(\psi(\mathfrak{q}\mathfrak{q}^*)P)$$

(see also [Lam14, Lemma 3.1.8]).

We recall from [Lam15, proof of Lemma 6.7] and [Lam14, proof of Theorem 3.1.9] that the poles of the function $\tilde{f} : P \mapsto \vartheta(P) \mod \pi$ are precisely elements of the form $U \ominus_E V^{\tau}$, where $U \in E_{\mathfrak{a}} \setminus \{0\}$ and $\tau \in \mathrm{Gal}(\mathscr{R}(\mathfrak{f})/K)$. In particular, there exists a primitive $\mathfrak{f}\mathfrak{a}q$-division point P such that $\tilde{f}$ has a pole at $\psi(\mathfrak{q}\mathfrak{q}^*)P$ and $\tilde{f}$ is regular at P, $\psi(\mathfrak{q})P$, and $\psi(\mathfrak{q}^*)P$. Thus, the function

$$P \mapsto \tilde{f}(P) - \frac{1}{q}\theta(\tau_{\mathfrak{q}})\,\psi(\mathfrak{q})\,\tilde{f}(\psi(\mathfrak{q})P) - \frac{1}{q}\theta(\tau_{\mathfrak{q}^*})\,\psi(\mathfrak{q}^*)\,\tilde{f}(\psi(\mathfrak{q}^*)P) + \frac{1}{q^2}\theta(\tau_{\mathfrak{q}\mathfrak{q}^*})\,\psi(\mathfrak{q}\mathfrak{q}^*)\,\tilde{f}(\psi(\mathfrak{q}\mathfrak{q}^*)P)$$

is non-zero. Hence, $\mathrm{ord}_{\pi}\left(\vartheta^{\times}\right) = 0$, as desired. □

Let $F_{\infty} = \bigcup_{n \geq 1} \mathscr{R}(\mathfrak{f}q^n)$. Under the identification of $\mathrm{Gal}(F_{\infty}/\mathscr{R}(\mathfrak{f}q)) \simeq (1 + q\mathbb{Z}_q)^2$, we have:

Lemma 5.13. *Let χ be a character of $\mathrm{Gal}(F_n/\mathscr{R}(\mathfrak{f}q))$. Then*

$$\mathrm{ord}_{\pi}\left(\Gamma_{\alpha^{\times}}(\chi)\right) = \mathrm{ord}_{\pi}\left(\left(N(\mathfrak{a}) - \psi(\mathfrak{a})\theta\chi(\tau_{\mathfrak{a}})\right) L^{(\mathrm{alg})}_{\mathfrak{f}q}\left(\overline{\theta\chi\psi}\right)\right).$$

Proof. This is a special case of [KL25, Lemma 6.9]. □

Theorem 5.14. *For almost all finite-order characters χ of Ξ_{cyc},*

$$\mathrm{ord}_{\pi}\left(L^{(\mathrm{alg})}(\overline{\theta\chi\psi})\right) = 0.$$

Proof. Suppose that $\mathfrak{a} = (\lambda)$ is chosen as in Lemma 5.12. In particular, $\mathrm{ord}_{\pi}\left(\vartheta^{\times}\right) = 0$. After combining Lemma 5.13 and Theorem 5.9, we deduce

$$\mathrm{ord}_{\pi}\left(\left(N(\mathfrak{a}) - \psi(\mathfrak{a})\theta\chi(\tau_{\mathfrak{a}})\right) L^{(\mathrm{alg})}_{\mathfrak{f}q}\left(\overline{\theta\chi\psi}\right)\right) = \mathrm{ord}_{\pi}\left(\vartheta^{\times}\right) = 0.$$

It remains to show that for all but finitely many χ, the following holds

$$\mathrm{ord}_{\pi}\left(N(\mathfrak{a}) - \psi(\mathfrak{a})\theta\chi(\tau_{\mathfrak{a}})\right) = 0.$$

As in [Lam15, proof of Theorem 6.6], this is equivalent to the following

$$\bar{\lambda}\theta^{-1}(\tau_{\mathfrak{a}}) \not\equiv \chi(\tau_{\mathfrak{a}}) \mod \pi\mathfrak{O}.$$

This holds whenever χ is of order q^m, where $m \geq \mathrm{ord}_{\mathfrak{q}}(\lambda^{q-1}-1)-1$. Thus,

$$\mathrm{ord}_\pi\left(L_{\mathfrak{f}q}^{(\mathrm{alg})}(\overline{\theta\chi\psi})\right) = 0$$

for almost all χ. A similar argument applied to the Euler factors at primes dividing $\mathfrak{f}q$ implies that

$$\mathrm{ord}_\pi\left(L_{\mathfrak{f}q}^{(\mathrm{alg})}(\overline{\theta\chi\psi})\right) = \mathrm{ord}_\pi\left(L^{(\mathrm{alg})}(\overline{\theta\chi\psi})\right)$$

for almost all χ, which concludes the proof. □

We now prove the analytic NECV Conjecture for CM elliptic curves.

Corollary 5.15. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by the ring of integers of an imaginary quadratic field (of class number 1). Let p, q be distinct primes ≥ 5 which are both primes of good ordinary reduction for E. Then $\mathrm{ord}_p\left(\dfrac{L(E,\chi,1)}{\Omega_E}\right) = 0$ for all but finitely many $\chi \in \Xi_q$.*

Proof. Recall the definition of the algebraic L-function

$$L^{(\mathrm{alg})}(\overline{\theta\chi\psi}) := \frac{L(\overline{\theta\chi\psi},1)}{\Omega_\infty},$$

where θ is a finite-order character, ψ is the Hecke character over K attached to E, and $\chi \in \Xi_{\mathrm{cyc}}$.

To prove the analytic NECV Conjecture for CM elliptic curves, it will suffice to compare the periods. Indeed, recall from [Shi71, (7.8.11) on p. 219] and [CW77, discussion on p. 251] that the Hasse–Weil L-function of $E/\mathbb{Q}$ is equal to $L_{\mathfrak{f}q}(\psi, s) = L_{\mathfrak{f}q}(\overline{\psi}, s)$ up to finitely many Euler factors (which do not vanish at $s=1$), and analogously for twists. Thus, combining Lemma 3.1 and Theorem 5.14, we deduce

$$\mathrm{ord}_p\left(\frac{L(E,\chi,1)}{\Omega_\infty}\right) = 0 \tag{5.2}$$

for all but finitely many $\chi \in \Xi_q$.

Recall that Ω_∞ satisfies $\mathcal{L} = \Omega_\infty \mathcal{O}_K$ and $E(\mathbb{C}) = \mathbb{C}/\mathcal{L}$. Thus, if we write $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$, the real and imaginary Néron periods of E belong to $\{\zeta\Omega_\infty : \zeta \in \mu_K\} \cup \{\zeta\tau\Omega_\infty : \zeta \in \mu_K\}$. In particular, Ω_∞ and Ω_E differ by a p-adic unit. Thus, we may replace Ω_∞ by Ω_E in (5.2), as desired. □

5.5. **Algebraic side.** We closely follow the strategy of [Lam15, Section 7] to prove our main result.

5.5.1. *Iwasawa Main Conjecture.* Fix an elliptic curve $E/\mathbb{Q}$ with complex multiplication by an imaginary quadratic field K, and an odd prime p of good ordinary reduction as before. Let $\mathfrak{p} \mid p$ be a prime of K and set $L = K(E_{\mathfrak{p}})$. It follows that $L_\infty = K(E_{\mathfrak{p}^\infty})$ is a $\mathbb{Z}_p$-extension of L. We write

$$\Delta_0 = \mathrm{Gal}(L/K), \quad \Gamma_{\mathfrak{p}} = \mathrm{Gal}(L_\infty/L) \simeq \mathbb{Z}_p, \quad \mathcal{G} = \mathrm{Gal}(L_\infty/K) \simeq \Delta_0 \times \Gamma_{\mathfrak{p}}.$$

For $n \geq 0$, let K_n^c be the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of K and set

$$L_n = K_n^c(E_{\mathfrak{p}}) \quad \text{and} \quad L_{n,\infty} = K_n^c(E_{\mathfrak{p}^\infty}).$$

We further write

$$\Delta_n = \mathrm{Gal}(L_n/K) \quad \text{and} \quad \mathcal{G}_n = \mathrm{Gal}(L_{n,\infty}/K).$$

Set $\mathcal{K} = L_{n,\infty}$. For each finite extension $\mathfrak{L}$ of K_n^c contained inside $\mathcal{K}$, write $A(\mathfrak{L})$ for the p-part of the ideal class group of $\mathfrak{L}$, $\mathcal{E}(\mathfrak{L})$ for the group of global units of $\mathfrak{L}$, $\mathcal{C}(\mathfrak{L})$ for the group of elliptic units of $\mathfrak{L}$, and write $\mathcal{U}(\mathfrak{L})$ to denote the group of local units of $\mathfrak{L} \otimes K_{\mathfrak{p}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$. Further, define $\overline{\mathcal{E}}(\mathfrak{L})$ and $\overline{\mathcal{C}}(\mathfrak{L})$ as the closures of $\mathcal{E}(\mathfrak{L}) \cap \mathcal{U}(\mathfrak{L})$ and $\mathcal{C}(\mathfrak{L}) \cap \mathcal{U}(\mathfrak{L})$, respectively, in $\mathcal{U}(\mathfrak{L})$. Define

$$A_{\mathcal{K}} = \varprojlim_{\mathfrak{L}} A(\mathfrak{L}), \quad \mathcal{U}_{\mathcal{K}} = \varprojlim_{\mathfrak{L}} \mathcal{U}(\mathfrak{L}), \quad \overline{\mathcal{E}}_{\mathcal{K}} = \varprojlim_{\mathfrak{L}} \overline{\mathcal{E}}(\mathfrak{L}), \quad \overline{\mathcal{C}}_{\mathcal{K}} = \varprojlim_{\mathfrak{L}} \overline{\mathcal{C}}(\mathfrak{L}),$$

where all inverse limits are over finite extensions $\mathfrak{L}/F$ in $\mathcal{K} = L_{n,\infty}$, with respect to the norm maps.

We write $M_{\mathcal{K}}$ for the maximal abelian p-extension of $\mathcal{K}$ which is unramified outside the primes above $\mathfrak{p}$ and set $X_{\mathcal{K}} = \mathrm{Gal}(M_{\mathcal{K}}/\mathcal{K})$. In view of global class field theory, we have the following exact sequence

$$0 \longrightarrow \overline{\mathcal{E}}_{\mathcal{K}}/\overline{\mathcal{C}}_{\mathcal{K}} \longrightarrow \mathcal{U}_{\mathcal{K}}/\overline{\mathcal{C}}_{\mathcal{K}} \longrightarrow X_{\mathcal{K}} \longrightarrow A_{\mathcal{K}} \longrightarrow 0. \tag{5.3}$$

When E has good ordinary reduction at p, then $\mathcal{U}_{\mathcal{K}}/\overline{\mathcal{C}}_{\mathcal{K}}$ and $X_{\mathcal{K}}$ are torsion Iwasawa modules. An argument involving the Euler system of elliptic units is used to show that the (torsion) Iwasawa modules $\overline{\mathcal{E}}_{\mathcal{K}}/\overline{\mathcal{C}}_{\mathcal{K}}$ and $A_{\mathcal{K}}$ have the same characteristic ideal. Thus,

$$\text{(R-IMC)} \qquad \operatorname{char}_{\Lambda}(\mathcal{U}_{\mathcal{K}}/\overline{\mathcal{C}}_{\mathcal{K}}) = \operatorname{char}_{\Lambda}(X_{\mathcal{K}}).$$

Here, Λ is used to denote the (usual) 1-variable Iwasawa algebra. The above equality is (Rubin's) one-variable Iwasawa Main Conjecture for CM elliptic curves.

5.5.2. *An auxiliary step.* We first record a technical result from [Lam15]. Recall that

$$\Delta_n = \operatorname{Gal}(L_n/K) \simeq \operatorname{Gal}(K_n^c/K) \times \operatorname{Gal}(L_n/K_n^c) \simeq H_n \times \Delta_0,$$

where $H_n = \operatorname{Gal}(K_n^c/K) \simeq \mathbb{Z}/q^n\mathbb{Z}$. Any character ϱ of Δ_n is of the form $\varrho = \chi\theta_{\mathfrak{p}}^r$ where χ is a character of H_n (which is identified with a finite-order character of Ξ_{cyc}) and $\theta_{\mathfrak{p}}$ is the character of Δ_0 induced by its action on $E_{\mathfrak{p}}$, and r is a residue class modulo $p-1$.

Let $\mathfrak{D}$ (resp. $\mathfrak{D}_n$) denote the decomposition subgroup at $\mathfrak{p}$ inside $\mathcal{G}$ (resp. $\mathcal{G}_n$). Write $\mathfrak{P}$ to denote the prime above $\mathfrak{p}$ in L_∞. Note that $\mu_{p^\infty}(L_{\infty,\mathfrak{P}}) = \mu_{p^m}$ where m can be made precise (but is not required for our purposes). When $m \geq 1$, we say that E/K is *anomalous* at $\mathfrak{p}$. Since $p \nmid [L:K]$, the action of $\Delta_0 \cap \mathfrak{D}$ on μ_{p^m} gives a $\mathbb{Z}_p$-valued character

$$\varrho_{\mathrm{cyc}} \colon \Delta_0 \cap \mathfrak{D} \longrightarrow \mu_{p-1} \subset \mathbb{Z}_p^\times.$$

Theorem 5.16. *Suppose that $\varrho = \chi\theta_{\mathfrak{p}}$ is a character of $\Delta_n = H_n \times \Delta_0$. When E/K_n^c is anomalous at $\mathfrak{p}$, assume further that $\varrho|_{\Delta_n \cap \mathfrak{D}_n} \neq \varrho_{\mathrm{cyc}}$. Then*

$$\operatorname{ord}_\pi\left(\left(N(\mathfrak{a}) - \psi(\mathfrak{a})\chi(\tau_{\mathfrak{a}})\right) L_{\mathfrak{f}q}^{(\mathrm{alg})}(\overline{\chi\psi})\right) = 0 \Longrightarrow \overline{\mathcal{C}}_{n,\infty}^{\varrho} = \mathcal{U}_{n,\infty}^{\varrho}.$$

Proof. This is [Lam15, Theorem 7.7]. □

5.5.3. *Application.* Fix an integer $N \geq 0$ and let $n \geq N$. Instead of writing $\mathcal{Y}_{L_{n,\infty}}$, we will use the notation $\mathcal{Y}_{n,\infty}$, where $\mathcal{Y} \in \{X, \mathcal{U}, \overline{\mathcal{C}}\}$.

Theorem 5.17. *There exists an integer $N \geq 0$ such that $X_{n,\infty} = X_{N,\infty}$ for all $n \geq N$.*

Proof. The proof strategy we employ here is the same as [Lam15, Theorem 7.8]. We provide only a sketch of the proof that highlights the key differences.

Claim: To prove the theorem, it suffices to show that there exists $N \geq 0$ such that for all $n \geq N$,

$$\mathcal{U}_{n,\infty}/\overline{\mathcal{C}}_{n,\infty} = \mathcal{U}_{N,\infty}/\overline{\mathcal{C}}_{N,\infty}.$$

Justification: Indeed, once we prove the above equality, it follows from (R-IMC) that for all $n \geq N$

$$\operatorname{char}_{\Lambda}(X_{n,\infty}) = \operatorname{char}_{\Lambda}(X_{N,\infty}).$$

Consider the (surjective) restriction map $\pi_{n,N} : X_{n,\infty} \to X_{N,\infty}$. Since $\operatorname{char}_\Lambda$ is multiplicative in exact sequences, it forces the kernel of $\pi_{n,N}$ to be a finite $\Lambda(\mathcal{G}_n)$-module. Thus, $\ker(\pi_{n,N})$ must in fact be trivial as $X_{n,\infty}$ has no non-trivial finite $\Lambda(\mathcal{G}_n)$-submodules; see [Gre78, Theorem 1]. This shows the desired equality in the theorem, thereby proving the claim.

Choose λ as before so that $\mathfrak{a} = (\lambda)$. Fix $n_0 \geq 0$ such that E/K_{n_0} is anomalous at $\mathfrak{p}$. From now on, assume that $n \geq n_0$. Recall that the number of characters of Δ_n satisfying

$$\varrho|_{\Delta_n \cap \mathfrak{D}_n} = \varrho_{\mathrm{cyc}}$$

is a constant (independent of n) when $n \gg 0$. Thus, there exists an integer N such that for all $n \geq N$, the characters ϱ of Δ_n satisfying the above condition must factor through Δ_N. In other words, it follows from Theorem 5.16 that there exists $N \gg 0$ such that for all $n \geq N$, all characters ϱ of Δ_n that *do not* factor through Δ_N satisfy

$$\overline{\mathcal{C}}_{n,\infty}^{\varrho} = \mathcal{U}_{n,\infty}^{\varrho}.$$

Set $\mathcal{O}_{\mathrm{ur}}$ as the ring of integers of the completion of $\mathbb{Q}_p^{\mathrm{ur}}$. We have the decomposition

$$\mathcal{U}_{n,\infty}/\overline{\mathcal{C}}_{n,\infty}\hat{\otimes}_{\mathbb{Z}_p}\mathcal{O}_{\mathrm{ur}} = \bigoplus_{\varrho\in\widehat{\Delta_n}} (\mathcal{U}_{n,\infty}/\overline{\mathcal{C}}_{n,\infty})^{\varrho}.$$

Moreover, $\mathcal{U}_{N,\infty}/\overline{\mathcal{C}}_{N,\infty}\hat{\otimes}_{\mathbb{Z}_p}\mathcal{O}_{\mathrm{ur}}$ is the direct sum of the ϱ-components that factor through the restriction map $\Delta_n \to \Delta_N$. This completes the proof. □

The main result we prove in this section is the following theorem on the algebraic NECV Conjecture for CM curves.

Theorem 5.18. *There exists an integer $m \geq 0$ such that, for all $n \geq m$, the restriction map*

$$\mathrm{Sel}(E_{p^\infty}/K_m^c) \xrightarrow{\sim} \mathrm{Sel}(E_{p^\infty}/K_n^c)$$

is an isomorphism. In particular, there exists $m \geq 0$ such that $\mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(m)}) \simeq \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)})$ for all $n \geq m$.

Proof. We first recall a result of J. Coates (see [Coa83, Theorem 12]), which allows us to relate the Galois module $X_{n,\infty}$ to the Selmer group $\mathrm{Sel}(E_{\mathfrak{p}^\infty}/L_{n,\infty})$; more precisely

$$\mathrm{Sel}(E_{\mathfrak{p}^\infty}/L_{n,\infty}) \simeq \mathrm{Hom}(X_{n,\infty}, E_{\mathfrak{p}^\infty}) \text{ for all } n \geq 0.$$

Set $\mathrm{Sel}'(E_{\mathfrak{p}^\infty}/K_n^c) = \ker\left(H^1(K_n^c, E_{\mathfrak{p}^\infty}) \longrightarrow \prod_{v\nmid\mathfrak{p}} H^1(K_{n,v}^c, E)_{\mathfrak{p}^\infty}\right)$ and define $\mathrm{Sel}'(E_{\mathfrak{p}^\infty}/L_{n,\infty})$ similarly. It follows from [Coa83, Lemma 8 and Theorem 9] that

$$\mathrm{Sel}'(E_{\mathfrak{p}^\infty}/K_n^c) \simeq \mathrm{Sel}'(E_{\mathfrak{p}^\infty}/L_{n,\infty})^{\mathrm{Gal}(L_{n,\infty}/K_n^c)} = \mathrm{Sel}(E_{\mathfrak{p}^\infty}/L_{n,\infty})^{\mathrm{Gal}(L_{n,\infty}/K_n^c)}.$$

Since $p = \mathfrak{p}\mathfrak{p}^*$, we can write

$$\mathrm{Sel}(E_{p^\infty}/K_n^c) = \mathrm{Sel}(E_{\mathfrak{p}^\infty}/K_n^c) \oplus \mathrm{Sel}(E_{\mathfrak{p}^{*\infty}}/K_n^c).$$

Claim: Fix N as in Theorem 5.17. Then,

$$\mathrm{Sel}(E_{\mathfrak{p}^\infty}/K_n^c) \simeq \mathrm{Sel}(E_{\mathfrak{p}^\infty}/K_N^c) \text{ for all } n \geq N.$$

Justification: Consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(E_{\mathfrak{p}^\infty}/K_n^c) & \longrightarrow & \mathrm{Sel}'(E_{\mathfrak{p}^\infty}/K_n^c) & \longrightarrow & \prod_{v|\mathfrak{p}} H^1(K_{n,v}, E)_{\mathfrak{p}^\infty} \\
 & & \downarrow s & & \downarrow f & & \downarrow \gamma \\
0 & \longrightarrow & \mathrm{Sel}(E_{\mathfrak{p}^\infty}/K_N^c) & \longrightarrow & \mathrm{Sel}'(E_{\mathfrak{p}^\infty}/K_N^c) & \longrightarrow & \prod_{v|\mathfrak{p}} H^1(K_{N,v}, E)_{\mathfrak{p}^\infty}.
\end{array}$$

Since $X_{n,\infty} = X_{N,\infty}$ for all $n \geq N$ by Theorem 5.17, it follows from the above discussion that f is an isomorphism. In particular, s is injective. Using the inflation-restriction exact sequence and the fact that $p \neq q$, we deduce that $\ker(\gamma)$ is trivial. Applying a snake lemma argument, we conclude that s is surjective. This proves the claim.

The same argument implies that there exists an integer N' such that

$$\mathrm{Sel}(E_{\mathfrak{p}^{*\infty}}/K_n^c) \simeq \mathrm{Sel}(E_{\mathfrak{p}^{*\infty}}/K_{N'}^c) \text{ for all } n \geq N'.$$

Setting $m = \max\{N, N'\}$ gives

$$\mathrm{Sel}(E_{p^\infty}/K_m^c) \simeq \mathrm{Sel}(E_{p^\infty}/K_n^c)$$

for all $n \geq m$. The final assertion of the theorem follows from the decomposition

$$\mathrm{Sel}(E_{p^\infty}/K_n^c) \simeq \mathrm{Sel}(E_{p^\infty}/\mathbb{Q}_{(n)}) \oplus \mathrm{Sel}(E^K_{p^\infty}/\mathbb{Q}_{(n)}),$$

where E^K is the quadratic twist of E over K. □

References

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BL26] Andrea Bandini and Ignazio Longhi, *The algebra $\mathbb{Z}_\ell[\![\mathbb{Z}_p^d]\!]$ and applications to Iwasawa theory*, J. London Math. Soc. **113** (2026), no. 6, e70601.

[BSTW24] Ashay Burungale, Christopher Skinner, Ye Tian, and Xin Wan, *Zeta elements for elliptic curves and applications*, 2024, preprint, arXiv:2409.01350.

[CÇSS18] Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On the Iwasawa main conjectures for modular forms at non-ordinary primes*, 2018, preprint, arXiv:1804.10993.

[Coa83] John Coates, *Infinite descent on elliptic curves with complex multiplication*, Arithmetic and Geometry: Papers Dedicated to IR Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic, Springer, 1983, pp. 107–137.

[CW77] John Coates and Andrew Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.

[DD15] Tim Dokchitser and Vladimir Dokchitser, *Growth of Tate-Shafarevich group in towers for isogenous curves*, Compositio Mathematica **151** (2015), no. 11, 1981–2005.

[FL82] Jean-Marc Fontaine and Guy Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup. (4) **15** (1982), no. 4, 547–608.

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

[Gre78] Ralph Greenberg, *On the structure of certain Galois groups*, Invent. math. **47** (1978), no. 1, 85–99.

[Gre99a] ———, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry. IAS/Park City Math. Ser **9** (1999), 407–464.

[Gre99b] ———, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.

[IM15] Adrian Iovita and Adriano Marmora, *On the continuity of the finite Bloch-Kato cohomology*, Rend. Semin. Mat. Univ. Padova **134** (2015), 239–271.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[KL23] Debanjana Kundu and Antonio Lei, *Growth of p-parts of ideal class groups and fine Selmer groups in $\mathbb{Z}_q$-extensions with $p \neq q$*, Acta Arithmetica **207** (2023), 297–313.

[KL25] ———, *Non-vanishing modulo p of Hecke L-values over imaginary quadratic fields*, Israel J. Math. **266** (2025), no. 1, 307–339.

[Lam14] Jack Lamplugh, *Class numbers and Selmer groups in $\mathbb{Z}_S$-extensions of imaginary quadratic fields*, Ph.D. thesis, University of Cambridge, 2014.

[Lam15] ———, *An analogue of the Washington–Sinnott theorem for elliptic curves with complex multiplication I*, J. London Math. Soc. **91** (2015), no. 3, 609–642.

[LPP24] Antonio Lei, Robert Pollack, and Naman Pratap, *On the Iwasawa invariants of Mazur–Tate elements of elliptic curves at additive primes*, 2024, preprint, arXiv:2412.16629.

[Maz78] Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[PR04] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.

[Roh88] David E. Rohrlich, *L-functions and division towers*, Math. Ann. **281** (1988), no. 4, 611–632.

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[Rub00] ———, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Shi71] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, vol. No. 1, Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971, Publications of the Mathematical Society of Japan, No. 11.

[Sin87a] Warren Sinnott, *Γ-transforms of rational function measures on $\mathbf{Z}_S$*, Invent. Math. **89** (1987), no. 1, 139–157.

[Sin87b] ———, *On a theorem of L. Washington*, Astérisque **147** (1987), no. 148, 209–224.

[Spr24] Florian Ito Sprung, *On Iwasawa main conjectures for elliptic curves at supersingular primes: beyond the case $a_p = 0$*, Adv. Math. **449** (2024), Paper No. 109741, 47.

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

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.

[Tat84] John Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, Progress in Mathematics, vol. 47, Birkhäuser Boston, Inc., Boston, MA, 1984, notes by Bernardi, Dominique and Schappacher, Norbert.
[Vat99] Vinayak Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419.
[Was75] Lawrence C Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. **214** (1975), no. 2, 177–193.
[Was78] ———, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. **49** (1978), no. 1, 87–97.

(Kundu) Department of Mathematics and Statistics, University of Regina, 3737 Wascana Pkwy, Regina, SK, Canada S4S 0A2
Email address: debanjana.kundu@uregina.ca

(Lei) Department of Mathematics and Statistics, University of Ottawa, 150 Louis-Pasteur Pvt, Ottawa, ON, Canada K1N 6N5
Email address: antonio.lei@uottawa.ca