

MAIN CONJECTURES FOR NON-CM ELLIPTIC CURVES AT GOOD ORDINARY PRIMES

XIAOJUN YAN AND XIUWU ZHU

ABSTRACT. Let E/\mathbb{Q} be an elliptic curve, K an imaginary quadratic field, and let $p > 2$ be a prime that splits in K and at which E has good ordinary reduction. Assume that the residual Galois representation associated with (E, p) is irreducible. In this paper, we establish new cases of the two-variable Iwasawa main conjecture for E over K . As applications, we obtain more general results on the p -converse theorem and the p -part of the Birch and Swinnerton-Dyer formula in rank at most one.

CONTENTS

1. Introduction	1
1.1. Main result	2
1.2. Strategy	3
1.3. Acknowledgment	4
2. Selmer groups	4
2.1. Selmer groups for Iwasawa algebras	4
2.2. Selmer groups for Hida families	8
3. p -adic L -functions	9
3.1. A three-variable p -adic L -function	9
3.2. Two variable p -adic L -functions: type I	9
3.3. Cyclotomic p -adic L -function	10
3.4. Two variable p -adic L -functions: type II	11
3.5. BDP p -adic L -function	11
4. Main conjectures over K_∞	12
4.1. Two variable Iwasawa main conjectures	12
4.2. A three variable Iwasawa main conjecture	12
4.3. Proof of Theorem 4.2	13
5. Applications	14
5.1. Cyclotomic main conjectures	14
5.2. Anticyclotomic main conjectures	16
5.3. BSD conjectures	17
Conflict of interest	17
References	17

1. INTRODUCTION

Let E be an elliptic curve over \mathbb{Q} . Fix an odd prime p and embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let $T_p E$ denote the p -adic Tate module of E , $\rho_E : G_{\mathbb{Q}} \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ the associated p -adic Galois representation, and $\overline{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[p])$ the corresponding residual representation, i.e., the reduction modulo p of ρ_E .

To study the arithmetic properties of E , such as those predicted by the Birch and Swinnerton-Dyer conjecture, one often turns to tools from Iwasawa theory. There are two central objects in Iwasawa theory: Selmer groups over Iwasawa extensions and p -adic L -functions. The Iwasawa main conjectures establish a deep connection between them.

Let K be an imaginary quadratic field. Suppose that $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K , where \mathfrak{p} is the prime determined by the embedding ι_p . Let K_∞^+ and K_∞^- denote the cyclotomic and anticyclotomic \mathbb{Z}_p -extensions of K , respectively, and set $K_\infty = K_\infty^+ K_\infty^-$. Then the associated Iwasawa algebras are given

Key words and phrases. elliptic curve, Iwasawa main conjecture.

by

$$\Lambda_K^\pm = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty^\pm/K)]], \quad \Lambda_K = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]].$$

For any locally compact \mathbb{Z}_p -module M , let $M^\vee := \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ denote its Pontryagin dual.

We consider the following two types of Selmer groups over K_∞ :

- (1) the Λ_K -module Selmer group $H_{\mathcal{F}_{\mathrm{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)$, with ordinary local conditions at $v \mid p$;
- (2) the Λ_K -module Selmer group $H_{\mathcal{F}_{\mathrm{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)$, with relaxed local conditions at $v = \mathfrak{p}$ and strict conditions at $v = \bar{\mathfrak{p}}$.

As in Castella-Grossi-Skinner [CGS25], we have two versions of the two-variable p -adic L -function:

- (1) $\mathcal{L}_p^{\mathrm{PR}}(E/K) \in \Lambda_K$, which interpolates the algebraic parts of $L(E/K, \chi^{-1}, 1)$ for finite order characters χ of $\mathrm{Gal}(K_\infty/K)$;
- (2) $\mathcal{L}_p^{\mathrm{Gr}}(E/K) \in \Lambda_K^{\mathrm{ur}} := \Lambda_K \widehat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$, which interpolates the algebraic parts of $L(E/K, \chi, 1)$ for characters χ of $\mathrm{Gal}(K_\infty/K)$ with infinity type (b, a) such that $a \leq -1$ and $b \geq 1$, where $\mathbb{Z}_p^{\mathrm{ur}}$ denotes the ring of integers of the maximal unramified extension of \mathbb{Q}_p .

Conjecture 1.1. *Suppose that the residual representation $\bar{\rho}_E|_{G_K}$ is irreducible.*

- (1) $H_{\mathcal{F}_{\mathrm{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee$ is a torsion Λ_K -module and

$$\mathrm{Char}_{\Lambda_K} (H_{\mathcal{F}_{\mathrm{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee) = (\mathcal{L}_p^{\mathrm{PR}}(E/K)).$$

- (2) $H_{\mathcal{F}_{\mathrm{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee$ is a torsion Λ_K -module and

$$\mathrm{Char}_{\Lambda_K} (H_{\mathcal{F}_{\mathrm{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee) \Lambda_K^{\mathrm{ur}} = (\mathcal{L}_p^{\mathrm{Gr}}(E/K)).$$

1.1. Main result.

Theorem 1.2. *Suppose that the Heegner hypothesis holds (in particular, $\mathrm{sign}(E/K) = -1$), and that $\bar{\rho}_E|_{G_K}$ is absolutely irreducible. Then:*

- (1) $H_{\mathcal{F}_{\mathrm{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee$ is a torsion Λ_K -module, and

$$\mathrm{Char}_{\Lambda_K} (H_{\mathcal{F}_{\mathrm{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee) \subset (\mathcal{L}_p^{\mathrm{PR}}(E/K)).$$

- (2) $H_{\mathcal{F}_{\mathrm{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee$ is a torsion Λ_K -module, and

$$\mathrm{Char}_{\Lambda_K} (H_{\mathcal{F}_{\mathrm{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee) \Lambda_K^{\mathrm{ur}} \subset (\mathcal{L}_p^{\mathrm{Gr}}(E/K)).$$

Moreover, if

(Im) *there exists $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that $T_p E / (\rho_E(\tau) - 1)T_p E$ is free of rank one over \mathbb{Z}_p*

then Conjecture 1.1 holds.

Skinner-Urban [SU14] first proved Conjecture 1.1(1) using Eisenstein congruences on $GU(2, 2)$ under certain assumptions, in particular when $\mathrm{sign}(E/K) = +1$. Wan [Wan20, Wan21] proved Conjecture 1.1(2) via Eisenstein congruences on $GU(3, 1)$ under different assumptions, specifically when $\mathrm{sign}(E/K) = -1$ and E is semistable.

In [BSTW24], Burungale-Skinner-Tian-Wan established an equivalence between parts (1) and (2) of Conjecture 1.1 by employing Beilinson-Flach elements and an explicit reciprocity law. This, combined with the result of Skinner-Urban concerning Conjecture 1.1(1), enabled them to prove new cases of Conjecture 1.1(2).

Our proof of Theorem 1.2 adopts an approach similar to that presented in [BSTW24]. A key observation is that, under more general conditions, Skinner-Urban in fact proved that the left-hand side of Conjecture 1.1(1) is contained in the right-hand side after tensoring with the field of fractions of Λ_K^+ . To achieve full equality, they applied Vatsal's non-vanishing result [Vat03] on the μ -invariant of the anticyclotomic projection of $\mathcal{L}_p^{\mathrm{PR}}(E/K)$ to show that $\mathrm{ord}_P(\mathcal{L}_p^{\mathrm{PR}}(E/K)) = 0$ for height-one primes P of Λ_K coming from Λ_K^+ . This required the following conditions:

- (1) $N = N^+ N^-$, where N^+ is divisible only by primes that split in K and N^- is a square-free product of an odd number of primes that are inert in K , implying $\mathrm{sign}(E/K) = +1$;
- (2) For every $\ell \mid N^-$, the residual representation satisfies $\bar{\rho}_E|_{I_\ell} \neq 1$, where I_ℓ is the inertia subgroup at ℓ .

In particular, this forces E to have a bad semistable prime.

In this paper, using the equivalence in [BSTW24], we translate Skinner-Urban's results on Conjecture 1.1(1) into the setting of Conjecture 1.1(2). This allows us to conclude that the left-hand side of Conjecture 1.1(2) is contained in the right-hand side after tensoring with the fractional field of Λ_K^+ .

To obtain a full inclusion, we apply Hsieh's result [Hsi14] on the non-vanishing of the μ -invariant of the anticyclotomic projection of $\mathcal{L}_p^{\text{Gr}}(E/K)$ in the case $\text{sign}(E/K) = -1$. Since we work under the Heegner hypothesis, we can avoid the assumption that E has a bad semistable prime.

As in [SU14], we then invoke Kato's theorem on Mazur's main conjecture [Kat04] to complete the proof of Theorem 1.2.

Remark 1.3. Recently, using Wan's extension of Skinner-Urban's method to the setting of Hilbert modular forms [Wan15], together with a base change argument, Burungale-Castella-Skinner [BCS25] proved the rational version of Conjecture 1.1 (i.e., equality after tensoring with \mathbb{Q}_p) under the assumptions that $p > 3$ and $\bar{\rho}_E$ is irreducible, and proved the integral version when condition (Im) also holds.

Roughly speaking, by choosing a suitable real quadratic field F and a CM extension K'/F with $[K' : F] = 2$, they study a three-variable main conjecture for E_F/K' analogous to Conjecture 1.1(1). Following Skinner-Urban's method, Wan proves one direction of the divisibility result, similar to [SU14], and applies a non-vanishing theorem for the μ -invariant of an anticyclotomic p -adic L -function over totally real fields [Hum17].

In their setup, the analogue of N^- is a square-free product of an even number of primes of F inert in K' , which in particular may be trivial. Thus, they can derive results on various main conjectures for E without requiring E to have bad semistable reduction. Their arguments require $p > 3$ in order to apply [Hum17], but do not require (E, K) to satisfy the Heegner hypothesis.

As an application, we prove additional cases of one-variable main conjectures, the p -part of the Birch and Swinnerton-Dyer formula, and the p -converse theorem.

Corollary 1.4. *Let E/\mathbb{Q} be an elliptic curve of conductor N , and let $p \nmid 2N$ be a prime at which E has good ordinary reduction. If $r \leq 1$, then the following are equivalent:*

- (1) $\text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E/\mathbb{Q}) = r$;
- (2) $\text{ord}_{s=1} L(E/\mathbb{Q}, s) = r$.

Moreover, under either condition, if (Im) also holds, then the p -part of the Birch and Swinnerton-Dyer formula for E holds.

Remark 1.5. There has been extensive work on the p -part of the Birch and Swinnerton-Dyer formula and the p -converse theorem for elliptic curves. In our context, see [SU14], [Zha14], [JSW17], [BSTW24], [BCS25] for earlier results on the p -part of the BSD formula, and [Ski20], [Zha14], [BSTW24], [BCGS23] for related results on the p -converse theorem.

1.2. Strategy. By [CGS25, Proposition 4.2.1] or [BSTW24, Proposition 9.18], the use of Beilinson-Flach elements, combined with an explicit reciprocity law, establishes a connection between various formulations of the main conjectures. As a result, the inclusion relations (and their converses) in Theorem 1.2(1) and (2) are shown to be equivalent.

From the work of Skinner-Urban [SU14], especially Theorem 7.7 and Proposition 13.6(1), we have the following:

Theorem 1.6. *Suppose that the residual representation $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[p])$ is irreducible. Then for any height-one prime P of Λ_K , we have*

$$\text{ord}_P(\text{Char}_{\Lambda_K}(H_{\mathcal{F}_{\text{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee)) \geq \text{ord}_P(\mathcal{L}_p^{\text{PR}}(E/K)),$$

unless $P = P^+ \Lambda_K$ for some height-one prime $P^+ \subset \Lambda_K^+$.

Following [BSTW24, Proposition 9.18] (or [CGS25, Proposition 4.2.1]), we have:

Theorem 1.7. *Under the same assumptions as in the previous theorem, for any height-one prime P of Λ_K^{ur} , we have*

$$\text{ord}_P(\text{Char}_{\Lambda_K}(H_{\mathcal{F}_{\text{Gr}}}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee) \Lambda_K^{\text{ur}}) \geq \text{ord}_P(\mathcal{L}_p^{\text{Gr}}(E/K)),$$

unless $P = P^+ \Lambda_K^{\text{ur}}$ for some height-one prime $P^+ \subset \Lambda_K^{\text{ur},+}$.

However, by the result on the μ -invariant of the BDP p -adic L -function due to Hsieh [Hsi14], if $P \subset \Lambda_K^{\text{ur}}$ is a height-one prime of the form $P = P^+ \Lambda_K^{\text{ur}}$ for some $P^+ \subset \Lambda_K^{\text{ur},+}$, then

$$\text{ord}_P(\mathcal{L}_p^{\text{Gr}}(E/K)) = 0.$$

Therefore, Theorem 1.2(2) holds, which implies that Theorem 1.2(1) also holds. Moreover, if condition (Im) is satisfied, then as in [SU14, Theorem 3.30], we conclude that Conjecture 1.1(2) holds, and hence so does Conjecture 1.1(1).

1.3. Acknowledgment. The authors are grateful to Ye Tian and Wei He for their continuous encouragement and numerous helpful discussions, and to Ashay Burungale for his valuable comments. We are also grateful to the reviewer for the thoughtful suggestions and invested expertise, which were instrumental in strengthening the paper.

2. SELMER GROUPS

Let K be an imaginary quadratic field with discriminant D_K , and let $p > 2$ be a prime that splits in K , say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Let \mathbb{Q}_∞ denote the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} , and let K_∞ be the \mathbb{Z}_p^2 -extension of K . We write K_∞^+ and K_∞^- for the cyclotomic and anticyclotomic \mathbb{Z}_p -extensions of K , respectively.

Define the Galois groups

$$\Gamma_{\mathbb{Q}} := \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}), \quad \Gamma_K := \text{Gal}(K_\infty/K), \quad \Gamma_K^\pm := \text{Gal}(K_\infty^\pm/K).$$

We identify $\Gamma_K^+ = \text{Gal}(K_\infty^+/K)$ with $\Gamma_{\mathbb{Q}} = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Let γ^\pm be a topological generator of Γ_K^\pm .

Let

$$\Lambda_{\mathbb{Q}} := \mathbb{Z}_p[[\Gamma_{\mathbb{Q}}]], \quad \Lambda_K := \mathbb{Z}_p[[\Gamma_K]], \quad \Lambda_K^\pm := \mathbb{Z}_p[[\Gamma_K^\pm]]$$

be the associated Iwasawa algebras. These rings are equipped with natural characters

$$\varepsilon_{\mathbb{Q}} : G_{\mathbb{Q}} \rightarrow \Gamma_{\mathbb{Q}} \hookrightarrow \Lambda_{\mathbb{Q}}^\times, \quad \varepsilon_K : G_K \rightarrow \Gamma_K \hookrightarrow \Lambda_K^\times, \quad \varepsilon_{K,\pm} : G_K \rightarrow \Gamma_K^\pm \hookrightarrow \Lambda_K^{\pm,\times}$$

arising from projection. The Pontryagin duals $\Lambda_{\mathbb{Q}}^\vee$, Λ_K^\vee , and $\Lambda_K^{\pm,\vee}$ are endowed with $G_{\mathbb{Q}}$ - or G_K -actions via the inverses of these characters.

Throughout this paper, we normalize the reciprocity map of class field theory so that uniformizers correspond to arithmetic Frobenius elements. With this convention, we identify algebraic Hecke characters with their associated Galois characters.

2.1. Selmer groups for Iwasawa algebras. Let E/\mathbb{Q} be an elliptic curve of conductor N with $(N, D_K) = 1$. We assume that E has good ordinary reduction at p .

Discrete Selmer groups. Let F be either \mathbb{Q} or K . For a prime w of F above p , let \mathbb{F}_w be the residue field at w , and let $\tilde{E}_{/\mathbb{F}_w}$ be the reduction of E . The kernel of the reduction map on the Tate module is denoted by $\mathcal{F}_w^+ T_p E := \ker(T_p E \rightarrow T_p \tilde{E}_{/\mathbb{F}_w})$.

Definition 2.1. For any of $\Lambda_{\mathbb{Q}}, \Lambda_K$, or Λ_K^\pm , and for a prime w of F over p , we define the following local conditions:

- (1) $H_{\text{ord}}^1(F_w, T_p E \otimes \Lambda^\vee) := \text{Im}(H^1(F_w, \mathcal{F}_w^+ T_p E \otimes \Lambda^\vee) \rightarrow H^1(F_w, T_p E \otimes \Lambda^\vee))$,
- (2) $H_{\text{rel}}^1(F_w, T_p E \otimes \Lambda^\vee) := H^1(F_w, T_p E \otimes \Lambda^\vee)$,
- (3) $H_{\text{str}}^1(F_w, T_p E \otimes \Lambda^\vee) := 0$.

Let Σ be a set of places of F containing all places dividing $pN\infty$. In the anticyclotomic case ($F = K, \Lambda = \Lambda_K^-$), we assume moreover that every finite place in Σ splits completely in K/\mathbb{Q} . Let F_Σ be the maximal extension of F unramified outside Σ , and let $G_{F,\Sigma} := \text{Gal}(F_\Sigma/F)$.

In the case $F = \mathbb{Q}$, for $a \in \{\text{ord}, \text{str}, \text{rel}\}$ and $M = T_p E \otimes \Lambda_{\mathbb{Q}}^\vee$, we define the Selmer group

$$H_{\mathcal{F}_a}^1(\mathbb{Q}, M) := \ker \left(H^1(G_{\mathbb{Q},\Sigma}, M) \rightarrow \prod_{q \in \Sigma, q \nmid p\infty} H^1(\mathbb{Q}_q, M) \times \frac{H^1(\mathbb{Q}_p, M)}{H_a^1(\mathbb{Q}_p, M)} \right).$$

Its Pontryagin dual is denoted by

$$\mathcal{X}_{\mathcal{F}_a}(E/\mathbb{Q}_\infty) := H_{\mathcal{F}_a}^1(\mathbb{Q}, T_p E \otimes \Lambda_{\mathbb{Q}}^\vee)^\vee.$$

In the case $F = K$, for $a, b \in \{\text{ord}, \text{str}, \text{rel}\}$, $\Lambda \in \{\Lambda_K, \Lambda_K^-, \Lambda_K^+\}$, and $M = T_p E \otimes \Lambda^\vee$, we define

$$H_{\mathcal{F}_{a,b}}^1(K, M) := \ker \left(H^1(G_{K,\Sigma}, M) \rightarrow \prod_{q \in \Sigma, q \nmid p} H^1(K_q, M) \times \frac{H^1(K_{\mathfrak{p}}, M)}{H_a^1(K_{\mathfrak{p}}, M)} \times \frac{H^1(K_{\bar{\mathfrak{p}}}, M)}{H_b^1(K_{\bar{\mathfrak{p}}}, M)} \right).$$

For simplicity, we write

- (1) $H_{\mathcal{F}_a}^1(K, M) := H_{\mathcal{F}_{a,a}}^1(K, M)$ for $a \in \{\text{ord}, \text{str}, \text{rel}\}$,

$$(2) H_{\mathcal{F}_{\text{Gr}}}^1(K, M) := H_{\mathcal{F}_{\text{rel, str}}}^1(K, M).$$

For $a \in \{\text{ord, str, rel, Gr}\}$, we define the dual Selmer groups

$$\mathcal{X}_{\mathcal{F}_a}(E/K_\infty) := H_{\mathcal{F}_a}^1(K, T_p E \otimes \Lambda_K^\vee)^\vee, \quad \mathcal{X}_{\mathcal{F}_a}(E/K_\infty^\pm) := H_{\mathcal{F}_a}^1(K, T_p E \otimes \Lambda_K^{\pm, \vee})^\vee.$$

Lemma 2.2. *Let Λ be Λ_K , $\Lambda_{\mathbb{Q}}$, or Λ_K^\pm . For every prime \mathfrak{q} of K dividing p , we have*

$$H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, (T_p \tilde{E}/\mathbb{F}_{\mathfrak{q}} \otimes \Lambda^\vee)^{I_{\mathfrak{q}}}) = 0$$

Proof. We consider the case $\Lambda = \Lambda_K$; the other cases are similar.

Let $\alpha_{\mathfrak{q}} : G_{K_{\mathfrak{q}}} \rightarrow \mathbb{Z}_p^\times$ be the unramified character associated to $T_p \tilde{E}/\mathbb{F}_{\mathfrak{q}}$. The action of $G_{K_{\mathfrak{q}}}$ on the module $T_p \tilde{E}/\mathbb{F}_{\mathfrak{q}} \otimes \Lambda_K^\vee$ is then given by the character $\alpha_{\mathfrak{q}} \varepsilon_K^{-1}$. Let $C_{\mathfrak{q}} \subset \Lambda_K$ be the ideal generated by the set $\{\varepsilon_K(g) - 1 : g \in I_{\mathfrak{q}}\}$, and let $\sigma_{\mathfrak{q}} \in G_{K_{\mathfrak{q}}}$ be a lift of $\text{Frob}_{\mathfrak{q}}$. A standard calculation yields the isomorphism:

$$H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, (T_p \tilde{E}/\mathbb{F}_{\mathfrak{q}} \otimes \Lambda_K^\vee)^{I_{\mathfrak{q}}}) \simeq \text{Hom}_{\text{cont}}\left((\Lambda_K/C_{\mathfrak{q}})^{\varepsilon_K(\sigma_{\mathfrak{q}}) = \alpha_{\mathfrak{q}}^{-1}(\text{Frob}_{\mathfrak{q}})}, \mathbb{Q}_p/\mathbb{Z}_p\right),$$

where $(\Lambda_K/C_{\mathfrak{q}})^{\varepsilon_K(\sigma_{\mathfrak{q}}) = \alpha_{\mathfrak{q}}^{-1}(\text{Frob}_{\mathfrak{q}})}$ denotes the submodule of $\Lambda_K/C_{\mathfrak{q}}$ annihilated by the operator $\varepsilon_K(\sigma_{\mathfrak{q}}) - \alpha_{\mathfrak{q}}^{-1}(\text{Frob}_{\mathfrak{q}})$. By [Nr06, Lemma 12.5.4], for any embedding $\sigma : \mathbb{Q} \rightarrow \mathbb{C}$, $|\sigma(\alpha_{\mathfrak{q}}(\text{Frob}_{\mathfrak{q}}))| = p^{1/2}$. Thus, $\alpha_{\mathfrak{q}}(\text{Frob}_{\mathfrak{q}})$ is not a root of unity. Consequently, the submodule $(\Lambda_K/C_{\mathfrak{q}})^{\varepsilon_K(\sigma_{\mathfrak{q}}) = \alpha_{\mathfrak{q}}^{-1}(\text{Frob}_{\mathfrak{q}})}$ must be trivial, which completes the proof. \square

Remark 2.3. Lemma 2.2 shows that the ordinary local condition H_{ord}^1 defined here coincides with that in [SU14].

Lemma 2.4. *We have the following isomorphisms of Λ_K^+ -modules:*

$$\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty^+) \simeq \mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_\infty) \oplus \mathcal{X}_{\mathcal{F}_{\text{ord}}}(E^K/\mathbb{Q}_\infty)$$

and

$$\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/K_\infty^+) \simeq \mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/\mathbb{Q}_\infty) \oplus \mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E^K/\mathbb{Q}_\infty),$$

via the natural identification $\Lambda_K^+ \simeq \Lambda_{\mathbb{Q}}$, where E^K denotes the quadratic twist of E associated to the quadratic extension K/\mathbb{Q} .

Proof. See [SU14, Lemma 3.6]. \square

For any prime \mathfrak{q} of K , let $I_{\mathfrak{q}}$ denote the inertia subgroup of $G_{K_{\mathfrak{q}}}$.

Lemma 2.5. *Let Λ be Λ_K or Λ_K^+ . For any prime $\mathfrak{q} \nmid p$ of K , we have:*

- (1) $H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, (T_p E \otimes \Lambda^\vee)^{I_{\mathfrak{q}}}) = 0$.
- (2) $\text{Char}_\Lambda((H^1(I_{\mathfrak{q}}, T_p E \otimes \Lambda^\vee)^{G_{K_{\mathfrak{q}}}})^\vee) = (P_{\mathfrak{q}}(\varepsilon_K(\text{Frob}_{\mathfrak{q}}^{-1})))$, where

$$P_{\mathfrak{q}}(X) = \det(1 - \text{Nm}(\mathfrak{q})^{-1} X \cdot \text{Frob}_{\mathfrak{q}} | V_p E^{I_{\mathfrak{q}}}).$$

Proof. We consider the case $\Lambda = \Lambda_K$; the other case is similar. For simplicity, let $M := T_p E \otimes \Lambda_K^\vee$ and $N := T_p E \otimes \Lambda_K$. We have a natural G_K -equivariant perfect pairing

$$M \times N \rightarrow \mathbb{Q}_p/\mathbb{Z}_p(1),$$

which induces the perfect local Tate pairing

$$H^1(K_{\mathfrak{q}}, M) \times H^1(K_{\mathfrak{q}}, N) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

for every place \mathfrak{q} . Let $\mathfrak{q} \nmid p$ be a prime of K .

(1) Since $G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}} = \langle \text{Frob}_{\mathfrak{q}} \rangle \simeq \widehat{\mathbb{Z}}$ has cohomological dimension 1, the groups $H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, N^{I_{\mathfrak{q}}})$ and $H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, M^{I_{\mathfrak{q}}})$ annihilate each other under local Tate duality. The inflation-restriction exact sequence is

$$0 \rightarrow H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, N^{I_{\mathfrak{q}}}) \rightarrow H^1(G_{K_{\mathfrak{q}}}, N) \rightarrow H^1(I_{\mathfrak{q}}, N)^{G_{K_{\mathfrak{q}}}} \rightarrow 0.$$

Thus, to prove (1), it suffices to show that $H^1(I_{\mathfrak{q}}, N)^{G_{K_{\mathfrak{q}}}} = 0$.

Since $\mathfrak{q} \nmid p$, the inertia group $I_{\mathfrak{q}}$ contains a unique closed subgroup $J_{\mathfrak{q}}$ such that $I_{\mathfrak{q}}/J_{\mathfrak{q}} \simeq \mathbb{Z}_p(1)$ as a $\text{Gal}(K_{\mathfrak{q}}^{\text{ur}}/K_{\mathfrak{q}})$ -module, and $J_{\mathfrak{q}}$ has pro-finite order prime to p . The inflation-restriction sequence yields

$$H^1(I_{\mathfrak{q}}, N) \cong H^1(I_{\mathfrak{q}}/J_{\mathfrak{q}}, N^{J_{\mathfrak{q}}}).$$

Let $N_0 := T_p E^{J_q}$. Since $\varepsilon_K(I_q) = 1$, we have $N^{J_q} = N_0 \otimes \Lambda_K$. Let σ_q be a topological generator of I_q/J_q . For any cocycle ϕ representing a class in $H^1(I_q/J_q, N_0 \otimes \Lambda_K)^{G_{K_q}}$ and any $g \in G_{K_q}$, we have the relation $g \cdot \phi = \phi$. This implies that for some integer $r = r(g)$,

$$g^{-1}(\phi(\sigma_q)) = \phi(g^{-1}\sigma_q g) = \phi(\sigma_q^r) = (1 + \sigma_q + \cdots + \sigma_q^{r-1})\phi(\sigma_q).$$

As \mathfrak{q} does not split completely in K_∞/K , the image $\varepsilon_K(G_{K_q})$ is nontrivial. We can therefore choose g such that $\varepsilon_K(g) \neq 1$. However, since $\varepsilon_K(\sigma_q) = 1$, it follows that $\phi(\sigma_q) = 0$, which implies that $H^1(I_q, N)^{G_{K_q}} = 0$.

(2) Now we prove the second part. As before, we have the duality

$$(H^1(I_q, M)^{G_{K_q}})^\vee \simeq H^1(G_{K_q}/I_q, N^{I_q}).$$

Since

$$H^1(G_{K_q}/I_q, N^{I_q}) \simeq (T_p E^{I_q} \otimes \Lambda_K)/(1 - \text{Frob}_q^{-1}),$$

it follows that

$$\text{Fitt}_{\Lambda_K}((H^1(I_q, M)^{G_{K_q}})^\vee) = (P_q(\varepsilon_K(\text{Frob}_q^{-1}))).$$

This Fitting ideal is principal and therefore divisorial. The characteristic ideal $\text{Char}_{\Lambda_K}((H^1(I_q, M)^{G_{K_q}})^\vee)$ is the minimal divisorial ideal containing the Fitting ideal. Hence, we have

$$\text{Char}_{\Lambda_K}((H^1(I_q, M)^{G_{K_q}})^\vee) = (P_q(\varepsilon_K(\text{Frob}_q^{-1}))).$$

□

Lemma 2.6. *The natural Λ_K^- -module homomorphism*

$$\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)/(\gamma^+ - 1)\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty) \rightarrow \mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty^-)$$

is a pseudo-isomorphism.

Proof. The result follows from [Wan21, Proposition 3.1] combined with Lemma 2.5(1). Note that in our case, every finite place in Σ splits in K . □

We also consider an imprimitive Selmer group. For $M = T_p E \otimes \Lambda_K^\vee$, we define

$$H_{\mathcal{F}_{\text{ord}}^\Sigma}^1(K, M) := \ker \left(H^1(G_{K, \Sigma}, M) \rightarrow \prod_{\mathfrak{q}|p} \frac{H^1(K_{\mathfrak{q}}, M)}{H_{\text{ord}}^1(K_{\mathfrak{q}}, M)} \right)$$

and its Pontryagin dual $\mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}^1(E/K_\infty) := H_{\mathcal{F}_{\text{ord}}^\Sigma}^1(K, M)^\vee$.

Lemma 2.7. *Suppose that the residual representation $\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$ is irreducible. Then there is no nontrivial \mathbb{F}_p -subquotient of $E[p]$ on which G_{K_∞} acts trivially.*

Proof. Let L be the fixed field of $\ker(\bar{\rho}_E|_{G_K})$. By the properties of the Weil pairing, we have $L \supset K(\mu_p)$. Let $L_0 := L \cap K_\infty$. Then $\text{Gal}(L/L_0)$ is the image of the natural map $G_{K_\infty} \rightarrow \text{Gal}(L/K)$.

We first claim that if the restriction $\bar{\rho}_E|_{G_{L_0}}$ is reducible, then $p \nmid \#\text{Gal}(L/L_0)$. Indeed, since G_{L_0} is a normal subgroup of G_K , if $W \subset E[p]$ is a one-dimensional \mathbb{F}_p -subspace invariant under G_{L_0} , then for any $g \in G_K$, the subspace $gW \subset E[p]$ is also invariant under G_{L_0} . By the irreducibility of $\bar{\rho}_E|_{G_K}$, there exists a $g_0 \in G_K$ such that $g_0W \neq W$. Consequently, $E[p] = W \oplus g_0W$ as a G_{L_0} -module. We can therefore choose an \mathbb{F}_p -basis of $E[p]$ such that the image of G_{L_0} is contained in the diagonal matrix group. Since the order of the diagonal matrix group is $(p-1)^2$, which is coprime to p , we conclude that $p \nmid \#\text{Gal}(L/L_0)$.

Now, suppose there exists a one-dimensional G_{K_∞} -stable \mathbb{F}_p -subspace $C \subset E[p]$ such that the action on C or on $E[p]/C$ is trivial; in particular, the restriction $\bar{\rho}_E|_{G_{K_\infty}}$ is reducible. Let $P \in C - \{0\}$, and choose $Q \in E[p] - C$. Since the action of G_{K_∞} factors through $\text{Gal}(L/L_0)$, the restriction $\bar{\rho}_E|_{G_{L_0}}$ is reducible, and for any $\sigma \in \text{Gal}(L/L_0)$, we have

$$\sigma P = \alpha(\sigma)P, \quad \sigma Q = \beta(\sigma)P + \gamma(\sigma)Q$$

with coefficients $\alpha(\sigma), \beta(\sigma), \gamma(\sigma) \in \mathbb{F}_p$ satisfying

- (1) either $\alpha(\sigma) = 1$ for all $\sigma \in \text{Gal}(L/L_0)$, or $\gamma(\sigma) = 1$ for all $\sigma \in \text{Gal}(L/L_0)$.
- (2) $\alpha(\sigma)\gamma(\sigma) = \omega(\sigma)$, where ω is the Teichmüller character.

Consider the subgroup $\text{Gal}(L/L_0(\mu_p)) \subset \text{Gal}(L/L_0)$. For any $\sigma \in \text{Gal}(L/L_0(\mu_p))$, we have $\omega(\sigma) = 1$, hence $\alpha(\sigma) = \gamma(\sigma) = 1$. Therefore we obtain an embedding

$$\text{Gal}(L/L_0(\mu_p)) \hookrightarrow \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p \right\} \simeq \mathbb{F}_p.$$

Since $\text{Gal}(L/L_0(\mu_p))$ is a subgroup of $\text{Gal}(L/L_0)$ and $p \nmid \#(\text{Gal}(L/L_0))$ as shown previously, we have that $L = L_0(\mu_p)$. On the other hand, since $[K(\mu_p) : K]$ divides $p - 1$ and $[L_0 : K]$ is a power of p , we have that $L_0 \cap K(\mu_p) = K$. Hence L is an abelian extension of K , with Galois group $\text{Gal}(L/K) \simeq \text{Gal}(L/L_0) \times \text{Gal}(L/K(\mu_p))$, and therefore the representation $\bar{\rho}_E|_{G_K}$ is reducible over $\overline{\mathbb{F}}_p$. Moreover, let $\alpha(\sigma), \gamma(\sigma) \in \overline{\mathbb{F}}_p^\times$ denote the eigenvalues of $\sigma \in \text{Gal}(L_0(\mu_p)/K)$. We have

- (1) If $\sigma \in \text{Gal}(L/L_0)$, then at least one of $\alpha(\sigma), \gamma(\sigma)$ is equal to one, and $\alpha(\sigma) \cdot \gamma(\sigma) = \omega(\sigma) \in \mathbb{F}_p^\times$, hence both $\alpha(\sigma)$ and $\gamma(\sigma)$ belong to \mathbb{F}_p^\times .
- (2) If $\sigma \in \text{Gal}(L/K(\mu_p)) \simeq \text{Gal}(L_0/K)$, since $\text{Gal}(L_0/K)$ has p -power order, $\alpha(\sigma)^{p^m} = 1 = \gamma(\sigma)^{p^m} \in \overline{\mathbb{F}}_p^\times$ for some integer m , which implies that $\alpha(\sigma) = 1 = \gamma(\sigma) \in \mathbb{F}_p^\times$.

Consequently, for any $\sigma \in \text{Gal}(L/K)$, the eigenvalues $\alpha(\sigma), \gamma(\sigma)$ belong to \mathbb{F}_p^\times , contradicting the assumption that $\bar{\rho}_E|_{G_K}$ is irreducible. We complete the proof. \square

Lemma 2.8. *If the residual representation $\bar{\rho}_E|_{G_K}$ is irreducible, then $\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/K_\infty)$ is a torsion Λ_K -module.*

Proof. By [Kat04, Theorem 17.4 (1)], both $\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/\mathbb{Q}_\infty)$ and $\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E^K/\mathbb{Q}_\infty)$ are torsion $\Lambda_{\mathbb{Q}}$ -modules. Consequently, Lemma 2.4 implies that $\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/K_\infty^+)$ is a torsion Λ_K^+ -module. Therefore, by [SU14, Proposition 3.9], Lemma 2.7, and Remark 2.3, we conclude that $\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/K_\infty)$ is a torsion Λ_K -module. \square

Together with Lemma 2.5, we have the following corollary.

Corollary 2.9. *$\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)$ is Λ_K -torsion, and*

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(E/K_\infty)) \supset \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) \prod_{\mathfrak{q} \in \Sigma - \{\mathfrak{p}, \bar{\mathfrak{p}}\}} (P_{\mathfrak{q}}(\varepsilon_K(\text{Frob}_{\mathfrak{q}}^{-1}))).$$

Proof. By definition, we have the following exact sequence,

$$0 \rightarrow H_{\mathcal{F}_{\text{ord}}}^1(K, T_p E \otimes \Lambda_K^\vee) \rightarrow H_{\mathcal{F}_{\text{ord}}^\Sigma}^1(K, T_p E \otimes \Lambda_K^\vee) \rightarrow \bigoplus_{\mathfrak{q} \in \Sigma - \{\mathfrak{p}, \bar{\mathfrak{p}}\}} H^1(G_{K_{\mathfrak{q}}}, T_p E \otimes \Lambda_K^\vee).$$

Taking Pontryagin duals yields the exact sequence,

$$\bigoplus_{\mathfrak{q} \in \Sigma - \{\mathfrak{p}, \bar{\mathfrak{p}}\}} H^1(G_{K_{\mathfrak{q}}}, T_p E \otimes \Lambda_K^\vee)^\vee \rightarrow \mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}(E/K_\infty) \rightarrow \mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty) \rightarrow 0.$$

Hence we have

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}(E/K_\infty)) \supset \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) \prod_{\mathfrak{q} \in \Sigma - \{\mathfrak{p}, \bar{\mathfrak{p}}\}} \text{Char}_{\Lambda_K}(H^1(G_{K_{\mathfrak{q}}}, T_p E \otimes \Lambda_K^\vee)^\vee).$$

For every $\mathfrak{q} \nmid p$, by the inflation-restriction sequence and the fact that $G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}} = \langle \text{Frob}_{\mathfrak{q}} \rangle \simeq \widehat{\mathbb{Z}}$ has cohomological dimension 1, we have the following exact sequence

$$0 \rightarrow H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, (T_p E \otimes \Lambda_K^\vee)^{I_{\mathfrak{q}}}) \rightarrow H^1(G_{K_{\mathfrak{q}}}, T_p E \otimes \Lambda_K^\vee) \rightarrow H^1(I_{\mathfrak{q}}, T_p E \otimes \Lambda_K^\vee)^{G_{K_{\mathfrak{q}}}} \rightarrow 0.$$

Therefore by Lemma 2.5, we have

$$\text{Char}_{\Lambda_K}(H^1(G_{K_{\mathfrak{q}}}, (T_p E \otimes \Lambda_K^\vee)^\vee)) = \text{Char}_{\Lambda_K}((H^1(I_{\mathfrak{q}}, T_p E \otimes \Lambda_K^\vee)^{G_{K_{\mathfrak{q}}}})^\vee) = P_{\mathfrak{q}}(\varepsilon_K(\text{Frob}_{\mathfrak{q}}^{-1})),$$

which completes the proof. \square

2.2. Selmer groups for Hida families. Let W be an indeterminate and $\Lambda_W = \mathbb{Z}_p[[W]]$. We identify Λ_W with Λ_K^+ by mapping the topological generator γ^+ to $1+W$, which induces the character $\varepsilon_W : G_K \rightarrow \Lambda_W^\times$.

Let $L \subset \bar{\mathbb{Q}}_p$ be a finite extension of \mathbb{Q}_p with ring of integers \mathcal{O} . Let \mathbb{I} be a local reduced finite integral extension of $\Lambda_{W,\mathcal{O}} := \Lambda_W \otimes_{\mathbb{Z}_p} \mathcal{O}$. Recall that a continuous \mathcal{O} -algebra homomorphism $\phi \in \text{Hom}_{\text{cont } \mathcal{O}\text{-alg}}(\mathbb{I}, \bar{\mathbb{Q}}_p)$ is said to be arithmetic if it satisfies the condition $\phi(1+W) = \zeta_\phi(1+p)^{k_\phi-2}$ for some p -power root of unity ζ_ϕ and some integer k_ϕ . Let $t_\phi > 0$ be the integer such that ζ_ϕ is a primitive $p^{t_\phi-1}$ -th root of unity, and let $\chi_\phi : \mathbb{A}_{\bar{\mathbb{Q}}}^\times / \mathbb{Q}^\times \rightarrow \mu_{p^\infty}$ be the unique character that has a p -power conductor and satisfies $\chi_{\phi,p}(1+p) = \zeta_\phi^{-1}$. We define the set of arithmetic points with weight $k_\phi \geq 2$ as

$$\mathfrak{X}_{\mathbb{I},\mathcal{O}}^a = \{ \phi \in \text{Hom}_{\text{cont } \mathcal{O}\text{-alg}}(\mathbb{I}, \bar{\mathbb{Q}}_p) : \phi \text{ is arithmetic, } k_\phi \geq 2 \}.$$

Let \mathbf{f} be an \mathbb{I} -adic ordinary eigenform of tame level N and nebentypus $\chi_{\mathbf{f}} = 1$, namely a formal q -expansion $\mathbf{f} = \sum_{n=1} \mathbf{a}_n(\mathbf{f})q^n \in \mathbb{I}[[q]]$ with the property that for any arithmetic point $\phi \in \mathfrak{X}_{\mathbb{I},\mathcal{O}}^a$, the corresponding specialization

$$\mathbf{f}_\phi = \sum_{n=1} \phi(\mathbf{a}_n(\mathbf{f}))q^n$$

is an ordinary modular form in the space $M_{k_\phi}(Np^{t_\phi}, \omega^{k_\phi-2}\chi_\phi; \phi(\mathbb{I}))$. Here, ω denotes the Teichmüller character.

We assume that \mathbf{f} satisfies the following irreducibility condition:

(irred $_{\mathbf{f}}$) the residue representation of $\rho_{\mathbf{f}_\phi}$ is irreducible for some (hence all) $\phi \in \mathfrak{X}_{\mathbb{I},\mathcal{O}}^a$.

Under this condition, there exists a continuous, \mathbb{I} -linear Galois representation $\rho_{\mathbf{f}} : G_{\mathbb{Q}} \rightarrow \text{GL}_{\mathbb{I}}(T_{\mathbf{f}})$, where the representation space $T_{\mathbf{f}}$ is a free \mathbb{I} -module of rank two. This representation is unramified at all primes $\ell \nmid Np$ and is uniquely characterized by the relations:

$$\text{tr} \rho_{\mathbf{f}}(\text{Frob}_\ell) = a_\ell(\mathbf{f}), \quad \ell \nmid Np,$$

and

$$\det(\rho_{\mathbf{f}}) = \epsilon \varepsilon_W,$$

where ϵ is the p -adic cyclotomic character.

Let $F_{\mathbb{I}}$ be the field of fractions of the integral domain \mathbb{I} , and let $V_{\mathbf{f}} := T_{\mathbf{f}} \otimes_{\mathbb{I}} F_{\mathbb{I}}$. Since \mathbf{f} is ordinary, there exists a one-dimensional $F_{\mathbb{I}}$ -subspace $V_{\mathbf{f}}^+ \subset V_{\mathbf{f}}$ that is stable under the action of $G_{\mathbb{Q}_p}$. Furthermore, $G_{\mathbb{Q}_p}$ acts on the quotient space $V_{\mathbf{f}}^- := V_{\mathbf{f}}/V_{\mathbf{f}}^+$ via an unramified character $\delta_{\mathbf{f}}$, which is characterized by the condition $\delta_{\mathbf{f}}(\text{Frob}_p) = a_p(\mathbf{f})$. Since the nebentypus $\chi_{\mathbf{f}} = 1$, \mathbf{f} satisfies the following condition given in [SU14]:

(dist $_{\mathbf{f}}$) $\delta_{\mathbf{f}}^2 \not\equiv \chi_{\mathbf{f}} \omega \pmod{\mathfrak{m}_{\mathbb{I}}}$,

where $\mathfrak{m}_{\mathbb{I}}$ is the maximal ideal of \mathbb{I} . Hence, by Nakayama's lemma, the intersection $T_{\mathbf{f}}^+ := T_{\mathbf{f}} \cap V_{\mathbf{f}}^+$ is then a rank-one free \mathbb{I} -summand of $T_{\mathbf{f}}$. Consequently, the quotient module $T_{\mathbf{f}}^- := T_{\mathbf{f}}/T_{\mathbf{f}}^+$ is also a free \mathbb{I} -module of rank one.

Let E/\mathbb{Q} be an elliptic curve with good ordinary reduction at p . By [Hid86, Corollary 1.5], there exist an \mathbb{I} -adic ordinary eigenform \mathbf{f} with trivial nebentypus and a weight 2 arithmetic specialization $\phi \in \mathfrak{X}_{\mathbb{I},\mathcal{O}}^a$ (i.e., $\phi(1+W) = 1$) such that the specialized form $\phi(\mathbf{f})$ is the p -stabilization of the newform associated to E .

Corollary 2.10. *Let $\mathfrak{p}_\phi := \ker \phi$. Assume that the residual representation $\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$ is irreducible. Then there is a natural isomorphism:*

$$\mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}(\mathbf{f}/K_\infty)/\mathfrak{p}_\phi \mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}(\mathbf{f}/K_\infty) \otimes_{\mathbb{I},\phi} \mathcal{O} \simeq \mathcal{X}_{\mathcal{F}_{\text{ord}}^\Sigma}(E/K_\infty).$$

Proof. Since \mathbf{f} is an \mathbb{I} -adic ordinary eigenform of trivial nebentypus, recall that there exists a free \mathbb{I} -submodule $T_{\mathbf{f}}^+ \subset T_{\mathbf{f}}$ of rank one such that the quotient module $T_{\mathbf{f}}^- := T_{\mathbf{f}}/T_{\mathbf{f}}^+$ is also free of rank one, and the inertia group I_p acts trivially on $T_{\mathbf{f}}^-$. By Lemma 2.7 and Nakayama's lemma, there is no nontrivial \mathbb{I}_K -subquotient of $T_{\mathbf{f}}^-$ on which G_{K_∞} acts trivially.

Consequently, the desired result follows from [SU14, Proposition 3.7] and Remark 2.3. \square

3. p -ADIC L -FUNCTIONS

3.1. A three-variable p -adic L -function. Let \mathbf{f} be an \mathbb{I} -adic ordinary eigenform of tame level N and trivial nebentypus as described in Section 2.2. Suppose L contains $\mathbb{Q}[\mu_{Np}, i, D_K^{1/2}]$.

Define

$$\mathfrak{X}_{\mathbb{I}_K, \mathcal{O}}^a := \{\phi \in \text{Hom}_{\text{cont } \mathcal{O}\text{-alg}}(\mathbb{I}_K, \bar{\mathbb{Q}}_p) : \phi|_{\mathbb{I}} \in \mathfrak{X}_{\mathbb{I}, \mathcal{O}}^a, \phi(\gamma^+) = \zeta_+(1+p)^{k_{\phi|_{\mathbb{I}}}-2}, \phi(\gamma^-) = \zeta_-\},$$

where ζ_{\pm} are p -power roots of unity. For each $\phi \in \mathfrak{X}_{\mathbb{I}_K, \mathcal{O}}^a$, let k_{ϕ} , t_{ϕ} , and χ_{ϕ} be the corresponding data associated with $\phi|_{\mathbb{I}}$. Define

$$\xi_{\phi} := \phi \circ (\varepsilon_K / \varepsilon_W), \quad \theta_{\phi} := \omega^{2-k_{\phi}} \chi_{\phi}^{-1} \xi_{\phi}.$$

These are finite-order idele class characters of \mathbb{A}_K^{\times} . For an idele class character ψ , denote its conductor by \mathfrak{f}_{ψ} . Set

$$\mathfrak{X}'_{\mathbb{I}_K, \mathcal{O}} := \{\phi \in \mathfrak{X}_{\mathbb{I}_K, \mathcal{O}}^a : p \mid \mathfrak{f}_{\xi_{\phi}}, p^{t_{\phi}} \mid \text{Nm}(\mathfrak{f}_{\xi_{\phi}}), p \mid \mathfrak{f}_{\theta_{\phi}}\}.$$

Theorem 3.1. *Let Σ be a finite set of primes containing all primes dividing pND_K . Let \mathbf{f} be an \mathbb{I} -adic ordinary eigenform of tame level N and trivial nebentypus. Assume \mathbf{f} satisfies (irred \mathbf{f}). Then there exists $\mathcal{L}_{\mathbf{f}, K}^{\Sigma} \in \mathbb{I}_K$ such that for every $\phi \in \mathfrak{X}'_{\mathbb{I}_K, \mathcal{O}}$,*

$$\begin{aligned} \mathcal{L}_{\mathbf{f}, K}^{\Sigma}(\phi) &= u_{\mathbf{f}_{\phi}} a_p(\mathbf{f}_{\phi})^{-\text{ord}_p(\text{Nm}(\mathfrak{f}_{\theta_{\phi}}))} \\ &\quad \times \frac{((k_{\phi} - 2)!)^2 \mathfrak{g}(\theta_{\phi}^{-1}) \text{Nm}(\mathfrak{f}_{\theta_{\phi}} \delta_K)^{k_{\phi}-2} L^{\Sigma}(\mathbf{f}_{\phi}/K, \theta_{\phi}^{-1}, \theta_{\phi} - 1)}{(-2\pi i)^{2k_{\phi}-2} \Omega_{\mathbf{f}_{\phi}}^+ \Omega_{\mathbf{f}_{\phi}}^-}, \end{aligned}$$

where $u_{\mathbf{f}_{\phi}}$ is a p -adic unit depending only on \mathbf{f}_{ϕ} , $\mathfrak{g}(\theta_{\phi}^{-1})$ is the global Gauss sum, δ_K is the differential ideal, $\Omega_{\mathbf{f}_{\phi}}^{\pm}$ are the canonical periods associated to \mathbf{f}_{ϕ} , and

$$L^{\Sigma}(\mathbf{f}_{\phi}/K, \theta_{\phi}^{-1}, s) := L^{\Sigma}(\mathbf{f}_{\phi}/K, \theta_{\phi}^{-1}, s) \cdot \prod_{\mathfrak{q} \in \Sigma - \{\infty\}} L_{\mathfrak{q}}(\mathbf{f}_{\phi}/K, \theta_{\phi}^{-1}, s)^{-1}$$

with

$$L_{\mathfrak{q}}(\mathbf{f}_{\phi}/K, \theta_{\phi}^{-1}, s) := \det \left(1 - \text{Nm}(\mathfrak{q})^{-s} \cdot \text{Frob}_{\mathfrak{q}} \mid \left(V_{\phi, \ell}|_{G_K} \otimes \theta_{\phi}^{-1} \right)^{I_{\mathfrak{q}}} \right)^{-1}$$

being the local Euler factor at \mathfrak{q} , here $\ell \notin \Sigma$ is a prime number and $V_{\phi, \ell}$ is the ℓ -adic Galois representation associated to \mathbf{f}_{ϕ} (in the manner as Section 2.2).

Proof. See [SU14, Section 3.4.5]. □

Remark 3.2. Note that we adopt the arithmetic Frobenius normalization for the reciprocity map of class field theory, whereas [SU14] employs the geometric Frobenius convention.

3.2. Two variable p -adic L -functions: type I. Let $f = \sum_n a_n q^n \in S_2(\Gamma_0(N))$ be a newform with $p \nmid a_p$, and let $c_f \in \mathbb{Z}_p$ be the congruence number associated with f as defined in [Hid81, Section 7] or [Rib83].

Theorem 3.3. *There exists an element $\mathcal{L}_p^I(f/K) \in c_f^{-1} \Lambda_K$ such that for every finite-order nontrivial character ξ of Γ_K of conductor $\mathfrak{p}^m \bar{\mathfrak{p}}^n$ with $m + n > 0$, we have*

$$\mathcal{L}_p^I(f/K)(\xi) = W(\xi) p^{\text{ord}_p(\text{Nm}(\mathfrak{f}_{\xi}))/2} \alpha_p^{-\text{ord}_p(\text{Nm}(\mathfrak{f}_{\xi}))} \left(1 - \frac{p}{\alpha_p^2}\right)^{-1} \left(1 - \frac{1}{\alpha_p^2}\right)^{-1} \frac{L(f/K, \xi^{-1}, 1)}{8\pi^2 \langle f, f \rangle},$$

where α_p is the p -adic unit root of the polynomial $x^2 - a_p x + p$, $\langle f, g \rangle = \int_{\Gamma_0(N) \backslash \mathcal{H}} \overline{f(\tau)} g(\tau) d\tau$ denotes the Petersson inner product on $S_2(\Gamma_1(N))$, and $W(\xi)$ is the Artin root number.

Proof. This is a reformulation of [PR86, Theorem 1.1] following Hida's p -adic Rankin method [Hid85], as given in [CGS25, Theorem 2.2.1]. □

Let E/\mathbb{Q} be an elliptic curve with good ordinary reduction at the prime p . Let $f_E \in S_2(\Gamma_0(N))$ denote the newform associated with E , and let $\pi_E : X_0(N) \rightarrow E$ be a modular parametrization.

Definition 3.4 (Perrin-Riou's p -adic L -function). *Define Perrin-Riou's p -adic L -function as*

$$\mathcal{L}_p^{\text{PR}}(E/K) := \left(1 - \frac{p}{\alpha_p^2}\right) \left(1 - \frac{1}{\alpha_p^2}\right) \cdot \frac{\text{deg}(\pi_E)}{c_E^2} \cdot \mathcal{L}_p^I(f_E/K) \in \Lambda_K,$$

where c_E denotes the Manin constant.

Let \mathbf{f} be an \mathbb{I} -adic ordinary eigenform and $\phi \in \mathfrak{X}_{\mathbb{I}, \mathcal{O}}^a$ as in Section 2.2, with $\phi(1+W) = 1$ and \mathbf{f}_ϕ equal to the p -stabilization of f_E .

Proposition 3.5. *Assume that the residual representation $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[p])$ is irreducible. Then*

$$\mathcal{L}_{\mathbf{f}, K}^{\Sigma}(\phi \otimes \text{id}) = \alpha \cdot \prod_{\mathfrak{q} \in \Sigma, \mathfrak{q} \nmid p} P_{\mathfrak{q}}(\varepsilon_K(\text{Frob}_{\mathfrak{q}}^{-1})) \cdot \mathcal{L}_p^{\text{PR}}(E/K),$$

where

$$P_{\mathfrak{q}}(X) = \det(1 - \text{Nm}(\mathfrak{q})^{-1} X \cdot \text{Frob}_{\mathfrak{q}} | V_p E^{I_{\mathfrak{q}}})$$

is the local Euler factor, α is a p -adic unit independent of ξ , and

$$\phi \otimes \text{id} : \mathbb{I}_K = \mathbb{I} \hat{\otimes} \Lambda_K \rightarrow \phi(\mathbb{I}) \otimes \Lambda_K$$

is the natural homomorphism.

Proof. We have $W(\xi) = g(\bar{\xi})/\sqrt{\text{Nm}(\mathfrak{f}_{\xi})}$. By [Maz78, Corollary 4.1], c_E is a p -adic unit. According to [CGS25, Lemma 4.1.2], $\deg(\pi_E) = c_{f_E}$ up to a p -adic unit. Additionally, [SZ14, Lemma 9.5] shows that

$$\frac{\langle f_E, f_E \rangle}{c_{f_E}} = i(2\pi i)^2 \Omega_{f_E}^+ \Omega_{f_E}^-.$$

These results establish the desired equality. \square

3.3. Cyclotomic p -adic L -function. Let E/\mathbb{Q} be an elliptic curve with good ordinary reduction at the prime p . Choose generators δ^{\pm} of $H_1(E, \mathbb{Z})^{\pm}$, and define the Néron periods Ω_E^{\pm} by

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

where ω_E is a minimal differential on E . We normalize δ^{\pm} so that $\Omega_E^+ \in \mathbb{R}_{>0}$ and $\Omega_E^- \in i\mathbb{R}_{>0}$.

Let a_p be the p -th Fourier coefficient of the newform f_E associated with E , and let α_p be the p -adic unit root of $x^2 - a_p x + p$, as defined previously.

Theorem 3.6. *There exists an element $\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q}) \in \Lambda_{\mathbb{Q}}$ such that for every finite-order character χ of $\Gamma_{\mathbb{Q}}$,*

$$\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q})(\chi) = \begin{cases} \frac{p^r}{g(\bar{\chi})\alpha_p^r} \cdot \frac{L(E, \bar{\chi}, 1)}{\Omega_E^+}, & \chi \text{ is of conductor } p^r \neq 1, \\ (1 - \alpha_p^{-1})^2 \cdot \frac{L(E, 1)}{\Omega_E^+}, & \chi = 1. \end{cases}$$

where $g(\bar{\chi}) = \sum_{a \bmod p^r} \bar{\chi}(a) e^{2\pi i a/p^r}$ is the Gauss sum.

Proof. See [CGS25, Theorem 2.1.1]. \square

Let $\mathcal{L}_p^{\text{PR}}(E/K)^+ \in \Lambda_{\mathbb{Q}} \simeq \Lambda_K^+$ be the image of $\mathcal{L}_p^{\text{PR}}(E/K)$ under the map induced by the projection $\Gamma_K \twoheadrightarrow \Gamma_K^+ \simeq \Gamma_{\mathbb{Q}}$.

Proposition 3.7. *We have*

$$\mathcal{L}_p^{\text{PR}}(E/K)^+ = \mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q}) \cdot \mathcal{L}_p^{\text{MSD}}(E^K/\mathbb{Q}),$$

up to a unit in $\Lambda_{\mathbb{Q}}^{\times}$.

Proof. See [CGS25, Proposition 2.2.4]. \square

Proposition 3.8. *Both $\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q})$ and $\mathcal{L}_p^{\text{PR}}(E/K)$ are non-vanishing.*

Proof. According to [Roh84], there exists a finite-order character χ of $\Gamma_{\mathbb{Q}}$ such that $\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q})(\chi) \neq 0$, which implies $\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q}) \neq 0$. Similarly, we have $\mathcal{L}_p^{\text{MSD}}(E^K/\mathbb{Q}) \neq 0$. By Proposition 3.7, it follows that $\mathcal{L}_p^{\text{PR}}(E/K)^+ \neq 0$, and hence $\mathcal{L}_p^{\text{PR}}(E/K) \neq 0$. \square

3.4. Two variable p -adic L -functions: type II.

Theorem 3.9. *There exists an element $\mathcal{L}_p^{II}(f/K) \in \text{Frac } \Lambda_K$ such that for every character ξ of Γ_K crystalline at both \mathfrak{p} and $\bar{\mathfrak{p}}$, and of infinity type (b, a) with $a \leq -1$ and $b \geq 1$,*

$$\mathcal{L}_p^{II}(f/K)(\xi) = \frac{2^{a-b} i^{b-a-1} \Gamma(b+1) \Gamma(b) N^{a+b+1}}{(2\pi)^{2b+1} \langle \theta_{\xi_b}, \theta_{\xi_b} \rangle} \cdot \frac{\mathcal{E}(\xi, f, 1)}{(1 - \xi^{1-\tau}(\bar{\mathfrak{p}}))(1 - p^{-1} \xi^{1-\tau}(\bar{\mathfrak{p}}))} \cdot L(f/K, \xi, 1),$$

where θ_{ξ_b} is the theta series associated to the Hecke character $\xi_b = \xi|\cdot|^{-b}$, τ denotes complex conjugation, and

$$\mathcal{E}(\xi, f, 1) = (1 - p^{-1} \xi(\bar{\mathfrak{p}}) \alpha_p) (1 - \xi(\bar{\mathfrak{p}}) \alpha_p^{-1}) (1 - p^{-1} \xi^{-1}(\mathfrak{p}) \alpha_p) (1 - \xi^{-1}(\mathfrak{p}) \alpha_p^{-1}).$$

Proof. This is another instance of Hida's p -adic Rankin L -series in [LLZ15, Theorem 6.1.3], with the roles of \mathfrak{p} and $\bar{\mathfrak{p}}$ reversed. See also [CGS25, Theorem 2.4.1]. \square

Let $\Lambda_K^{\text{ur}} := \Lambda_K \widehat{\otimes} \mathbb{Z}_p^{\text{ur}}$, where \mathbb{Z}_p^{ur} is the completion of the ring of integers of the maximal unramified extension of \mathbb{Q}_p .

Theorem 3.10. *There exists an element $\mathcal{L}_p(K) \in \Lambda_K^{\text{ur}}$ such that for every character ξ of Γ_K of infinity type (j, k) with $0 \leq -j \leq k$,*

$$\mathcal{L}_p(K)(\xi) = \frac{\Omega_p^{k-j}}{\Omega_K^{k-j}} \cdot \Gamma(k) \cdot \left(\frac{\sqrt{D_K}}{2\pi} \right)^j \cdot (1 - \xi^{-1}(\mathfrak{p}) p^{-1}) (1 - \xi(\bar{\mathfrak{p}})) \cdot L(\xi, 0),$$

where Ω_p and Ω_K are the CM periods associated with K .

Proof. See [dS87, Theorem II.4.14]. \square

Definition 3.11 (Greenberg's p -adic L -function). *Define Greenberg's p -adic L -function as*

$$\mathcal{L}_p^{\text{Gr}}(f/K) := h_K \cdot \mathcal{L}_p(K)' \cdot \mathcal{L}_p^{II}(f/K),$$

where h_K denotes the class number of K , and $\mathcal{L}_p(K)'$ is the image of $\mathcal{L}_p(K)$ under the map $\Lambda_K^{\text{ur}} \rightarrow \Lambda_K^{\text{ur}}$, $\gamma \mapsto \gamma^{1-\tau}$ for $\gamma \in \Gamma_K$.

Lemma 3.12. *Greenberg's p -adic L -function $\mathcal{L}_p^{\text{Gr}}(f/K)$ is integral, i.e., it belongs to Λ_K^{ur} .*

Proof. See [CGS25, Lemma 2.4.4]. \square

3.5. BDP p -adic L -function. Assume that D_K is odd, $D_K \neq -3$, and that the Heegner hypothesis holds. Fix an integral ideal $\mathfrak{n} \subset \mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$. Define $\Lambda_K^{\text{ur}, \pm} := \Lambda_K^{\pm} \widehat{\otimes} \mathbb{Z}_p^{\text{ur}}$.

Theorem 3.13. *There exists an element $\mathcal{L}_p^{\text{BDP}}(f/K) \in \Lambda_K^{\text{ur}, -}$ characterized by the following interpolation property: for every character ξ of Γ_K^- crystalline at both \mathfrak{p} and $\bar{\mathfrak{p}}$, corresponding to a Hecke character of K of infinity type $(n, -n)$ with $n \in \mathbb{Z}_{>0}$ and $n \equiv 0 \pmod{p-1}$,*

$$\mathcal{L}_p^{\text{BDP}}(f/K)(\xi) = \frac{\Omega_p^{4n}}{\Omega_K^{4n}} \cdot \frac{\Gamma(n) \Gamma(n+1) \xi(\mathfrak{n}^{-1})}{4(2\pi)^{2n+1} \sqrt{D_K}^{2n-1}} \cdot (1 - a_p \xi(\bar{\mathfrak{p}}) p^{-1} + \xi(\bar{\mathfrak{p}})^2 p^{-1})^2 \cdot L(f/K, \xi, 1).$$

Proof. This was originally constructed in [BDP13] (as a continuous function of ξ). See [CGLS22, Theorem 2.1.1] for this refined construction, which is based on [CH18, Section 3]. \square

Let $\mathcal{L}_p^{\text{Gr}}(f/K)^{\pm}$ denote the image of $\mathcal{L}_p^{\text{Gr}}(f/K)$ under the natural projection $\Lambda_K^{\text{ur}} \rightarrow \Lambda_K^{\text{ur}, \pm}$. We have the following proposition.

Proposition 3.14.

$$\mathcal{L}_p^{\text{Gr}}(f/K)^- \cdot \Lambda_K^{\text{ur}, -} = \mathcal{L}_p^{\text{BDP}}(f/K) \cdot \Lambda_K^{\text{ur}, -}.$$

Proof. See [CGS25, Proposition 2.4.5]. \square

4. MAIN CONJECTURES OVER K_∞

4.1. Two variable Iwasawa main conjectures. Let E/\mathbb{Q} be an elliptic curve of conductor N and $p > 2$ be a prime at which E has good ordinary reduction. Let K be an imaginary quadratic field in which the prime p splits, i.e., $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Assume that the residual representation

$$\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$$

is irreducible.

Let f be the newform associated to E . For the remainder of this paper, we will denote $\mathcal{L}^{\text{Gr}}(f/K)$ by $\mathcal{L}^{\text{Gr}}(E/K)$, and similarly $\mathcal{L}_p^{\text{Gr}}(f/K)^\pm$ and $\mathcal{L}^{\text{BDP}}(f/K)$ by analogous notation involving E/K . We consider the following two-variable Iwasawa main conjectures:

Conjecture 4.1. (1) $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)$ is Λ_K -torsion and

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) = (\mathcal{L}_p^{\text{PR}}(E/K)).$$

(2) $\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)$ is Λ_K -torsion and

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty))\Lambda_K^{\text{ur}} = (\mathcal{L}_p^{\text{Gr}}(E/K)).$$

The main theorem we will establish is the following:

Theorem 4.2. *Suppose the residual representation $\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$ is absolutely irreducible. If the Heegner hypothesis holds (in particular, $\text{sign}(E/K) = -1$), then:*

(1) $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)$ is Λ_K -torsion and

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) \subset (\mathcal{L}_p^{\text{PR}}(E/K)).$$

(2) $\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)$ is Λ_K -torsion and

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty))\Lambda_K^{\text{ur}} \subset (\mathcal{L}_p^{\text{Gr}}(E/K)).$$

Moreover, if the following condition

(Im) *there exists $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that $T_p E/(\rho_E(\tau) - 1)T_p E$ is free of rank one over \mathbb{Z}_p holds, then Conjecture 4.1 is true.*

We will prove Theorem 4.2 in the following two subsections.

4.2. A three variable Iwasawa main conjecture. Let \mathbf{f} be an \mathbb{I} -adic ordinary eigenform of tame level N and trivial nebentypus as in Section 2.2. Suppose that $L \supset \mathbb{Q}[\mu_{Np}, i, D_K^{1/2}]$, \mathbb{I} is a normal domain, and \mathbf{f} satisfies (irred $_{\mathbf{f}}$). Note that in our case, \mathbf{f} satisfies (dist $_{\mathbf{f}}$) since \mathbf{f} has trivial nebentypus.

Conjecture 4.3 ([SU14]). *Let Σ be a finite set of primes containing all primes dividing pND_K . Then*

$$\text{Char}_{\mathbb{I}_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(\mathbf{f}/K_\infty)) = (\mathcal{L}_{\mathbf{f},K}^\Sigma).$$

Theorem 4.4. *Under the conditions of Conjecture 4.3, we have, for any height one prime P of $\mathbb{I}_K = \mathbb{I}[[\Gamma_K]]$,*

$$\text{ord}_P(\text{Char}_{\mathbb{I}_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(\mathbf{f}/K_\infty))) \geq \text{ord}_P(\mathcal{L}_{\mathbf{f},K}^\Sigma),$$

unless $P = P^+ \mathbb{I}[[\Gamma_K]]$ for some height one prime P^+ of $\mathbb{I}[[\Gamma_K^+]]$.

Proof. Let $\mathbf{D} = (A, \mathbf{f}, 1, 1, \Sigma)$ be a p -adic Eisenstein datum as defined in [SU14], with $A \supset \mathbb{Z}_p[i, D_K]$ a finite \mathbb{Z}_p -algebra. Define $\Lambda_{\mathbf{D}} := \mathbb{I}[[\Gamma_K]][[\Gamma_K^-]]$ as in [SU14]. The proof follows essentially from Section 7.4 of [SU14], with the exception that we exclude primes $P = P^+ \Lambda_{\mathbf{D}}$ for some height one prime P^+ of $\mathbb{I}[[\Gamma_K^+]]$.

By [SU14, Proposition 13.6(1)], for sufficiently large Σ , there exists a p -adic Eisenstein series $\mathbf{E}_{\mathbf{D}}$ whose formal q -expansion coefficients lie in $\Lambda_{\mathbf{D}}$, along with a set $\mathcal{C}_{\mathbf{D}}$ of coefficients of $\mathbf{E}_{\mathbf{D}}$. This set satisfies that any height one prime P of $\Lambda_{\mathbf{D}}$ containing $\mathcal{C}_{\mathbf{D}}$ must be of the form $P = P^+ \Lambda_{\mathbf{D}}$ for a height one prime P^+ of $\mathbb{I}[[\Gamma_K^+]]$.

By [SU14, Theorem 7.7], we have

$$\text{ord}_P(\text{Char}_{\mathbb{I}_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(\mathbf{f}/K_\infty))) \geq \text{ord}_P(\mathcal{L}_{\mathbf{f},K}^\Sigma)$$

for all height one primes P of $\Lambda_{\mathbf{D}}$ satisfying

(1) $\mathbf{E}_{\mathbf{D}}$ is non-zero modulo P .

- (2) $\text{ord}_P(\mathcal{L}_1^\Sigma) = 0$, where $\mathcal{L}_1^\Sigma \in \mathbb{I}[[\Gamma_K^+]]$ denotes the auxiliary p -adic L-function defined in [SU14, Section 6.5.3] (in fact, it is the image of the p -adic L-function of the trivial Dirichlet character under the composition of the identification $A[[\Gamma_{\mathbb{Q}}]] \simeq A[[\Gamma_K^+]]$ and the map $A[[\Gamma_K^+]] \rightarrow \mathbb{I}[[\Gamma_K]]$, $\gamma^+ \mapsto (1+W)^{-1}(\gamma^+)^2$).

Consequently, for all height one primes P not of the form $P^+ \Lambda_{\mathbf{D}}$,

$$\text{ord}_P(\text{Char}_{\mathbb{I}_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(\mathbf{f}/K_\infty))) \geq \text{ord}_P(\mathcal{L}_{\mathbf{f},K}^\Sigma).$$

□

Remark 4.5. Since primes of the form $P = P^+ \Lambda_{\mathbf{D}}$ for height one primes P^+ of $\mathbb{I}[[\Gamma_K^+]]$ are excluded, Proposition 13.6 (2) of [SU14] is unnecessary. Hence, we omit the conditions on N and on $\bar{\rho}_{\mathbf{f}}|_{I_\ell}$ for primes $\ell \mid N$, where $\bar{\rho}_{\mathbf{f}} := \rho_{\mathbf{f}} \bmod \mathfrak{m}_{\mathbb{I}}$, with $\mathfrak{m}_{\mathbb{I}}$ being the maximal ideal of \mathbb{I} . See also the remark after Theorem 3.26 in [SU14].

Corollary 4.6. *Assume that the residual representation $\bar{\rho}_E|_{G_K}$ is irreducible. There exists a nontrivial multiplicative set $S \subset \Lambda_K^+ \subset \Lambda_K$ such that*

$$S^{-1} \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) \subset (\mathcal{L}_p^{\text{PR}}(E/K))$$

holds in $S^{-1} \Lambda_K$.

Proof. By [Hid86, Corollary 1.5], there exist an \mathbb{I} -adic ordinary eigenform \mathbf{f} with trivial nebentypus and a weight 2 arithmetic specialization $\phi \in \mathfrak{X}_{\mathbb{I}, \mathcal{O}}^a$ such that the specialized form $\phi(\mathbf{f})$ is the p -stabilization of the newform associated to E . Let \mathfrak{p}_ϕ be the kernel of the specialization map ϕ .

By Propositions 3.5 and 3.8, the p -adic L -function $\mathcal{L}_{\mathbf{f},K}^\Sigma$ is not contained in $\mathfrak{p}_\phi \mathbb{I}_K$. Let $\{P_1, \dots, P_n\}$ be the set of all height one primes of \mathbb{I}_K such that $P_i = P_i^+ \mathbb{I}_K$ for some height one prime P_i^+ of $\mathbb{I}[[\Gamma_K^+]]$ and $\text{ord}_{P_i}(\mathcal{L}_{\mathbf{f},K}^\Sigma) > 0$. It follows that $P_i \not\subset \mathfrak{p}_\phi \mathbb{I}_K$ for all i . For each i , choose an element $h_i \in P_i - \mathfrak{p}_\phi \mathbb{I}_K$, and let T be the multiplicative set generated by $\{h_i : i = 1, \dots, n\}$. Then for any height one prime P of \mathbb{I}_K with $P \cap T = \emptyset$, either $\text{ord}_P(\mathcal{L}_{\mathbf{f},K}^\Sigma) = 0$ or P is not of the form $P^+ \mathbb{I}_K$ for any height one prime P^+ of $\mathbb{I}[[\Gamma_K^+]]$. Hence by Theorem 4.4, we have that

$$T^{-1} \text{Char}_{\mathbb{I}_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}^\Sigma(\mathbf{f}/K_\infty)) \subset (\mathcal{L}_{\mathbf{f},K}^\Sigma).$$

Set $S = \phi(T)$. The result then follows from applying [SU14, Corollary 3.8 (ii)], Corollary 2.10, Corollary 2.9, and Proposition 3.5. □

4.3. Proof of Theorem 4.2.

Theorem 4.7. *For every nontrivial multiplicative set $S \subset \Lambda_K$, the following statements are equivalent:*

- (1) $S^{-1} \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_\infty)) \subset (\mathcal{L}_p^{\text{PR}}(E/K))$.
- (2) $S^{-1} \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)) \Lambda_K^{\text{ur}} \subset (\mathcal{L}_p^{\text{Gr}}(E/K))$.

The same equivalence also holds for the reverse inclusions.

Proof. This result is essentially [BSTW24, Proposition 9.18] in the two-variable (or $\cdot = \emptyset$ in *loc. cit.*) case, building on explicit reciprocity laws for the Beilinson-Flach classes and global Poitou-Tate duality. See also [BCS25, Proposition 4.1.3] and [CGS25, Proposition 4.2.1]. □

By Theorem 4.7 and Corollary 4.6, there exists a nontrivial multiplicative set $S \subset \Lambda_K^+ \subset \Lambda_K$ such that

$$S^{-1} \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)) \Lambda_K^{\text{ur}} \subset (\mathcal{L}_p^{\text{Gr}}(E/K)).$$

We may assume S is generated by prime elements in the unique factorization domain Λ_K . For a height-one prime $P \subset \Lambda_K^{\text{ur}}$ with $P \cap S \neq \emptyset$, we have $P = P^+ \Lambda_K^{\text{ur}}$ for some prime $P^+ \subset \Lambda_K^{\text{ur},+}$. However, by [Hsi14, Theorem B] and Proposition 3.14,

$$\mu(\mathcal{L}_p^{\text{Gr}}(E/K)^-) = \mu(\mathcal{L}_p^{\text{BDP}}(E/K)) = 0,$$

where $\mu(\cdot)$ denotes the μ -invariant. Hence, we have

$$\text{ord}_P(\mathcal{L}_p^{\text{Gr}}(E/K)) = 0$$

if $P \subset \Lambda_K^{\text{ur}}$ is a height-one prime of the form $P = P^+ \Lambda_K^{\text{ur}}$ for some $P^+ \subset \Lambda_K^{\text{ur},+}$. It follows that

$$\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty)) \Lambda_K^{\text{ur}} \subset (\mathcal{L}_p^{\text{Gr}}(E/K)).$$

Moreover, if condition (Im) holds, we can establish that part (1) of Conjecture 1.1 is true. The argument is analogous to that of [SU14, Theorem 3.30], employing the results of Kato in [Kat04, Theorem

17.4], Lemma 2.4, and a commutative algebra lemma from [SU14, Lemma 3.2]. The validity of part (1) of the conjecture, in turn, implies that part (2) also holds. We note that while the original proof in [SU14] assumes the stronger condition $\text{Im } \rho_E \supset \text{SL}_2(\mathbb{Z}_p)$, this requirement can be relaxed to our condition (Im), as is discussed in the final paragraph of [Ski16, page 187].

5. APPLICATIONS

5.1. Cyclotomic main conjectures. Let E/\mathbb{Q} be an elliptic curve of conductor N , and let $p > 2$ be a prime at which E has good ordinary reduction. Assume that the residual representation $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[p])$ is irreducible.

Conjecture 5.1 (Mazur's main conjecture). $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})$ is $\Lambda_{\mathbb{Q}}$ -torsion and

$$\text{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})) = (\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q})).$$

As in [SU14, Theorem 3.29], we have the following result.

Theorem 5.2. $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})$ is $\Lambda_{\mathbb{Q}}$ -torsion and

$$\text{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})) \otimes \mathbb{Q}_p = (\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q}))$$

in $\Lambda_{\mathbb{Q}} \otimes \mathbb{Q}_p$. Moreover, if condition (Im) holds, we have

$$\text{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})) = (\mathcal{L}_p^{\text{MSD}}(E/\mathbb{Q}))$$

in $\Lambda_{\mathbb{Q}}$.

Lemma 5.3. Let K be an imaginary quadratic field, and $I \subset \Lambda_K$ the kernel of the natural projection $\Lambda_K \rightarrow \Lambda_K^+$. Suppose that the residual representation $\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$ is irreducible. Then

$$\text{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/\mathbb{Q}_{\infty})) \cdot \text{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E^K/\mathbb{Q}_{\infty})) \subset \text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty})) \pmod{I}$$

in $\Lambda_K^+ \simeq \Lambda_{\mathbb{Q}}$.

Proof. Let Σ be a set of places of K containing all places dividing $pN\infty$ as before, $\Sigma_0 := \{\mathfrak{q} \in \Sigma : \mathfrak{q} \nmid p\}$. Let $M := T_p E \otimes \Lambda_K^{\vee}$ and $N := T_p E \otimes \Lambda_K^{+, \vee}$ for simplicity.

We have the following commutative diagram of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_{\mathcal{F}_{\text{ord}}}^1(K, N) & \longrightarrow & H_{\mathcal{F}_{\text{ord}}^{\Sigma}}^1(K, N) & \xrightarrow{s} & \bigoplus_{\mathfrak{q} \in \Sigma_0} H^1(G_{K_{\mathfrak{q}}}, N) \\ & & \downarrow f & & \downarrow g & & \downarrow h \\ 0 & \longrightarrow & H_{\mathcal{F}_{\text{ord}}}^1(K, M)[I] & \longrightarrow & H_{\mathcal{F}_{\text{ord}}^{\Sigma}}^1(K, M)[I] & \longrightarrow & \bigoplus_{\mathfrak{q} \in \Sigma_0} H^1(G_{K_{\mathfrak{q}}}, M)[I] \end{array},$$

where f, g, h, s are the natural maps. We claim that h is injective. To see this, for any primes $\mathfrak{q} \in \Sigma_0$, we consider the following commutative diagram of inflation-restriction sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, N^{I_{\mathfrak{q}}}) & \longrightarrow & H^1(G_{K_{\mathfrak{q}}}, N) & \longrightarrow & H^1(I_{\mathfrak{q}}, N) \\ & & \downarrow & & \downarrow h_{\mathfrak{q}} & & \downarrow t_{\mathfrak{q}} \\ 0 & \longrightarrow & H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, M^{I_{\mathfrak{q}}})[I] & \longrightarrow & H^1(G_{K_{\mathfrak{q}}}, M)[I] & \longrightarrow & H^1(I_{\mathfrak{q}}, M)[I] \end{array},$$

where $h_{\mathfrak{q}}, t_{\mathfrak{q}}$ are the natural maps. Since $H^1(G_{K_{\mathfrak{q}}}/I_{\mathfrak{q}}, N^{I_{\mathfrak{q}}}) = 0$ by Lemma 2.5 (1), to prove that $h_{\mathfrak{q}}$ is injective, it suffices to show that $t_{\mathfrak{q}}$ is injective. Fix a topological generator γ^- of $\text{Gal}(K_{\infty}^-/K) \simeq \text{Gal}(K_{\infty}/K_{\infty}^+)$, then we have $I = (\gamma^- - 1) \subset \Lambda_K$ as an ideal. Then we have the long exact sequence

$$H^0(I_{\mathfrak{q}}, M) \xrightarrow{(\gamma^- - 1)} H^0(I_{\mathfrak{q}}, M) \rightarrow H^1(I_{\mathfrak{q}}, N) \xrightarrow{t_{\mathfrak{q}}} H^1(I_{\mathfrak{q}}, M)$$

induced by the short exact sequence

$$0 \rightarrow N \rightarrow M \xrightarrow{(\gamma^- - 1)} M \rightarrow 0,$$

hence to prove the injectivity of $t_{\mathfrak{q}}$, it suffices to show $H^0(I_{\mathfrak{q}}, M)/IH^0(I_{\mathfrak{q}}, M) = 0$. However, since \mathfrak{q} is unramified in K_{∞}/K , let $W := T_p \otimes \mathbb{Q}_p/\mathbb{Z}_p$, then we have that

$$H^0(I_{\mathfrak{q}}, M) = (T_p E \otimes \text{Hom}_{\text{cont}}(\Lambda_K, \mathbb{Q}_p/\mathbb{Z}_p))^{I_{\mathfrak{q}}} \simeq \text{Hom}_{\text{cont}}(\Lambda_K, W)^{I_{\mathfrak{q}}} = \text{Hom}_{\text{cont}}(\Lambda_K, W^{I_{\mathfrak{q}}}).$$

Since

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cont}}(\Lambda_K, W^{I_q}) &\simeq \mathrm{Hom}_{\mathrm{cont}}(\Lambda_K, \mathrm{Hom}(\mathrm{Hom}(W^{I_q}, \mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Q}_p/\mathbb{Z}_p)) \\ &\simeq \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Hom}(W^{I_q}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \Lambda_K, \mathbb{Q}_p/\mathbb{Z}_p),\end{aligned}$$

we have

$$\mathrm{Hom}(\mathrm{Hom}_{\mathrm{cont}}(\Lambda_K, W^{I_q}), \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Hom}(W^{I_q}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \Lambda_K.$$

Hence

$$\mathrm{Hom}(H^0(I_q, M)/IH^0(I_q, M), \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Hom}(W^{I_q}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \Lambda_K[I] = 0.$$

Therefore $H^0(I_q, M)/IH^0(I_q, M) = 0$, which completes the proof of our claim.

Let $A := \mathrm{Im} \, s \subset \bigoplus_{q \in \Sigma_0} H^1(G_{K_q}, N)$. Then by the snake lemma, we have the following exact sequence

$$0 \rightarrow \ker f \rightarrow \ker g \rightarrow \ker h|_A \rightarrow \mathrm{coker} f \rightarrow \mathrm{coker} g.$$

By [SU14, Proposition 3.9], Remark 2.3, Lemma 2.7 and Nakayama's lemma, we have that the map g is an isomorphism. Hence we have $\ker f = 0$ and $\mathrm{coker} f \simeq \ker h|_A = 0$, which implies that the map f is an isomorphism. Then we have that the natural Λ_K^+ -module homomorphism

$$\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty)/I\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty) \rightarrow \mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty^+)$$

is an isomorphism. By [SU14, Corollary 3.8 (ii)], we have that

$$\mathrm{Char}_{\Lambda_K^+}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty^+)) \subset \mathrm{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty)) \bmod I$$

in Λ_K^+ . Together with Lemma 2.4, we complete the proof. \square

Proof of Theorem 5.2. By a result of Serre ([Ser87, Section 3.3]), the irreducibility of $\bar{\rho}_E$ implies that it is absolutely irreducible when $p > 2$. Choose an imaginary quadratic field K such that all primes dividing pN split in K and the restriction $\bar{\rho}_E|_{G_K}$ remains absolutely irreducible. Let $I \subset \Lambda_K$ be the kernel of the natural projection $\Lambda_K \rightarrow \Lambda_K^+$. Applying Theorem 4.2, Proposition 3.7, and the preceding lemma, we obtain

$$\begin{aligned}\mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/\mathbb{Q}_\infty)) \cdot \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E^K/\mathbb{Q}_\infty)) &\subset \mathrm{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/K_\infty)) \bmod I \\ &\subset (\mathcal{L}_p^{\mathrm{PR}}(E/K)) \bmod I = (\mathcal{L}_p^{\mathrm{PR}}(E/K)^+) = (\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})) \cdot (\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q}))\end{aligned}$$

in $\Lambda_{\mathbb{Q}} \simeq \Lambda_K^+$. On the other hand, by [Kat04, Theorem 17.14], we have that

$$(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})) \subset \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/\mathbb{Q}_\infty)), \quad (\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q})) \subset \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E^K/\mathbb{Q}_\infty))$$

in $\Lambda_{\mathbb{Q}} \otimes \mathbb{Q}_p$ and even in $\Lambda_{\mathbb{Q}}$ under the condition (Im) (See the discussions in the final paragraph of [Ski16, page 187], as noted previously). If one of the above inclusions is not an equality, then

$$(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})) \cdot (\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q})) \subsetneq \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/\mathbb{Q}_\infty)) \cdot \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E^K/\mathbb{Q}_\infty)),$$

which contradicts the inclusion established above:

$$\mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/\mathbb{Q}_\infty)) \cdot \mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E^K/\mathbb{Q}_\infty)) \subset (\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})) \cdot (\mathcal{L}_p^{\mathrm{MSD}}(E^K/\mathbb{Q}))$$

Therefore it must be that

$$\mathrm{Char}_{\Lambda_{\mathbb{Q}}}(\mathcal{X}_{\mathcal{F}_{\mathrm{ord}}}(E/\mathbb{Q}_\infty)) = (\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}))$$

in $\Lambda_{\mathbb{Q}} \otimes \mathbb{Q}_p$ and even in $\Lambda_{\mathbb{Q}}$ under the condition (Im). \square

As a corollary, we obtain the following result concerning the cyclotomic analogue of the BDP main conjecture.

Corollary 5.4. *If $\mathcal{L}_p^{\mathrm{Gr}}(E/K)^+$ is nontrivial, then $\mathcal{X}_{\mathcal{F}_{\mathrm{Gr}}}(E/K_\infty^+)$ is Λ_K^+ -torsion and*

$$\mathrm{Char}_{\Lambda_K^+}(\mathcal{X}_{\mathcal{F}_{\mathrm{Gr}}}(E/K_\infty^+))\Lambda_K^{\mathrm{ur},+} \otimes \mathbb{Q}_p = (\mathcal{L}_p^{\mathrm{Gr}}(E/K)^+)$$

in $\Lambda_K^{\mathrm{ur},+} \otimes \mathbb{Q}_p$. Moreover, if condition (Im) holds, we have

$$\mathrm{Char}_{\Lambda_K^+}(\mathcal{X}_{\mathcal{F}_{\mathrm{Gr}}}(E/K_\infty^+))\Lambda_K^{\mathrm{ur},+} = (\mathcal{L}_p^{\mathrm{Gr}}(E/K)^+)$$

in $\Lambda_K^{\mathrm{ur},+}$.

Proof. This result follows from a combination of Theorem 5.2 (applied to E and E^K), Lemma 2.4, Proposition 3.7, [CGS25, Proposition 4.2.1] (a cyclotomic analogue of Theorem 4.7, see also [BSTW24, Proposition 9.18]), and Proposition 3.8. \square

5.2. Anticyclotomic main conjectures. Let E/\mathbb{Q} be an elliptic curve of conductor N , let $p > 2$ be a prime such that E has good ordinary reduction at p , and let K be an imaginary quadratic field such that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K and the pair (E, K) satisfies the Heegner hypothesis. Assume that the residual representation $\bar{\rho}_E|_{G_K} : G_K \rightarrow \text{Aut}(E[p])$ is irreducible.

Conjecture 5.5 (BDP main conjecture). $\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-)$ is Λ_K^- -torsion and

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-))\Lambda_K^{\text{ur},-} = (\mathcal{L}_p^{\text{BDP}}(E/K)).$$

We define the compact Selmer group

$$S_{\text{ord}}(E/K_{\infty}^-) = \varprojlim_n \varprojlim_m \text{Sel}_{p^m}(E/K_n^-),$$

where K_n^- is the subfield of K_{∞}^- with $[K_n^- : K] = p^n$ for each positive integer n .

Fix a modular parametrization $\pi : X_0(N) \rightarrow E$. In [PR87], Perrin-Riou constructed an element $\kappa \in S_{\text{ord}}(E/K_{\infty}^-)$ using the Kummer images of Heegner points on $X_0(N)$, which is non-torsion over Λ_K^- by a result of Cornut-Vatsal [CV07]. She then formulated the anticyclotomic main conjecture as follows.

Conjecture 5.6 (Heegner point main conjecture). *The modules $S_{\text{ord}}(E/K_{\infty}^-)$ and $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)$ are both of Λ_K^- -rank one, and*

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) = \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2.$$

Theorem 5.7. (1) $\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-)$ is Λ_K^- -torsion and

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-))\Lambda_K^{\text{ur},-} \otimes \mathbb{Q}_p = (\mathcal{L}_p^{\text{BDP}}(E/K))$$

holds in $\Lambda_K^{\text{ur},-} \otimes \mathbb{Q}_p$. Moreover, if the representation $\rho_E|_{G_K} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ is surjective, then

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-))\Lambda_K^{\text{ur},-} = (\mathcal{L}_p^{\text{BDP}}(E/K)).$$

(2) *The modules $S_{\text{ord}}(E/K_{\infty}^-)$ and $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)$ are both of Λ_K^- -rank one, and*

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \otimes \mathbb{Q}_p = \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2 \otimes \mathbb{Q}_p$$

holds in $\Lambda_K^- \otimes \mathbb{Q}_p$. Moreover, if the representation $\rho_E|_{G_K} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ is surjective, then

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) = \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2.$$

We prove this theorem in the remainder of this subsection. We begin by recalling some results concerning the Heegner point main conjecture.

Theorem 5.8. *Assume that $E(K)[p] = 0$. Then the modules $S_{\text{ord}}(E/K_{\infty}^-)$ and $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)$ are both of Λ_K^- -rank one, and*

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \otimes \mathbb{Q}_p \supset \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2 \otimes \mathbb{Q}_p$$

holds in $\Lambda_K^- \otimes \mathbb{Q}_p$. Moreover, if the representation $\rho_E|_{G_K} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ is surjective, then

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \supset \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2.$$

Proof. By [CGS25, Theorem 6.5.2], the modules $S_{\text{ord}}(E/K_{\infty}^-)$ and $\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)$ both have Λ_K^- -rank one, and the inclusion

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \otimes \mathbb{Q}_p \supset \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2 \otimes \mathbb{Q}_p$$

holds in $\Lambda_K^- \otimes \mathbb{Q}_p$. Moreover, if the representation $\rho_E|_{G_K} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ is surjective, then by [How04, Theorem B], the inclusion

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \supset \text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2$$

holds in Λ_K^- (i.e., without inverting p). □

Arguing as in [BCK21, Theorem 5.2], we obtain the following result.

Theorem 5.9. *The module $\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-)$ is Λ_K^- -torsion, and for every nontrivial multiplicative set $S \subset \Lambda_K^-$, the following statements are equivalent:*

$$(1) S^{-1}\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_{\infty}^-))\Lambda_K^{\text{ur},-} \supset (\mathcal{L}_p^{\text{BDP}}(E/K)).$$

$$(2) S^{-1}\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{ord}}}(E/K_{\infty}^-)_{\text{tor}}) \supset S^{-1}\text{Char}_{\Lambda_K^-}(S_{\text{ord}}(E/K_{\infty}^-)/\Lambda_K^- \cdot \kappa)^2.$$

The equivalence also holds with the divisibility reversed.

Since $\mathcal{L}_p^{\text{BDP}}(E/K)$ is non-zero ([BCK21, Corollary 4.5]), by the arguments presented in Section 4.3, there exists a nontrivial multiplicative set $S \subset \Lambda_K^+ \subset \Lambda_K$ such that for any $s \in S$, $\gamma^+ - 1 \nmid s$, and

$$S^{-1}\text{Char}_{\Lambda_K}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty))\Lambda_K^{\text{ur}} \subset (\mathcal{L}_p^{\text{Gr}}(E/K)).$$

By Lemma 2.6 and standard properties of characteristic ideals (see, e.g., [SU14, Corollary 3.8]), we have

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty^-))\Lambda_K^{\text{ur},-} \otimes \mathbb{Q}_p \subset (\mathcal{L}_p^{\text{BDP}}(E/K)).$$

The reverse divisibility is established by combining Theorem 5.8 and Theorem 5.9.

Moreover, if the representation $\rho_E|_{G_K} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p}(T_p E)$ is surjective, then by Theorem 4.2 and Lemma 2.6,

$$\text{Char}_{\Lambda_K^-}(\mathcal{X}_{\mathcal{F}_{\text{Gr}}}(E/K_\infty^-))\Lambda_K^{\text{ur},-} \subset (\mathcal{L}_p^{\text{BDP}}(E/K)),$$

and the rest of the argument follows from Theorem 5.8 and Theorem 5.9 as before.

Remark 5.10. Via [BSTW24, Proposition 12.7], the condition in Theorem 5.7 that $\rho_E|_{G_K}$ has full image can be weakened to condition (Im).

5.3. BSD conjectures. Let E/\mathbb{Q} be an elliptic curve of conductor N , and let $p > 2$ be a prime such that E has good ordinary reduction at p .

Theorem 5.11. *Let $r \leq 1$ be an integer. The following statements are equivalent:*

- (1) $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$ and $\#\text{III}(E/\mathbb{Q}) < \infty$;
- (2) $\text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E/\mathbb{Q}) = r$;
- (3) $\text{ord}_{s=1} L(E/\mathbb{Q}, s) = r$.

Under any of the above conditions, if condition (Im) also holds, then the p -part of the BSD formula for E is valid, i.e.,

$$\left| \frac{L^{(r)}(1, E)}{r! \cdot \Omega_E R_E} \right|_p = \left| \frac{\#\text{III}(E)[p^\infty] \cdot \prod_{\ell|N} c_\ell(E)}{(\#E(\mathbb{Q})_{\text{tor}})^2} \right|_p,$$

where R_E is the regulator of $E(\mathbb{Q})$, Ω_E is the Néron period, $c_\ell(E)$ is the Tamagawa number at a prime ℓ , and $|\cdot|_p$ denotes the p -adic absolute value.

Proof. The implication (1) \Rightarrow (2) is immediate.

The implication (3) \Rightarrow (1) is established by the work of Gross-Zagier [GZ86] and Kolyvagin [Kol90].

For the implication (2) \Rightarrow (3), one can choose an imaginary quadratic field K such that $\text{ord}_{s=1} L(E^K, s) = 1$ and (E, K) satisfies the Heegner hypothesis, as shown in [FH95]. Analogously to [Wan21, Theorem 1.9], by applying descent arguments to the rational part of Theorem 5.7(2) and using the Gross-Zagier formula, we obtain

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E/K) = 1 \quad \Rightarrow \quad \text{ord}_{s=1} L(E/K, s) = 1,$$

thus establishing (2) \Rightarrow (3).

The p -part of the BSD formula in the rank zero case follows from the integral part of Theorem 5.2, combined with descent arguments (see [SU14, Section 3.6.1] for details).

Similarly, by choosing an imaginary quadratic field K as described above, the p -part of the BSD formula in the rank one case follows from the integral part of Corollary 5.4, [CGS25, Proposition 3.4.2], the fact that $\mathcal{L}_p^{\text{Gr}}(E/K)^+(1) = \mathcal{L}_p^{\text{Gr}}(E/K)^-(1) \neq 0$, and the descent arguments in [JSW17]. \square

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

- [BCGS23] Ashay Burungale, Francesc Castella, Giada Grossi, and Christopher Skinner, *Non-vanishing of kolyvagin systems and iwawata theory*, arXiv preprint arXiv:2312.09301 (2023).
- [BCK21] Ashay Burungale, Francesc Castella, and Chan-Ho Kim, *A proof of Perrin-Riou's Heegner point main conjecture*, Algebra Number Theory **15** (2021), no. 7, 1627–1653 (English).
- [BCS25] Ashay Burungale, Francesc Castella, and Christopher Skinner, *Base change and Iwasawa main conjectures for GL_2* , Int. Math. Res. Not. IMRN (2025), no. 8, Paper No. rnaaf082, 15. MR 4894178
- [BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p -adic Rankin L -series*, Duke Math. J. **162** (2013), no. 6, 1033–1148, With an appendix by Brian Conrad. MR 3053566
- [BSTW24] Ashay Burungale, Christopher Skinner, Ye Tian, and Xin Wan, *Zeta elements for elliptic curves and applications*, Preprint, arXiv:2409.01350 [math.NT] (2024).

- [CGLS22] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner, *On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes*, Invent. Math. **227** (2022), no. 2, 517–580. MR 4372220
- [CGS25] Francesc Castella, Giada Grossi, and Christopher Skinner, *Mazur’s main conjecture at Eisenstein primes*, Math. Ann. **393** (2025), no. 2, 2451–2506. MR 4984348
- [CH18] Francesc Castella and Ming-Lun Hsieh, *Heegner cycles and p -adic L -functions*, Math. Ann. **370** (2018), no. 1-2, 567–628. MR 3747496
- [CV07] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg L -functions and CM points, L -functions and Galois representations*, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186. MR 2392354
- [dS87] Ehud de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987, p -adic L functions. MR 917944
- [FH95] Solomon Friedberg and Jeffrey Hoffstein, *Nonvanishing theorems for automorphic L -functions on $GL(2)$* , Ann. of Math. (2) **142** (1995), no. 2, 385–423. MR 1343325
- [GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L -series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 833192
- [Hid81] Haruzo Hida, *Congruence of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), no. 2, 225–261. MR 610538
- [Hid85] ———, *A p -adic measure attached to the zeta functions associated with two elliptic modular forms. I*, Invent. Math. **79** (1985), no. 1, 159–195. MR 774534
- [Hid86] ———, *Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85** (1986), no. 3, 545–613. MR 848685
- [How04] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472. MR 2098397
- [Hsi14] Ming-Lun Hsieh, *Special values of anticyclotomic rankin-selberg l -functions*, Documenta Mathematica **19** (2014), 709–767.
- [Hun17] Pin-Chi Hung, *On the non-vanishing mod ℓ of central L -values with anticyclotomic twists for Hilbert modular forms*, J. Number Theory **173** (2017), 170–209. MR 3581914
- [JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434. MR 3684675
- [Kat04] Kazuya Kato, *p -adic Hodge theory and values of zeta functions of modular forms.*, Cohomologies p -adiques et applications arithmétiques (III), Paris: Société Mathématique de France, 2004, pp. 117–290 (English).
- [Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR 1106906
- [LLZ15] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for modular forms over imaginary quadratic fields*, Compos. Math. **151** (2015), no. 9, 1585–1625. MR 3406438
- [Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230
- [Nr06] Jan Nekovář, *Selmer complexes*, Astérisque (2006), no. 310, viii+559. MR 2333680
- [PR86] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p -adiques*, C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), no. 5, 165–168. MR 854725
- [PR87] ———, *Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456. MR 928018
- [Rib83] Kenneth A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205. MR 688264
- [Roh84] David E Rohrlich, *On L -functions of elliptic curves and cyclotomic towers*, Inventiones mathematicae **75** (1984), no. 3, 409–423.
- [Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), no. 1, 179–230. MR 885783
- [Ski16] Christopher Skinner, *Multiplicative reduction and the cyclotomic main conjecture for GL_2* , Pacific J. Math. **283** (2016), no. 1, 171–200. MR 3513846
- [Ski20] ———, *A converse to a theorem of gross, zagier, and kolyvagin*, Annals of Mathematics **191** (2020), no. 2, 329–354.
- [SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for GL_2* , Inventiones mathematicae **195** (2014), 1–277.
- [SZ14] Christopher Skinner and Wei Zhang, *Indivisibility of Heegner points in the multiplicative case*, arXiv preprint arXiv:1407.1099 (2014).
- [Vat03] V. Vatsal, *Special values of anticyclotomic L -functions*, Duke Math. J. **116** (2003), no. 2, 219–261. MR 1953292
- [Wan15] Xin Wan, *The Iwasawa main conjecture for Hilbert modular forms*, Forum Math. Sigma **3** (2015), Paper No. e18, 95. MR 3482263
- [Wan20] ———, *Iwasawa main conjecture for Rankin-Selberg p -adic L -functions*, Algebra Number Theory **14** (2020), no. 2, 383–483. MR 4195651
- [Wan21] ———, *Heegner point Kolyvagin system and Iwasawa main conjecture*, Acta Math. Sin., Engl. Ser. **37** (2021), no. 1, 104–120 (English).
- [Zha14] Wei Zhang, *Selmer groups and the indivisibility of heegner points*, Cambridge Journal of Mathematics **2** (2014), no. 2, 191–253.

ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE, CHINESE ACADEMY OF SCIENCES, BEIJING 100190, CHINA.
Email address: xjyan95@amss.ac.cn

BEIJING INSTITUTE OF MATHEMATICAL SCIENCES AND APPLICATIONS, BEIJING 101408, CHINA;

YAU MATHEMATICAL SCIENCES CENTER, TSINGHUA UNIVERSITY, BEIJING 100084, CHINA.
Email address: xwzhu@bimsa.cn