PERRIN-RIOU'S MAIN CONJECTURE FOR ELLIPTIC CURVES AT SUPERSINGULAR PRIMES

FRANCESC CASTELLA AND XIN WAN

Abstract. In 1987, B. Perrin-Riou formulated a Heegner point main conjecture for elliptic curves at primes of ordinary reduction. In this paper, we formulate an analogue of Perrin-Riou's main conjecture for supersingular primes. We then prove this conjecture under mild hypotheses, and deduce from this result a Λ-adic extension of Kobayashi's p-adic Gross–Zagier formula, new cases of B.-D. Kim's doubly-signed main conjectures, and a strengthened version of Skinner's converse to the Gross–Zagier–Kolyvagin theorem for supersingular primes.

Contents

2010 *Mathematics Subject Classification.* 11R23 (primary); 11G05, 11G40 (secondary).

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 682152).

1. Introduction

1.1. **Perrin-Riou's main conjecture.** Let $E/\mathbf{Q}$ be an elliptic curve of conductor of N, let f be the associated newform on $\Gamma_0(N)$, and fix an odd prime $p \nmid N$. Let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant prime to N. Writing

$$N = N^+N^-$$

with N^+ (resp. N^-) only divisible by primes which split (resp. are inert) in K, assume that the following *generalized Heegner hypothesis* is satisfied:

(Heeg) N^- is the square-free product of an even number of primes.

Assuming that p is *ordinary* for E, Perrin-Riou formulated in [PR87a] an Iwasawa-theoretic main conjecture for Heegner points over the anticyclotomic tower. To recall its statement, let $K_\infty^{\mathrm{ac}} = \bigcup_n K_n^{\mathrm{ac}}$ be the anticyclotomic $\mathbf{Z}_p$-extension of K, with K_n^{ac} the unique subextension of K_∞^{ac} of degree p^n over K, and set

$$\mathrm{Sel}_{p^\infty}(E/K_\infty^{\mathrm{ac}}) := \varinjlim_n \varinjlim_m \mathrm{Sel}_{p^m}(E/K_n^{\mathrm{ac}}), \quad \mathrm{Sel}(K_\infty^{\mathrm{ac}}, T_pE) := \varprojlim_n \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n^{\mathrm{ac}}), \tag{1.1}$$

where

$$\mathrm{Sel}_{p^m}(E/K_n^{\mathrm{ac}}) := \ker\left\{ H^1(K_n^{\mathrm{ac}}, E[p^m]) \longrightarrow \prod_w H^1(K_{n,w}^{\mathrm{ac}}, E) \right\} \tag{1.2}$$

is the p^m-descent Selmer group of E over K_n^{ac}. Another assumption in [PR87a] is that $N^- = 1$. Taking Heegner points on $X_0(N)$ and mapping them to E by a fixed modular parametrization

$$\varphi : X_0(N) \longrightarrow E$$

one can construct a Λ_{ac}-module $H_\infty \subset \mathrm{Sel}(K_\infty^{\mathrm{ac}}, T_pE)$, where

$$\Lambda_{\mathrm{ac}} := \mathbf{Z}_p[[\mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)]]$$

is the anticyclotomic Iwasawa algebra. After the work of Cornut [Cor02] and Vatsal [Vat02], the module H_∞ is known to be free of rank 1, say $H_\infty = \Lambda_{\mathrm{ac}} \cdot \mathbf{z}_\infty$.

Let $c_E \in \mathbf{Q}^\times$ be the Manin constant associated with φ (i.e., if ω is a Néron differential of E and f is the newform associated with E, then $\varphi^*\omega = c_E \cdot 2\pi i f(z)dz$), and let $u_K := |\mathcal{O}_K^\times|/2$.

Conjecture 1.1 (Perrin-Riou)**.** *Assume that $N^- = 1$ and that p is a prime of good ordinary reduction of E. Then the Pontrjagin dual $X_{p^\infty}(E/K_\infty^{\mathrm{ac}})$ of $\mathrm{Sel}_{p^\infty}(E/K_\infty^{\mathrm{ac}})$ has Λ_{ac}-rank 1, and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(X_{p^\infty}(E/K_\infty^{\mathrm{ac}})_{\mathrm{tors}}) = \frac{1}{c_E^2 u_K^2} \cdot \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathrm{Sel}(K_\infty^{\mathrm{ac}}, T_pE)}{\Lambda_{\mathrm{ac}} \cdot \mathbf{z}_\infty} \right)^2,$$

where the subscript tors *denotes the Λ^{ac}-torsion submodule.*

The important works of Bertolini [Ber95] and Howard [How04b] led to the proof (under mild hypotheses) of one of the divisibilities predicted by Conjecture 1.1, while later in [How04c] Howard formulated an extension of Conjecture 1.1 to abelian varieties of GL_2-type over totally real fields, and extended the results of [How04b] to this context.

Our first main goal in this paper is to formulate an extension of Conjecture 1.1 to good supersingular primes, working under the generalized Heegner hypothesis (Heeg). A fundamental obstacle to such extension is the fact that, in the non-ordinary case, i.e., when p divides

$$a_p := p + 1 - |E(\mathbf{F}_p)|,$$

Heegner points on E give rise to compatible systems of classes with *unbounded* growth over the anticyclotomic tower. As a result, there is no obvious analogue of the submodule H_∞ of $\mathrm{Sel}(K_\infty^{\mathrm{ac}}, T_pE)$ for supersingular primes p. Nonetheless, following ideas of Kobayashi [Kob03],

and their extension by B.-D. Kim [Kim14a], we will succeed in formulating the right analogue of Conjecture 1.1 assuming in addition[1] that $a_p = 0$ and that

$$p = \mathfrak{p}\overline{\mathfrak{p}} \text{ splits in } K. \tag{spl}$$

Indeed, following these methods, in Section 3 we define four pairs of doubly-signed Selmer groups

$$\mathfrak{Sel}_{p^\infty}^{\pm,\pm}(E/K_\infty^{\mathrm{ac}}) \subset \mathrm{Sel}_{p^\infty}(E/K_\infty^{\mathrm{ac}}), \quad \mathfrak{Sel}^{\pm,\pm}(K_\infty^{\mathrm{ac}}, T_pE) \supset \mathrm{Sel}(K_\infty^{\mathrm{ac}}, T_pE)$$

obtained by replacing the local conditions in (1.2) at the primes above $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. On the other hand, in Section 5 we construct two bounded cohomology classes

$$\mathbf{z}^+ \in \mathfrak{Sel}^{+,+}(K_\infty^{\mathrm{ac}}, T_pE), \quad \mathbf{z}^- \in \mathfrak{Sel}^{-,-}(K_\infty^{\mathrm{ac}}, T_pE).$$

obtained by dividing the natural systems of Heegner points over K_∞^{ac}/K by certain analogues of Pollack's [Pol03] half-logarithms. By (Heeg), the curve E is isogenous to a quotient

$$\pi : J_{N^+,N^-} \longrightarrow E' \tag{1.3}$$

of the Jacobian of a Shimura curve X_{N^+,N^-} attached to an indefinite quaternion algebra over $\mathbf{Q}$ of discriminant N^-, and the Heegner points used to construct $\mathbf{z}^\pm$ come from X_{N^+,N^-}. Let $\delta(N^+,N^-) = \pi \circ \pi^\vee$ be the modular degree of the parametrization (1.3), and assuming that E is the strong Weil curve in its isogeny class, set

$$\delta_{N^+,N^-} := \frac{\delta(N^+,N^-)}{\delta(N,1)},$$

where $\delta(N,1) = \varphi\circ\varphi^\vee$ is the modular degree of φ. We are now ready to state our generalization of Conjecture 1.1.

Conjecture 1.2. *Assume the generalized Heegner hypothesis* (Heeg) *holds, and let $p > 3$ be a prime of good supersingular reduction of E which splits in K. Then, for each $\varepsilon \in \{\pm\}$, the Pontrjagin dual $\mathfrak{X}_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty^{\mathrm{ac}})$ of $\mathfrak{Sel}_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty^{\mathrm{ac}})$ has Λ_{ac}-rank 1, and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty^{\mathrm{ac}})_{\mathrm{tors}}) = \frac{\delta_{N^+,N^-}}{c_E^2 u_K^2} \cdot \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_\infty^{\mathrm{ac}}, T_pE)}{\Lambda_{\mathrm{ac}} \cdot \mathbf{z}_\infty^\varepsilon}\right)^2,$$

where the subscript tors *denotes the Λ_{ac}-torsion submodule.*

1.2. **Statement of the main results.** As mentioned above, one of the divisibilities in Perrin-Riou's main conjecture follows from [Ber95] and [How04b]. More recently, the authors established the converse divisibility, leading to a proof of Conjecture 1.1 under mild hypotheses (see [Wan14] and [Cas17]). As for the supersingular setting, our first main result in this paper is the following result on Conjecture 1.2:

Theorem A. *Assume that:*

- *N is square-free,*
- *$N^- \neq 1$,*
- *$E[p]$ is ramified at every prime $\ell \mid N^-$.*

Then Conjecture 1.2 holds.

Similarly as in [Wan14], Theorem A yields in particular a converse to the Gross–Zagier–Kolyvagin theorem, in the same spirit as the result first obtained by Skinner [Ski14, Thm. B] for ordinary primes (*cf.* W. Zhang's result [Zha14, Thm. 1.3], still for ordinary primes). Both approaches make crucial use of Iwasawa theory, but by working with Heegner points over the

[1]Note that, by the Hasse bound, the condition $a_p = 0$ holds for all supersingular primes $p > 3$.

tower K_∞^{ac}/K, our result does *not* require any injectivity hypothesis on the localization maps at places above p:

$$\mathrm{loc}_p : \mathrm{Sel}(K, V_pE) \longrightarrow \prod_{w|p} H^1(K_w, V_pE),$$

thereby dispensing with the finiteness of the p-primary part of $Ш(E/K)$ (see [Ski14, Lem. 2.2.2]), and rather deducing it as a consequence.

Theorem B. *Under the hypotheses in Theorem A, the following implication holds:*

$$\mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}_{p^\infty}(E/K) = 1 \quad \Longrightarrow \quad \mathrm{ord}_{s=1}L(E/K, s) = 1.$$

In the course of proving Theorem A, we also obtain new cases of B.-D. Kim's doubly-signed main conjectures for elliptic curves at supersingular primes [Kim14a]. For the statement, fix a root α of $x^2 - a_p x + p = x^2 + p$, let $\beta = -\alpha$ be the other root, and denote by $\Gamma_K := \mathrm{Gal}(K_\infty/K)$ the Galois group of the unique $\mathbf{Z}_p^2$-extension of K. Building upon Haran's construction [Har87] of Mazur–Tate elements for automorphic forms on GL_2 over number fields, Loeffler introduced in [Loe14]:

- Four unbounded distributions on Γ_K:

$$L_{p,(\alpha,\alpha)}(E/K), \quad L_{p,(\alpha,\beta)}(E/K), \quad L_{p,(\beta,\alpha)}(E/K), \quad L_{p,(\beta,\beta)}(E/K), \tag{1.4}$$

  interpolating the Rankin–Selberg L-values $L(E/K, \psi, 1)$, as ψ runs over the finite order characters of Γ_K;
- Four bounded $\mathbf{Q}_p$-valued measures on Γ_K:

$$L_p^{+,+}(E/K), \quad L_p^{-,+}(E/K), \quad L_p^{+,-}(E/K), \quad L_p^{-,-}(E/K), \tag{1.5}$$

  for which one has the decomposition

$$\begin{aligned} L_{p,(\alpha,\beta)}(E/K) = {} & L_p^{+,+}(E/K) \cdot \log_{\mathfrak{p}}^{+} \log_{\overline{\mathfrak{p}}}^{+} \\ & + L_p^{-,+}(E/K) \cdot \log_{\mathfrak{p}}^{+} \log_{\overline{\mathfrak{p}}}^{-} \cdot \alpha + L_p^{+,-}(E/K) \cdot \log_{\mathfrak{p}}^{-} \log_{\overline{\mathfrak{p}}}^{+} \cdot \beta \\ & + L_p^{-,-}(E/K) \cdot \log_{\mathfrak{p}}^{-} \log_{\overline{\mathfrak{p}}}^{-} \cdot \alpha\beta, \end{aligned} \tag{1.6}$$

  and similarly for the other three distributions in (1.4), for certain elements $\log_{\mathfrak{p}}^{\pm}, \log_{\overline{\mathfrak{p}}}^{\pm} \in \mathbf{Q}_p[[\Gamma_K]]$ generalizing Pollack's [Pol03] half-logarithms.

On the arithmetic side, B.-D. Kim [Kim14a] introduced four doubly-signed Selmer groups $\mathrm{Sel}_{p^\infty}^{\pm,\pm}(E/K_\infty)$, which he conjectured to be cotorsion over the two-variable Iwasawa algebra $\Lambda_K := \mathbf{Z}_p[[\Gamma_K]]$, with characteristic ideal generated by $L_p^{\pm,\pm}(E/K)$ (*cf.* [Kim14a, Conj. 3.1]):

Conjecture 1.3 (Kim)**.** *For each $\bullet, \circ = \{\pm\}$, the Pontrjagin dual $X_{p^\infty}^{\bullet,\circ}(E/K_\infty)$ of $\mathrm{Sel}_{p^\infty}^{\bullet,\circ}(E/K_\infty)$ is Λ_K-torsion, and*

$$\mathrm{Char}_{\Lambda_K}(X_{p^\infty}^{\bullet,\circ}(E/K_\infty)) = (L_p^{\bullet,\circ}(E/K))$$

as ideals in Λ_K.

Note that Conjecture 1.3 is the combination of four different main conjectures, which no direct connection *a priori* between them. In [Wan16], the second named author has obtained (under mild hypotheses) the proof one of the divisibilities predicted by the two equal-sign cases of Conjecture 1.3 when the global root number of E/K is $+1$ (so that N^- is the product of an *odd* number of primes). In this paper, we extend this result to the cases when the global root number of E/K is -1:

Theorem C. *Under the hypotheses in Theorem A, for each $\varepsilon \in \{\pm\}$ the module $X_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty)$ is Λ_K-torsion, and*

$$\mathrm{Char}_{\Lambda_K}(X_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty)) = (L_p^{\varepsilon,\varepsilon}(E/K))$$

as ideals in Λ_K.

Finally, we note that our methods also yield a proof under mild hypotheses of the Iwasawa–Greenberg main conjecture for the p-adic L-functions of Bertolini–Darmon–Prasanna [BDP13] (see Theorem 6.1), as well as a Λ_{ac}-adic extension of Kobayashi's p-adic Gross–Zagier formula [Kob13] (see Theorem 6.6) for elliptic curves at supersingular primes $p > 3$.

1.3. **Outline of the proofs.** The proofs of our main results are via Iwasawa theory, exploiting the connections between Heegner points, Beilinson–Flach classes, and their explicit reciprocity laws. Recall that α and β denote the roots of $x^2 + p$, and let f_α and f_β be the p-stabilizations of f with U_p-eigenvalues α and β, respectively. In [LZ16], Loeffler and Zerbes have defined three-variable systems of cohomology classes $\mathcal{BF}_{\mathbf{f},\mathbf{g}}$ interpolating the Beilinson–Flach classes of [LLZ14] attached to the different specializations of two Coleman families $\mathbf{f}$ and $\mathbf{g}$ and their cyclotomic twists. Letting $\mathbf{f}$ be the Coleman family passing through f_α and f_β, respectively, and $\mathbf{g}$ be a certain Hida family of CM forms, we deduce from their work the construction of two-variable classes

$$\mathcal{BF}_\alpha,\ \mathcal{BF}_\beta \in \mathbf{Q}_p[[\Gamma_K]] \otimes_{\Lambda_K} H^1_{\mathrm{Iw}}(K_\infty, T_pE). \tag{1.7}$$

In analogy with (1.4), the classes (1.7) have unbounded growth over the tower K_∞/K, but building on the explicit reciprocity laws of [LZ16] we deduce from them the construction of two *bounded* elements $\mathcal{BF}^\pm \in H^1_{\mathrm{Iw}}(K_\infty, T_pE)$. Moreover, we construct four Λ_K-linear maps[2]

$$\mathrm{Col}^\pm : \frac{H^1_{\mathrm{Iw}}(K_{\infty,\overline{\mathfrak{p}}}, T_pE)}{H^1_{\pm,\mathrm{Iw}}(K_{\infty,\overline{\mathfrak{p}}}, T_pE)} \longrightarrow \Lambda_K, \qquad \mathrm{Log}^\pm : H^1_{\pm,\mathrm{Iw}}(K_{\infty,\mathfrak{p}}, T_pE) \longrightarrow \Lambda_K,$$

such that

$$\mathrm{Col}^\circ(\mathrm{loc}_{\overline{\mathfrak{p}}}(\mathcal{BF}^\bullet)) = L_p^{\bullet,\circ}(E/K) \tag{1.8}$$

for all $\bullet, \circ \in \{\pm\}$, and

$$\mathrm{Log}^\varepsilon(\mathrm{loc}_{\mathfrak{p}}(\mathcal{BF}^\varepsilon)) = L_{\mathfrak{p}}(E/K) \tag{1.9}$$

for all $\varepsilon \in \{\pm\}$, where $H^1_{\pm,\mathrm{Iw}}(K_{\infty,\overline{\mathfrak{p}}}, T_pE)$ is the local condition defining $\mathrm{Sel}^{\pm,\pm}(K_\infty, T_pE)$ at the places above $\overline{\mathfrak{p}}$, and similarly $H^1_{\pm,\mathrm{Iw}}(K_{\infty,\mathfrak{p}}, T_pE)$ for the places above $\mathfrak{p}$, and $L_{\mathfrak{p}}(E/K)$ is a Rankin–Selberg p-adic L-function constructed in [Wan16].

The Iwasawa–Greenberg main conjecture [Gre94] predicts that $L_{\mathfrak{p}}(E/K)$ generates the characteristic ideal of a certain torsion Selmer group:

$$\mathrm{Char}_{\Lambda_K}(\mathfrak{X}_{p^\infty}^{\mathrm{rel,str}}(E/K_\infty)) \stackrel{?}{=} (L_{\mathfrak{p}}(E/K)), \tag{1.10}$$

where $\mathfrak{X}_{p^\infty}^{\mathrm{rel,str}}(E/K_\infty)$ is the Pontrjagin dual of a Selmer group $\mathfrak{Sel}_{p^\infty}^{\mathrm{rel,str}}(f/K_\infty)$ defined by imposing local triviality (resp. no condition) at the places above $\overline{\mathfrak{p}}$ (resp. $\mathfrak{p}$). In [Wan16], the second named author has obtained one of the divisibilities in conjecture (1.10). By descending to the anticyclotomic line, we show that this leads to the divisibility

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{p^\infty}^{\mathrm{rel,str}}(E/K_\infty^{\mathrm{ac}})) \subseteq (\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(E/K)^2) \tag{1.11}$$

in the Iwasawa–Greenberg main conjecture for (the square of) the p-adic L-function of [BDP13]. On the other hand, by an extension of Howard's techniques [How04b] to the Heegner classes $\mathbf{z}^\pm$, in Section 5.4 we prove a divisibility in the opposite direction in Conjecture 1.2:

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty^{\mathrm{ac}})_{\mathrm{tors}}) \supseteq \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_\infty^{\mathrm{ac}}, T_pE)}{\Lambda_{\mathrm{ac}} \cdot \mathbf{z}_\infty^\varepsilon}\right)^2, \tag{1.12}$$

[2]The maps $\mathrm{Log}^\pm$ are in fact valued in a large scalar extension of Λ_K that we suppress here for the ease of exposition.

By the explicit reciprocity law, analogous to (1.9), that we obtain in Theorem 5.6:

$$\mathrm{Log}_{\mathrm{ac}}^{\varepsilon}(\mathrm{res}_{\mathfrak{p}}(\mathbf{z}^{\varepsilon})) = \mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(E/K)$$

we show that the divisibilities (6.4) and (1.12) complement each other, leading to the equalities in both. In particular, Theorem A follows, and using the reciprocity laws (1.8) and (1.9) we deduce from this the proof of Theorem C.

We end this Introduction with a few remarks on related results in the literature, especially in the works of Longo–Vigni [LV15] and Büyükboduk–Lei [BL16]. More precisely, one of the main results of [LV15] amounts to the "rank part" of our Conjecture 1.2. The results of [LV15] are based on an extension of Bertolini's techniques [Ber95] to supersingular primes, whereas here we deduce this portion of Theorem A from an analogous extension of Howard's [How04b] (giving us access to the Λ_{ac}-torsion submodule of $X_{p^\infty}^{\varepsilon,\varepsilon}(E/K_\infty^{\mathrm{ac}})$ as well). On the other hand, *twisted* versions of Theorem C and the rank part of Theorem A are also contained in [BL16]. Their methods share with ours that use of Beilinson–Flach classes and their explicit reciprocity laws, but they differ in a critical aspect: we only need to apply the method Euler/Kolyvagin systems to the plus/minus Heegner points $\mathbf{z}^{\pm}$ constructed in this paper, whereas in [BL16] this method is applied to a variant of the classes $\mathcal{BF}^{\pm}$. As a consequence, when specialized to the setting considered here, the main results in [BL16] are for the twists of E by "p-distinguished" characters, whereas such twists can be avoided here.

Acknowledgements. A substantial part of this paper was written while the first named author visited the Morningside Center of Mathematics during March 2016, and he would like to thank Professor Ye Tian and the Chinese Academy of Sciences for their hospitality and support. We would also like to thank the anonymous referees for a very careful reading of a previous version of the paper, which greatly helped us to improve the exposition of our results.

2. p-adic L-functions

Throughout this section, we let $f = \sum_{n=1}^{\infty} a_n(f)q^n \in S_2(\Gamma_0(N_f))$ be a newform of level N_f, and K be an imaginary quadratic field of discriminant $-D_K < 0$ prime to N_f. Fix a prime $p \nmid 6N_fD_K$ and a choice of complex and p-adic embeddings $\mathbf{C} \overset{\iota_\infty}{\hookleftarrow} \overline{\mathbf{Q}} \overset{\iota_p}{\hookrightarrow} \mathbf{C}_p$; since it will suffice for our applications in this paper, we also assume that the image under ι_p of the number field generated by the Fourier coefficients $a_n(f)$ is contained in $\mathbf{Q}_p$.

2.1. p-adic Rankin–Selberg L-functions.

Let Ξ_K denote the set of algebraic Hecke characters $\psi : K^\times\backslash\mathbb{A}_K^\times \to \mathbf{C}^\times$. We say that $\psi \in \Xi_K$ has infinity type $(\ell_1, \ell_2) \in \mathbf{Z}^2$ if

$$\psi_\infty(z) = z^{\ell_1}\overline{z}^{\ell_2},$$

where for each place v of K, we let $\psi_v : K_v^\times \to \mathbf{C}^\times$ be the v-component of ψ. The conductor of ψ is the largest ideal $\mathfrak{c}_\psi \subset \mathcal{O}_K$ such that $\psi_{\mathfrak{q}}(u) = 1$ for all $u \in (1 + \mathfrak{c}_\psi\mathcal{O}_{K,\mathfrak{q}})^\times \subset K_{\mathfrak{q}}^\times$. If ψ has conductor $\mathfrak{c}_\psi$ and $\mathfrak{a}$ is any fractional ideal of K prime to $\mathfrak{c}_\psi$, we write $\psi(\mathfrak{a})$ for $\psi(a)$, where a is an idele satisfying $a\hat{\mathcal{O}}_K \cap K = \mathfrak{a}$ and such that $a_{\mathfrak{q}} = 1$ for all $\mathfrak{q} \mid \mathfrak{c}_\psi$. As a function on fractional ideals, then ψ satisfies

$$\psi((\alpha)) = \alpha^{-\ell_1}\overline{\alpha}^{-\ell_2}$$

for all $\alpha \in K^\times$ with $\alpha \equiv 1 \pmod{\mathfrak{c}_\psi}$.

We say that a Hecke character ψ of infinity type (ℓ_1, ℓ_2) is *critical for* f if $s = 1$ is a critical value in the sense of Deligne for

$$L(f/K, \psi, s) = L\left(\pi_f \times \pi_\psi, s + \frac{\ell_1 + \ell_2 - 1}{2}\right),$$

where $L(\pi_f \times \pi_\psi, s)$ is the L-function for the Rankin–Selberg convolution of the cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A})$ associated with f and the theta series of ψ, respectively. The set of infinity types of critical characters can be written as the disjoint union

$$\Sigma = \Sigma^- \sqcup \Sigma^+ \sqcup \Sigma^{+'},$$

with $\Sigma^- = \{(0,0)\}$, $\Sigma^+ = \{(\ell_1,\ell_2)\colon \ell_1 \leqslant -1, \ell_2 \geqslant 1\}$, $\Sigma^{+'} = \{(\ell_1,\ell_2)\colon \ell_2 \leqslant -1, \ell_1 \geqslant 1\}$.

The involution $\psi \mapsto \psi^\rho$ on Ξ_K, where ψ^ρ is obtained by composing ψ with the complex conjugation on $\mathbb{A}_K^\times$, has the effect on infinity types of interchanging the regions Σ^+ and $\Sigma^{+'}$ (while leaving Σ^- stable). Since the values $L(f/K,\psi,1)$ and $L(f/K,\psi^\rho,1)$ are the same, for the purposes of p-adic interpolation we may restrict our attention to the first two subsets in the above decomposition of Σ.

Definition 2.1. Let $\psi = \psi^\infty\psi_\infty \in \Xi_K$ be an algebraic Hecke character of infinity type (ℓ_1,ℓ_2). The *p-adic avatar* $\hat\psi : K^\times\backslash\hat K^\times \to \mathbf{C}_p^\times$ of ψ is defined by

$$\hat\psi(z) = \imath_p\imath_\infty^{-1}(\psi^\infty(z))z_{\mathfrak{p}}^{\ell_1}z_{\overline{\mathfrak{p}}}^{\ell_2}.$$

For each ideal $\mathfrak{m} \subset \mathcal{O}_K$ let $H_{\mathfrak{m}} = \mathrm{Gal}(K(\mathfrak{m})/K)$ be the ray class group of K modulo $\mathfrak{m}$, and set $H_{p^\infty} = \varprojlim_r H_{p^r}$. Via the Artin reciprocity map, the correspondence $\psi \mapsto \hat\psi$ establishes a bijection between the set of algebraic Hecke characters of K of conductor dividing p^∞ and the set of locally algebraic $\overline{\mathbf{Q}}_p$-valued characters of H_{p^∞}.

Following the terminology in [Loe14, §2.3], for any $r,s \in \mathbf{R}_{\geqslant 0}$ we let $D^{(r,s)}(H_{p^\infty})$ be the space of $\mathbf{Q}_p$-valued distributions on H_{p^∞} of order (r,s) with respect to the quasi-factorization of H_{p^∞} induced by the ray class groups $H_{\mathfrak{p}^\infty}$ and $H_{\overline{\mathfrak{p}}^\infty}$ (see [*loc.cit.*, Prop. 4]).

On the other hand, let

$$\Omega_f^{\mathtt{Hida}} := \frac{8\pi^2\langle f,f\rangle}{c_f} \in \overline{\mathbf{Q}}_p^\times \tag{2.1}$$

be Hida's canonical period, where

$$\langle f,f\rangle = \int_{\Gamma_0(N)\backslash\mathfrak{H}} |f(z)|^2 dxdy$$

is the Petersson norm of f, and c_f is the congruence number of f (*cf.* [SZ14, §9.3], where c_f is denoted by $\eta_f(N)$).

Theorem 2.2. *Assume that $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K, let α and β be the roots of $x^2 - a_p(f)x + p$, and set $r := v_p(\alpha)$ and $s := v_p(\beta)$.*

(i) *There exists an element $L_p(f/K,\Sigma^+) \in \mathrm{Frac}(\mathbf{Z}_p[[H_{p^\infty}]] \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$ such that for every $\psi \in \Xi_K$ of trivial conductor and infinity type $(\ell_1,\ell_2) \in \Sigma^+$, we have*

$$L_p(f/K,\Sigma^+)(\hat\psi) = \frac{\Gamma(\ell_2)\Gamma(\ell_2+1)\cdot\mathcal{E}(f,\psi)}{(1-\psi^{1-\rho}(\mathfrak{p}))(1-p^{-1}\psi^{1-\rho}(\mathfrak{p}))} \cdot \frac{L(f/K,\psi,1)}{(2\pi)^{2\ell_2+1}\cdot\langle\theta_{\psi_{\ell_2}},\theta_{\psi_{\ell_2}}\rangle},$$

where $\theta_{\psi_{\ell_2}}$ is the theta series of weight $\ell_2-\ell_1+1 \geqslant 3$ associated to the Hecke character $\psi_{\ell_2} := \psi\mathbf{N}_K^{\ell_2}$ of infinity type $(\ell_1-\ell_2,0)$, and

$$\mathcal{E}(f,\psi) = (1-p^{-1}\psi(\mathfrak{p})\alpha)(1-p^{-1}\psi(\mathfrak{p})\beta)(1-\psi^{-1}(\overline{\mathfrak{p}})\alpha^{-1})(1-\psi^{-1}(\overline{\mathfrak{p}})\beta^{-1}).$$

(ii) *If $r<1$ and $s<1$, then for each $\underline{\alpha} := (\alpha_{\mathfrak{p}},\alpha_{\overline{\mathfrak{p}}}) \in \{(\alpha,\alpha),(\alpha,\beta),(\beta,\alpha),(\beta,\beta)\}$ there exists an element $L_{p,\underline{\alpha}}(f/K,\Sigma^-) \in D^{(r,s)}(H_{p^\infty})$ such that for every finite order character $\psi \in \Xi_K$ of conductor $\mathfrak{c}_\psi \mid p^\infty$, we have*

$$L_{p,\underline{\alpha}}(f/K,\Sigma^-)(\hat\psi) = \left(\prod_{\mathfrak{q}\mid p}\alpha_{\mathfrak{q}}^{-v_{\mathfrak{q}}(\mathfrak{c}_\psi)}\right)\cdot\frac{\mathcal{E}(\psi,f)}{\mathfrak{g}(\psi)\cdot|\mathfrak{c}_\psi|}\cdot\frac{L(f/K,\psi,1)}{\Omega_f^{\mathtt{Hida}}},$$

where

$$\mathcal{E}(\psi, f) = \prod_{\mathfrak{q}|p,\ \mathfrak{q}\nmid \mathfrak{c}_\psi} (1-\alpha_{\mathfrak{q}}^{-1}\psi(\mathfrak{q}))(1-\alpha_{\mathfrak{q}}^{-1}\psi^{-1}(\mathfrak{q})).$$

Proof. The first part is a reformulation of [LLZ15, Thm. 6.1.3(i)], and the second follows from [Loe14, Thm. 9] and [*loc. cit.*, Prop. 7]. (See also Remark 2.4 below.) □

2.2. **The two-variable plus/minus p-adic L-functions.** Let $\Phi_n(X) = \sum_{i=0}^{p-1} X^{p^{n-1}i}$ be the p^n-th cyclotomic polynomial. Fix a topological generator $\gamma_v \in H_{v^\infty}$ for each prime $v \mid p$, and define the 'half-logarithms'

$$\log_v^+ := \frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m}(\gamma_v)}{p}, \qquad \log_v^- := \frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m-1}(\gamma_v)}{p}.$$

These are elements in $D^{1/2}(H_{v^\infty})$ which will be seen in $D^{(1/2,1/2)}(H_{p^\infty})$ via pullback.

Theorem 2.3. *Assume that $a_p(f) = 0$. Then there exist four bounded $\mathbf{Q}_p$-valued distributions on H_{p^∞}:*

$$L_p^{+,+}(f/K),\ L_p^{-,+}(f/K),\ L_p^{+,-}(f/K),\ L_p^{-,-}(f/K)$$

such that for every $\underline{\alpha} = (\alpha_{\mathfrak{p}}, \alpha_{\overline{\mathfrak{p}}})$ as in Theorem 2.2 we have

$$\begin{aligned} L_{p,\underline{\alpha}}(f/K,\Sigma^-) &= L_p^{+,+}(f/K)\cdot \log_{\mathfrak{p}}^+ \log_{\overline{\mathfrak{p}}}^+ \\ &\quad + L_p^{-,+}(f/K)\cdot \log_{\mathfrak{p}}^- \log_{\overline{\mathfrak{p}}}^+ \cdot\alpha_{\mathfrak{p}} + L_p^{+,-}(f/K)\cdot \log_{\mathfrak{p}}^+ \log_{\overline{\mathfrak{p}}}^- \cdot\alpha_{\overline{\mathfrak{p}}} \\ &\quad + L_p^{-,-}(f/K)\cdot \log_{\mathfrak{p}}^- \log_{\overline{\mathfrak{p}}}^- \cdot\alpha_{\mathfrak{p}}\alpha_{\overline{\mathfrak{p}}}. \end{aligned}$$

Moreover, if ϕ is a finite order character of H_{p^∞} of conductor $\mathfrak{p}^{n_{\mathfrak{p}}}\overline{\mathfrak{p}}^{n_{\overline{\mathfrak{p}}}}$ with $n_{\mathfrak{p}}, n_{\overline{\mathfrak{p}}} > 0$, then $L_p^{\bullet,\circ}(f/K)$ vanishes at ϕ unless $\bullet = (-1)^{n_{\mathfrak{p}}}$ and $\circ = (-1)^{n_{\overline{\mathfrak{p}}}}$.

Proof. This is shown in [Loe14, §5]. For our later use, we record the construction of the four $L_p^{*,\circ}(f/K)$ as an explicit linear combination of the four $L_{p,\underline{\alpha}} := L_{p,\underline{\alpha}}(f/K,\Sigma^-)$. Fix a root α of the Hecke polynomial $x^2 - a_p(f)x + p = x^2 + p$, and let β be the other root. Then:

$$\begin{aligned} L_p^{+,+}(f/K) &= \frac{L_{p,(\alpha,\alpha)} + L_{p,(\beta,\alpha)} + L_{p,(\alpha,\beta)} + L_{p,(\beta,\beta)}}{4\log_{\mathfrak{p}}^+ \log_{\overline{\mathfrak{p}}}^+}, \\ L_p^{-,+}(f/K) &= \frac{L_{p,(\alpha,\alpha)} - L_{p,(\beta,\alpha)} + L_{p,(\alpha,\beta)} - L_{p,(\beta,\beta)}}{4\log_{\mathfrak{p}}^- \log_{\overline{\mathfrak{p}}}^+ \cdot\alpha}, \\ L_p^{+,-}(f/K) &= \frac{L_{p,(\alpha,\alpha)} + L_{p,(\beta,\alpha)} - L_{p,(\alpha,\beta)} - L_{p,(\beta,\beta)}}{4\log_{\mathfrak{p}}^+ \log_{\overline{\mathfrak{p}}}^- \cdot\alpha}, \\ L_p^{-,-}(f/K) &= \frac{L_{p,(\alpha,\alpha)} - L_{p,(\beta,\alpha)} - L_{p,(\alpha,\beta)} + L_{p,(\beta,\beta)}}{4\log_{\mathfrak{p}}^- \log_{\overline{\mathfrak{p}}}^- \cdot\alpha^2}. \end{aligned}$$

Using the relation $\beta = -\alpha$, it is immediate to check that the four identities (2.2) hold. □

Remark 2.4. In their original construction in [Loe14], the p-adic L-functions $L_{p,\underline{\alpha}}(f/K,\Sigma^-)$ are normalized with a period Ω_Π attached to the base change to K of the cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ associated with f. However, it is easy to see that Loeffler's Ω_Π agrees with our $\Omega_f^{\mathtt{Hida}}$ up to a nonzero factor in $\mathbf{Q}^\times$, and so the conclusion of Theorem 2.3 also holds for our periods. Moreover, under mild hypotheses one can show that with our normalizations the elements $L_p^{\bullet,\circ}(f/K)$ are in fact integral (see Corollary 6.3).

2.3. **Anticyclotomic p-adic L-functions.** Write

$$N_f = N^+N^-$$

with N^+ (resp. N^-) only divisible by primes which split (resp. remain inert) in K. Similarly as in the Introduction, we say that the pair (f, K) satisfies the *generalized Heegner hypothesis* if

(Heeg) N^- is the square-free product of an even number of primes.

Let K_∞/K be the $\mathbf{Z}_p^2$-extension of K, and set $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. We may decompose

$$H_{p^\infty} \simeq \Delta \times \Gamma_K$$

with Δ a finite group. The Galois group $\mathrm{Gal}(K/\mathbf{Q})$ acts on Γ_K by conjugation. Let $\Gamma^{\mathrm{cyc}} \subseteq \Gamma_K$ be the fixed part by this action, and set $\Gamma^{\mathrm{ac}} := \Gamma_K/\Gamma^{\mathrm{cyc}}$. Then $\Gamma^{\mathrm{ac}} \simeq \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)$ is the Galois group of the *anticyclotomic* $\mathbf{Z}_p$-extension of K, on which we have $\tau\sigma\tau^{-1} = \sigma^{-1}$ for the non-trivial element $\tau \in \mathrm{Gal}(K/\mathbf{Q})$. Similarly, we say that a character ψ of G_K is *anticyclotomic* if $\psi(\tau\sigma\tau^{-1}) = \psi^{-1}(\sigma)$ for all σ, i.e., $\psi^\rho = \psi^{-1}$.

Let $L_{p,\underline{\alpha}}^{\mathrm{ac}}(f/K)$ be the image of the p-adic L-function $L_{p,\underline{\alpha}}(f/K, \Sigma^-)$ of Theorem 2.2 under the natural projection $D^{(r,s)}(H_{p^\infty}) \to D^{(r,s)}(\Gamma^{\mathrm{ac}})$.

Proposition 2.5. *If* (Heeg) *holds, then* $L_{p,(\alpha,\alpha)}^{\mathrm{ac}}(f/K)$ *and* $L_{p,(\beta,\beta)}^{\mathrm{ac}}(f/K)$ *are identically zero.*

Proof. Via Rankin–Selberg convolution techniques, B.-D. Kim has constructed in [Kim14b] p-adic L-functions $\mathcal{L}_{p,(\alpha,\alpha)}(f/K)$ and $\mathcal{L}_{p,(\beta,\beta)}(f/K)$ which are easily seen to be nonzero constant multiples of Loeffler's $L_{p,(\alpha,\alpha)}(f/K, \Sigma^-)$ and $L_{p,(\beta,\beta)}(f/K, \Sigma^-)$, respectively (see the remarks in [Loe14, p. 378]). Via the usual identifications $\mathbf{Q}_p[[H_{\mathfrak{p}^\infty}]] \simeq \mathbf{Q}_p[[X]]$ and $\mathbf{Q}_p[[H_{\overline{\mathfrak{p}}^\infty}]] \simeq \mathbf{Q}_p[[Y]]$ sending $\gamma_{\mathfrak{p}} \mapsto 1 + X$ and $\gamma_{\overline{\mathfrak{p}}} \mapsto 1 + Y$, we may view these p-adic L-functions as two-variable power series in the variables X and Y. Let ε_K denote the quadratic character associated with K by class field theory. The same argument as in [PR87b, Thm. 1.1] and [Dis15, §4.2], then shows that $\mathcal{L}_{p,(\alpha,\alpha)}(f/K)$ (and hence also $L_{p,(\alpha,\alpha)}(f/K, \Sigma^-)$) satisfies the functional equation

$$\mathcal{L}_{p,(\alpha,\alpha)}(f/K)\left(\frac{1}{1+Y} - 1, \frac{1}{1+X} - 1\right) = \epsilon\mathcal{L}_{p,(\alpha,\alpha)}(f/K)(X, Y), \tag{2.2}$$

where $\epsilon = -\varepsilon_K(N)$, and similarly for $\mathcal{L}_{p,(\beta,\beta)}(f/K)$. Since the change of variables $(X, Y) \mapsto (\frac{1}{1+Y}-1, \frac{1}{1+X}-1)$ corresponds to the transformation $\phi \mapsto \phi^{-\rho}$ on characters of H_{p^∞}, this shows that under the generalized Heegner hypothesis (which implies $\epsilon = -1$) both $L_{p,(\alpha,\alpha)}(f/K, \Sigma^-)$ and $L_{p,(\beta,\beta)}(f/K, \Sigma^-)$ vanish at all anticyclotomic characters of H_{p^∞}, whence the result. □

Throughout the following, we shall identify the space of bounded $\mathbf{Q}_p$-valued measures on a compact p-adic Lie group G with the Iwasawa algebra $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[G]]$. Viewing the measures $L_p^{\bullet,\circ}(f/K)$ of Theorem 2.3 as elements in $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[H_{p^\infty}]]$, we thus denote by $L_{p,\mathrm{ac}}^{\bullet,\circ}(f/K)$ their images under the natural projection $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[H_{p^\infty}]] \to \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]]$.

Corollary 2.6. *Assume that* $a_p(f) = 0$. *If* (Heeg) *holds, then* $L_{p,\mathrm{ac}}^{\varepsilon,\varepsilon}(f/K)$ *is identically zero for all* $\varepsilon \in \{+, -\}$.

Proof. As in [Pol03, Thm. 5.13], the idea is to use the decomposition in Proposition 2.3 to deduce from the functional equation for $L_{p,\underline{\alpha}}(f/K, \Sigma^-)$ a similar one for $L_p^{\varepsilon,\varepsilon}(f/K)$ forcing the vanishing of $L_{p,\mathrm{ac}}^{\varepsilon,\varepsilon}(f/K)$ under our generalized Heegner hypothesis.

Indeed, writing the functional equation (2.2) for $L_{p,(\alpha,\alpha)}(f/K,\Sigma^-)$ in terms of the signed p-adic L-functions $L_p^{\bullet,\circ} := L_p^{\bullet,\circ}(f/K)$ we obtain

$$\begin{aligned}
&\log_{\mathfrak{p}}^+\log_{\overline{\mathfrak{p}}}^+\cdot\left(L_p^{+,+}(X,Y)-\epsilon L_p^{+,+}\left(\frac{1}{1+Y}-1,\frac{1}{1+X}-1\right)\right)\\
&+\log_{\mathfrak{p}}^-\log_{\overline{\mathfrak{p}}}^-\left(L_p^{-,-}(X,Y)-\epsilon L_p^{-,-}\left(\frac{1}{1+Y}-1,\frac{1}{1+X}-1\right)\right)\cdot\alpha^2\\
=&\log_{\mathfrak{p}}^+\log_{\overline{\mathfrak{p}}}^-\left(-L_p^{+,-}(X,Y)+\epsilon L_p^{+,-}\left(\frac{1}{1+Y}-1,\frac{1}{1+X}-1\right)\right)\cdot\alpha\\
&+\log_{\mathfrak{p}}^-\log_{\overline{\mathfrak{p}}}^+\left(-L_p^{-,+}(X,Y)+\epsilon L_p^{-,+}\left(\frac{1}{1+Y}-1,\frac{1}{1+X}-1\right)\right)\cdot\alpha,
\end{aligned}\tag{2.3}$$

where $\epsilon=-\varepsilon_K(N)$. Since $\mathrm{ord}_p(\alpha)=1/2$, the nonzero coefficients in the left-hand side of this equality have coefficients with p-adic valuations in $\mathbf{Z}$, whereas the nonzero coefficients in the right-hand side have p-adic valuations in $\frac{1}{2}\mathbf{Z}\smallsetminus\mathbf{Z}$. This forces both sides to be identically zero, and so we obtain

$$L_p^{+,+}(f/K)\left(\frac{1}{1+Y}-1,\frac{1}{1+X}-1\right)=\epsilon L_p^{+,+}(f/K)(X,Y),$$

and similarly for $L_p^{-,-}(f/K)$. Since (Heeg) implies that $\epsilon=-1$, this shows that $L_{p,\mathrm{ac}}^{+,+}(f/K)$ and $L_{p,\mathrm{ac}}^{-,-}(f/K)$ are then identically zero, as was to be shown. □

The following anticyclotomic p-adic L-function will play a key role in this paper. Let R_0 denote the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$.

Theorem 2.7. *Assume hypothesis* (Heeg) *and that $p=\mathfrak{p}\overline{\mathfrak{p}}$ splits in K. Then there exists a p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)\in R_0[[\Gamma^{\mathrm{ac}}]]$ such that if $\hat{\psi}:\Gamma^{\mathrm{ac}}\to\mathbf{C}_p^\times$ has trivial conductor and infinity type $(-\ell,\ell)$ with $\ell\geqslant 1$, then*

$$\left(\frac{\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)(\hat{\psi})}{\Omega_p^{2\ell}}\right)^2=\Gamma(\ell)\Gamma(\ell+1)\cdot(1-p^{-1}\psi(\mathfrak{p})\alpha)^2(1-p^{-1}\psi(\mathfrak{p})\beta)^2\cdot\frac{L(f/K,\psi,1)}{\pi^{2\ell+1}\cdot\Omega_K^{4\ell}},$$

where $\Omega_p\in R_0^\times$ and $\Omega_K\in\mathbf{C}^\times$ are CM periods attached to K.

Proof. This follows from the results in [CH17, §3.3]. (See the proof of Theorem 5.6 below for the precise relation between the construction in *loc. cit.* and the above $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$.) □

We next recall some of the nontriviality properties one knows about $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$, which we will also need. Let $\rho_f:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to\mathrm{Aut}_{\mathbf{Q}_p}(V_f)\simeq\mathrm{GL}_2(\mathbf{Q}_p)$ be the p-adic Galois representation attached to f, and let $\overline{\rho}_f$ denote its associated semi-simple mod p representation.

Theorem 2.8. *In addition to the hypotheses in Theorem 2.7, assume that:*

- *$\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbf{Q}}/K)}$ is absolutely irreducible,*
- *$\overline{\rho}_f$ is ramified at every prime $\ell\mid N^-$.*

Then $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ is not identically zero, and it has trivial μ-invariant.

Proof. The nonvanishing of $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ follows from [CH17, Thm. 3.7], where it is deduced from [Hsi14, Thm. C]. The vanishing of $\mu(\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K))$ similarly follows from [Hsi14, Thm. B] (or alternatively, from [Bur17, Thm. B] in the cases where the number of prime factors in N^- is positive, noting that by the discussion in [Pra06, p. 912] our last assumption guarantees that the term $\alpha(f,f_B)$ in [Bur17, Thm. 5.6] is a p-adic unit). □

Letting $L_{p,\mathrm{ac}}(f/K)$ be the image of the p-adic L-function $L_p(f/K,\Sigma^+)$ of Theorem 2.2 under the natural map induced by the natural projection $H_{p^\infty}\to\Gamma^{\mathrm{ac}}$, we see that $L_{p,\mathrm{ac}}(f/K)$ and *the square* of the p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ are defined by the interpolation of the same L-values. However, the archimedean periods used in their construction are different, and so these p-adic L-functions need not be equal (even up to units in the Iwasawa algebra). In fact, as shown in Theorem 2.10 below, the ratio between these different periods is interpolated by an anticyclotomic projection of a Katz p-adic L-function.[3]

Before we state the defining property of the Katz p-adic L-function, recall that the Hecke L-function of $\psi\in\Xi_K$ is defined by (the analytic continuation of) the Euler product

$$L(\psi,s)=\prod_{\mathfrak{l}}\left(1-\frac{\psi(\mathfrak{l})}{N(\mathfrak{l})^s}\right)^{-1},$$

where $\mathfrak{l}$ runs over all prime ideals of K, with the convention that $\psi(\mathfrak{l})=0$ for $\mathfrak{l}\mid\mathfrak{c}_\psi$. The set of infinity types of $\psi\in\Xi_K$ for which $s=0$ is a critical value of $L(\psi,s)$ can be written as the disjoint union $\Sigma_K\sqcup\Sigma_K'$, where $\Sigma_K=\{(\ell_1,\ell_2):\ell_2\leqslant 0<\ell_1\}$ and $\Sigma_K'=\{(\ell_1,\ell_2):\ell_1\leqslant 0<\ell_2\}$.

Theorem 2.9. *Assume that $p=\mathfrak{p}\overline{\mathfrak{p}}$ splits in K. Then there is a p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)\in R_0[[H_{p^\infty}]]$ such that if $\psi\in\Xi_K$ has trivial conductor and infinity type $(\ell_1,\ell_2)\in\Sigma_K$, then*

$$\frac{\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)(\hat{\psi})}{\Omega_p^{\ell_1-\ell_2}}=\left(\frac{\sqrt{D_K}}{2\pi}\right)^{\ell_2}\cdot\Gamma(\ell_1)\cdot(1-\psi(\overline{\mathfrak{p}}))(1-p^{-1}\psi^{-1}(\mathfrak{p}))\cdot\frac{L(\psi,0)}{\Omega_K^{\ell_1-\ell_2}},$$

where Ω_p and Ω_K are as in Theorem 2.7.

Proof. See [Kat78, §5.3.0], or [dS87, Thm. II.4.14]. □

Denote by $\mathscr{L}_{\mathfrak{p},\mathrm{ac}}^{\mathtt{Katz}}(K)$ the image of $\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)$ under the projection $R_0[[H_{p^\infty}]]\to R_0[[\Gamma^{\mathrm{ac}}]]$.

Theorem 2.10. *Assume hypothesis* (Heeg) *and that $p=\mathfrak{p}\overline{\mathfrak{p}}$ splits in K. Then*

$$L_{p,\mathrm{ac}}(f/K)(\hat{\psi})=\frac{w_K}{h_K}\cdot\frac{\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2(\hat{\psi})}{\mathscr{L}_{\mathfrak{p},\mathrm{ac}}^{\mathtt{Katz}}(K)(\hat{\psi}^{\rho-1})}$$

up to a unit in $\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]]^\times$, where $w_K=|\mathcal{O}_K^\times|$ and h_K is the class number of K.

Proof. This is [Cas17, Thm. 1.7], whose proof does not make use of the underlying ordinarity hypothesis on f made in *loc.cit.*. See also [JSW17, §5.3] for a similar calculation. □

2.4. **Another p-adic Rankin–Selberg L-function.** Recall the decomposition $H_{p^\infty}\simeq\Delta\times\Gamma_K$, set $\Lambda:=\mathbf{Z}_p[[\Gamma_K]]$, $\Lambda_{R_0}:=R_0[[\Gamma_K]]$, and $\Lambda_{\mathrm{ac}}:=\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]]$, and continue to denote by

$$L_p(f/K,\Sigma^+)\in\mathrm{Frac}(\Lambda\otimes_{\mathbf{Z}_p}\mathbf{Q}_p)\qquad\text{and}\qquad\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)\in\Lambda_{R_0}$$

the natural projections of the p-adic L-functions $L_p(f/K,\Sigma^+)$ and $\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)$ of Theorem 2.2 and Theorem 2.9, respectively.

Theorem 2.11. *Assume that $p=\mathfrak{p}\overline{\mathfrak{p}}$ splits in K. There exists a p-adic L-function*

$$L_{\mathfrak{p}}(f/K)\in\Lambda_{R_0}$$

such that if $\hat{\psi}:\Gamma\to\mathbf{C}_p^\times$ has trivial conductor and infinity type $(\ell_1,\ell_2)\in\Sigma^+$, then

$$L_{\mathfrak{p}}(f/K)(\hat{\psi})=\frac{\Gamma(\ell_2)\Gamma(\ell_2+1)}{\pi^{2\ell_2+1}}\cdot\mathcal{E}(f,\psi)\cdot\frac{\Omega_p^{2(\ell_2-\ell_1)}}{\Omega_K^{2(\ell_2-\ell_1)}}\cdot L(f/K,\psi,1),$$

[3]This phenomenon appears to have been first observed by Hida–Tilouine [HT93, §8] in a slightly different context; see also [DLR15, §3.2].

where $\mathcal{E}(f,\psi) = (1-p^{-1}\psi(\mathfrak{p})\alpha)(1-p^{-1}\psi(\mathfrak{p})\beta)(1-\psi^{-1}(\overline{\mathfrak{p}})\alpha^{-1})(1-\psi^{-1}(\overline{\mathfrak{p}})\beta^{-1})$, *and* Ω_K *and* Ω_p *are as in Theorem 2.7. Moreover,* $L_{\mathfrak{p}}(f/K)$ *differs from the product*

$$\widetilde{L}_{\mathfrak{p}}(f/K)(\hat{\psi}) := L_p(f/K,\Sigma^+)(\hat{\psi})\cdot\frac{h_K}{w_K}\cdot\mathscr{L}_{\mathfrak{p},\mathrm{ac}}^{\mathtt{Katz}}(K)(\hat{\psi}^{\rho-1}) \tag{2.4}$$

by a unit in $\Lambda^\times$, *and it is not identically zero.*

Proof. The construction of $L_{\mathfrak{p}}(f/K)$ is given in [Wan16, §4.6]. On the other hand, the fact that the product (2.4) has the claimed interpolation property follows by a straightforward adaptation of the calculations in [Cas17, Thm. 1.7] (or [JSW17, §5.3]). Finally, the fact that $L_{\mathfrak{p}}(f/K)$ is not the zero function follows from the fact that for some of the characters ψ in the range of p-adic interpolation, the Euler product defining $L(f/K,\psi,s)$ converges at $s=1$. □

Corollary 2.12. *Assume hypothesis* (Heeg) *and that* $p=\mathfrak{p}\overline{\mathfrak{p}}$ *splits in* K, *and let* $L_{\mathfrak{p},\mathrm{ac}}(f/K)$ *be the image of the* p*-adic* L*-function* $L_{\mathfrak{p}}(f/K)$ *of Theorem 2.11 under the projection* $\Lambda_{R_0}\to\Lambda_{R_0}^{\mathrm{ac}}$. *Then*

$$L_{\mathfrak{p},\mathrm{ac}}(f/K) = \mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2$$

up to a unit in $\Lambda_{\mathrm{ac}}^\times$, *where* $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ *is as in Theorem 2.7.*

Proof. This follows from a direct comparison of their interpolation properties. □

3. Selmer groups

3.1. **Local conditions at** p**.** In this section, we develop some local results for studying the anticyclotomic Iwasawa theory for elliptic curves at supersingular primes. Throughout, we let $E/\mathbf{Q}$ be an elliptic curve of conductor N, $p>3$ be a prime of good supersingular reduction for E, and $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant prime to N and such that

$$p=\mathfrak{p}\overline{\mathfrak{p}} \quad \text{splits in } K.$$

We keep the notations introduced in Section 2; in particular, we have $a_p(f)=0$, and K_∞^{ac}/K denotes the anticyclotomic $\mathbf{Z}_p$-extension of K.

It is easy to see that every prime $v\mid p$ is finitely decomposed in K_∞^{ac}/K, say as the product $v_1v_2\cdots v_{p^t}$; then v is also decomposed into p^t distinct primes in K_∞/K. Let Γ_1 (resp. Γ_1^{ac}) be the decomposition group of v_1 in Γ (resp. Γ^{ac}). Let H_K be the Hilbert class field of K, set $K_0^{\mathrm{ac}}:=K_\infty^{\mathrm{ac}}\cap H_K$, and let K_m^{ac} be the unique subfield of K_∞^{ac} with $[K_m^{\mathrm{ac}}:K_0^{\mathrm{ac}}]=p^m$. Let a be the inertial degree of K_0^{ac}/K at any $v\mid p$.

We denote by $\mathbf{Q}_p^{\mathrm{ur}}$ and $\mathbf{Q}_{p,\infty}$ the unramified and the cyclotomic $\mathbf{Z}_p$-extensions of $\mathbf{Q}_p$, respectively, and let $\mathbf{Q}_{p,\infty}^{\mathrm{ur}}$ denote their composition. For $v\mid p$, we identify $K_v\simeq\mathbf{Q}_p$. Let u_v and γ_v be topological generators of $U_v:=\mathrm{Gal}(\mathbf{Q}_{p,\infty}^{\mathrm{ur}}/\mathbf{Q}_{p,\infty})$ and $\Gamma_v:=\mathrm{Gal}(\mathbf{Q}_{p,\infty}^{\mathrm{ur}}/\mathbf{Q}_p^{\mathrm{ur}})$; these are chosen so that u_v is the arithmetic Frobenius and (using additive notation) $-p^a u_v+\gamma_v$ is a topological generator of $\mathrm{Gal}(K_{\infty,v}/K_{\infty,v}^{\mathrm{ac}})$. Let $X_v=\gamma_v-1$ and $Y_v=u_v-1$. Finally, let $\gamma_{\mathrm{ac}}\in\Gamma^{\mathrm{ac}}$ be a topological generator, so that $\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]]\simeq\mathbf{Z}_p[[T]]$ via $\gamma_{\mathrm{ac}}\mapsto T+1$.

Following [Kob03] (see also [Kim14a, §2.1]), for any unramified extension k of $\mathbf{Q}_p$ we define the subgroups $E^\pm(k(\mu_{p^{n+1}}))$ of $E(k(\mu_{p^{n+1}}))$ by

$$E^+(k(\mu_{p^{n+1}})) := \left\{P\in E(k(\mu_{p^{n+1}}))\;\middle|\;\mathrm{tr}_{k(\mu_{p^{\ell+2}})}^{k(\mu_{p^{n+1}})}(P)\in E(k(\mu_{p^{\ell+1}}))\text{ for }0\leqslant\ell<n,\text{ even }\ell\right\},$$

$$E^-(k(\mu_{p^{n+1}})) := \left\{P\in E(k(\mu_{p^{n+1}}))\;\middle|\;\mathrm{tr}_{k(\mu_{p^{\ell+2}})}^{k(\mu_{p^{n+1}})}(P)\in E(k(\mu_{p^{\ell+1}}))\text{ for }-1\leqslant\ell<n,\text{ odd }\ell\right\}.$$

Letting $\hat{E}$ denote the formal group associated to the minimal model of E over $\mathbf{Z}_p$, we may similarly define the subgroups $\hat{E}^\pm(\mathfrak{m}_{k(\mu_{p^{n+1}})})$ of $\hat{E}(\mathfrak{m}_{k(\mu_{p^{n+1}})})$, and using that $a_p:=a_p(f)=0$

one easily checks that

$$E^{\pm}(k(\mu_{p^{n+1}}))\otimes \mathbf{Q}_p/\mathbf{Z}_p = \hat{E}^{\pm}(\mathfrak{m}_{k(\mu_{p^{n+1}})})\otimes \mathbf{Q}_p/\mathbf{Z}_p.$$

Fix a compatible system $\{\zeta_{p^n}\}_{n\geqslant 0}$ of primitive p^n-th roots of unity ζ_{p^n} (i.e., $\zeta_{p^{n+1}}^p=\zeta_{p^n}$ for n and $\zeta_p\neq 1$). Let φ be the Frobenius on $k/\mathbf{Q}_p$, and for any polynomial $f\in k[X]$ set

$$\log_f(X)=\sum_{n=0}^{\infty}(-1)^n\frac{f^{(2n)}(X)}{p^n},$$

where $f^{(2n)}(X)=f^{\varphi^{2n-1}}\circ\cdots\circ f^{\varphi}\circ f(X)$. As in [Kim07, §3.2], for any unit $z\in\mathcal{O}_k^{\times}$ one can construct a point $\tilde{c}_{n,z}\in\hat{E}(\mathfrak{m}_{k(\mu_{p^n})})$ such that

$$\log_{\hat{E}}(\tilde{c}_{n,z})=\left[\sum_{i=1}^{\infty}(-1)^{i-1}z^{\varphi^{-(n+2i)}}\cdot p^i\right]+\log_{f_z^{\varphi^{-n}}}(z^{\varphi^{-n}}\cdot(\zeta_{p^n}-1)), \tag{3.1}$$

with $f_z(X):=(X+z)^p-z^p$.

Remark 3.1. Since $\hat{E}(\mathfrak{m}_{k(\mu_{p^n})})$ is torsion-free (see [Kob03, Prop. 8.7] and [Kim07, Prop. 3.1]), the formal group logarithm $\log_{\hat{E}}$ is injective, and hence the point $\tilde{c}_{n,z}$ is uniquely defined by (3.1).

Let $k_n\subset k(\mu_{p^{n+1}})$ be the unique subfield of degree p^n over k, and let $\mathfrak{m}_{k,n}$ be the maximal ideal of the valuation ring of k_n. Let $\hat{E}^{\pm}(\mathfrak{m}_{k,n})$ be the image of $\hat{E}^{\pm}(\mathfrak{m}_{k(\mu_{p^{n+1}})})$ under $\mathrm{tr}_{k_n}^{k(\mu_{p^{n+1}})}$, define $E^{\pm}(k_n)$ similarly, and set

$$c_{n,z}:=\mathrm{tr}_{k_n}^{k(\mu_{p^{n+1}})}(\tilde{c}_{n+1,z})\in\hat{E}(\mathfrak{m}_{k,n}). \tag{3.2}$$

Let $\Phi_m(X)=\sum_{i=0}^{p-1}X^{p^{m-1}i}$ be the p^m-th cyclotomic polynomial, define

$$\tilde{\omega}_n^{+}(X):=\prod_{\substack{1\leqslant m\leqslant n\\ m\text{ even}}}\Phi_m(1+X),\qquad \tilde{\omega}_n^{-}(X):=\prod_{\substack{1\leqslant m\leqslant n\\ m\text{ odd}}}\Phi_m(1+X),$$

and set $\omega_n^{\pm}(X)=X\tilde{\omega}_n^{\pm}(X)$. We denote by k^m the unramified extension of $\mathbf{Q}_p$ of degree p^m, write $k_{n,m}$ and $\mathfrak{m}_{n,m}$ for the above k_n and $\mathfrak{m}_{k,n}$ with $k=k^m$, and set

$$\Lambda_{n,m}:=\mathbf{Z}_p[\mathrm{Gal}(k_{n,m}/\mathbf{Q}_p)],\quad \Lambda_{n,m}^{\pm}:=\mathbf{Z}_p[[\Gamma_1]]/(\omega_n^{\pm}(X),(1+Y)^{p^m}-1)\simeq\tilde{\omega}_n^{\mp}(X)\Lambda_{n,m},$$

where the last isomorphism follows from the relation $(1+X)^{p^n}-1=X\tilde{\omega}_n^{+}(X)\tilde{\omega}_n^{-}(X)$.

Lemma 3.2. *There is a sequence of points $c_{n,m}\in\hat{E}(\mathfrak{m}_{n,m})$ satisfying the compatibilities:*

$$\mathrm{tr}_{k_{n,m-1}}^{k_{n,m}}(c_{n,m})=c_{n,m-1},\qquad \mathrm{tr}_{k_{n-1,m}}^{k_{n,m}}(c_{n,m})=-c_{n-2,m}.$$

Moreover, for even (resp. odd) values of n, $c_{n,m}$ generates $\hat{E}^{+}(\mathfrak{m}_{n,m})$ (resp. $\hat{E}^{-}(\mathfrak{m}_{n,m})$) as a $\Lambda_{n,m}$-module.

Proof. The first part is shown in [Wan16, Lem. 6.2]. For our later use, we recall the construction of $c_{n,m}$. By the normal basis theorem, we may fix an element $d=\{d_m\}_m\in\varprojlim_m\mathcal{O}_{k^m}^{\times}$ generating $\varprojlim_m\mathcal{O}_{k^m}^{\times}$ as a $\mathbf{Z}_p[[U]]$-module. Writing $d_m=\sum_j a_{m,j}\zeta_j$, with ζ_j roots of unity and $a_{m,j}\in\mathbf{Z}_p$, one then defines

$$c_{n,m}:=\sum_j a_{m,j}c_{n,\zeta_j}, \tag{3.3}$$

where c_{n,ζ_j} is as in (3.2). The proof of the above trace relations then follows from an explicit calculation of the images under $\log_{\hat{E}}$ of both sides using (3.1). The second claim in the lemma is contained in [Wan16, Lem. 6.4]. □

Definition 3.3. Let T be the p-adic Tate module of E. We define $H^1_\pm(k_{n,m},T)\subseteq H^1(k_{n,m},T)$ to be the orthogonal complement of $E^\pm(k_{n,m})\otimes\mathbf{Q}_p/\mathbf{Z}_p$ under the local Tate pairing

$$(\ ,\ )_{n,m}: H^1(k_{n,m},T)\times H^1(k_{n,m},E[p^\infty])\longrightarrow \mathbf{Q}_p/\mathbf{Z}_p,$$

where we view $E^\pm(k_{n,m})\otimes\mathbf{Q}_p/\mathbf{Z}_p$ as embedded in $H^1(k_{n,m},E[p^\infty])$ by the Kummer map.

3.2. **The plus/minus Coleman maps.** We recall Kobayashi's construction of the plus/minus Coleman maps for the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$, as extended by B.-D. Kim [Kim14a] to finite unramified extensions of $\mathbf{Q}_p$.

Define the maps $P_{c_{n,m}}: H^1(k_{n,m},T)\to\Lambda_{n,m}=\mathbf{Z}_p[\mathrm{Gal}(k_{n,m}/\mathbf{Q}_p)]$ by

$$P_{c_{n,m}}(z)=\sum_{\sigma\in\mathrm{Gal}(k_{n,m}/\mathbf{Q}_p)}(c^\sigma_{n,m},z)_{n,m},$$

and set $P^\pm_{c_{n,m}}:=(-1)^{[\frac{n+1}{2}]}P_{c^\pm_{n,m}}$, where

$$c^+_{n,m}=\begin{cases}c_{n,m} & \text{if } n \text{ is even},\\ c_{n-1,m} & \text{if } n \text{ is odd},\end{cases}\qquad c^-_{n,m}=\begin{cases}c_{n-1,m} & \text{if } n \text{ is even},\\ c_{n,m} & \text{if } n \text{ is odd}.\end{cases}$$

By Lemma 3.2, the maps $P^\pm_{c_{n,m}}$ factor through the quotient by $H^1_\pm(k_{n,m},T)$ and they satisfy natural compatibilities for varying n and m. Moreover, as shown in [Kim14a, Thms. 2.7-8] (see also [Kob03, §8.5]), there are unique maps $\mathrm{Col}^\pm_{n,m}$ making the following diagram commute:

$$\begin{array}{ccc} H^1(k_{n,m},T) & \xrightarrow{\mathrm{Col}^\pm_{n,m}} & \Lambda^\pm_{n,m}\\ \downarrow & & \downarrow{\scriptstyle \cdot\tilde\omega_n^{\mp}}\\ H^1(k_{n,m},T)/H^1_\pm(k_{n,m},T) & \xrightarrow{P^\pm_{c_{n,m}}} & \Lambda_{n,m}.\end{array}$$

The maps $\mathrm{Col}^\pm_{n,m}$ are isomorphisms and passing to the limit they define Λ-linear isomorphisms

$$\mathrm{Col}^\pm:\varprojlim_{n,m}\frac{H^1(k_{n,m},T)}{H^1_\pm(k_{n,m},T)}\xrightarrow{\sim}\varprojlim_{n,m}\Lambda_{n,m}\simeq\mathbf{Z}_p[[\Gamma_1]]. \tag{3.4}$$

3.3. **The plus/minus logarithm maps.** We now define local big logarithm maps $\mathrm{Log}^\pm_{\mathrm{ac}}$ on $H^1_\pm(K_v,\mathbf{T}^{\mathrm{ac}})$, where

$$\mathbf{T}^{\mathrm{ac}}:=T\otimes\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]](\Psi^{-1}) \tag{3.5}$$

for the canonical character $\Psi:\Gamma^{\mathrm{ac}}\hookrightarrow\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}]]^\times$. As it will be clear to the reader, these maps are the restriction to the "anticyclotomic line" of the two-variable plus/minus logarithm maps $\mathrm{Log}^\pm$ introduced in [Wan16, §6.1]. We still keep the notations from Section 3.1.

Via the natural inclusion

$$E(k_{n,m})\otimes\mathbf{Q}_p/\mathbf{Z}_p=(E(k_{n,m})\otimes\mathbf{Q}_p/\mathbf{Z}_p)^\perp\subseteq(E^\pm(k_{n,m})\otimes\mathbf{Q}_p/\mathbf{Z}_p)^\perp=H^1_\pm(k_{n,m},T),$$

the points $c_{n,m}$ lie in the $\Lambda_{n,m}$-module $H^1_\pm(k_{n,m},T)$. By [Wan16, Lem. 6.9], one can choose norm-compatible classes $b^\pm_{n,m}\in H^1_\pm(k_{n,m},T)$ with the property that

$$\tilde\omega_n^{-\epsilon}(X)b^\epsilon_{n,m}=(-1)^{[\frac{n+1}{2}]}c_{n,m},$$

where $\epsilon=(-1)^n$, and such that $\varprojlim_{n,m}b^\pm_{n,m}$ generates $\varprojlim_{m,n}H^1_\pm(k_{n,m},T)$ as a free $\mathbf{Z}_p[[\Gamma_1]]$-module of rank one. Noting that $K^{\mathrm{ac}}_{m,v}\subseteq k_{m,m+a}$, we define

$$E^+(K^{\mathrm{ac}}_{m,v}):=\left\{P\in E(K^{\mathrm{ac}}_{m,v})\ \middle|\ \mathrm{tr}^{K^{\mathrm{ac}}_{m,v}}_{K^{\mathrm{ac}}_{\ell+1,v}}(P)\in E(K^{\mathrm{ac}}_{\ell,v})\text{ for }0\leqslant\ell<m,\text{ even }\ell\right\},$$

$$E^-(K^{\mathrm{ac}}_{m,v}):=\left\{P\in E(K^{\mathrm{ac}}_{m,v})\ \middle|\ \mathrm{tr}^{K^{\mathrm{ac}}_{m,v}}_{K^{\mathrm{ac}}_{\ell+1,v}}(P)\in E(K^{\mathrm{ac}}_{\ell,v})\text{ for }-1\leqslant\ell<m,\text{ odd }\ell\right\},$$

and we easily see that

$$E^{\pm}(K^{\mathrm{ac}}_{m,v})\otimes\mathbf{Q}_p/\mathbf{Z}_p = (E^{\pm}(k_{m,m+a})\otimes\mathbf{Q}_p/\mathbf{Z}_p)\cap H^1(K^{\mathrm{ac}}_{m,v},E[p^\infty]).$$

Let $H^1_{\pm}(K^{\mathrm{ac}}_{m,v},T)$ be the image of $H^1_{\pm}(k_{m,m+a},T)$ under corestriction from $k_{m,m+a}$ to K^{ac}_m. Set $\mathbf{T}^{\mathrm{ac}}_1 = T\otimes\mathbf{Z}_p[[\Gamma_1]](\Psi^{-1})$, where $\Psi:\Gamma^{\mathrm{ac}}_1\hookrightarrow\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}_1]]^\times$ is the canonical character, and we let G_{K_v} act diagonally on the tensor product $\mathbf{T}^{\mathrm{ac}}_1$. Then $H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}_1)\simeq\varprojlim_m H^1_{\pm}(K^{\mathrm{ac}}_{m,v},T)$ by Shapiro's lemma, and the elements

$$a^{\pm}_m := \mathrm{tr}^{k_{m,m+a}}_{K^{\mathrm{ac}}_{m,v}}(b^{\pm}_{m,m+a})$$

are norm-compatible, with $a^{\pm}:=\varprojlim a^{\pm}_m$ generating $H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}_1)$ as a free $\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}_1]]$-module.

Recall that $v_1,v_2,\dots,v_{p^t}$ are the primes over a place $v\mid p$ in K_∞/K. Since every prime above p is totally ramified in $K_\infty/K^{\mathrm{ac}}_\infty$, by abuse of notation we will still denote by $v_1,v_2,\dots,v_{p^t}$ the primes above v in K^{ac}_∞/K. Let $\gamma_1=\mathrm{id},\gamma_2,\dots,\gamma_{p^t}\in\Gamma^{\mathrm{ac}}$ be such that $\gamma_i v_1=v_i$. Then we have the direct sum decompositions

$$\Lambda_{\mathrm{ac}} = \bigoplus_{i=1}^{p^t}\gamma_i\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}_1]],\qquad H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}) = \bigoplus_{i=1}^{p^t}\gamma_i H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}_1), \tag{3.6}$$

where $\mathbf{T}^{\mathrm{ac}}:=T\otimes\Lambda_{\mathrm{ac}}$ equipped with the diagonal G_K-action similarly as before.

Definition 3.4. For every $v\mid p$ in K, define the maps

$$\mathrm{Log}^{\pm}_{\mathrm{ac}}: H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}_1)\longrightarrow\mathbf{Z}_p[[\Gamma^{\mathrm{ac}}_1]]$$

by the relation

$$x = \mathrm{Log}^{\pm}_{\mathrm{ac}}(x)\cdot a^{\pm}$$

for all $x\in H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}}_1)$. This naturally extends to a map $\mathrm{Log}^{\pm}_{\mathrm{ac}}:H^1_{\pm}(K_v,\mathbf{T}^{\mathrm{ac}})\longrightarrow\Lambda_{\mathrm{ac}}$ using (3.6). which does not depend on the choice of γ_i.

The following result establishes the interpolation property satisfied by the map $\mathrm{Log}^{+}_{\mathrm{ac}}$ (the result for $\mathrm{Log}^{-}_{\mathrm{ac}}$ is entirely similar).

Lemma 3.5. *Let $\phi:\Gamma^{\mathrm{ac}}\to\mathbf{C}_p^\times$ be a finite order character of conductor p^n, with $n>0$ even. If $x=\varprojlim_n x_n\in H^1_+(K_v,\mathbf{T}^{\mathrm{ac}})$, then the following formulas hold:*

$$\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\log_{\hat{E}}(x_n^\tau)\cdot\tilde{\omega}_n^-(\phi) = \phi^{-1}\big(\mathrm{Log}^+_{\mathrm{ac}}(x)\big)\cdot(-1)^{n/2}\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\log_{\hat{E}}(c^\tau_{n,n+a}),$$

$$\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\log_{\hat{E}}(c^\tau_{n,n+a}) = \frac{\mathfrak{g}(\phi)}{\phi(p^n)}\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\ d^\tau_{n+a},$$

where $\mathfrak{g}(\phi)=\sum_{u\bmod p^n}\phi(u)\zeta_{p^n}^u$ is the Gauss sum of ϕ.

Proof. The first equality follows directly from the definitions. On the other hand, an immediate calculation using (3.1) and (3.3) (cf. [Wan16, Lemma 6.2]) reveals that

$$\log_{\hat{E}}(c_{n,n+a}) = \sum_i(-1)^{i-1}d_{n+a}^{\varphi^{-(n+2i)}}\cdot p^i + \sum_{0\leqslant 2k<n}(-1)^k d_{n+a}^{\varphi^{2k-n}}\cdot\frac{\zeta_{p^{n-2k}}-1}{p^k}.$$

Thus we find that

$$\begin{aligned}\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\log_{\hat{E}}(c^\tau_{n,n+a}) &= \sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\ d_{n+a}^{\varphi^{-n}\tau}\cdot(\zeta_{p^n}^\tau-1)\\ &= \mathfrak{g}(\phi)\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\ d_{n+a}^{\varphi^{-n}\tau} = \frac{\mathfrak{g}(\phi)}{\phi(p^n)}\sum_{\tau\in\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}}\phi(\tau)\ d^\tau_{n+a}.\end{aligned}$$

□

3.4. **The two-variable plus/minus Selmer groups.** As in the preceding sections, let T denote the p-adic Tate module of E, and set $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $A = V/T \simeq E[p^\infty]$. Let Σ be a finite set of places of K containing those dividing $Np\infty$, and let $\mathfrak{G}_{K,\Sigma}$ be the Galois group of the maximal extension of F unramified outside the places above Σ. Recall that Γ_K is the Galois group of the $\mathbf{Z}_p^2$-extension K_∞/K, and define the $\Lambda = \mathbf{Z}_p[[\Gamma_K]]$-modules

$$\mathbf{T} := T \otimes_{\mathbf{Z}_p} \Lambda(\Psi^{-1}), \qquad \mathbf{A} := \mathbf{T} \otimes_\Lambda \mathrm{Hom}_{\mathbf{Z}_p}(\Lambda, \mathbf{Q}_p/\mathbf{Z}_p),$$

where $\Psi : \Gamma_K \hookrightarrow \Lambda^\times$ is the map sending $\gamma \in \Gamma_K$ to the corresponding group-like element in $\Lambda^\times$. We shall also need to consider the modules $\mathbf{T}^{\mathrm{ac}}$, $\mathbf{A}^{\mathrm{ac}}$, $\mathbf{T}^{\mathrm{cyc}}$, and $\mathbf{A}^{\mathrm{cyc}}$, obtained by replacing Γ_K in the preceding definitions by the Galois group Γ^{ac} and Γ^{cyc} of the anticyclotomic and the cyclotomic $\mathbf{Z}_p$-extension of K, respectively.

In the following definitions, we let $\mathbf{M}$ denote either of the modules $\mathbf{T}$, $\mathbf{T}^{\mathrm{ac}}$, $\mathbf{T}^{\mathrm{cyc}}$, or any of their specializations.

Definition 3.6. The p-relaxed Selmer group of $\mathbf{M}$ is

$$\mathcal{Sel}^{\{p\}}(K, \mathbf{M}) := \ker\left\{ H^1(\mathfrak{G}_{K,\Sigma}, \mathbf{M}) \longrightarrow \bigoplus_{v \in \Sigma \smallsetminus \{p\}} \frac{H^1(K_v, \mathbf{M})}{H^1_{\mathrm{ur}}(K_v, \mathbf{M})} \right\},$$

where

$$H^1_{\mathrm{ur}}(K_v, \mathbf{M}) := \ker\{ H^1(K_v, \mathbf{M}) \longrightarrow H^1(K_v^{\mathrm{ur}}, \mathbf{M}) \}$$

is the unramified local condition.

Our Selmer groups of interest in this paper are obtained from cutting the p-relaxed ones by various local conditions at the primes above p.

Definition 3.7. For $\mathfrak{q} \in \{\mathfrak{p}, \bar{\mathfrak{p}}\}$ and $\mathscr{L}_\mathfrak{q} \in \{\mathrm{rel}, \pm, \mathrm{str}\}$, set

$$H^1_{\mathscr{L}_\mathfrak{q}}(K_\mathfrak{q}, \mathbf{M}) = \begin{cases} H^1(K_\mathfrak{q}, \mathbf{M}) & \text{if } \mathscr{L}_\mathfrak{q} = \mathrm{rel}, \\ H^1_\pm(K_\mathfrak{p}, \mathbf{M}) & \text{if } \mathscr{L}_\mathfrak{q} = \pm, \\ \{0\} & \text{if } \mathscr{L}_\mathfrak{q} = \mathrm{str}, \end{cases}$$

and for $\mathscr{L} = \{\mathscr{L}_\mathfrak{p}, \mathscr{L}_{\bar{\mathfrak{p}}}\}$, define

$$\mathcal{Sel}^{\mathscr{L}}(K, \mathbf{M}) := \ker\left\{ \mathrm{Sel}^{\{p\}}(K, \mathbf{M}) \longrightarrow \bigoplus_{\mathfrak{q} \in \{\mathfrak{p}, \bar{\mathfrak{p}}\}} \frac{H^1(K_\mathfrak{q}, \mathbf{M})}{H^1_{\mathscr{L}_\mathfrak{q}}(K_\mathfrak{q}, \mathbf{M})} \right\},$$

and similarly for $\mathrm{Sel}^{\mathscr{L}}(K, \mathbf{M})$

Thus, for example, $\mathcal{Sel}^{\mathrm{rel,str}}(K, \mathbf{M})$ is the submodule of $\mathcal{Sel}^{\{p\}}(K, \mathbf{M})$ consisting of classes which are trivial at $\bar{\mathfrak{p}}$ (with no condition at $\mathfrak{p}$). Also, letting $\mathbf{W}$ denote either of the modules $\mathbf{A}$, $\mathbf{A}^{\mathrm{ac}}$, $\mathbf{A}^{\mathrm{cyc}}$, or any of their specilizations, we define $\mathcal{Sel}^{\{p\}}(K, \mathbf{W})$ and $\mathrm{Sel}^{\{p\}}(K, \mathbf{W})$ just as in Definition 3.6, and set

$$\mathcal{Sel}^{\mathscr{L}}(K, \mathbf{W}) := \ker\left\{ \mathcal{Sel}^{\{p\}}(K, \mathbf{W}) \longrightarrow \bigoplus_{\mathfrak{q} \in \{\mathfrak{p}, \bar{\mathfrak{p}}\}} \frac{H^1(K_\mathfrak{q}, \mathbf{W})}{H^1_{\mathscr{L}_\mathfrak{q}}(K_\mathfrak{q}, \mathbf{M})^\perp} \right\},$$

where $H^1_{\mathscr{L}_\mathfrak{q}}(K_\mathfrak{q}, \mathbf{M})^\perp$ is the orthogonal complement of $H^1_{\mathscr{L}_\mathfrak{q}}(K_\mathfrak{q}, \mathbf{M})$ under local Tate duality. Finally, we let

$$\mathfrak{X}^{\mathscr{L}}(K, \mathbf{A}) := \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{Sel}^{\mathscr{L}}(K, \mathbf{A}), \mathbf{Q}_p/\mathbf{Z}_p)$$

be the Pontrjagin dual of $\mathcal{Sel}^{\mathscr{L}}(K, \mathbf{A})$, and similarly define $\mathfrak{X}^{\mathscr{L}}(K, \mathbf{A}^{\mathrm{ac}})$ and $\mathfrak{X}^{\mathscr{L}}(K, \mathbf{A}^{\mathrm{cyc}})$.

Anticyclotomic Selmer groups. Let $\iota : \Lambda_{\mathrm{ac}} \to \Lambda_{\mathrm{ac}}$ the involution given by $\gamma \mapsto \gamma^{-1}$ on group-like elements, and for any Λ_{ac}-module M, let M^{ι} denote the underlying module M with the Λ_{ac}-module structure given by $\Lambda_{\mathrm{ac}} \xrightarrow{\iota} \Lambda_{\mathrm{ac}} \to \mathrm{End}(M)$. Denote by M_{tors} the Λ_{ac}-torsion submodule of M.

Lemma 3.8. *For every $\varepsilon \in \{\pm\}$ we have* $\mathrm{rank}_{\Lambda_{\mathrm{ac}}}\mathfrak{X}^{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}) = 1 + \mathrm{rank}_{\Lambda_{\mathrm{ac}}}\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})$, *and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(X^{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) = \mathrm{Char}_{\Lambda_{\mathrm{ac}}}(X^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}})$$

as ideals in Λ_{ac}.

Proof. We shall adapt the arguments in [AH06, §1.2]. By Lemma 3.5.3 and Theorem 4.1.13 of [MR04], for every continuous character $\psi : \Gamma^{\mathrm{ac}} \to L^{\times}$ with values in some finite extension $L/\mathbf{Q}_p$ with ring of integers $\mathfrak{O}_L$, there is a non-canonical isomorphism

$$H^1_{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi))[p^i] \simeq (L/\mathfrak{O}_L)^r[p^i] \oplus H^1_{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}(\psi^{-1}))[p^i] \tag{3.7}$$

for all positive i. Here $H^1_{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi)) \subset \mathrm{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi))$ is the generalized Selmer group consisting of classes whose restriction at $\mathfrak{p}$ lies in $H^1(K_{\mathfrak{p}},\mathbf{A}^{\mathrm{ac}}(\psi))_{\mathrm{div}}$, while $H^1_{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}(\psi^{-1}))$ is the same as $\mathrm{Sel}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}(\psi^{-1}))$, and r is the *core rank* (see [MR04, Def. 4.1.11]) of the Selmer conditions defining $H^1_{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi))$, which by [DDT94, Thm. 2.18] it is given by the quantity

$$\mathrm{corank}_{\mathfrak{O}_L}H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{A}^{\mathrm{ac}}(\psi)) + \mathrm{corank}_{\mathfrak{O}_L}H^1(K_{\overline{\mathfrak{p}}},\mathbf{A}^{\mathrm{ac}}(\psi)) - \mathrm{corank}_{\mathfrak{O}_L}H^0(K_w,\mathbf{A}^{\mathrm{ac}}(\psi)), \tag{3.8}$$

where w denotes the infinite place of K. By the local Euler characteristic formula, the first two terms in (3.8) are equal to 1 and 2, respectively, while the third one clearly equals 2. Thus $r = 1$ in (3.7) and letting $i \to \infty$ we conclude that

$$H^1_{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi)) \simeq (L/\mathfrak{O}_L) \oplus H^1_{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}(\psi^{-1})). \tag{3.9}$$

Now, it is easy to show that the natural restriction maps

$$H^1_{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}}(\psi)) \longrightarrow \mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}})(\psi)^{\Gamma^{\mathrm{ac}}}$$
$$H^1_{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}(\psi^{-1})) \longrightarrow \mathfrak{Sel}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})(\psi^{-1})^{\Gamma^{\mathrm{ac}}}$$

are injective with finite bounded cokernel as ψ varies (cf. [AH06, Lem. 1.2.4]), and since

$$\mathfrak{Sel}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})(\psi^{-1})^{\Gamma^{\mathrm{ac}}} \simeq \mathfrak{Sel}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})(\psi)^{\Gamma^{\mathrm{ac}}}$$

by the action of complex conjugation, the result follows from (3.9) by the same argument as in [AH06, Lem. 1.2.6], proceeding as in [How04b, Thm. 2.2.1] to handle the prime $p\Lambda_{\mathrm{ac}}$. □

4. Beilinson–Flach classes

4.1. **The plus/minus Beilinson–Flach classes.** In this section, building on the work of Loeffer–Zerbes [LZ14], we show the existence of certain plus/minus Beilinson–Flach classes $\mathcal{BF}^{\pm}$ which map to the plus/minus p-adic L-functions of §2.2 under the plus/minus Coleman maps. We maintain the set-up introduced in Section 3.1, and let $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ be the normalized newform associated with E. In particular, $a_p = 0$.

Recall the $\mathbf{Z}_p[[\Gamma_1]]$-linear maps $\mathrm{Col}^{\pm}$ introduced in (3.4), and extend them (using the analogue of the decomposition (3.6) with Γ in place of Γ^{ac}) to Λ-linear isomorphisms

$$\mathrm{Col}^{\pm} : \frac{H^1(K_v,\mathbf{T})}{H^1_{\pm}(K_v,\mathbf{T})} \longrightarrow \Lambda$$

for each prime v above p. On the other hand, the p-adic L-function $L_{\mathfrak{p}}(f/K)$ of Theorem 2.11 we defined as an element in Λ_{R_0}, but (as we show in §5.1) the corresponding principal ideal in Λ_{R_0} can be generated by an element $\mathcal{L}_{\mathfrak{p}}(f/K) \in \Lambda$.

In the following, we let $\gamma_{\mathrm{ac}} \in \Gamma^{\mathrm{ac}}$ be a topological generator, and let $P \subseteq \Lambda$ be the pullback of the augmentation ideal $(\gamma_{\mathrm{ac}} - 1) \subseteq \Lambda_{\mathrm{ac}}$.

Theorem 4.1. *For every $\varepsilon \in \{\pm\}$ there exist an element $\mathcal{BF}^{\varepsilon} \in \mathrm{Sel}^{\varepsilon,\mathrm{rel}}(K, \mathbf{T})$ such that*

$$\mathrm{Col}^{\varepsilon}(\mathrm{res}_{\overline{\mathfrak{p}}}(\mathcal{BF}^{\varepsilon})) = u \cdot h^{\varepsilon} \cdot L_p^{\varepsilon,\varepsilon}(f/K), \quad \mathrm{Log}^{\varepsilon}(\mathrm{res}_{\mathfrak{p}}(\mathcal{BF}^{\varepsilon})) = h^{\varepsilon} \cdot \mathcal{L}_{\mathfrak{p}}(f/K),$$

for some nonzero $u \in \Lambda[1/P]$ and $h^{\varepsilon} \in \Lambda$.

Proof. This is shown in [Wan16, §7.3], where it is deduced from the work of Loeffler–Zerbes on Beilinson–Flach classes in Coleman families and their explicit reciprocity laws [LZ16]. (Note that [Wan16] only deals with $\varepsilon = +1$, but the case $\varepsilon = -1$ is done completely analogously.) The element h^{ε} is needed to establish integrality of the class $\mathcal{BF}^{\varepsilon}$, while u is the ratio between two periods attached to a certain Hida family of CM forms, whose integrality (up to powers of the "exceptional prime" P) is shown in [Wan16, §8.1] building on work of Rubin [Rub91] and Hida–Tilouine [HT94]. Thus it remains to take care of the ratio between Hida's canonical period $\Omega_f^{\mathtt{Hida}}$ in (2.1) and the Petersson inner product period used in [LZ16], which we do with the following comparison. (This may be well-known to experts, but we provide the details for the convenience of the reader.)

Letting D_{FL} denote the Fontaine–Laffaille functor, we have

$$D_{\mathrm{FL}}(H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)) = H^1(X_0(N), \Omega^{\bullet}_{X_0(N)/\mathbf{Z}_p})$$

(see [LLZ14, §6.10]). The Galois representation $T \simeq T_f^*$ is given by $H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)[\lambda_f]$, where $[\lambda_f]$ denotes the maximal submodule of $H^1_{\text{ét}}(X_0(N), \mathbf{Z}_p)$ on which the Hecke algebra $\mathbb{T}_0(N)$ acts with the same eigenvalues as in f, and hence

$$D_{\mathrm{FL}}(T) = H^1(X_0(N), \Omega^{\bullet}_{X_0(N)/\mathbf{Z}_p})[\lambda_f].$$

On the other hand, we have an exact sequence of localized Hecke modules

$$H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Z}_p})_{\mathfrak{m}_f} \hookrightarrow H^1(X_0(N), \Omega^{\bullet}_{X_0(N)/\mathbf{Z}_p})_{\mathfrak{m}_f} \twoheadrightarrow H^1(X_0(N), \mathcal{O}_{X_0(N)})_{\mathfrak{m}_f}.$$

The last term is free of rank one over $\mathbb{T}_0(N)_{\mathfrak{m}_f}$, while the first is isomorphic to $S(X_0(N), \mathbf{Z}_p)_{\mathfrak{m}_f}$. Unravelling the definitions, we see that the class $\eta_f \in H^1(X_0(N), \mathbf{Z}_p)_{\mathfrak{m}_f} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ constructed in [LLZ14, §6.10] corresponds to the projector to the f-component under the identification of $H^1(X_0(N), \mathbf{Z}_p)_{\mathfrak{m}_f} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ with $\mathbb{T}_0(N)_{\mathfrak{m}_f}$, while we have an isomorphism

$$D_{\mathrm{FL}}(T)/\mathrm{Fil}^0 D_{\mathrm{FL}}(T) \simeq H^1(X_0(N), \mathcal{O}_{X_0(N)})_{\mathfrak{m}_f}[\lambda_f].$$

Thus the ratio of a generator of $D_{\mathrm{FL}}(T)/\mathrm{Fil}^0 D_{\mathrm{FL}}(T)$ over η_f is, by definition, the congruence number c_f of f, from where the desired comparison follows by (2.1). □

Remark 4.2. By the construction in [Wan16, §7.3], the element h^{ε} divides the half-logarithm $\log_{\mathfrak{p}}^{\varepsilon}$. Since the latter does not vanish identically along the anticyclotomic line, the same is true for h^{ε}.

4.2. **Two-variable main conjectures.** As shown below, by Theorem 4.1 the following three different variants of Iwasawa's main conjecture for elliptic curves $E/\mathbf{Q}$ at supersingular primes $p > 3$ base-changed to an imaginary quadratic field K in which $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits are essentially equivalent:

(1) The main conjecture 'without p-adic zeta functions' for the two-variable plus/minus Selmer groups.
(2) The Iwasawa–Greenberg main conjecture for $L_{\mathfrak{p}}(f/K)$.
(3) The equal-sign cases of Kim's two-variable main conjectures [Kim14a].

More precisely, we have the following:

Theorem 4.3. *Let $\varepsilon \in \{\pm\}$. The following two statements are equivalent:*

(1) $\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A})$ *is* Λ*-torsion, and*

$$\mathrm{Char}_\Lambda(\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A})) = (\mathcal{L}_\mathfrak{p}(f/K))$$

as ideals in Λ*.*

(2) $\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})$ *is* Λ*-torsion,* $\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})$ *has* Λ*-rank* 1*, and*

$$\mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}))\cdot\mathcal{H}^\varepsilon = \mathrm{Char}_\Lambda\left(\frac{\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})}{\Lambda\cdot\mathcal{BF}^\varepsilon}\right),$$

where $\mathcal{H}^\varepsilon\subseteq\Lambda$ *is the ideal generated by the element* h^ε *in Theorem 4.1.*

Moreover, $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})$ *is* Λ*-torsion, and if the above two statements hold, then we have the divisibility*

$$\mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}))\subseteq(L_p^{\varepsilon,\varepsilon}(f/K))$$

in $\Lambda[1/P]$*.*

Proof. This is essentially shown in [Wan16, §8.1]. For the convenience of the reader, we briefly recall the argument. Poitou–Tate global duality gives rise to the exact sequences

$$0\longrightarrow\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})\longrightarrow H^1_\varepsilon(K_\mathfrak{p},\mathbf{T})\longrightarrow\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A})\longrightarrow\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})\longrightarrow 0, \tag{4.1}$$

$$0\longrightarrow\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})\longrightarrow\frac{H^1(K_{\overline{\mathfrak{p}}},\mathbf{T})}{H^1_\varepsilon(K_{\overline{\mathfrak{p}}},\mathbf{T})}\longrightarrow\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})\longrightarrow\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})\longrightarrow 0, \tag{4.2}$$

where exactness on the leftmost terms relies on the nonvanishing of $L_p^{\varepsilon,\varepsilon}(f/K)$ and $L_\mathfrak{p}(f/K)$.

By control theorem [Wan16, Prop. 8.7], Kobayashi's result [Kob03, Thm. 1.2] implies that $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})$ is Λ-torsion. By (4.2), it follows that $\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})$ is Λ-torsion and $\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})$ has Λ-rank one, and by (4.2), that $\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A})$ is Λ-torsion. Finally, [Wan16, Cor. 7.9] and Theorem 4.1 yield the following exact sequences from the above:

$$0\longrightarrow\frac{\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})}{\Lambda\cdot\mathcal{BF}^\varepsilon}\longrightarrow\frac{\Lambda}{\mathcal{H}^\varepsilon\cdot(\mathcal{L}_\mathfrak{p}(f/K))}\longrightarrow\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A})\longrightarrow\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})\longrightarrow 0,$$

$$0\longrightarrow\frac{\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})}{\Lambda\cdot\mathcal{BF}^\varepsilon}\longrightarrow\frac{\Lambda}{\mathcal{H}^\varepsilon\cdot\mathcal{U}\cdot(L_p^{\varepsilon,\varepsilon}(f/K))}\longrightarrow\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})\longrightarrow\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})\longrightarrow 0,$$

where $\mathcal{U}\subset\Lambda[1/P]$ is the ideal generated by the element u in Theorem 4.1. By the multiplicativity of characteristic ideals along exact sequences, the result follows. □

Corollary 4.4. *If any of the equivalent statements in Theorem 4.3 holds, then*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}))\cdot\mathcal{H}^\varepsilon_{\mathrm{ac}} = \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\cdot\mathcal{BF}^\varepsilon_{\mathrm{ac}}}\right),$$

where $\mathcal{BF}^\varepsilon_{\mathrm{ac}}$ *is the image of* $\mathcal{BF}^\varepsilon$ *under the projection* $\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})\to\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$ *and* $\mathcal{H}^\varepsilon_{\mathrm{ac}}$ *is the image of* $\mathcal{H}^\varepsilon$ *in* Λ_{ac}*.*

Proof. Of course, this follows from descending part (2) of Theorem 4.3 from K_∞ to K_∞^{ac}. Let $\gamma_{\mathrm{cyc}}\in\Gamma^{\mathrm{cyc}}$ be a topological generator, and let $I^{\mathrm{cyc}}:=(\gamma_{\mathrm{cyc}}-1)\Lambda\subset\Lambda$. As in [SU14, Prop. 3.9] (with the roles of the cyclotomic and anticyclotomic $\mathbf{Z}_p$-extensions reversed) we have

$$\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})/I^{\mathrm{cyc}}\mathfrak{X}^{\pm,\mathrm{str}}(K,\mathbf{A})\simeq\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}),$$

and by [Rub91, Lem. 6.2(ii)] it follows that

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})) = \mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}))\cdot\mathfrak{D}, \tag{4.3}$$

where $\mathfrak{D}:=\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})[I^{\mathrm{cyc}}])$. On the other hand, set

$$Z(K_\infty):=\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})/(\mathcal{BF}^\varepsilon),\quad Z(K_\infty^{\mathrm{ac}}):=\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})/(\mathcal{BF}^\varepsilon_{\mathrm{ac}}).$$

Using the fact that I^{cyc} is principal, an application of snake's lemma yields the exactness of

$$\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})[I^{\mathrm{cyc}}] \longrightarrow Z(K_\infty)[I^{\mathrm{cyc}}] \longrightarrow (\mathcal{BF}^\varepsilon)/I^{\mathrm{cyc}}(\mathcal{BF}^\varepsilon). \tag{4.4}$$

Arguing as in the proof of [AH06, Prop. 2.4.15] we see that the natural Λ_{ac}-module map

$$Z(K_\infty)/I^{\mathrm{cyc}}Z(K_\infty) \longrightarrow Z(K_\infty^{\mathrm{ac}})$$

is injective with cokernel having characteristic ideal $\mathfrak{D}$, and hence

$$Ch_{\Lambda^{\mathrm{ac}}}(Z(K_\infty^{\mathrm{ac}})) = Ch_{\Lambda_{\mathrm{ac}}}(Z(K_\infty)/I^{\mathrm{cyc}}Z(K_\infty))\cdot\mathfrak{D}. \tag{4.5}$$

Since $H^1(K,\mathbf{T})$ has trivial Λ-torsion, the leftmost term in (4.4) vanishes; on the other hand, the rightmost one is clearly torsion-free, and hence $Z(K_\infty)[I^{\mathrm{cyc}}]$ is torsion-free. Since [Rub91, Lem. 6.2(i)] and equality (4.5) imply that $Z(K_\infty)[I^{\mathrm{cyc}}]$ is also a torsion Λ_{ac}-module (using the nonvanishing of the terms in that equality), we conclude that $Z(K_\infty)[I^{\mathrm{cyc}}] = \{0\}$, and by [Rub91, Lem. 6.2(ii)] it follows that

$$\mathrm{Char}_\Lambda(Z(K_\infty))\cdot\Lambda_{\mathrm{ac}} = \mathrm{Char}_{\Lambda_{\mathrm{ac}}}(Z(K_\infty)/I^{\mathrm{cyc}}Z(K_\infty)). \tag{4.6}$$

Combined with (4.3), we thus arrive at

$$\begin{aligned}\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})) &= \mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}))\cdot\mathfrak{D}\\ &= \mathcal{H}^\varepsilon\cdot\mathrm{Char}_\Lambda(Z(K_\infty))\cdot\mathfrak{D}\\ &= \mathcal{H}^\varepsilon_{\mathrm{ac}}\cdot\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(Z(K_\infty^{\mathrm{ac}})),\end{aligned}$$

using (4.5) and (4.6) for the last equality. This completes the proof. □

4.3. **Rubin's height formula.** We keep the notations introduced in §2.3, assume that the generalized Heegner hypothesiss (Heeg) in that section holds, and still denote by $L_p^{\bullet,\circ}(f/K)$ the image of the p-adic L-functions $L_p^{\bullet,\circ}(f/K)$ of Proposition 2.3 under the projection

$$\mathbf{Z}_p[[H_{p^\infty}]]\otimes_{\mathbf{Z}_p}\mathbf{Q}_p \longrightarrow \Lambda\otimes_{\mathbf{Z}_p}\mathbf{Q}_p.$$

Let $\gamma_{\mathrm{cyc}}\in\Gamma^{\mathrm{cyc}}$ be a topological generator, and using the identification $\Lambda\simeq\Lambda^{\mathrm{ac}}[[\Gamma^{\mathrm{cyc}}]]$ expand

$$L_p^{\bullet,\circ}(f/K) = L_{p,0}^{\bullet,\circ}(f/K) + L_{p,1}^{\bullet,\circ}(f/K)(\gamma_{\mathrm{cyc}}-1)+\cdots \tag{4.7}$$

as a power series in $\gamma_{\mathrm{cyc}}-1$ with coefficients in $\Lambda_{\mathrm{ac}}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$. Thus $L_{p,0}^{\bullet,\circ}(f/K)$ is identified with the anticyclotomic projection $L_{p,\mathrm{ac}}^{\bullet,\circ}(f/K)$, and so

$$L_{p,0}^{\varepsilon,\varepsilon}(f/K) = 0$$

for each $\varepsilon\in\{\pm\}$ by Corollary 2.6. In particular, by Theorem 4.1 and the injectivity of the map Col^ε, it follows that the classes $\mathcal{BF}^\varepsilon$ have images $\mathcal{BF}^\varepsilon_{\mathrm{ac}}$ under the projection $H^1(K,\mathbf{T})\to H^1(K,\mathbf{T}^{\mathrm{ac}})$ landing in $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})\subset\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$.

In the following, let $h_0^\varepsilon\in\Lambda_{\mathrm{ac}}$ and $u_0\in\Lambda_{\mathrm{ac}}[1/P]$ to be the constant term in the expansion of the elements h^ε and u in Theorem 4.1 as a power series in $\gamma_{\mathrm{cyc}}-1$, so that $\mathcal{H}^\varepsilon_{\mathrm{ac}}=(h_0^\varepsilon)$ in the notations of Corollary 4.4. Also, we let $L_n = K_n^{\mathrm{ac}}K_\infty^{\mathrm{cyc}}$, and think of $\mathcal{BF}^\varepsilon\in H^1(K,\mathbf{T})\simeq H^1_{\mathrm{Iw}}(K_\infty,T)$ as a compatible system of classes $\mathcal{BF}^\varepsilon_{\mathrm{cyc},n}\in H^1_{\mathrm{Iw}}(L_n,T)$.

Lemma 4.5. *For every n there is a unique element*

$$\beta_n^\varepsilon\in\frac{H^1_{\mathrm{Iw}}(L_{n,\bar{\mathfrak{p}}},T)}{H^1_{\mathrm{Iw},\varepsilon}(L_{n,\bar{\mathfrak{p}}},T)}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$$

such that

$$(\gamma^{\mathrm{cyc}}-1)\beta_n^\varepsilon = \mathrm{loc}_{\bar{\mathfrak{p}}}(\mathcal{BF}^\varepsilon_{\mathrm{cyc},n}).$$

Letting $\beta_n^\varepsilon(\mathbb{1})$ be the image of β_n^ε in $H^1(K_{n,\overline{\mathfrak{p}}}^{\mathrm{ac}},T)/H^1_\varepsilon(K_{n,\overline{\mathfrak{p}}}^{\mathrm{ac}},T)[1/p]$, the elements $\beta_n^\varepsilon(\mathbb{1})$ define an element $\beta_\infty^\varepsilon(\mathbb{1})\in H^1(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})/H^1_\varepsilon(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})[1/p]$, and the map Col^ε yields an identification

$$\frac{H^1(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})}{H^1_\varepsilon(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p\simeq\Lambda^{\mathrm{ac}}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$$

sending $\beta_\infty^\varepsilon(\mathbb{1})$ to the product $u_0\cdot h_0^\varepsilon\cdot L_{p,1}^{\varepsilon,\varepsilon}(f/K)$.

Proof. Since $u_0\cdot h_0^\varepsilon\cdot L_{p,1}^{\varepsilon,\varepsilon}(f/K)$ is clearly the coefficient in the linear term of the expansion of $u\cdot h^\varepsilon\cdot L_p^{\varepsilon,\varepsilon}(f/K)$ as a power series in $\gamma_{\mathrm{cyc}}-1$, the result follows from the definition of $\beta_\infty^\varepsilon(\mathbb{1})$ and Theorem 4.1. □

Let $\mathcal{I}\subseteq\mathbf{Z}_p[[\Gamma^{\mathrm{cyc}}]]$ be the augmentation ideal, and set $\mathcal{J}=\mathcal{I}/\mathcal{I}^2$.

Theorem 4.6. *For every n there is a canonical (up to sign) p-adic height pairing*

$$\langle\ ,\ \rangle_{K_n^{\mathrm{ac}}}^{\mathrm{cyc}}:\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_n^{\mathrm{ac}},T)\times\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_n^{\mathrm{ac}},T)\longrightarrow p^{-k}\mathbf{Z}_p\otimes_{\mathbf{Z}_p}\mathcal{J}$$

for some $k\in\mathbf{Z}_{\geqslant 0}$ independent of n, such that for every $b\in\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_n^{\mathrm{ac}},T)$, we have

$$\langle\mathcal{BF}^\varepsilon_{\mathrm{cyc},n}(\mathbb{1}),b\rangle_{K_n^{\mathrm{ac}}}^{\mathrm{cyc}}=(\beta_n^\varepsilon(\mathbb{1}),\mathrm{loc}_{\overline{\mathfrak{p}}}(b))_n\otimes(\gamma_{\mathrm{cyc}}-1),\tag{4.8}$$

where $(\ ,\ )_n$ is the $\mathbf{Q}_p$-linear extension of the local Tate pairing

$$\frac{H^1(K_{n,\overline{\mathfrak{p}}}^{\mathrm{ac}},T)}{H^1_\varepsilon(K_{n,\overline{\mathfrak{p}}}^{\mathrm{ac}},T)}\times H^1_\varepsilon(K_{n,\overline{\mathfrak{p}}}^{\mathrm{ac}},T)\longrightarrow\mathbf{Z}_p.$$

Proof. Since by [Kim07, Prop. 4.11] the local conditions defining $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K_n^{\mathrm{ac}},T)$ at the primes $v\mid p$ are their own orthogonal complement under the local Tate pairing, the construction of the cyclotomic p-adic height pairings $\langle\ ,\rangle_{K_n^{\mathrm{ac}}}^{\mathrm{cyc}}$ can be deduced from [How04a, Thm. 1.11]. The p-adic height formula (4.8) then follows from [How04a, Thm. 2.5(c)]. □

5. Heegner points

Let $E/\mathbf{Q}$ be an elliptic curve, let $f=\sum_{n=1}^\infty a_nq^n\in S_2(\Gamma_0(N))$ be the associated newform, and assume that $p>3$ is a prime of good supersingular reduction for E (so $a_p=0$). Let $K/\mathbf{Q}$ be an imaginary quadratic field in which $p=\mathfrak{p}\overline{\mathfrak{p}}$ splits. Throughout this section, we assume that the pair (f,K) satisfies the generalized Heegner hypothesis (Heeg) introduced in §2.3.

5.1. **The plus/minus Heegner classes.** Let X_{N^+,N^-} be the Shimura curve (with the cusps added if $N^-=1$) over $\mathbf{Q}$ attached to a quaternion algebra $B/\mathbf{Q}$ of discriminant N^- and an Eichler order $R\subset\mathcal{O}_B$ of level N^+. We embed X_{N^+,N^-} into its Jacobian J_{N^+,N^-} by choosing an auxiliary prime $\ell\nmid Np$ and defining

$$\iota_\ell:X_{N^+,N^-}\longrightarrow J_{N^+,N^-}$$

by $x\mapsto(T_\ell-\ell-1)[x]$, where T_ℓ is the usual Hecke correspondence on X_{N^+,N^-}, and $[x]\in\mathrm{Div}(X_{N^+,N^-})$ is the divisor class of $x\in X_{N^+,N^-}$.

Recall that we let $K[m]$ denote the ring class field of K of conductor m.

Proposition 5.1. *For every positive integer m prime to N, there are Heegner points $P[m]\in E(K[m])$ such that*

$$\mathrm{tr}^{K[mp^{k+2}]}_{K[mp^{k+1}]}(P[mp^{k+2}])=a_pP[mp^{k+1}]-P[mp^k]$$

for all $k\geqslant 0$.

Proof. This is standard: after fixing a modular parametrization

$$\pi : J_{N^+,N^-} \longrightarrow E,$$

a system of points as in the Proposition is obtained by letting $P[m]$ be the image of CM points $h[m] \in X_{N^+,N^-}(K[m])$ (see e.g. [How04c, Prop. 1.2.1]) under the composite map $\pi \circ \iota_\ell$. □

Since the $G_{\mathbf{Q}}$-representation $E[p] \simeq \bar{\rho}_f$ is irreducible by [Edi92], we may choose the above prime ℓ so that $a_\ell - \ell - 1$ is a unit in $\mathbf{Z}_p^\times$, and we then let

$$z[m] \in H^1(K[m], T)$$

be the image of $P[m] \otimes (a_\ell - \ell - 1)^{-1}$ under the Kummer map $E(K[m]) \otimes \mathbf{Z}_p \to H^1(K[m], T)$. (Thus $z[m]$ is independent of the choice of ℓ.)

The anticyclotomic $\mathbf{Z}_p$-extension K_∞^{ac}/K is contained in $\widetilde{K}_\infty = \bigcup_{k \geqslant 0} K[p^k]$, and $\mathrm{Gal}(\widetilde{K}_\infty/K)$ is isomorphic to $\Gamma^{\mathrm{ac}} \times \Delta$, with Δ finite. For every positive integer S coprime to Np and every $n \geqslant 0$, we let $K_n^{\mathrm{ac}}[S]$ denote the compositum $K_n^{\mathrm{ac}} K[S]$, and set

$$z_n[S] := \mathrm{cor}_{K_n^{\mathrm{ac}}[S]}^{K[Sp^{k(n)}]}(z[Sp^{k(n)}])$$

where $k(n) := \min\{k \ : \ K_n^{\mathrm{ac}} \subset K[p^k]\}$. Letting cor_n^{n+1} be corestriction map for the extension $K_{n+1}^{\mathrm{ac}}[S]/K_n^{\mathrm{ac}}[S]$, it follows from the norm-compatibility in Proposition 5.1 that

$$\mathrm{cor}_n^{n+1}(z_{n+1}[S]) = -z_{n-1}[S], \tag{5.1}$$

since $a_p = 0$.

Lemma 5.2. *The classes $z_n[S]$ lie in the image of the natural map*

$$H^1(K[S], \mathbf{T}^{\mathrm{ac}}) \longrightarrow H^1(K_n^{\mathrm{ac}}[S], T).$$

Proof. The obvious long exact sequence shows that the cokernel of the map in the statement is controlled by

$$H^2(K[S], \mathbf{T}^{\mathrm{ac}})[\omega_n]. \tag{5.2}$$

Since $H^2(K[S], \mathbf{T}^{\mathrm{ac}})$ is finitely generated over Λ_{ac}, the module (5.2) stabilizes for $n \gg 0$. On the other hand, from the norm-relation (5.1) we immediately see that

$$\frac{\omega_{n'}^\epsilon}{\omega_n^\epsilon} z_{n'}[S] = \pm z_n[S]$$

for all $n' > n$ with $n' \equiv n \pmod 2$, where $\epsilon = (-1)^n$. Letting $n' \to \infty$, this shows that $z_n[S]$ must have zero image in (5.2), hence the result. □

The next result will be a key ingredient in our construction of plus/minus Heegner classes.

Lemma 5.3. *Assume that $E[p]|_{G_K}$ is irreducible. Then $H^1(K[S], \mathbf{T}^{\mathrm{ac}})$ is free over Λ_{ac}.*

Proof. Let $M_S := H^1(K[S], \mathbf{T}^{\mathrm{ac}})$, and identify $\Lambda_{\mathrm{ac}} \simeq \mathbf{Z}_p[[X]]$ via $\gamma_{\mathrm{ac}} \mapsto 1 + X$. We first claim that the two maps

$$\alpha : M_S \xrightarrow{X} M_S, \quad \beta : M_S/XM_S \xrightarrow{p} M_S/XM_S$$

are injective. Indeed, the irreducibility assumption on $E[p]|_{G_K}$ implies that $T^{G_{K_\infty^{\mathrm{ac}}}} = \{0\}$, and hence the injectivity of α follows from [PR00, §1.3.3]. We thus get an injection $M_S/XM_S \hookrightarrow H^1(K[S], T)$, and so to establish the injectivity of β is suffices to show the injectivity of the map

$$H^1(K[S], T) \xrightarrow{p} H^1(K[S], T),$$

but this follows again from the G_K-irreducibility of $E[p]$. By the structure theorem for finitely generated modules over Λ_{ac}, the above shows that M_S injects into a free module of finite rank with finite cokernel N. If $N \neq \{0\}$, then $\mathrm{Tor}_1^{\Lambda_{\mathrm{ac}}}(N, \Lambda_{\mathrm{ac}}/X\Lambda_{\mathrm{ac}})$ is a nonzero $\mathbf{Z}_p$-torsion module

injecting into M_S/XM_S, contradicting the injectivity of β. Hence $N = \{0\}$ and M_S is free over Λ_{ac}. □

Set $\omega_n^{\pm} := \omega_n^{\pm}((1+Y)^{p^a}-1)$ to lighten the notation. A straightforward induction argument using (5.1) shows that

$$\omega_n^{\epsilon} z_n[S] = 0,$$

where ε is the sign $(-1)^n$ (see [DI08, Lem. 4.2]). By Lemma 5.2 Lemma 5.3, this implies that there is a unique class

$$z_n[S]^{\varepsilon} \in H^1(K_n^{\mathrm{ac}}[S], T)/\omega_n^{\varepsilon} H^1(K_n^{\mathrm{ac}}[S], T)$$

such that

$$\tilde{\omega}_n^{-\varepsilon} z_n[S]^{\varepsilon} = (-1)^{[\frac{n+1}{2}]} z_n[S].$$

Lemma 5.4. *For each $\varepsilon \in \{\pm\}$ the sequences $\{z_n[S]^{\varepsilon}\}_{n\equiv\varepsilon \pmod 2}$ are compatible under the natural projections*

$$H^1(K_n^{\mathrm{ac}}[S], T)/\omega_n^{\varepsilon} H^1(K_n^{\mathrm{ac}}[S], T) \longrightarrow H^1(K_{n-2}^{\mathrm{ac}}[S], T)/\omega_{n-2}^{\epsilon} H^1(K_{n-2}^{\mathrm{ac}}[S], T)$$

induced by corestriction.

Proof. In light of the freeness result of Lemma 5.3, the argument in [DI08, Lem. 2.9] applies verbatim. □

For every $\varepsilon \in \{\pm\}$ and $S > 0$ prime to Np we may thus define classes $\mathbf{z}[S]^{\varepsilon} \in H^1(K[S], \mathbf{T}^{\mathrm{ac}})$ by

$$\mathbf{z}[S]^{\varepsilon} := \varprojlim_n z_n[S]^{\varepsilon}, \tag{5.3}$$

where the limit is over n with the fixed parity determined by ε. Since $\{\omega_n^{\varepsilon}\}_n$ forms a basis for the topology of Λ_{ac}, the class $\mathbf{z}[S]^{\varepsilon}$ is well-defined.

5.2. **Explicit reciprocity law.** As we show in this section, similarly as in [CH17] for ordinary primes, the classes $\mathbf{z}^{\pm} := \mathbf{z}[1]^{\pm}$ satisfy an explicit reciprocity law relating them to some of the anticyclotomic p-adic L-functions in §2.3.

Recall from §3.1 the element $d = \{d_m\}_m \in \varprojlim_m \mathcal{O}_{k^m}^{\times}$ generating this $\mathbf{Z}_p[[U]]$-module, and let

$$F_{d,2} := \varprojlim_m \sum_{\sigma \in U/p^m U} d_m^{\sigma} \cdot \sigma^2,$$

viewed as an element in Λ_{R_0}. By the discussion in [LZ14, §6.4] on the Katz p-adic L-function (see also [*loc.cit.*, §3.2]), the quotient $\mathscr{L}_{\mathfrak{p}}^{\mathtt{Katz}}(K)/F_{d,2}$ gives rise to a nonzero element in Λ_{ac}, rather than just $\Lambda_{R_0}^{\mathrm{ac}}$.

Lemma 5.5. *We have the equality*

$$F_{d,2} = \left(\varprojlim_m \sum_{\sigma \in U/p^m U} d_m^{\sigma} \cdot \sigma \right)^2$$

up to a unit in $\mathbf{Z}_p[[U]]^{\times}$.

Proof. This follows from a straightforward calculation. □

Thus setting $F_d := \varprojlim_m \sum_{\sigma \in U/p^m U} d_m^{\sigma} \cdot \sigma$, the p-adic L-function $L_{\mathfrak{p}}(f/K)$ of Theorem 2.11 may be written as the product

$$L_{\mathfrak{p}}(f/K) = \mathcal{L}_{\mathfrak{p}}(f/K) \cdot F_d^2 \cdot U, \tag{5.4}$$

for some $\mathcal{L}_{\mathfrak{p}}(f/K) \in \Lambda$ and $U \in \Lambda^{\times}$, and letting $\mathcal{L}_{\mathfrak{p},\mathrm{ac}}(f/K) \in \Lambda_{\mathrm{ac}}$ be the image of $\mathcal{L}_{\mathfrak{p}}(f/K)$ under the projection $\Lambda \to \Lambda_{\mathrm{ac}}$, we see from Corollary 2.12 that

$$\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2 = \mathcal{L}_{\mathfrak{p},\mathrm{ac}}(f/K) \cdot F_d^2 \cdot U' \tag{5.5}$$

for some $U' \in \Lambda_{\mathrm{ac}}^{\times}$.

Note that for every $\varepsilon \in \{\pm\}$ and $v \mid p$ the classes $\mathbf{z}^{\varepsilon}$ satisfy $\mathrm{loc}_v(\mathbf{z}^{\varepsilon}) \in H^1_{\varepsilon}(K, \mathbf{T}^{\mathrm{ac}})$, and so we may consider the image of $\mathrm{loc}_v(\mathbf{z}^{\varepsilon})$ under the signed logarithm map $\mathrm{Log}_{\mathrm{ac}}^{\varepsilon}$ constructed in §3.3.

Theorem 5.6 (Explicit reciprocity law)**.** *For every $\varepsilon \in \{\pm\}$, we have the equality*

$$\mathrm{Log}_{\mathrm{ac}}^{\varepsilon}(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^{\varepsilon})) = \mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K) \cdot F_d \cdot \sigma_{-1,\mathfrak{p}}, \tag{5.6}$$

where $\sigma_{-1,\mathfrak{p}} := \mathrm{rec}_{\mathfrak{p}}(-1)|_{K_\infty^{\mathrm{ac}}} \in \Gamma^{\mathrm{ac}}$. In particular, the class $\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^{\varepsilon})$ is non-torsion.

Proof. We give the proof for $\varepsilon = +$, the proof for the other sign being virtually the same. Let ψ be an anticyclotomic Hecke character of infinity type $(1,-1)$ and conductor prime to p, and let $\mathscr{L}_{\mathfrak{p},\psi}(f) \in R_0[[\Gamma^{\mathrm{ac}}]]$ be as in [CH17, Def. 3.5]. The p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ of Theorem 2.7 is then given by

$$\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K) = \mathrm{Tw}_{\psi^{-1}}(\mathscr{L}_{\mathfrak{p},\psi}(f)),$$

where $\mathrm{Tw}_{\psi^{-1}} : R_0[[\Gamma^{\mathrm{ac}}]] \to R_0[[\Gamma^{\mathrm{ac}}]]$ is the R_0-linear isomorphism given by $\gamma \mapsto \psi^{-1}(\gamma)\gamma$ for $\gamma \in \Gamma^{\mathrm{ac}}$. Let $\phi : \Gamma^{\mathrm{ac}} \to \mu_{p^\infty}$ be a nontrivial finite order character, let $n > 0$ be the smallest positive integer such that ϕ factors through $\Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}$ (using additive notation), and assume that n is even. Following the calculations in [CH17, Thm. 4.8], we then find that

$$\begin{aligned}
\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)(\phi^{-1}) &= \mathfrak{g}(\phi^{-1})\phi(p^n)p^{-n} \sum_{\sigma \in \Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}} \phi(\sigma)\log_{\hat{E}}(\sigma P[p^n]) \\
&= \phi(-1) \cdot \frac{\phi(p^n)}{\mathfrak{g}(\phi)} \cdot (-1)^{n/2}\tilde{\omega}_n^-(\phi) \sum_{\sigma \in \Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}} \phi(\sigma)\log_{\hat{E}}(\sigma P[p^n]^+),
\end{aligned}$$

where we used the definition of $P[p^n]^+$ for the second equality. Combined with the interpolation properties of the map Log^+ (see Lemma 3.5), this shows that

$$\begin{aligned}
\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)(\phi^{-1}) &= \phi(-1) \cdot \frac{\phi(p^n)}{\mathfrak{g}(\phi)} \sum_{\sigma \in \Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}} \phi(\sigma)\log_{\hat{E}}(c_n^\sigma) \cdot \mathrm{Log}_{\mathrm{ac}}^+(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^+))(\phi^{-1}) \\
&= \phi(-1) \sum_{\sigma \in \Gamma^{\mathrm{ac}}/p^n\Gamma^{\mathrm{ac}}} \phi(\sigma) d_{n+a}^\sigma \cdot \mathrm{Log}_{\mathrm{ac}}^+(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^+))(\phi^{-1}).
\end{aligned} \tag{5.7}$$

Letting ϕ vary, equality (5.6) follows immediately from (5.7).

With the explicit reciprocity law (5.6) in hand, the nontrivality of $\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^{\pm})$ follows from the nonvanishing of $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ in Theorem 2.7. □

Remark 5.7. That the classes $\mathbf{z}^{\pm}$ are non-torsion over Λ_{ac} can also be deduced from the proof by Cornut–Vatsal of Mazur's conjecture on higher Heegner points (see [CV07, Thm. 1.5] and the discussion right after it). However, the local refinement provided by Theorem 5.6 will be a vital ingredient for our main results in this paper.

5.3. **Anticyclotomic main conjectures.** By (5.4) and (5.5), there is an element $\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ in Λ_{ac} such that

$$(\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2) = (\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2) = (\mathcal{L}_{\mathfrak{p},\mathrm{ac}}(f/K)) \tag{5.8}$$

as principal ideals of $R_0[[\Gamma^{\mathrm{ac}}]]$. The Iwasawa–Greenberg main conjecture [Gre94] for the p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)$ of Theorem 2.7 may thus be formulated as follows:

Conjecture 5.8 (Iwasawa–Greenberg main conjecture)**.** *The module* $\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})$ *is* Λ_{ac}*-torsion, and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})) = (\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2)$$

as ideals in $\Lambda_{\mathrm{ac}}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$*.*

As we show in Section 6.1, Conjecture 5.8 is intimatelly related to the analogue of Perrin-Riou's Heegner point main conjecture [PR87a] formulated in the Introduction of this paper (see Conjecture 1.2). The following three lemmas will be used to relate the two, where we let $\varepsilon\in\{\pm\}$ be a fixed sign.

Lemma 5.9. *Assume that* $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ *has* Λ_{ac}*-rank* 1*. Then*

$$\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) = \mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}}) \tag{5.9}$$

and $\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})$ *is a torsion* Λ_{ac}*-module.*

Proof. Consider the exact sequence

$$\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}}) \longrightarrow \mathfrak{X}^{\mathrm{rel},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}}) \longrightarrow \mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}}) \longrightarrow 0. \tag{5.10}$$

Since $\mathbf{z}^{\varepsilon}$ lands in $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$, by Theorem 5.6 the image of the map $\mathrm{loc}_{\mathfrak{p}}$ is not Λ_{ac}-torsion, and since $H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})$ has Λ_{ac}-rank 1, it follows that $\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})$ is Λ_{ac}-torsion. On the other hand, by Proposition 5.15 below the assumption in the lemma implies that $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$ has Λ_{ac}-rank 1, and so from (5.10) we conclude that

$$\mathrm{rank}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\mathrm{rel},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})) = 1. \tag{5.11}$$

Since $\mathfrak{X}^{\mathrm{rel},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}}) \simeq \mathfrak{X}^{\varepsilon,\mathrm{rel}}(K,\mathbf{A}^{\mathrm{ac}})$ by the action of complex conjugation, we deduce from (5.11) and Lemma 3.8 that $\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion. Finally, since $H^1(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})/H^1_{\varepsilon}(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})$ has Λ_{ac}-rank 1, counting ranks in the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) \longrightarrow \mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}}) &\xrightarrow{\mathrm{loc}_{\overline{\mathfrak{p}}}} \frac{H^1(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})}{H^1_{\varepsilon}(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})} \\ &\longrightarrow \mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}}) \longrightarrow \mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}}) \longrightarrow 0, \end{aligned}$$

we see that $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ and $\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$ have both Λ_{ac}-rank 1, and since the quotient $H^1(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})/H^1_{\varepsilon}(K_{\overline{\mathfrak{p}}},\mathbf{T}^{\mathrm{ac}})$ is also Λ_{ac}-torsion-free, equality (5.9) follows. □

Lemma 5.10. *Assume that* $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ *has* Λ_{ac}*-rank* 1*. Then for any height one prime* $\mathfrak{P}$ *of* Λ_{ac} *we have*

$$\mathrm{ord}_{\mathfrak{P}}(\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)) = \mathrm{length}_{\mathfrak{P}}(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})) + \mathrm{length}_{\mathfrak{P}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\cdot\mathbf{z}^{\varepsilon}}\right),$$

where $\mathrm{loc}_{\mathfrak{p}} : \mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) \to H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})$ *is the natural restriction map.*

Proof. Consider the tautological exact sequence

$$0 \longrightarrow \mathfrak{Sel}^{\mathrm{str},\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) \longrightarrow \mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) \longrightarrow H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}}) \longrightarrow \mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}) \longrightarrow 0. \tag{5.12}$$

By Theorem 5.6, the image of $\mathbf{z}^{\varepsilon}\in\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ under the map $\mathrm{loc}_{\mathfrak{p}}$ is not Λ_{ac}-torsion. Since $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ has Λ_{ac}-rank 1 by assumption, this shows that $\mathfrak{Sel}^{\mathrm{str},\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ is Λ_{ac}-torsion, and since $H^1(K,\mathbf{T}^{\mathrm{ac}})$ is Λ_{ac}-torsion-free (see e.g. [How04b, Lem. 2.2.9]), it follows that

$$\mathfrak{Sel}^{\mathrm{str},\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) = \{0\}. \tag{5.13}$$

From (5.12) we thus deduce the exact sequence

$$0 \longrightarrow \frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot\mathbf{z}^{\varepsilon}} \longrightarrow \frac{H^1_{\varepsilon}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}^{\varepsilon})} \longrightarrow \mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}) \longrightarrow 0,$$

and since by the explicit reciprocity law of Theorem 5.6 the map $\mathrm{Log}_{\mathrm{ac}}^{\varepsilon}$ induces a Λ_{ac}-module isomorphism

$$\frac{H^1_\varepsilon(K_\mathfrak{p},\mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot \mathrm{loc}_\mathfrak{p}(\mathbf{z}^\varepsilon)} \xrightarrow{\simeq} \frac{\Lambda_{\mathrm{ac}}}{\Lambda_{\mathrm{ac}}\cdot \mathcal{L}_\mathfrak{p}^{\mathtt{BDP}}(f/K)},$$

the result follows. □

Lemma 5.11. *Assume that $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ has Λ_{ac} rank 1. Then the module $\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion, and for any height one prime $\mathfrak{P}$ of Λ_{ac} we have*

$$\mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})) = \mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) + 2\,\mathrm{length}_\mathfrak{P}(\mathrm{coker}(\mathrm{loc}_\mathfrak{p})),$$

where $\mathrm{loc}_\mathfrak{p}:\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})\to H^1_\varepsilon(K_\mathfrak{p},\mathbf{T}^{\mathrm{ac}})$ is the natural restriction map.

Proof. Global duality yields the exact sequence

$$0\longrightarrow \mathrm{coker}(\mathrm{loc}_\mathfrak{p})\longrightarrow \mathfrak{X}^{\mathrm{rel},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})\longrightarrow \mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})\longrightarrow 0. \tag{5.14}$$

As shown in the proof of Lemma 5.10, the first term in the sequence is Λ_{ac}-torsion; since by Proposition 5.15 below the assumption implies that $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$ has Λ_{ac}-rank 1, this shows that the same is true for $\mathfrak{X}^{\mathrm{rel},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$, and by Lemma 3.8 it follows that $\mathfrak{X}^{\mathrm{str},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion. Thus taking Λ_{ac}-torsion in (5.14) and using Lemma 3.8 again, it follows that

$$\mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\mathrm{str},\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})) = \mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) + \mathrm{length}_\mathfrak{P}(\mathrm{coker}(\mathrm{loc}_\mathfrak{p})) \tag{5.15}$$

for any height one prime $\mathfrak{P}$ of Λ_{ac}.

Another application of global duality yields the exact sequence

$$0\longrightarrow \mathrm{coker}(\mathrm{loc}_\mathfrak{p}^{\mathrm{rel}})\longrightarrow \mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})\longrightarrow \mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})\longrightarrow 0, \tag{5.16}$$

where $\mathrm{loc}_\mathfrak{p}^{\mathrm{rel}}:\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})\to H^1_\varepsilon(K_\mathfrak{p},\mathbf{T}^{\mathrm{ac}})$ is the natural restriction map. By Lemma 5.9, this is the same as the map $\mathrm{loc}_\mathfrak{p}$ in the statement, and hence $\mathrm{coker}(\mathrm{loc}_\mathfrak{p}^{\mathrm{rel}}) = \mathrm{coker}(\mathrm{loc}_\mathfrak{p})$ is Λ_{ac}-torsion. Since $\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion by Lemma 5.9, we conclude from (5.16) that $\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion. Combining (5.16) and (5.15), we thus have

$$\begin{aligned}\mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})) &= \mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}^{\mathrm{ac}})) + \mathrm{length}_\mathfrak{P}(\mathrm{coker}(\mathrm{loc}_\mathfrak{p}))\\ &= \mathrm{length}_\mathfrak{P}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) + 2\,\mathrm{length}_\mathfrak{P}(\mathrm{coker}(\mathrm{loc}_\mathfrak{p}))\end{aligned}$$

for any height one prime $\mathfrak{P}$ of Λ_{ac}, as was to be shown. □

5.4. **Kolyvagin system argument.** The purpose of this section is to prove the following result, establishing under mild assumptions one of the divisibility predicted by Conjecture 1.2.

Theorem 5.12. *Assume that $\mathrm{Gal}(\overline{\mathbf{Q}}/K)\to \mathrm{Aut}_{\mathbf{Z}_p}(T)$ is surjective, and that $E[p]$ is ramified at every prime $\ell \mid N^-$. Let $\varepsilon\in\{\pm\}$. Then $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$ and $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ both have Λ_{ac}-rank 1, and we have the divisibility*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) \supseteq \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot\mathbf{z}^\varepsilon}\right)^2.$$

For the proof of Theorem 5.12, we will adapt to our supersingular setting the Kolyvagin system techniques developed by Howard [How04b] in the ordinary case. More precisely, we will use the classes $P[S]^\varepsilon$ introduced in (5.3) to build a certain Kolyvagin system for $\mathbf{T}^{\mathrm{ac}}$; the nontriviality of this system will follow from the nontriviality of $\mathbf{z}^\varepsilon$ established in Theorem 5.6, and Theorem 5.12 will then follow from a suitable adaptation of Howard's arguments.

As in [How04b, §1.1], by a Selmer structure on $\mathbf{T}^{\mathrm{ac}}$ we mean a choice of a local condition $H^1_{\mathcal{F}}(K_v,\mathbf{T}^{\mathrm{ac}})\subseteq H^1(K_v,\mathbf{T}^{\mathrm{ac}})$ for each place $v\in\Sigma$. (Here Σ is any finite set of places of K containing those above p, those above ∞, and those where V ramifies.) We define the Selmer structure $\mathcal{F}^\pm$ on $\mathbf{T}^{\mathrm{ac}}$ to be the unramified local condition at the places in Σ not dividing p, and the plus/minus local condition $H^1_\pm(K_v,\mathbf{T}^{\mathrm{ac}})$ at the primes v above p.

For the statement of the next result, we refer the reader to [How04b, §1.2] for the definition of the module of Kolyvagin systems $\mathbf{KS}(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}, \mathcal{L})$ attached to a Selmer structure $\mathcal{F}$ on $\mathbf{T}^{\mathrm{ac}}$ and a certain set $\mathcal{L}$ of primes inert in K.

Theorem 5.13. *For each $\varepsilon \in \{\pm\}$ there exists a Kolyvagin system $\kappa^{\varepsilon} \in \mathbf{KS}(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}^{\varepsilon}, \mathcal{L})$ with $\kappa_1^{\varepsilon} = \mathbf{z}^{\varepsilon}$.*

Proof. Let $\mathcal{L}_0$ be the set of rational primes ℓ not dividing pN and inert in K. For each $\ell \in \mathcal{L}_0$, let λ be the prime of K above ℓ, and denote by I_ℓ the smallest ideal of Λ^{ac} containing $\ell+1$ for which the Frobenius element $\mathrm{Fr}_\lambda \in G_{K_\lambda}$ acts trivially on $\mathbf{T}^{\mathrm{ac}}/I_\ell\mathbf{T}^{\mathrm{ac}}$. Let $\mathcal{L} = \mathcal{L}(\mathbf{T}^{\mathrm{ac}}) \subseteq \mathcal{L}_0$ consist of the primes $\ell \in \mathcal{L}_0$ with $I_\ell \subseteq p\mathbf{Z}_p$, and let $\mathcal{N}$ be the set of square-free products S of primes in $\mathcal{L}$, with the convention that $1 \in \mathcal{N}$. For each $S \in \mathcal{N}$, define $I_S = \sum_{\ell|S} I_\ell$.

Applied to the Heegner classes $\mathbf{z}[S]^{\varepsilon}$ defined in (5.3), the derivative construction in [How04b, §1.7] produces classes

$$\kappa_S^{\varepsilon} \in H^1(K, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}}),$$

indexed by the products $S \in \mathcal{N}$, with $\kappa_1^{\varepsilon} = \mathbf{z}[1]^{\varepsilon} = \mathbf{z}^{\varepsilon}$. The verification that these classes form a Kolyvagin system for the Selmer structure $\mathcal{F}^{\varepsilon}$ on $\mathbf{T}^{\mathrm{ac}}$ follows from the same argument as in [How04b, Lem. 2.3.4] (as extended in [How04c, Prol. 3.4.1] to cover the primes $v \mid N^-$), the only difference being at the primes $v \mid p$, where we are led to show that the localization of κ_S^{ε} at v is contained in $H^1_{\mathcal{F}^{\varepsilon}}(K_v, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$, defined as the image of the natural map

$$H^1_{\mathcal{F}^{\varepsilon}}(K_v, \mathbf{T}^{\mathrm{ac}}) \longrightarrow H^1(K_v, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}}).$$

But this follows from the same argument as in the proof of Lemma 5.3. □

Let $\mathfrak{P}$ be a height one prime of Λ_{ac}, let $S_{\mathfrak{P}}$ denote the integral closure of $\Lambda_{\mathrm{ac}}/\mathfrak{P}$, and let $\varpi_{\mathfrak{P}} \in S_{\mathfrak{P}}$ be a uniformizer. Define the Galois representations

$$T_{\mathfrak{P}} := \mathbf{T}^{\mathrm{ac}} \otimes_{\Lambda_{\mathrm{ac}}} S_{\mathfrak{P}}, \qquad A_{\mathfrak{P}} := \mathbf{A}^{\mathrm{ac}} \otimes_{\Lambda_{\mathrm{ac}}} S_{\mathfrak{P}},$$

and let $T_{\mathfrak{P},m}$ and $A_{\mathfrak{P},m}$ be their reduction modulo $\varpi_{\mathfrak{P}}^m$.

For each place $v \mid p$ in K, define $H^1_{\pm}(K_v, T_{\mathfrak{P}}) \subseteq H^1(K_v, T_{\mathfrak{P}})$ to be the image of the natural map

$$H^1_{\mathcal{F}^{\pm}}(K_v, \mathbf{T}^{\mathrm{ac}}) \longrightarrow H^1(K_v, \mathbf{T}^{\mathrm{ac}} \otimes_{\Lambda^{\mathrm{ac}}} \Lambda^{\mathrm{ac}}/\mathfrak{P}) \longrightarrow H^1(K_v, T_{\mathfrak{P}}),$$

and define $H^1_{\pm}(K_v, T_{\mathfrak{P},m}) \subseteq H^1(K_v, T_{\mathfrak{P},m})$ in the same manner. Also, let $H^1_{\pm}(K_v, A_{\mathfrak{P}})$ (resp. $H^1_{\pm}(K_v, A_{\mathfrak{P},m})$) be the orthogonal complement of $H^1_{\pm}(K_v, T_{\mathfrak{P}})$ (resp. $H^1_{\pm}(K_v, T_{\mathfrak{P},m})$) under the local Tate pairing.

Lemma 5.14. *For every height one prime $\mathfrak{P} \subseteq \Lambda_{\mathrm{ac}}$ with $\mathfrak{P} \neq p\Lambda_{\mathrm{ac}}$, and for every place v of K, the natural maps*

$$H^1_{\mathcal{F}^{\pm}}(K_v, \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}}) \longrightarrow H^1_{\mathcal{F}^{\pm}_{\mathfrak{P}}}(K_v, T_{\mathfrak{P}}),$$
$$H^1_{\mathcal{F}^{\pm}_{\mathfrak{P}}}(K_v, A_{\mathfrak{P}}) \longrightarrow H^1_{\mathcal{F}^{\pm}}(K_v, \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}])$$

have finite kernel and cokernel of order bounded by a constant depending only on $[S_{\mathfrak{P}} : \Lambda_{\mathrm{ac}}/\mathfrak{P}]$.

Proof. Let m be any positive integer, and $n \gg 0$ be such that we have the inclusion of ideals of Λ_{ac}:

$$(\omega_n(X), p^m) \subseteq (\mathfrak{P}, p^m).$$

Then it follows from [Kim07, Prop. 3.14] (*cf.* [Kim07, Prop. 4.11]) that for each $v \mid p$ in K, the module $H^1_{\pm}(K_v, T_{\mathfrak{P},m})$ is the exact annihilator of $H^1_{\pm}(K_{\overline{v}}, T_{\mathfrak{P},m})$ under local Tate duality. In particular, $H^1_{\pm}(K_v, A_{\mathfrak{P},m})$ can be identified with $H^1_{\pm}(K_{\overline{v}}, T_{\mathfrak{P},m})$. Hence by [Kim07, Prop. 4.18] the second map in the statement has kernel and cokernel with the required bounds, and taking duals the same properties for the first map follow. □

Proposition 5.15. *For every $\varepsilon \in \{\pm\}$ we have*

$$\mathrm{rank}_{\Lambda_{\mathrm{ac}}}(\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})) = \mathrm{rank}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})).$$

Proof. Since the Selmer structure $\mathcal{F}^{\varepsilon}$ introduced above is such that

$$\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}}) = H^1_{\mathcal{F}^{\varepsilon}}(K,\mathbf{T}^{\mathrm{ac}}),$$

the result follows from Lemma 5.14 in the same manner that Proposition 2.2.8 in [How04b] is deduced from [How04b, Lem. 2.2.7] (see also [Wan14, Lem. 3.5]). □

Proof of Theorem 5.12. We can now adapt the argument in the proof [How04b, Thm. 2.2.10]. Indeed, for every height one prime $\mathfrak{P} \subseteq \Lambda_{\mathrm{ac}}$ with $\mathfrak{P} \neq p\Lambda_{\mathrm{ac}}$, we have a map

$$\mathbf{KS}(\mathbf{T}^{\mathrm{ac}},\mathcal{F}^{\varepsilon},\mathcal{L}(\mathbf{T}^{\mathrm{ac}})) \longrightarrow \mathbf{KS}(T_{\mathfrak{P}},\mathcal{F}^{\varepsilon}_{\mathfrak{P}},\mathcal{L}(T_{\mathfrak{P}})),$$

where $\mathcal{F}^{\varepsilon}_{\mathfrak{P}}$ is the Selmer structure on $T_{\mathfrak{P}}$ naturally induced from $\mathcal{F}^{\varepsilon}$. Letting $\kappa^{\varepsilon}(\mathfrak{P})$ be the image of the Kolyvagin system κ^{ε} of Theorem 5.13 under this map, it follows from Theorem 5.6 and Lemma 5.14 that $\kappa^{\varepsilon}_1(\mathfrak{P})$ generates and infinite $S_{\mathfrak{P}}$-submodule of $H^1_{\mathcal{F}^{\varepsilon}_{\mathfrak{P}}}(K,T_{\mathfrak{P}})$ for all but finitely many $\mathfrak{P}$. To deduce, as in [How04b, Prop. 2.1.3], that for any such $\mathfrak{P}$ the module $H^1_{\mathcal{F}^{\varepsilon}_{\mathfrak{P}}}(K,T_{\mathfrak{P}})$ is free of rank one over $S_{\mathfrak{P}}$, it suffices to show that the triple $(T_{\mathfrak{P}},\mathcal{F}^{\varepsilon}_{\mathfrak{P}},\mathcal{L}(T_{\mathfrak{P}}))$ satisfies the hypotheses (H.0)–(H.5) of [*loc.cit.*,§1.2]. The only difference here with respect to the verification of these hypotheses in [How04b, Prop. 2.1.3] is the self-duality condition in hypothesis (H.4), but this follows from [Kim07, Prop. 3.14] as indicated above.

By Lemma 5.14, this shows that $H^1_{\mathcal{F}^{\varepsilon}}(K,\mathbf{T}^{\mathrm{ac}}) \otimes_{\Lambda_{\mathrm{ac}}} S_{\mathfrak{P}}$ is a free $S_{\mathfrak{P}}$-module of rank 1, from where the first part of Theorem 5.12 follows immediately, and for the second part the argument in [How04b, Thm. 2.2.10] applies verbatim. □

6. Main results

6.1. **Proof of the main conjectures.** For the ease of notation, set

$$\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}) := \mathfrak{X}^{\mathrm{rel,str}}(K,\mathbf{A}),$$

and similarly for $\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}})$.

Theorem 6.1. *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N with good supersingular reduction at p, and let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant prime to N. Assume that the triple (E,p,K) satisfy the following:*

- *$p \geqslant 5$,*
- *$p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K,*
- *hypothesis* (Heeg) *holds,*
- *N is square-free,*
- *$N^- \neq 1$,*
- *$E[p]$ is ramified at every prime $\ell | N^-$,*
- *$\mathrm{Gal}(\overline{\mathbf{Q}}/K) \to \mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$ is surjective.*

Then:

(1) *For each $\varepsilon \in \{\pm\}$ both $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$ and $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ have Λ_{ac}-rank 1, and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) = \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot\mathbf{z}^{\varepsilon}}\right)^2$$

as ideals in Λ_{ac}.

(2) *$\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion, and*

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}})) = (\mathcal{L}_{\mathfrak{p}}^{\mathsf{BDP}}(f/K)^2)$$

as ideals in Λ_{ac}.

Proof. By Theorem 5.12 we know that $\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})$ has Λ_{ac}-rank 1. By Proposition 5.15 the same is true for $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})$, and by Lemma 5.11 the module $\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}})$ is Λ_{ac}-torsion. Let $\mathfrak{P}$ be a height one prime of Λ_{ac}. Then by the divisibility in Theorem 5.12 we have

$$\mathrm{length}_{\mathfrak{P}}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) \leqslant 2\,\mathrm{length}_{\mathfrak{P}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{A}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}}\cdot\mathbf{z}^{\varepsilon}}\right). \tag{6.1}$$

Combined with Lemma 5.11 and Lemma 5.10, respectively, this implies that

$$\begin{aligned}\mathrm{length}_{\mathfrak{P}}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}})) &\leqslant 2\,\mathrm{length}_{\mathfrak{P}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\cdot\mathbf{z}^{\varepsilon}}\right)+2\,\mathrm{length}_{\mathfrak{P}}(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}))\\ &= 2\,\mathrm{ord}_{\mathfrak{P}}(\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)),\end{aligned}$$

and hence we have the divisibility

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}}))\ \supseteq\ (\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2). \tag{6.2}$$

It remains to show the two divisibilities $\subseteq$ in the theorem. Let $I^{\mathrm{cyc}}:=(\gamma_{\mathrm{cyc}}-1)\subset\Lambda$ be the principal ideal generated by $\gamma_{\mathrm{cyc}}-1$. Similarly as in [SU14, Prop. 3.9], the natural restriction map $H^1(K_\infty^{\mathrm{ac}},E[p^\infty])\to H^1(K_\infty,E[p^\infty])$ induces a Λ_{ac}-module isomorphism

$$\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A})/I^{\mathrm{cyc}}\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A})\simeq\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}}). \tag{6.3}$$

By (5.5), the two-variable divisibility in [Wan16, Thm. 6.13] thus yields the divisibility

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}^{\mathrm{ac}}))\subseteq(\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K)^2) \tag{6.4}$$

in $\Lambda_{\mathrm{ac}}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$; however, since $\mu(\mathcal{L}_{\mathfrak{p}}^{\mathtt{BDP}}(f/K))=0$ by Theorem 2.8, the divisibility (6.4) holds already in Λ_{ac}, and therefore equality holds in (6.2). This shows part (1) of Theorem 6.1, and part (2) follows from it by Lemma 5.10 and Lemma 5.11. □

Theorem 6.2. *Let $\varepsilon\in\{\pm\}$. Under the hypotheses of Theorem 6.1, the following hold:*

(1) *$\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A})$ is Λ-torsion, $\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})$ has Λ-rank 1, and*

$$\mathrm{Char}_{\Lambda}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K,\mathbf{A}))\cdot\mathcal{H}^{\varepsilon}=\mathrm{Char}_{\Lambda}\left(\frac{\mathfrak{Sel}^{\varepsilon,\mathrm{rel}}(K,\mathbf{T})}{\Lambda\cdot\mathcal{BF}^{\varepsilon}}\right)$$

as ideals in Λ.

(2) *$\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A})$ is Λ-torsion, and*

$$\mathrm{Char}_{\Lambda}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A}))=(\mathcal{L}_{\mathfrak{p}}(f/K))$$

as ideals in Λ.

Proof. Given the equalities in the anticyclotomic main conjecture established in Theorem 6.1, we shall first deduce part (2) of the theorem by an anticyclotomic analogue of the argument in [SU14, Thm. 3.30]. Let I^{cyc} be the ideal of Λ generated by $\gamma_{\mathrm{cyc}}-1$, let

$$X:=\mathrm{Char}_{\Lambda}(\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A})),\quad Y:=(\mathcal{L}_{\mathfrak{p}}(f/K)).$$

Similarly as in the proof of Theorem 6.1, the divisibility in [Wan16, Thm. 6.13] yields the divisibility $X\subseteq Y$ as ideals in Λ. On the other hand, in light of (6.3) and Corollary 2.12, Theorem 6.1 implies that $\mathfrak{X}_{\mathfrak{p}}(K,\mathbf{A})$ is Λ-torsion and that $X=Y\pmod{I^{\mathrm{cyc}}}$. The equality $X=Y$ as ideals in Λ, i.e., the equality in part (2) of the theorem, thus follows from [SU14, Lem. 3.2]; by Theorem 4.3, the equality in part (1) also follows. □

Corollary 6.3. *Let $\varepsilon\in\{\pm\}$. Under the hypotheses of Theorem 6.1, $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})$ is Λ-torsion, and*

$$\mathrm{Char}_{\Lambda}(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A}))=(L_p^{\varepsilon,\varepsilon}(f/K))$$

as ideals in Λ.

Proof. In light of Theorem 4.3, the result of Theorem 6.2 implies that $\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})$ is Λ-torsion, and we have the divisibility

$$\mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})) \subseteq (L_p^{\varepsilon,\varepsilon}(f/K)) \tag{6.5}$$

as ideals in Λ. We note that *a priori* this divisibility holds just in $\Lambda[1/P]$, but by the nonvanishing of the cyclotomic specialization of $L_p^{\varepsilon,\varepsilon}(f/K)$ (which follows from the nonvanishing of the p-adic L-functions constructed by Kobayashi [Kob03] and the discussion in the paragraphs below), the divisibility holds as stated.

Similarly as in the proof of Theorem 6.2, we will deduce that equality holds in (6.5) by an appropriate application of [SU14, Lem. 3.2]. Set

$$X := \mathrm{Char}_\Lambda(\mathfrak{X}^{\varepsilon,\varepsilon}(K,\mathbf{A})), \qquad Y := (L_p^{\varepsilon,\varepsilon}(f/K)),$$

and let I^{ac} be the kernel of the canonical projection $\Lambda \twoheadrightarrow \Lambda_{\mathrm{cyc}}$. Let $\mathcal{L}_p^{\pm}(E/\mathbf{Q})$ and $\mathcal{L}_p^{\pm}(E^{(K)}/\mathbf{Q})$ be the p-adic L-functions constructed in [Kob03, §3] for the elliptic curve E and its quadratic twist $E^{(K)}$, respectively, and set

$$\mathcal{L}_p^{\varepsilon,\varepsilon}(f/K) := \mathcal{L}_p^{\varepsilon}(E/\mathbf{Q}) \cdot \mathcal{L}_p^{\varepsilon}(E^{(K)}/\mathbf{Q}).$$

By the control theorem of [Wan16, Prop. 8.7] and (see also [SU14, Lem. 3.6]), the divisibility in [Kob03, Thm. 4.1] applied to E and $E^{(K)}$ yields the divisibility

$$(X \bmod I^{\mathrm{ac}}) \supseteq (\mathcal{L}_p^{\varepsilon,\varepsilon}(f/K)) \tag{6.6}$$

as ideals in Λ_{cyc}. Thus it remains to compare the periods $\Omega_E^+ \cdot \Omega_E^-$ used in the construction of $\mathcal{L}_p^{\varepsilon,\varepsilon}(f/K)$ with Hida's canonical period used in the construction of $L_p^{\varepsilon,\varepsilon}(f/K)$ in Theorem 2.3. By [SZ14, Lem. 9.5], the ratio of periods is a p-adic unit which we can clearly ignore. This shows that (6.5) and (6.6) yield the equality $X = Y \pmod{I^{\mathrm{ac}}}$, and so the equality in Corollary 6.3 follows from the divisibility (6.5) by virtue of [SU14, Lem. 3.2]. (Meanwhile we used the fact that by the argument in [Wan16, Lem. 8.6] the two variable p-adic L-functions $L_p^{\varepsilon,\varepsilon}(f/K)$ are integral.) □

6.2. **A converse to Gross–Zagier–Kolyvagin.** Let

$$y_K := P_0[1] = \mathrm{tr}_K^{K[1]}(P[1]) \in E(K)$$

be the Heegner point introduced in §5.1.

Our next result is an analogue for supersingular primes of Skinner's converse to a theorem of Gross–Zagier and Kolyvagin (*cf.* [Ski14, Thm. B]) holding under slightly weaker conditions than in *loc.cit.* (as explained in the Introduction before the statement of Theorem B).

Theorem 6.4. *Let the hypotheses be as in Theorem 6.1, and assume that* $\mathrm{Sel}_{p^\infty}(f/K)$ *has* $\mathbf{Z}_p$*-corank* 1. *Then* $y_K \neq 0 \in E(K) \otimes_{\mathbf{Z}} \mathbf{Q}$. *In particular,* $\mathrm{ord}_{s=1} L(E/K,s) = 1$.

Proof. Let $\gamma_{\mathrm{ac}} \in \Gamma^{\mathrm{ac}}$ be a topological generator, and set $I^{\mathrm{ac}} = (\gamma_{\mathrm{ac}} - 1) \subseteq \Lambda_{\mathrm{ac}}$. We shall work with the sign $\varepsilon = +1$. By Kobayashi's control theorem (as extended by B.-D. Kim [Kim14a] to more general $\mathbf{Z}_p$-extensions), there is natural surjective map

$$\mathfrak{X}^{+,+}(K,\mathbf{A}^{\mathrm{ac}})/I^{\mathrm{ac}}\mathfrak{X}^{+,+}(K,\mathbf{A}^{\mathrm{ac}}) \longrightarrow \mathrm{Sel}_{p^\infty}(f/K)^\vee$$

with finite kernel, where

$$\mathrm{Sel}_{p^\infty}(f/K)^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}_{p^\infty}(f/K), \mathbf{Q}_p/\mathbf{Z}_p)$$

is the Pontrjagin dual. The assumption that $\mathrm{Sel}_{p^\infty}(f/K)$ has $\mathbf{Z}_p$-corank 1 thus implies that $\mathfrak{X}^{+,+}(K,\mathbf{A}^{\mathrm{ac}})/I^{\mathrm{ac}}\mathfrak{X}^{+,+}(K,\mathbf{A}^{\mathrm{ac}})$ is not $\mathbf{Z}_p$-torsion. By part (1) of Theorem 6.1, this forces $\mathbf{z}^+$ to have nontorsion image in $\mathfrak{Sel}^{+,+}(K,\mathbf{T}^{\mathrm{ac}})/I^{\mathrm{ac}}\mathfrak{Sel}^{+,+}(K,\mathbf{T}^{\mathrm{ac}})$. By the natural injection

$$\mathfrak{Sel}^{+,+}(K,\mathbf{T}^{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/I^{\mathtt{ac}}\mathfrak{Sel}^{+,+}(K,\mathbf{T}^{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p) \hookrightarrow \mathrm{Sel}(K, T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$$

this shows that $\mathbf{z}^+$ has nonzero image $\mathbf{z}_1^+ \in \mathrm{Sel}(K, T\otimes_{\mathbf{Z}_p}\mathbf{Q}_p)$; since by construction $\mathbf{z}_1^+ = z_0[1]$ is the Kummer image of y_K, the result follows. The last claim follows from the Gross–Zagier formula on Shimura curves [YZZ13]. □

6.3. **Λ-adic Gross–Zagier formula.** In this section we obtain an analogue of Howard's Λ-adic Gross–Zagier formula [How05] for supersingular primes. Recall the p-adic height pairings $\langle\ ,\ \rangle^{\mathrm{cyc}}_{K_n^{\mathrm{ac}}}$ on the plus/minus Selmer groups $\mathrm{Sel}^{\varepsilon,\varepsilon}(K_n^{\mathrm{ac}}, T)$ introduced in Theorem 4.6, and define the Λ_{ac}-adic height pairing

$$\langle\ ,\ \rangle^{\mathrm{cyc}}_{K_\infty^{\mathrm{ac}}} : \mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}}) \otimes_{\Lambda_{\mathrm{ac}}} \mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}})^\iota \longrightarrow \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathcal{J} \tag{6.7}$$

by the formula

$$\langle a_\infty, b_\infty\rangle^{\mathrm{cyc}}_{K_\infty^{\mathrm{ac}}} = \varprojlim_n \sum_{\sigma\in\mathrm{Gal}(K_n^{\mathrm{ac}}/K)} \langle a_n, b_n^\sigma\rangle^{\mathrm{cyc}}_{K_n^{\mathrm{ac}}} \cdot \sigma.$$

Recall that $\mathcal{J} = \mathcal{I}/\mathcal{I}^2$ for $\mathcal{I}$ the augmentation ideal of $\mathbf{Z}_p[[\Gamma^{\mathrm{cyc}}]]$. Upon choosing a topological generator $\gamma_{\mathrm{cyc}} \in \Gamma^{\mathrm{cyc}} \simeq \mathcal{J}$ the height pairing (6.7) may be seen as taking values in $\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$; we thus define the cyclotomic Λ_{ac}-adic cyclotomi regulator $\mathcal{R}^\varepsilon_{\mathrm{cyc}} \subseteq \Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ to be the characteristic ideal of the cokernel of $(\gamma_{\mathrm{cyc}} - 1)^{-1} \circ (6.7)$.

Theorem 6.5. *Let $\varepsilon \in \{\pm\}$, and denote by $\mathcal{X}^\varepsilon_{\mathrm{tors}}$ be the characteristic ideal of $\mathfrak{X}^{\varepsilon,\varepsilon}(K, \mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}$. Then*

$$\mathcal{R}^\varepsilon_{\mathrm{cyc}} \cdot \mathcal{X}^\varepsilon_{\mathrm{tors}} = (L^{\varepsilon,\varepsilon}_{p,1}(f/K))$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$.

Proof. The height formula of Theorem 4.6 and Lemma 4.5 immediately yield the equality

$$\mathcal{R}^\varepsilon_{\mathrm{cyc}} \cdot \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}} \cdot \mathcal{BF}^\varepsilon_{\mathrm{ac}}}\right) = \mathcal{U}_{\mathrm{ac}} \cdot \mathcal{H}^\varepsilon_{\mathrm{ac}} \cdot (L^{\varepsilon,\varepsilon}_{p,1}(f/K)) \cdot \eta^\iota \tag{6.8}$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$, where $\mathcal{U}_{\mathrm{ac}} = (u_0)$ and $\mathcal{H}^\varepsilon_{\mathrm{ac}} = (h^\varepsilon_0)$ in the notations of §4.3, and

$$\eta := \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{H^1_\varepsilon(K_{\mathfrak{p}}, \mathbf{T}^{\mathrm{ac}})}{\mathrm{loc}_{\mathfrak{p}}(\mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}}))}\right).$$

By Theorem 5.6, we see that η (and therefore η^ι) is nonzero, while the nonvanishing of h^ε_0 follows from the construction (see Remark 4.2). On the other hand, from global Poitou–Tate duality we have the exact sequence

$$0 \longrightarrow \frac{H^1_\varepsilon(K_{\mathfrak{p}}, \mathbf{T}^{\mathrm{ac}})}{\mathrm{loc}_{\mathfrak{p}}(\mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}}))} \longrightarrow \mathfrak{X}^{\mathrm{rel},\varepsilon}(K, \mathbf{A}^{\mathrm{ac}}) \longrightarrow \mathfrak{X}^{\varepsilon,\varepsilon}(K, \mathbf{A}^{\mathrm{ac}}) \longrightarrow 0. \tag{6.9}$$

Taking Λ_{ac}-torsion in (6.9) and applying Lemma 3.8 we obtain the equality

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\mathrm{str}}(K, \mathbf{A}^{\mathrm{ac}})) = \mathcal{X}^\varepsilon_{\mathrm{tors}} \cdot \eta^\iota \tag{6.10}$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$. Combined with Corollary 4.4 (which applies thanks to Theorem 6.1) and Lemma 5.9, equation (6.10) implies that

$$\mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}} \cdot \mathcal{BF}^\varepsilon_{\mathrm{ac}}}\right) = \mathcal{H}^\varepsilon_{\mathrm{ac}} \cdot \mathcal{X}^\varepsilon_{\mathrm{tors}} \cdot \eta^\iota \tag{6.11}$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$. Since the ideal $\mathcal{U}_{\mathrm{ac}}$ is invertible by the combination of Theorem 4.3 and Corollary 6.3, substituting (6.11) into (6.8), the result follows. □

Note that the formula of Theorem 6.5 has the shape of a Λ_{ac}-adic analogue of the Birch and Swinnerton-Dyer conjecture. Moreover, by the Heegner point main conjecture of Theorem 6.1, it is essentially equivalent to the following Λ_{ac}-adic Gross–Zagier formula.

Theorem 6.6. *Let $\varepsilon \in \{\pm\}$. Under the hypotheses in Theorem 6.1, we have the equality*

$$(L_{p,1}^{\varepsilon,\varepsilon}(f/K)) = (\langle \mathbf{z}^\varepsilon, \mathbf{z}^\varepsilon \rangle_{K_\infty^{\mathrm{ac}}}^{\mathrm{cyc}})$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$.

Proof. Combining Theorem 6.1 and Theorem 6.5, we obtain

$$\begin{aligned}(L_{p,1}^{\varepsilon,\varepsilon}(f/K)) &= \mathcal{R}_{\mathrm{cyc}}^\varepsilon \cdot \mathrm{Char}_{\Lambda_{\mathrm{ac}}}(\mathfrak{X}^{\varepsilon,\varepsilon}(K, \mathbf{A}^{\mathrm{ac}})_{\mathrm{tors}}) \\ &= \mathcal{R}_{\mathrm{cyc}}^\varepsilon \cdot \mathrm{Char}_{\Lambda_{\mathrm{ac}}}\left(\frac{\mathfrak{Sel}^{\varepsilon,\varepsilon}(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda_{\mathrm{ac}} \cdot \mathbf{z}^\varepsilon} \right)^2 \\ &= (\langle \mathbf{z}^\varepsilon, \mathbf{z}^\varepsilon \rangle_{K_\infty^{\mathrm{ac}}}^{\mathrm{cyc}})\end{aligned}$$

in $(\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)/\Lambda_{\mathrm{ac}}^\times$, where the last equality follows from the definition of $\mathcal{R}_{\mathrm{cyc}}^\varepsilon$. □

Remark 6.7. The equality in Theorem 6.6 can easily be rewritten in the form of a Λ_{ac}-adic Gross–Zagier formula. Indeed, the two elements in $\Lambda_{\mathrm{ac}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ appearing in that formula are invariant under the $\mathbf{Z}_p$-isomorphism ι sending $\gamma_{\mathrm{ac}} \mapsto \gamma_{\mathrm{ac}}^{-1}$; letting $y' \in \Lambda_{\mathrm{ac}}^\times$ denote the ratio of those two elements, we can find (by making an appropriate choice of $\Omega_f^{\mathtt{Hida}}$, which is determined up to a p-adic unit) an element $y \in 1 + (\gamma_{\mathrm{ac}} - 1)\Lambda_{\mathrm{ac}}$ such that $y = \iota(y)$ and $y^2 = y'$. Setting $z_\infty^\varepsilon := y\mathbf{z}^\varepsilon$, we thus get another generator of $\Lambda_{\mathrm{ac}} \cdot \mathbf{z}^\varepsilon$ satisfying

$$L_{p,1}^{\varepsilon,\varepsilon}(f/K) = y\iota(y)\langle \mathbf{z}^\varepsilon, \mathbf{z}^\varepsilon \rangle_{K_\infty^{\mathrm{ac}}}^{\mathrm{cyc}} = \langle z_\infty^\varepsilon, z_\infty^\varepsilon \rangle_{K_\infty^{\mathrm{ac}}}^{\mathrm{cyc}}.$$

In particular, specialized at the trivial character of Λ_{ac}, this yields a new proof of Kobayashi's p-adic Gross–Zagier formula [Kob13] (which our formula extends to all characters of Λ_{ac}).

References

[AH06] Adebisi Agboola and Benjamin Howard, *Anticyclotomic Iwasawa theory of CM elliptic curves*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 4, 1001–1048. MR 2266884 (2009b:11098)

[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. MR 3053566

[Ber95] Massimo Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions*, Compositio Math. **99** (1995), no. 2, 153–182. MR 1351834

[BL16] Kâzım Büyükboduk and Antonio Lei, *Iwasawa theory of elliptic modular forms over imaginary quadratic fields at non-ordinary primes*, preprint, `arXiv:1605.05310` (2016).

[Bur17] Ashay A. Burungale, *On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, II: Shimura curves*, J. Inst. Math. Jussieu **16** (2017), no. 1, 189–222. MR 3591965

[Cas17] Francesc Castella, *p-adic heights of Heegner points and Beilinson-Flach classes*, J. Lond. Math. Soc. (2) **96** (2017), no. 1, 156–180.

[CH17] Francesc Castella and Ming-Lun Hsieh, *Heegner cycles and p-adic L-functions*, Math. Ann., to appear (2017).

[Cor02] Christophe Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523. MR 1908058 (2004e:11069a)

[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 (2009m:11088)

[DDT94] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154. MR 1474977 (99d:11067a)

[DI08] Henri Darmon and Adrian Iovita, *The anticyclotomic main conjecture for elliptic curves at supersingular primes*, J. Inst. Math. Jussieu **7** (2008), no. 2, 291–325. MR 2400724 (2009d:11155)

[Dis15] Daniel Disegni, *p-adic heights of Heegner points on Shimura curves*, Algebra Number Theory **9** (2015), no. 7, 1571–1646. MR 3404649

[DLR15] Henri Darmon, Alan Lauder, and Victor Rotger, *Stark points and p-adic iterated integrals attached to modular forms of weight one*, Forum Math. Pi **3** (2015), e8, 95. MR 3456180

[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 (89g:11046)

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[Gre94] Ralph Greenberg, *Iwasawa theory and p-adic deformations of motives*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 193–223. MR 1265554 (95i:11053)

[Har87] Shai Haran, *p-adic L-functions for modular forms*, Compositio Math. **62** (1987), no. 1, 31–46. MR 892149 (88k:11036)

[How04a] Benjamin Howard, *Derived p-adic heights and p-adic L-functions*, Amer. J. Math. **126** (2004), no. 6, 1315–1340. MR 2102397 (2005m:11104)

[How04b] ———, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472. MR 2098397 (2006a:11070)

[How04c] ———, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45. MR 2072210 (2005f:11117)

[How05] ———, *The Iwasawa theoretic Gross-Zagier theorem*, Compos. Math. **141** (2005), no. 4, 811–846. MR 2148200 (2006f:11074)

[Hsi14] Ming-Lun Hsieh, *Special values of anticyclotomic Rankin-Selberg L-functions*, Doc. Math. **19** (2014), 709–767. MR 3247801

[HT93] H. Hida and J. Tilouine, *Anti-cyclotomic Katz p-adic L-functions and congruence modules*, Ann. Sci. École Norm. Sup. (4) **26** (1993), no. 2, 189–259. MR 1209708 (93m:11044)

[HT94] ———, *On the anticyclotomic main conjecture for CM fields*, Invent. Math. **117** (1994), no. 1, 89–147. MR 1269427 (95d:11149)

[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

[Kat78] Nicholas M. Katz, *p-adic L-functions for CM fields*, Invent. Math. **49** (1978), no. 3, 199–297. MR MR513095 (80h:10039)

[Kim07] Byoung Du Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. **143** (2007), no. 1, 47–72. MR 2295194

[Kim14a] ———, *Signed-Selmer groups over the* $\mathbb{Z}_p^2$*-extension of an imaginary quadratic field*, Canad. J. Math. **66** (2014), no. 4, 826–843. MR 3224266

[Kim14b] ———, *Two-variable p-adic L-functions of modular forms for non-ordinary primes*, J. Number Theory **144** (2014), 188–218. MR 3239158

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36. MR 1965358 (2004b:11153)

[Kob13] Shinichi Kobayashi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629. MR 3020170

[LLZ14] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for Rankin-Selberg convolutions of modular forms*, Ann. of Math. (2) **180** (2014), no. 2, 653–771. MR 3224721

[LLZ15] ———, *Euler systems for modular forms over imaginary quadratic fields*, Compos. Math. **151** (2015), no. 9, 1585–1625. MR 3406438

[Loe14] David Loeffler, *p-adic integration on ray class groups and non-ordinary p-adic L-functions*, Iwasawa theory 2012, Contrib. Math. Comput. Sci., vol. 7, Springer, Heidelberg, 2014, pp. 357–378. MR 3586820

[LV15] Matteo Longo and Stefano Vigni, *Plus/minus Heegner points and Iwasawa theory for elliptic curves at supersingular primes*, preprint, `arXiv:1503.07812` (2015).

[LZ14] David Loeffler and Sarah Livia Zerbes, *Iwasawa theory and p-adic L-functions over* $\mathbb{Z}_p^2$*-extensions*, Int. J. Number Theory **10** (2014), no. 8, 2045–2095. MR 3273476

[LZ16] ———, *Rankin-Eisenstein classes in Coleman families*, Res. Math. Sci. **3** (2016), Paper No. 29, 53. MR 3552987

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR 2031496 (2005b:11179)

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558. MR 1983040 (2004e:11050)

[PR87a] Bernadette Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456. MR 928018 (89d:11094)

[PR87b] ———, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** (1987), no. 3, 455–510. MR 903381 (89d:11034)

[PR00] ———, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, Providence, RI, 2000, Translated from the 1995 French original by Leila Schneps and revised by the author. MR 1743508 (2000k:11077)

[Pra06] Kartik Prasanna, *Integrality of a ratio of Petersson norms and level-lowering congruences*, Ann. of Math. (2) **163** (2006), no. 3, 901–967. MR 2215136

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68. MR 1079839 (92f:11151)

[Ski14] Christopher Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, preprint, `arXiv:1405.7294` (2014).

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for GL_2*, Invent. Math. **195** (2014), no. 1, 1–277. MR 3148103

[SZ14] Christopher Skinner and Wei Zhang, *Indivisibility of Heegner points in the multiplicative case*, preprint, `arXiv:1407.1099` (2014).

[Vat02] V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), no. 1, 1–46. MR 1892842 (2003j:11070)

[Wan14] Xin Wan, *Heegner point Kolyvagin system and Iwasawa main conjecture*, preprint, `arXiv:1408.4043` (2014).

[Wan16] ———, *Iwasawa main conjecture for supersingular elliptic curves*, preprint, `arXiv:1411.6352` (2016).

[YZZ13] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies, vol. 184, Princeton University Press, Princeton, NJ, 2013. MR 3237437

[Zha14] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253. MR 3295917

Department of Mathematics, Princeton University, Fine Hall, Princeton, NJ 08544-1000, USA
E-mail address: `fcabello@math.princeton.edu`

Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Science, No. 55 Zhongguancun East Road, Beijing, 100190, China
E-mail address: `xwan@math.ac.cn`