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

FRANCESC CASTELLA AND XIN WAN

ABSTRACT. Let $E/\mathbf{Q}$ be a semistable elliptic curve, and $p > 3$ a prime of good supersingular reduction for E. In this paper we prove the following p-converse to a theorem of Gross–Zagier and Kolyvagin:

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

In particular, this gives new mod p criteria for a rational elliptic curve to satisfy the Birch–Swinnerton-Dyer conjecture. For good ordinary primes p, the implication is due to Skinner and Wei Zhang independently. A key new ingredient in our proof is a result towards a Heegner point main conjecture in the style of Perrin-Riou formulated in this paper.

1. INTRODUCTION

The purpose of this paper is to prove a p-converse to the theorem of Gross–Zagier and Kolyvagin for good supersingular primes. With "supersingular" replaced by "ordinary", such a p-converse is due to Skinner [Ski20] and Wei Zhang [Zha14] independently.

1.1. Statement of the main results.

Let $E/\mathbf{Q}$ be an elliptic curve, and p a prime of good reduction for E. Let $\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) \subset \mathrm{H}^1(\mathbf{Q}, E[p^\infty])$ be the p^∞-Selmer group fitting into the descent exact sequence

$$0 \to E(\mathbf{Q}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) \to Ш(E/\mathbf{Q})[p^\infty] \to 0, \tag{1.1}$$

where $Ш(E/\mathbf{Q})$ is the Tate–Shafarevich group of E. In rank one, the Birch–Swinnerton-Dyer conjecture predicts the finiteness of $Ш(E/\mathbf{Q})$, and that the following are equivalent:

(i) $\mathrm{ord}_{s=1}L(E,s) = 1$;
(ii) $\mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) = 1$.

The implication (i) $\Rightarrow$ (ii) follows from the celebrated works of Gross–Zagier and Kolyvagin in the 1980s, which also yield the finiteness of $Ш(E/\mathbf{Q})$ when $\mathrm{ord}_{s=1}L(E,s) = 1$. More recently, the converse (ii) $\Rightarrow$ (i) was obtained by Skinner [Ski20] and Wei Zhang [Zha14] independently in the p-ordinary case.

The main result of this paper is a proof of the implication (ii) $\Rightarrow$ (i) when p is supersingular for E.

2020 *Mathematics Subject Classification.* 11R23 (primary); 11G05, 11G40 (secondary).

Theorem A. *Let $E/\mathbf{Q}$ be a semistable elliptic curve and $p > 3$ a prime of good supersingular reduction. Then*

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

In particular, if $\mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) = 1$ *then* $\#Ш(E/\mathbf{Q}) < \infty$.

Note that Theorem A concludes the finiteness of the full $Ш(E/\mathbf{Q})$, not just of its p-primary part. In particular, Theorem A yields the following mod p criterion for a rational elliptic curve to satisfy the Birch–Swinnerton-Dyer conjecture. Let $\mathrm{Sel}_p(E/\mathbf{Q}) \subset \mathrm{H}^1(\mathbf{Q}, E[p])$ be the p-Selmer group.

Corollary B. *Let $E/\mathbf{Q}$ be a semistable elliptic curve, and $p > 3$ a prime of good supersingular reduction for E. If* $\mathrm{Sel}_p(E/\mathbf{Q}) \simeq \mathbf{Z}/p\mathbf{Z}$, *then*

$$\mathrm{rank}_{\mathbf{Z}}E(\mathbf{Q}) = \mathrm{ord}_{s=1}L(E,s) = 1$$

and $\#Ш(E/\mathbf{Q}) < \infty$.

Proof. Since $E[p]$ is irreducible as a $G_{\mathbf{Q}_p}$-module by a well-known result of Fontaine (see e.g. [Edi92]), the natural surjection

$$\mathrm{Sel}_p(E/\mathbf{Q}) \to \mathrm{Sel}_{p^\infty}(E/\mathbf{Q})[p]$$

is an isomorphism. By the exact sequence (1.1) and the non-degeneracy of the Cassels–Tate pairing on $Ш(E/\mathbf{Q})/Ш(E/\mathbf{Q})_{\mathrm{div}}$, we thus see that

$$\mathrm{Sel}_p(E/\mathbf{Q}) \simeq \mathbf{Z}/p\mathbf{Z} \quad \Longrightarrow \quad \mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) \simeq \mathbf{Q}_p/\mathbf{Z}_p,$$

and therefore $\mathrm{ord}_{s=1}L(E,s) = 1$ by Theorem A. The conclusion now follows from the work of Gross–Zagier [GZ86] and Kolyvagin [Kol88]. □

Remark 1.1. The mod p criterion of Corollary B for a rational elliptic curve to have algebraic and analytic rank 1 extends to supersingular primes p an analogous criterion in the p-ordinary case[1] originally due to Skinner [Ski20] and Wei Zhang [Zha14]. See the work of Bhargava–Skinner–Zhang [BSZ14] for an application of such criteria to the proof that a large proportion of rational elliptic curves statisfy the Birch–Swinnerton-Dyer conjecture.

1.2. **Main ideas of the proof.** A key input in the proof of the p-converse for ordinary primes in [Ski20] is the "lower bound" divisibility in a Greenberg type Iwasawa main conjecture for Rankin–Selberg convolutions obtained by the second author in [Wan20] by a delicate study of Eisenstein congruences on $\mathrm{GU}(3,1)$. Similarly, a key input in our proof of Theorem A is a divisibility towards a Greenberg type Iwasawa main conjecture for Rankin–Selberg convolutions obtained in recent work of the authors with Zheng Liu [CLW22], extending the main results of [Wan20] to the non-ordinary case.

In this sense, our approach to the p-converse is similar in spirit to Skinner's proof in the p-ordinary case, but our method does not require the hypothesis that $\#Ш(E/\mathbf{Q})[p^\infty] < \infty$ (cf. [Ski20, Rem. 2.9.1(x)]). This improvement is

[1] See also [Wan23] for a proof in the p-ordinary case of a similar mod p criterion for higher weight modular forms.

ultimately explained by the fact that our approach takes advantage of the presence of Heegner points over the anticyclotomic tower, rather than just over the base. In practice, as a key to the proof of Theorem A, in this paper we initiate the study of the anticyclotomic Iwasawa theory of Heegner points at supersingular primes, extending a theory first systematically developed by Perrin-Riou [PR87] in the p-ordinary case.

More precisely, for any elliptic curve $E/\mathbf{Q}$ with good supersingular reduction at p satisfying the condition (automatic if $p > 3$) that

$$a_p := p + 1 - \#E(\mathbf{F}_p) = 0,$$

in §4 we construct signed Λ^{ac}-adic Heegner classes $\mathbf{z}_\infty^\pm$ attached to an imaginary quadratic field K in which p splits and satisfying a "generalized Heegner hypothesis". Here $\Lambda^{\mathrm{ac}} = \mathbf{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)]\!]$ denotes the Iwasawa algebra for the anticyclotomic $\mathbf{Z}_p$-extension K_∞^{ac}/K. We show that the classes $\mathbf{z}_\infty^\pm$ land in a signed Selmer group $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ in the style of Kobayashi's [Kob03], and extending Perrin-Riou's Heegner point main conjecture [PR87, Conj. B] to the supersingular case, we conjecture that the classes $\mathbf{z}_\infty^\pm$ are not Λ^{ac}-torsion, that both $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ and the Pontryagin dual $X^\pm$ of its analogue for torsion coefficients have Λ^{ac}-rank one, and that

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(X^\pm_{\mathrm{tors}}\right) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_\infty^\pm}\right)^2 \tag{1.2}$$

as ideals in Λ^{ac}, where the subscript tors denotes the Λ^{ac}-torsion submodule (see Conjecture 4.8).

Contrary to the usual Selmer groups, the signed Selmer groups satisfy a version of Mazur's control theorem (see Lemma 6.5), and from this one sees that the implication

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

follows from Conjecture 4.8 and the Gross–Zagier formula [YZZ13]. In fact, the divisibility "$\subset$" in (1.2) after inverting p suffices for the above implication.

The proof of Theorem A is thus deduced from the following result, where K is any imaginary quadratic field in which p splits and satisfying the generalized Heegner hypothesis (gen-H) in §2.

Theorem C. *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, and $p > 3$ a prime of good supersingular reduction for E. Assume that:*

(i) *N is squarefree,*
(ii) *some prime $\ell \mid N$ is non-split in K,*
(iii) *if N is odd, then 2 splits in K.*

Then the classes $\mathbf{z}_\infty^\pm$ are not Λ^{ac}-torsion, $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ and $X^\pm$ both have Λ^{ac}-rank one, and

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(X^\pm_{\mathrm{tors}}\right) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_\infty^\pm}\right)^2$$

as ideals in $\Lambda^{\mathrm{ac}}[1/p]$. *If in addition* $E[p]$ *is ramified at every prime* $\ell \mid N^-$, *then the above equality holds in* Λ^{ac}, *and so Conjecture 4.8 holds.*

For the proof of the key Theorem C, we first obtain an explicit reciprocity law (see Theorem 6.2)

$$\mathrm{Log}_{\mathfrak{p}}^{\pm}(\mathrm{res}_{\mathfrak{p}}(\mathbf{z}_{\infty}^{\pm})) = \sigma_{-1,\mathfrak{p}} \cdot \frac{\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}}{\Xi_d}$$

relating the image of $\mathbf{z}_{\infty}^{\pm}$ under certain anticyclotomic signed logarithm maps constructed in §3 to the p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ first studied by Bertolini–Darmon–Prasanna [BDP13]. In particular, it follows from this result and the nonvanishing of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ that the classes $\mathbf{z}_{\infty}^{\pm}$ are not Λ^{ac}-torsion. With this result in hand, in §6.2 we establish the equivalence between our Perrin-Riou Heegner point main conjecture and the Iwasawa–Greenberg main conjecture for $(\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}})^2$. Since divisibilities are preserved under the equivalence, we are thus ultimately able to deduce Theorem C from the main result in [CLW22].

Remark 1.2. Applied for a suitable auxiliary imaginary quadratic field K, the main result of [CLW22] (a divisibility in a 2-variable Iwasawa–Greenberg main conjecture; see the proof of Theorem 5.3) is also a key ingredient in the proof by the second author [Wan21b] of Kobayashi's cyclotomic main conjecture [Kob03]. In that case, Beilinson–Flach classes and their reciprocity laws are used in the passage between different main conjectures. As a result, another key ingredient in [Wan21b] is a study of big Galois representations associated with certain CM Hida families carried out by Burungale–Skinner–Tian [BST21]. In this paper, we do not use Beilinson–Flach classes, and the results of [BST21] are not needed.

Finally, we conclude this Introduction by noting that the method introduced in this paper to deduce a p-converse theorem from a divisibility in an Iwasawa main conjecture for Heegner points[2] has influenced subsequent work in this direction, notably [BT20, BCST22, Kri20] (CM cases) and [CGLS22] (residually reducible case).

Acknowledgements. It is a pleasure to thank Ashay Burungale, Kazim Büyükboduk, Mirela Çiperiani, Antonio Lei, Katharina Müller, Chris Skinner, and Ye Tian for useful conversations related to the topics of this paper. A substantial part of this work was written during visits of the first author to the Morningside Center of Mathematics (MCM) in Beijing, and he would like to thank Ye Tian and MCM for their hospitality and support. We would also like to heartily thank for anonymous referee for a very careful reading of the paper, whose suggestions led to significant improvements in the exposition and a strengthening of our results.

[2]An idea first appeared in an early draft of this paper [CW15] (not for publication), and in [Wan21a] in the ordinary case.

The research of the first author is partially supported by the grants DMS-1946136 and DMS-2101458 from the National Science Foundation. The research of the second author is partially supported by the National Key R&D Program of China 2020YFA0712600 and NSFC grants 11688101, 11621061.

1.3. **Notations.** For every prime p we fix once and for all complex and p-adic embeddings $\mathbf{C} \overset{\iota_\infty}{\hookleftarrow} \overline{\mathbf{Q}} \overset{\iota_p}{\hookrightarrow} \mathbf{C}_p$, and use them to view algebraic numbers as lying in both $\mathbf{C}$ and $\mathbf{C}_p$. For L an algebraic extension of $\mathbf{Q}$ or $\mathbf{Q}_p$, we let G_L denote the corresponding absolute Galois group. If L is a number field and v a finite place of L, we let $\mathrm{rec}_L : \mathbb{A}_L^\times \to G_L^{\mathrm{ab}}$ and $\mathrm{rec}_v : L_v^\times \to G_{L_v}^{\mathrm{ab}}$ be the global and local reciprocity maps of class field theory, respectively. In this paper we take their geometric normalization, i.e., rec_v sends a uniformizer ϖ_v to a geometric Frobenius $\mathrm{Frob}_v \in G_{L_v}/I_v$, where $I_v \subset G_{L_v}$ is the inertia subgroup, and $\mathrm{rec}_L|_{L_v^\times} = \mathrm{rec}_{L_v}$.

2. p-ADIC L-FUNCTIONS

In this section we introduce the p-adic L-functions that will appear in our arguments. Throughout this section, we let $E/\mathbf{Q}$ be an elliptic curve of conductor N, let $f \in S_2(\Gamma_0(N))$ be the associated newform, and let $p \geq 5$ be a prime of good reduction for E. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and discriminant $D_K < 0$. Writing

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

with N^+ the largest factor of N divisible only by primes which are split or ramified in K, we assume that K satisfies the following *generalized Heegner hypothesis*:

(gen-H) N^- is the squarefree product of an even number of primes,

and fix an integral ideal $\mathfrak{N}^+$ such that $\mathcal{O}_K/\mathfrak{N}^+ = \mathbf{Z}/N^+\mathbf{Z}$. In addition, we assume that

(spl) $$(p) = \mathfrak{p}\bar{\mathfrak{p}} \text{ splits in } K,$$

with $\mathfrak{p}$ be the prime K above p induced by ι_p.

Let $\Gamma^{\mathrm{ac}} = \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)$ be the Galois group of the anticyclotomic $\mathbf{Z}_p$-extension of K, and set

$$\Lambda^{\mathrm{ac}} = \mathbf{Z}_p[\![\Gamma^{\mathrm{ac}}]\!], \qquad \Lambda^{\mathrm{ur}} = \Lambda^{\mathrm{ac}} \hat{\otimes}_{\mathbf{Z}_p} \mathbf{Z}_p^{\mathrm{ur}},$$

where $\mathbf{Z}_p^{\mathrm{ur}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$. Note that since $\Gamma^{\mathrm{ac}} \simeq \mathbf{Z}_p$ (non-canonically), Λ^{ac} is isomorphic to a power series ring in one variable (so in particular, is a domain).

We say that an algebraic Hecke character $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbf{C}^\times$ has infinity type $(\ell_1, \ell_2) \in \mathbf{Z}^2$ if $\chi_\infty(z) = z^{\ell_1}\bar{z}^{\ell_2}$ for all $z \in (K \otimes_{\mathbf{Q}} \mathbf{R})^\times \simeq \mathbf{C}^\times$, where χ_∞ is the component of χ at the archimedean place, and we say that a locally algebraic p-adic character $\hat{\chi} : G_K^{\mathrm{ab}} \to \mathbf{C}_p^\times$ has weight $(\ell_1, \ell_2) \in \mathbf{Z}^2$ if $\hat{\chi}(\mathrm{rec}_K(a)) = a^{\ell_1}\bar{a}^{\ell_2}$ for all $a \in (K \otimes_{\mathbf{Q}} \mathbf{Q}_p)^\times$ close to 1 (*cf.* [Ser98, §III.2]).

Associated with a locally algebraic p-adic character $\hat{\chi}$ of weight (ℓ_1, ℓ_2) there is an algebraic Hecke character χ of infinity type (ℓ_1, ℓ_2) given by

$$\chi(a) = \iota_\infty \iota_p^{-1}(\hat{\chi}(\mathrm{rec}_K(a)) a_{\mathfrak{p}}^{-\ell_1} a_{\bar{\mathfrak{p}}}^{-\ell_2}) a_\infty^{\ell_1} \bar{a}_\infty^{\ell_2}, \tag{2.1}$$

where $(a_{\mathfrak{p}}, a_{\bar{\mathfrak{p}}}) = (K \otimes_{\mathbf{Q}} \mathbf{Q}_p)^\times$ and $a_\infty \in (K \otimes_{\mathbf{Q}} \mathbf{R})^\times$ are the components of a at p and ∞, respectively.

Let Π be the cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ such that $L(\Pi, s - 1/2) = L(f, s)$, and put

$$L(f, \chi, s) = L(\Pi_K \otimes \chi, s - 1/2),$$

where Π_K denotes the base change of Π to an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_K)$.

Proposition 2.1. *There exists a square-root p-adic L-function*

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}} \in \Lambda^{\mathrm{ur}}$$

characterized by the following interpolation property. If $N^- \neq 1$, assume that N is squarefree. Then for every locally algebraic character $\hat{\chi} : \Gamma^{\mathrm{ac}} \to \mathbf{C}_p^\times$ of weight $(n, -n)$ with $n \in \mathbf{Z}_{>0}$ and $n \equiv 0 \pmod{p-1}$ and crystalline at both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we have

$$\begin{aligned}\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(\hat{\chi})^2 = \left(\frac{\Omega_p}{\Omega_K}\right)^{4n} \cdot \frac{\Gamma(n)\Gamma(n+1)\chi(x_{\mathfrak{N}^+})^{-1}}{4(2\pi)^{2n+1}\sqrt{D_K}^{2n-1}} \cdot \alpha(f, f_B)^{-1} \\ \times \left(1 - a_p \chi(x_{\bar{\mathfrak{p}}}) p^{-1} + \chi(x_{\bar{\mathfrak{p}}})^2 p^{-1}\right)^2 \cdot L(f, \chi, 1),\end{aligned}$$

where

- $x_{\mathfrak{N}^+} \in \mathbb{A}_K^{\infty,\times}$ *is such that* $\mathrm{ord}_w(x_{\mathfrak{N}^+,w}) = \mathrm{ord}_w(\mathfrak{N}^+)$ *for all finite places w of K,*
- $\Omega_p \in (\mathbf{Z}_p^{\mathrm{ur}})^\times$ *and* $\Omega_\infty \in \mathbf{C}^\times$ *are CM periods attached to K as in* [CH18, §2.5] *and* [JSW17, §4.5.5],
- $\alpha(f, f_B) = \frac{\langle f, f\rangle}{\langle f_B, f_B\rangle}$ *is a ratio of Petersson norms normalized as in* [Pra06, §1] *when $N^- \neq 1$, and $\alpha(f, f_B) = 1$ otherwise.*

Proof. This is a refinement of the p-adic L-function constructed in [BDP13] for $N^- = 1$ and [HB15] for $N^- \neq 1$. As an element in Λ^{ur}, the construction of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ can be found in [BCK21, §4], where it is deduced from an extension of the construction in [CH18]. The proof of the stated interpolation property, building on a explicit Waldspurger formula [Pra06, Thm. 3.2] is then deduced as in [HB15, §8]. □

Remark 2.2. The CM period $\Omega_K \in \mathbf{C}^\times$ in Proposition 2.1 agrees with that in [BDP13, (5.1.16)], but is *different* from the period Ω_∞ defined in [dS87, p. 66] and [HT93, (4.4b)]. In fact, one has

$$\Omega_\infty = 2\pi i \cdot \Omega_K.$$

In terms of Ω_∞, the interpolation formula in Proposition 2.1 reads

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(\hat{\chi})^2 = \left(\frac{\Omega_p}{\Omega_\infty}\right)^{4n} \cdot \frac{\Gamma(n)\Gamma(n+1)\chi(x_{\mathfrak{N}^+})^{-1}}{4(2\pi)^{1-2n}\sqrt{D_K}^{2n-1}} \cdot \alpha(f,f_B)^{-1} \times \left(1 - a_p\chi(x_{\bar{\mathfrak{p}}})p^{-1} + \chi(x_{\bar{\mathfrak{p}}})^2 p^{-1}\right)^2 \cdot L(f,\chi,1),$$

This is the form of the interpolation that we shall use later.

By an extension of Hida's methods [Hid10], the p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ of Proposition 2.1 is known to have vanishing μ-invariant (and in particular, to be nonzero) under a mild hypothesis.

Theorem 2.3. *Assume that $E[p]$ is absolutely irreducible as a G_K-module. Then $\mu(\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}) = 0$.*

Proof. This follows from [Hsi14, Thm. B] for $N^- = 1$ and [Bur17, Thm. B] for $N^- \neq 1$. □

As noted in the proof of Proposition 2.1, the proof of the interpolation property of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ in [BDP13] is based on an explicit from of Waldspurger's formula [Wal85]. Later we shall use the fact that, up to unit, the construction of another element of Λ^{ur} with the same interpolation property as the square of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ (and hence equal to it) can be deduced from the work of Hida and Katz. We explain this in the remainder of this section. (It should be possible to extract the following results from [JSW17, §§5.2-5.3], but we provide full details for the convenience of the reader.)

Let $\mathbf{\Gamma}$ be the Galois group of the $\mathbf{Z}_p^2$-extension of K, and set $\mathbf{\Lambda} = \mathbf{Z}_p[\![\mathbf{\Gamma}]\!]$ and $\mathbf{\Lambda}^{\mathrm{ur}} = \mathbf{\Lambda}\hat{\otimes}_{\mathbf{Z}_p}\mathbf{Z}_p^{\mathrm{ur}}$.

Theorem 2.4 (Katz)**.** *There exists a p-adic L-function*

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}} \in \mathbf{\Lambda}^{\mathrm{ur}}$$

such that for every locally algebraic character $\hat{\chi} : \mathbf{\Gamma} \to \mathbf{C}_p^\times$ of weight (k,j) with $0 \leqslant -j < k$ crystalline at both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we have

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}}(\hat{\chi}) = \left(\frac{\Omega_p}{\Omega_\infty}\right)^{k-j} \cdot \Gamma(k) \cdot \left(\frac{\sqrt{D_K}}{2\pi i}\right)^j \times \left(1 - \chi^{-1}(x_{\mathfrak{p}})p^{-1}\right) \cdot \left(1 - \chi(x_{\bar{\mathfrak{p}}})\right) \cdot L(\chi,0),$$

where Ω_p and Ω_∞ are periods as in Theorem 2.1 and Remark 2.2, respectively, and $L(\chi,s)$ is the Hecke L-function of χ. Moreover, we have the functional equation

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}}((\hat{\chi}^{\mathbf{c}})^{-1}\mathbf{N}^{-1}) = \mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}}(\hat{\chi}),$$

where the equality is up to a p-adic unit and $\hat{\chi}^{\mathbf{c}}$ denotes composition of $\hat{\chi}$ with the non-trivial automorphism of $K/\mathbf{Q}$.

Proof. See [Kat78, §5.3.0], or [dS87, Thm. II.4.14]. for the construction, and [Kat78, §5.3.7] or [dS87, Thm. II.6.4] for the functional equation. □

Write $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ for the newform associated to E, and let $M = \mathrm{lcm}(N, D_K)$.

Theorem 2.5 (Hida)**.** *There exists a p-adic L-function*

$$L_{\mathfrak{p}}^{\mathrm{Hida}} \in \mathrm{Frac}(\mathbf{\Lambda} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$$

such that for every locally algebraic character $\hat{\psi} : \mathbf{\Gamma} \to \mathbf{C}_p^\times$ of weight $(\ell_2, \ell_1) \in \mathbf{Z}^2$ with $\ell_2 \geqslant -\ell_1 > 0$ and crystalline at both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we have

$$L_{\mathfrak{p}}^{\mathrm{Hida}}(\hat{\psi}) = \frac{2^{\ell_1-\ell_2} i^{\ell_2-\ell_1-1} M^{\ell_1+\ell_2+1}}{(2\pi)^{2\ell_2+1} \cdot \langle \theta_{\psi_{\ell_2}}, \theta_{\psi_{\ell_2}} \rangle_M} \cdot \Gamma(\ell_2)\Gamma(\ell_2+1) \times \frac{\mathcal{E}(\psi, f, 1)}{\left(1 - \frac{\psi(x_{\bar{\mathfrak{p}}})}{\psi(x_{\mathfrak{p}})}\right)\left(1 - \frac{\psi(x_{\bar{\mathfrak{p}}})}{p\psi(x_{\mathfrak{p}})}\right)} \cdot L(f, \psi, 1),$$

where $\theta_{\psi_{\ell_2}}$ is the theta series of weight $\ell_2 - \ell_1 + 1 \geqslant 3$ associated to the Hecke character $\psi_{\ell_2} := \psi |\cdot|_{\mathbb{A}_K^\times}^{-\ell_2}$, $\langle g, g \rangle_M$ is the Petersson norm on $\Gamma_1(M)$, and $\mathcal{E}(\psi, f, 1)$ is given by

$$(1 - p^{-1}\psi(x_{\bar{\mathfrak{p}}})\alpha)(1 - p^{-1}\psi(x_{\bar{\mathfrak{p}}})\beta)(1 - \psi^{-1}(x_{\mathfrak{p}})\alpha^{-1})(1 - \psi^{-1}(x_{\mathfrak{p}})\beta^{-1}),$$

with α and β the roots of $X^2 - a_p X + p$.

Proof. This is a special case of the p-adic Rankin–Selberg L-functions constructed by Hida [Hid88]. In the form stated here, the result is given [LLZ15, Thm. 6.1.3(ii)] after reversing the roles $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ (which accounts for our unconventional ordering (ℓ_2, ℓ_1) in the statement). □

Since p is odd, the Galois group $\mathbf{\Gamma}$ decomposes as the product $\mathbf{\Gamma}^+ \times \mathbf{\Gamma}^-$ of its eigenspaces under the action of complex conjugation, with the minus eigenspace corresponding to the anticyclotomic Galois group $\Gamma^{\mathrm{ac}} \simeq \mathbf{\Gamma}^-$. Thus in particular $\mathbf{\Lambda} \simeq \Lambda^{\mathrm{ac}} \hat{\otimes}_{\mathbf{Z}_p} \mathbf{Z}_p[\![\mathbf{\Gamma}^+]\!]$.

Definition 2.6. Let $L_{\mathfrak{p}}^{\mathrm{RS}}$ to be the element in the fraction field of $\mathbf{\Lambda}^{\mathrm{ur}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ given by

$$L_{\mathfrak{p}}^{\mathrm{RS}} := \frac{h_K}{w_K} \cdot \mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz},-} \cdot L_{\mathfrak{p}}^{\mathrm{Hida}},$$

where h_K is the class number of K, $w_K = |\mathcal{O}_K^\times|$, and $\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz},-}$ is the image of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}}$ under the map $\mathbf{\Lambda}^{\mathrm{ur}} \to \mathbf{\Lambda}^{\mathrm{ur}}$ given by $\gamma \mapsto \gamma(\gamma^{\mathbf{c}})^{-1}$.

Let $\mathrm{pr}_{\Gamma^{\mathrm{ac}}}(L_{\mathfrak{p}}^{\mathrm{RS}})$ be the image of $L_{\mathfrak{p}}^{\mathrm{RS}}$ under the map induced by the natural projection $\mathbf{\Gamma} \to \mathbf{\Gamma}^- \simeq \Gamma^{\mathrm{ac}}$, which *a priori* defines an element in $\mathrm{Frac}(\Lambda^{\mathrm{ur}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$, and put

$$L_{\mathfrak{p}}^{\mathrm{BDP}} := (\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}})^2. \tag{2.2}$$

Proposition 2.7. *If $N^- \neq 1$, assume that N is squarefree. Then $\mathrm{pr}_{\Gamma^{\mathrm{ac}}}\left(L_{\mathfrak{p}}^{\mathrm{RS}}\right)$ is an element in Λ^{ur} and*

$$\left(\mathrm{pr}_{\Gamma^{\mathrm{ac}}}\left(L_{\mathfrak{p}}^{\mathrm{RS}}\right)\right) = \left(L_{\mathfrak{p}}^{\mathrm{BDP}} \cdot \alpha(f, f_B)\right)$$

as ideals in Λ^{ur}.

Proof. It suffices to show that after multiplication by a unit in Λ^{ur} the p-adic L-function $\mathrm{pr}_{\Gamma^{\mathrm{ac}}}(L_{\mathfrak{p}}^{\mathrm{RS}})$ satisfies the same interpolation property as the product $L_{\mathfrak{p}}^{\mathrm{BDP}} \cdot \alpha(f, f_B)$.

Let $\hat{\psi}$ be a character of $\mathbf{\Gamma}$ as in Theorem 2.5 factoring through Γ^{ac}, hence of weight $(n, -n)$ for some $n \in \mathbf{Z}_{>0}$; then $\langle \theta_{\psi_n}, \theta_{\psi_n} \rangle_M$ is the period appearing in the interpolation formula. Since θ_{ψ_n} has weight $2n+1$, by Hida's formula for the adjoint L-value [HT93, Thm .7.1] and Dirichlet's class number formula we obtain

$$\langle \theta_{\psi_n}, \theta_{\psi_n} \rangle_M \ \sim \ \frac{\Gamma(2n+1)}{\pi^{2n+1}} \cdot \frac{h_K}{w_K} \cdot L(\chi_n(\chi_n^{\mathbf{c}})^{-1}, 1),$$

where $\sim$ means the ratio between the two terms is interpolated by a unit in Λ^{ur} as n varies. Since $L(\chi_n(\chi_n^{\mathbf{c}})^{-1}, 1) = L(\chi_n(\chi_n^{\mathbf{c}})^{-1}\mathbf{N}^{-1}, 0)$ and $\chi_n(\chi_n^{\mathbf{c}})^{-1}\mathbf{N}^{-1}$ has infinity type $(2n+1, 1-2n)$ within the range of interpolation of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz}}$, by Theorem 2.4 it follows that

(2.3)

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{Katz},-}(\hat{\psi}) \ \sim \ \pi^{4n} \cdot \left(\frac{\Omega_p}{\Omega_\infty}\right)^{4n} \cdot \left(1 - \frac{\psi(x_{\bar{\mathfrak{p}}})}{\psi(x_{\mathfrak{p}})}\right)\left(1 - \frac{\psi(x_{\bar{\mathfrak{p}}})}{p\psi(x_{\mathfrak{p}})}\right) \cdot \langle \theta_{\psi_n}, \theta_{\psi_n} \rangle_M \cdot \frac{w_K}{h_K}.$$

Noting that the modified Euler factor $\mathcal{E}(\psi, f, 1)$ in Theorem 2.5 satisfies

$$\mathcal{E}(\psi, f, 1) = (1 - a_p\psi(x_{\bar{\mathfrak{p}}})p^{-1} + \psi(x_{\bar{\mathfrak{p}}})^2 p^{-1})^2,$$

substituting (2.3) into the definition of $L_{\mathfrak{p}}^{\mathrm{RS}}$ we thus see that

$$\mathrm{pr}_{\Gamma^{\mathrm{ac}}}(L_{\mathfrak{p}}^{\mathrm{RS}})(\hat{\psi}) \ \sim \ \mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(\hat{\psi})^2 \cdot \alpha(f, f_B)$$

by comparing the interpolation formulas in Theorem 2.5 and Theorem 2.1, and this yields the result. □

3. Local results

The results in this section will be used to study the local properties at the primes above p of the signed Heegner classes constructed later in the paper. Throughout this section, we let $E/\mathbf{Q}_p$ be an elliptic curve with good supersingular reduction at an odd prime p with

$$a_p := p + 1 - \#\tilde{E}(\mathbf{F}_p) = 0.$$

Let $\mathbf{Q}_{p,\infty}$ (resp. k_∞) be the cyclotomic (resp. unramified) $\mathbf{Z}_p$-extensions of $\mathbf{Q}_p$, and denote by L_∞ the compositum of $\mathbf{Q}_{p,\infty}$ and k_∞. Let

$$U := \mathrm{Gal}(k_\infty/\mathbf{Q}_p), \quad \Gamma := \mathrm{Gal}(\mathbf{Q}_{p,\infty}/\mathbf{Q}_p), \quad G_\infty := \mathrm{Gal}(L_\infty/\mathbf{Q}_p) \simeq U \times \Gamma,$$

and fix topological generators $\gamma \in \Gamma$ and $u \in U$, with u corresponding to the arithmetic Frobenius. Finally, we let $\Lambda = \mathbf{Z}_p[\![G_\infty]\!]$ and, letting $T = T_pE$ be the p-adic Tate module of E, we set

$$\mathbf{T}_p := T \hat{\otimes}_{\mathbf{Z}_p} \Lambda, \tag{3.1}$$

equipped with the diagonal Galois action, where $G_{\mathbf{Q}_p}$ acts on the second factor via the tautological character $G_{\mathbf{Q}_p} \twoheadrightarrow G_\infty \hookrightarrow \Lambda^\times$.

3.1. **Local points.** Let $k/\mathbf{Q}_p$ be a finite unramified extension with ring of integers $\mathcal{O}_k$ and maximal ideal $\mathfrak{m}_k$, and denote by σ the Frobenius automorphism of k. For $f \in k[\![X]\!]$, we let $f^\sigma \in k[\![X]\!]$ denote the result of applying σ to the coefficients of f.

Fix $z \in \mathcal{O}_k^\times$, and consider

$$\log_{\varphi_z}(X) = \sum_{j=1}^{\infty} (-1)^j \frac{\varphi_z^{(2j)}(X)}{p^j},$$

where $\varphi_z^{(2j)}(X) = \varphi_z^{\sigma^{2j-1}} \circ \cdots \circ \varphi_z^\sigma \circ \varphi_z(X)$ with $\varphi_z(X) = (X+z)^p - z^p$. For every $u = \sum_{\ell=0}^\infty b_\ell t^\ell \in \mathcal{O}_k[\![t]\!]$ and $f \in k[\![X]\!]$, let

$$u(\varphi_z)(f)(X) := \sum_{\ell=0}^{\infty} b_\ell^{\sigma^\ell} f(\varphi_z^{(\ell)}(X)).$$

As in [Kob03], we say that f has *Honda type* u if $u(\varphi_z)(f) \equiv 0 \pmod{p}$ and $f'(0) = 1$.

Lemma 3.1. *For every $n \geqslant 0$, $\log_{\varphi_z^{\sigma^{-n}}}$ is of Honda type $t^2 + p$.*

Proof. A straightforward computation (cf. [Kob03, §8.2]). □

Let $\hat{E}$ be the formal group associated to the minimal model of E over $\mathbf{Z}_p$. By Honda theory (see [Kob03, Thm. 8.3]), it follows from Lemma 3.1 that for every $n \geqslant 0$ there exists a formal group $\mathscr{F}_z^{[n]}$ over $\mathcal{O}_k$ whose logarithm is given by $\log_{\varphi_z^{\sigma^{-n}}}$ and for which the composition

$$\mathfrak{s}_n := \exp_{\hat{E}} \circ \log_{\mathscr{F}_z^{[n]}} : \mathscr{F}_z^{[n]} \to \hat{E} \tag{3.2}$$

is an isomorphism. Let $\epsilon_{n,z} \in \mathscr{F}_z^{[n]}(\mathfrak{m}_k)$ be such that

$$\log_{\mathscr{F}_z^{[n]}}(\epsilon_{n,z}) = \sum_{j=1}^{\infty} (-1)^{j-1} z^{\sigma^{-(n+2j)}} p^j$$

(this exists since $\log_{\mathscr{F}_z^{[n]}}$ defines an isomorphism $\mathscr{F}_z^{[n]}(\mathfrak{m}_k) \xrightarrow{\sim} \mathfrak{m}_k$), and define $\widetilde{c}_{n,z} \in \hat{E}(\mathfrak{m}_{k(\mu_{p^n})})$ by

$$\widetilde{c}_{n,z} := \mathfrak{s}_n\big(\epsilon_{n,z}[+]_{\mathscr{F}_z^{[n]}} z^{\sigma^{-n}}(\zeta_{p^n} - 1)\big), \tag{3.3}$$

where ζ_{p^n} is a primitive p^n-th root of unity. For varying n, we shall assume that the roots ζ_{p^n} have been chosen compatibly, so that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$.

Lemma 3.2. *Let $\mathrm{Tr}_n^{n+1} : \hat{E}(\mathfrak{m}_{k(\mu_{p^{n+1}})}) \to \hat{E}(\mathfrak{m}_{k(\mu_{p^n})})$ be the trace map. If $z \in \mathcal{O}_k^\times$ is a root of unity, then*

$$\mathrm{Tr}_n^{n+1}(\widetilde{c}_{n+1,z}) = -\widetilde{c}_{n-1,z}.$$

for every positive n.

Proof. Since $\mathrm{loc}_{\hat{E}}$ is injective on $\hat{E}(\mathfrak{m}_{k(\mu_{p^\infty})})$ by [Kob03, Prop. 8.7], it suffices to check the stated relation after applying $\log_{\hat{E}}$. Since z is a root of unity of order prime to p, for every $k \geqslant 0$ we have

$$(\varphi_z^{\sigma^{-n-1}})^{(2k)} = z^{\sigma^{2k-n-1}}(\zeta_{p^{n+1-2k}} - 1),$$

and this is zero for $2k > n+1$. Hence

$$\begin{aligned}
&\log_{\hat{E}}(\mathrm{Tr}_n^{n+1}(\widetilde{c}_{n+1,z})) \\
&= \mathrm{Tr}_n^{n+1}\left(\sum_{j=1}^{\infty}(-1)^{j-1}z^{\sigma^{-(n+1+2j)}}p^j + \sum_{k=0}^{\infty}(-1)^k\frac{z^{\sigma^{2k-n-1}}(\zeta_{p^{n+1-2k}}-1)}{p^k}\right) \\
&= p\sum_{j=1}^{\infty}(-1)^{j-1}z^{\sigma^{-(n+1+2j)}}p^j - pz^{\sigma^{-n-1}} + p\sum_{k=1}^{\infty}(-1)^k\frac{z^{\sigma^{2k-n-1}}(\zeta_{p^{n+1-2k}}-1)}{p^k} \\
&= -\log_{\hat{E}}(\widetilde{c}_{n-1,z}),
\end{aligned}$$

using that $\mathrm{Tr}_n^{n+1}(z^{\sigma^{-n-1}}(\zeta_{p^{n+1}}-1)) = -pz^{\sigma^{-n-1}}$ for the second equality. □

Let k_n be the subfield of $k(\mu_{p^{n+1}})$ with $\mathrm{Gal}(k_n/k) \simeq \mathbf{Z}/p^n\mathbf{Z}$, let $\mathfrak{m}_{k_n} \subset k_n$ be the maximal ideal, and denote by

$$c_{n,z} \in \hat{E}(\mathfrak{m}_{k_n}) \tag{3.4}$$

the image of $\widetilde{c}_{n+1,z}$ under the trace map $\hat{E}(\mathfrak{m}_{k(\mu_{p^{n+1}})}) \to \hat{E}(\mathfrak{m}_{k_n})$. Let

$$\tilde{\omega}_n^+(X) := \prod_{\substack{2\leqslant m\leqslant n\\ m \text{ even}}} \Phi_m(X+1), \qquad \tilde{\omega}_n^-(X) := \prod_{\substack{1\leqslant m\leqslant n\\ m \text{ odd}}} \Phi_m(X+1),$$

where $\Phi_m(X) = \sum_{i=0}^{p-1} X^{ip^{m-1}}$ is the p^m-th cyclotomic polynomial. Set also $\omega_n^\pm(X) = X\tilde{\omega}_n^\pm(X)$, and note that

$$\omega_n(X) := (X+1)^{p^n} - 1 = X\tilde{\omega}_n^\mp(X)\tilde{\omega}_n^\pm(X). \tag{3.5}$$

Let also $\Lambda_n = \mathbf{Z}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)]$.

Proposition 3.3. *There is an exact sequence*

$$0 \to \hat{E}(\mathfrak{m}_k) \to \Lambda_n c_{n,z} \oplus \Lambda_{n-1}c_{n-1,z} \to \hat{E}(\mathfrak{m}_{k_n}) \to 0,$$

where the first map is the diagonal embedding and the second map is $(P,Q) \mapsto P[-]_{\hat{E}}Q$.

Proof. This follows from Lemma 3.2 by the same argument as in the proof of [Kob03, Prop. 8.12] (see also [Kim14, Prop. 2.6]). □

Now let $k = \mathbf{Q}_{p^m} \subset \mathbf{Q}_p^{\mathrm{ur}}$ be the unramified extension of $\mathbf{Q}_p$ of degree p^m, and write $\mathfrak{m}_{m,n} \subset k_{m,n}$ for the previously defined $\mathfrak{m}_k \subset k$ with $k = \mathbf{Q}_{p^m}$. We identify Λ with the power series $\mathbf{Z}_p[\![X,U]\!]$ setting $X = \gamma - 1$, $U = u - 1$

for the topological generators γ and u fixed at the beginning of this section. We also set

$$\Lambda_{m,n} := \Lambda/(\omega_m(U), \omega_n(X)), \quad \Lambda^{\pm}_{m,n} := \Lambda/(\omega_m(U), \omega_n^{\pm}(X)) = \Lambda_{m,n}/(\omega_n^{\pm}(X)),$$

so that $\Lambda_{m,n} \simeq \mathbf{Z}_p[\mathrm{Gal}(k_{m,n}/\mathbf{Q}_p)]$ and $\Lambda^{\pm}_{m,n} \simeq \tilde{\omega}_n^{\mp}(X)\Lambda_{m,n}$ by the relation (3.5).

Lemma 3.4. *For $m, n \geqslant 0$ there exists $c_{m,n} \in \hat{E}(\mathfrak{m}_{m,n})$ such that*

$$\mathrm{Tr}^{m,n}_{m-1,n}(c_{m,n}) = c_{m-1,n}$$
$$\mathrm{Tr}^{m,n}_{m,n-1}(c_{m,n}) = -c_{m,n-2},$$

where $\mathrm{Tr}^{m,n}_{m',n'}$ is the trace map $\hat{E}(\mathfrak{m}_{m,n}) \to \hat{E}(\mathfrak{m}_{m',n'})$.

Proof. We first show the existence of points $\widetilde{c}_{m,n} \in \hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^m}(\mu_{p^{n+1}})})$ satisfying the stated compatibilities with respect to the trace maps

$$\mathrm{Tr}^{m,n}_{m',n'} : \hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^m}(\mu_{p^{n+1}})}) \to \hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^{m'}}(\mu_{p^{n'+1}})}). \tag{3.6}$$

The result will then follow by taking $c_{m,n}$ to be the image of $\widetilde{c}_{m,n}$ under the trace map $\hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^m}(\mu_{p^{n+1}})}) \to \hat{E}(\mathfrak{m}_{m,n})$.

Let $\mathbf{Z}_{p^m}$ be the ring of integers of $\mathbf{Q}_{p^m}$, and consider the module

$$\mathcal{O}_\infty := \varprojlim_m \mathbf{Z}_{p^m}$$

with limit with respect to the trace maps. As shown in [LZ14, Prop. 3.2], the module $\mathcal{O}_\infty$ is free of rank one over $\mathbf{Z}_p[\![U]\!]$. Let $d = \{d_m\}_m$ be a generator of $\mathcal{O}_\infty$ as a $\mathbf{Z}_p[\![U]\!]$-module, and write $d_m = \sum_j a_{m,j}\zeta_{m,j}$ with $a_{m,j} \in \mathbf{Z}_p$ and $\zeta_{m,j}$ roots of unity (as is possible by the normal basis theorem). Define $\widetilde{c}_{m,n}$ by

$$\widetilde{c}_{m,n} := \sum_j a_{m,j}\widetilde{c}_{n,\zeta_{m,j}}, \tag{3.7}$$

where $c_{n,\zeta_{m,j}} \in \hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^m}(\mu_{p^{n+1}})})$ is as in (3.3). Put $\mathrm{Tr} = \mathrm{Tr}^{m,n}_{m-1,n}$ for the trace map as in (3.6). Then similarly as in the proof of Lemma 3.2 we find:

$$\begin{aligned}
&\log_{\hat{E}}(\mathrm{Tr}(\widetilde{c}_{m,n})) \\
&= \mathrm{Tr}\left(\sum_{j=1}^{\infty}(-1)^{j-1}\sum_j a_{m,j}\zeta_{m,j}^{\sigma^{-(n+1+2j)}}p^j + \sum_{k=0}^{\infty}(-1)^k\frac{\sum_j a_{m,j}\zeta_{m,j}^{\sigma^{2k-n-1}}(\zeta_{p^{n+1-2k}}-1)}{p^k}\right) \\
&= \sum_{j=1}^{\infty}(-1)^{j-1}\mathrm{Tr}(d_m)^{\sigma^{-(n+1+2j)}}p^j + \sum_{k=0}^{\infty}(-1)^k\frac{\mathrm{Tr}(d_m)^{\sigma^{2k-n-1}}(\zeta_{p^{n+1-2k}}-1)}{p^k} \\
&= \log_{\hat{E}}(\widetilde{c}_{m-1,n})
\end{aligned}$$

using that $a_{m,j}$ is fixed by σ for the second equality and that $\mathrm{Tr}(d_m) = d_{m-1}$ for the third one. Since the second norm relation for $\widetilde{c}_{m,n}$ (i.e., with respect to $\mathrm{Tr}^{m,n}_{m,n-1}$) is immediate from Lemma 3.2, this concludes the proof. □

Keeping the notations in Lemma 3.4, define the plus/minus-norm subgroups $\hat{E}^{\pm}(\mathfrak{m}_{m,n}) \subset \hat{E}(\mathfrak{m}_{m,n})$ by

$$\hat{E}^{+}(\mathfrak{m}_{m,n}) := \big\{P \in \hat{E}(\mathfrak{m}_{m,n}) \mid \mathrm{Tr}^{m,n}_{m,\ell+1}(P) \in \hat{E}(\mathfrak{m}_{m,\ell}) \text{ for all } 0 \leqslant \ell < n, \text{ even } \ell\big\},$$

$$\hat{E}^{-}(\mathfrak{m}_{m,n}) := \big\{P \in \hat{E}(\mathfrak{m}_{m,n}) \mid \mathrm{Tr}^{m,n}_{m,\ell+1}(P) \in \hat{E}(\mathfrak{m}_{m,\ell}) \text{ for all } -1 \leqslant \ell < n, \text{ odd } \ell\big\}.$$

We conclude this section with the following definition of subsequences of $\{c_{m,n}\}_{m,n}$ which we shall use in the next section:

$$c^{+}_{m,n} = \begin{cases} c_{m,n} & \text{if } n \text{ is even,} \\ c_{m,n-1} & \text{if } n \text{ is odd,} \end{cases} \qquad c^{-}_{m,n} = \begin{cases} c_{m,n-1} & \text{if } n \text{ is even,} \\ c_{m,n} & \text{if } n \text{ is odd.} \end{cases} \tag{3.8}$$

From Lemma 3.4, we see that $c^{\pm}_{m,n} \in \hat{E}^{\pm}(\mathfrak{m}_{m,n})$.

Corollary 3.5. *The element $c^{\pm}_{m,n}$ generates $\hat{E}^{\pm}(\mathfrak{m}_{m,n})$ as a $\Lambda_{m,n}$-module, and we have*

$$\Lambda_{m,n}c^{\pm}_{m,n} \simeq \Lambda_{m,n}/(\omega^{\pm}_n(X)) \simeq \tilde{\omega}^{\mp}_n(X)\Lambda_{m,n}.$$

Proof. The first part follows immediately from Proposition 3.3. For the second part, suppose first that n is even and consider $c^{+}_{m,n}$. Using Lemma 3.4 repeatedly we obtain

$$\omega^{+}_n(X)c_{m,n} = \omega^{+}_{n-2}(X)\mathrm{Tr}^{m,n}_{m,n-1}(c_{m,n}) = -\omega^{+}_{n-2}(X)c_{m,n-2} = \cdots = \pm X c_{m,0} = 0.$$

Thus we have a natural surjection $\Lambda_{m,n}/(\omega^{+}_n(X)) \to \Lambda_{m,n}c^{+}_{m,n}$, which is readily seen to be an isomorphism by comparing $\mathbf{Z}_p$-ranks. Since multiplication by $\tilde{\omega}^{-}_n(X)$ on $\Lambda_{n,m}$ defines an isomorphism $\Lambda_{m,n}/(\omega^{+}_n(X)) \simeq \tilde{\omega}^{-}_n(X)\Lambda_{m,n}$ this completes the proof of the result in this case. The proof in the other cases is the same. □

3.2. **The plus/minus Coleman maps.** Let T be the p-adic Tate module of E, and consider the local Tate pairing

$$\langle\ ,\ \rangle_{m,n} : \mathrm{H}^1(k_{m,n}, E[p^\infty]) \times \mathrm{H}^1(k_{m,n}, T) \to \mathrm{H}^2(k_{m,n}, \mathbf{Q}_p/\mathbf{Z}_p(1)) \simeq \mathbf{Q}_p/\mathbf{Z}_p$$

obtained as the limit of the usual local Tate pairing associated to the Weil pairing $E[p^j] \times E[p^j] \to \mu_{p^j} = \mathbf{Z}/p^j\mathbf{Z}(1)$. We denote by

$$(\ ,\ )_{m,n} : \hat{E}(\mathfrak{m}_{m,n}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \times \mathrm{H}^1(k_{m,n}, T) \to \mathbf{Q}_p/\mathbf{Z}_p$$

the map obtained by pre-composing $\langle\ ,\ \rangle_{m,n}$ with the Kummer map $\hat{E}(\mathfrak{m}_{m,n}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{H}^1(k_{m,n}, E[p^\infty])$.

Definition 3.6. Let $\mathrm{H}^1_{\pm}(k_{m,n}, T)$ be the orthogonal complement of $E^{\pm}(k_{m,n}) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ under $(\ ,\ )_{m,n}$.

Let $c^{\pm}_{m,n}$ be as in (3.8), and define

$$P^{\pm}_{m,n} : \mathrm{H}^1(k_{m,n}, T) \to \Lambda_{m,n} = \mathbf{Z}_p[\mathrm{Gal}(k_{m,n}/\mathbf{Q}_p)]$$

by

$$P^{\pm}_{m,n}(x) = (-1)^{[\frac{n+1}{2}]} \sum_{\sigma \in \mathrm{Gal}(k_{m,n}/\mathbf{Q}_p)} ((c^{\pm}_{m,n})^{\sigma}, x)_{m,n}\, \sigma.$$

Corollary 3.5 easily implies that

$$\mathrm{H}^1_{\pm}(k_{m,n}, T) = \ker(P^{\pm}_{m,n}) \tag{3.9}$$

and the image of $P^{\pm}_{m,n}$ is contained in $\tilde{\omega}_n^{\mp}(X)\Lambda_{m,n}$ (see [Kob03, Props. 8.18, 8.19]). Thus there is a unique map $\mathrm{Col}^{\pm}_{m,n} : \mathrm{H}^1(k_{m,n}, T) \to \Lambda^{\pm}_{m,n}$ making the following diagram commutative

$$\begin{array}{ccc} \mathrm{H}^1(k_{m,n}, T) & \xrightarrow{\mathrm{Col}^{\pm}_{m,n}} & \Lambda^{\pm}_{m,n} \\ \downarrow & & \downarrow{\scriptstyle \times \tilde{\omega}_n^{\mp}(X)} \\ \mathrm{H}^1(k_{m,n}, T)/\mathrm{H}^1_{\pm}(k_{m,n}, T) & \xrightarrow{P^{\pm}_{m,n}} & \Lambda_{m,n}, \end{array}$$

where the right vertical map is given by multiplication by $\tilde{\omega}_n^{\mp}(X)$.

Proposition 3.7. *The maps $\mathrm{Col}^{\pm}_{m,n}$ are surjective, and for any $n > n'$, $m > m'$ the diagram*

$$\begin{array}{ccc} \mathrm{H}^1(k_{m,n}, T) & \xrightarrow{\mathrm{Col}^{\pm}_{m,n}} & \Lambda^{\pm}_{m,n} \\ \downarrow & & \downarrow \\ \mathrm{H}^1(k_{m',n'}, T) & \xrightarrow{\mathrm{Col}^{\pm}_{m',n'}} & \Lambda^{\pm}_{m',n'} \end{array}$$

commutes, where the left (resp. right) vertical map is given by corestriction (resp. the natural projection).

Proof. This follows from the same argument as in Propositions 8.21 and 8.23 of [Kob03]. □

Recall the $G_{\mathbf{Q}_p}$-module $\mathbf{T}_p$ in (3.1), and note that Shapiro's lemma yields an isomorphism

$$\mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p) \simeq \varprojlim_{m,n} \mathrm{H}^1(k_{m,n}, T), \tag{3.10}$$

where the limit is with respect to corestriction, and by Proposition 3.7 we may consider the map

$$\mathrm{Col}^{\pm} := \varprojlim_{m,n} \mathrm{Col}^{\pm}_{m,n} : \mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p) \to \Lambda, \tag{3.11}$$

noting that $\varprojlim_{m,n} \Lambda^{\pm}_{m,n} \simeq \Lambda$. Let $\mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p)$ be the submodule of $\mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p)$ corresponding to $\varprojlim_{m,n} \mathrm{H}^1_{\pm}(k_{m,n}, T)$ under (3.10).

Proposition 3.8. *The map* $\mathrm{Col}^{\pm}$ *defines an exact sequence*

$$0 \to \mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p) \to \mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p) \xrightarrow{\mathrm{Col}^{\pm}} \Lambda \to 0$$

between free Λ*-modules of rank* 1, 2, *and* 1, *respectively.*

Proof. By (3.9) and Proposition 3.7, the map $\mathrm{Col}^{\pm}$ defines an isomorphism $\mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p)/\mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p) \simeq \Lambda$. Note that the short exact sequence in the statement splits, and so $\mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p)$ is a direct summand of $\mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p)$. Since by [PR94, Prop. 3.2.1] the Λ-module $\mathrm{H}^1(\mathbf{Q}_p, \mathbf{T}_p)$ is free of rank 2, the result follows. □

3.3. **The plus/minus Logarithm maps.** As shown in the proof of Corollary 3.5, if $\epsilon = (-1)^n$ then

$$\omega_n^{\epsilon}(X) c_{m,n} = 0. \tag{3.12}$$

Via the natural inclusion

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

where $M^{\perp}$ denotes the orthogonal complement of M with respect to the local Tate pairing $(\ ,\ )_{m,n}$, we shall view $c_{m,n} \in \hat{E}(\mathfrak{m}_{m,n})$ as an element in $\mathrm{H}^1_{\pm}(k_{m,n}, T)$.

Lemma 3.9. $\mathrm{H}^1_{\pm}(k_{m,n}, T)$ *is a free* $\Lambda_{m,n}$*-module of rank one.*

Proof. This is an immediate consequence of [DI08, Lem. 3.9]. □

Lemma 3.10. *Let* $\epsilon = (-1)^n$. *There exists a unique class*

$$\beta^{\epsilon}_{m,n} \in \mathrm{H}^1_{\epsilon}(k_{m,n}, T)/\omega_n^{\epsilon}(X)\mathrm{H}^1_{\epsilon}(k_{m,n}, T)$$

such that $\tilde{\omega}_n^{-\epsilon}(X)\beta^{\epsilon}_{m,n} = c_{m,n}$.

Proof. Since multiplication by $\tilde{\omega}_n^{-\epsilon}(X)$ on $\Lambda_{m,n}$ yields an isomorphism

$$\Lambda_{m,n}/(\omega_n^{\epsilon}(X)) \simeq \tilde{\omega}_n^{-\epsilon}(X)\Lambda_{m,n},$$

the result follows from (3.12) and Lemma 3.9. □

Define $b^{\pm}_{m,n} \in \mathrm{H}^1_{\pm}(k_{m,n}, T)/\omega_n^{\pm}(X)\mathrm{H}^1_{\pm}(k_{m,n}, T)$ by

$$\begin{cases} b^{+}_{m,n} := (-1)^{n/2}\beta^{+}_{m,n} & \text{if } n \text{ is even,} \\ b^{-}_{m,n} := (-1)^{(n+1)/2}\beta^{-}_{m,n} & \text{if } n \text{ is odd.} \end{cases}$$

Proposition 3.11. *The class* $\beta^{\pm}_{m,n}$ *generates the free rank one* $\Lambda^{\pm}_{m,n}$*-module* $\mathrm{H}^1_{\pm}(k_{m,n}, T)/\omega_n^{\pm}(X)\mathrm{H}^1_{\pm}(k_{m,n}, T)$, *and the sequences*

$$\{b^{+}_{m,n}\}_{n \text{ even},m} \quad \{b^{-}_{m,n}\}_{n \text{ odd},m}$$

are compatible under corestriction.

Proof. Since $E(k_{m,n})$ is torsion-free, Corollary 3.5 gives $\hat{E}^{\pm}(\mathfrak{m}_{m,n}) \otimes \mathbf{Z}_p = \Lambda_{m,n} c_{m,n}$, and hence for the first part of the lemma it suffices to show that

$$\tilde{\omega}_n^{\mp} \mathrm{H}^1_{\pm}(k_{m,n}, T) = \mathrm{im}\big(\delta : \hat{E}^{\pm}(\mathfrak{m}_{m,n}) \otimes \mathbf{Z}_p \to \mathrm{H}^1(k_{m,n}, T)\big), \tag{3.13}$$

where δ is the Kummer map. Since local points are isotropic under $(\ ,\ )_{m,n}$, we have $\mathrm{im}(\delta) \subset \mathrm{H}^1_{\pm}(k_{m,n}, T)$; and since $\mathrm{H}^1(k_{m,n}, T)$ is $\Lambda_{m,n}$-free, from (3.12) we also have $\mathrm{im}(\delta) \subset \tilde{\omega}_n^{\mp}(X)\mathrm{H}^1(k_{m,n}, T)$. Thus

$$\mathrm{im}(\delta) \subset \mathrm{H}^1_{\pm}(k_{m,n}, T) \cap \tilde{\omega}_n^{\mp}(X)\mathrm{H}^1(k_{m,n}, T),$$

which implies (3.13). The second part of the lemma follows from the same argument as in [DI08, Lem. 2.9]. We explain the case n even, and the odd case is shown similarly. Let $\tilde{c}_{m,n}$ be a lift of $c_{m,n}$ to $\mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p)$. By Lemma 3.4 we then have

$$\tilde{c}_{m,n} \equiv -\Phi_{n-1}(X)\tilde{c}_{m,n-2} \pmod{\omega_{n-1}(X)\mathrm{H}^1_{+}(\mathbf{Q}_p, \mathbf{T}_p)},$$

and hence letting $\tilde{\beta}^{+}_{m,n}$ be a lift of $\beta^{+}_{m,n}$ to $\mathrm{H}^1_{+}(\mathbf{Q}_p, \mathbf{T}_p)$ we obtain, for some $d \in \mathrm{H}^1_{+}(\mathbf{Q}_p, \mathbf{T}_p)$, the equalities

$$\begin{aligned} \tilde{\omega}_n^{-}(X)\tilde{\beta}^{+}_{m,n} &= -\Phi_{n-1}(X)\tilde{\omega}^{-}_{n-2}(X)\tilde{\beta}^{+}_{m,n-2} + \omega_{n-1}(X)d \\ &= -\tilde{\omega}_n^{-}(X)\tilde{\beta}^{+}_{m,n-2} + \tilde{\omega}_n^{-}(X)\omega^{+}_{n-2}(X)d. \end{aligned}$$

Cancelling out $\tilde{\omega}_n^{-}(X)$, the result follows. □

By Proposition 3.11 for every sign ϵ we may consider

$$\boldsymbol{b}^{\epsilon} := \{b^{\epsilon}_{m,n}\}_{n \equiv \epsilon \pmod 2, m} \in \varprojlim \mathrm{H}^1_{\epsilon}(k_{m,n}, T)/\omega^{\epsilon}_n(X)\mathrm{H}^1_{\epsilon}(k_{m,n}, T) = \mathrm{H}^1_{\epsilon}(\mathbf{Q}_p, \mathbf{T}_p),$$

and $\boldsymbol{b}^{\epsilon}$ generates the free Λ-module $\mathrm{H}^1_{\epsilon}(\mathbf{Q}_p, \mathbf{T}_p)$.

Definition 3.12. The plus/minus logarithm map $\mathrm{Log}^{\pm} : \mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p) \to \Lambda$ is defined by

$$\boldsymbol{x} = \mathrm{Log}^{\pm}(\boldsymbol{x})\boldsymbol{b}^{\pm}$$

for all $\boldsymbol{x} \in \mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p)$.

Remark 3.13. Although not reflected in the above notation, we note that the map $\mathrm{Log}^{\pm}$ depends on the elements $d \in \mathcal{O}_{\infty}$ and $\zeta = \{\zeta_{p^n}\}_n$ chosen in the proof of Lemma 3.4. It is easy to see that a different choice of d and ζ scales $\mathrm{Log}^{\pm}$ be an element in $\Lambda^{\times}$.

Note that by Proposition 3.11 the map $\mathrm{Log}^{\pm}$ is a Λ-module isomorphism. The next result describes its interpolation property.

Proposition 3.14. *Let $\phi : G_{\infty} \to \mathbf{C}_p^{\times}$ be a finite order character such that $\phi(\gamma)$ is a primitive p^n-th root of unity and $\phi(u) \neq 1$ is a primitive p^m-th*

root of unity, and let $\boldsymbol{x} = \{x_{m,n}\}_{m,n} \in \mathrm{H}^1_\epsilon(\mathbf{Q}_p, \mathbf{T}_p)$*, where* $\epsilon = (-1)^n$*. Then*

$$\phi^{-1}\big(\mathrm{Log}^\epsilon(\boldsymbol{x})\big) \cdot \mathfrak{g}(\phi|_\Gamma)\phi(u)^{n+1} \sum_{\tau \in U_m} d_m^\tau \phi(\tau) \\ = (-1)^{[\frac{n+1}{2}]}\phi(\tilde{\omega}_n^{-\epsilon}(X)) \sum_{\tau \in \mathrm{Gal}(k_{m,n}/\mathbf{Q}_p)} \log_{\hat{E}}(x_{m,n}^\tau)\phi(\tau),$$

where $\mathfrak{g}(\phi|_\Gamma) = \sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^{n+1}})/\mathbf{Q}_p)} \phi(\gamma)\zeta_{p^{n+1}}^\gamma$ *is the Gauss sum of* ϕ*.*

Proof. As shown in the proof of Lemma 3.4, the point $c_{m,n}$ is obtained by tracing down to $\mathfrak{m}_{m,n}$ a point $\widetilde{c}_{m,n} \in \hat{E}(\mathfrak{m}_{\mathbf{Q}_{p^m}(\mu_{p^{n+1}})})$ satisfying

$$\log_{\hat{E}}(\tilde{c}_{m,n}) = \sum_{j=1}^{\infty}(-1)^{j-1} d_m^{u^{-(n+1+2j)}} + \sum_{k=0}^{\infty}(-1)^k \frac{d_m^{u^{2k-n-1}}(\zeta_{p^{n+1-2k}} - 1)}{p^k}.$$

Write Tr for the trace map $\mathbf{Q}_{p^m}(\mu_{p^{n+1}}) \to k_{m,n}$. Twisting the above expression by ϕ and summing over τ we then obtain

$$\sum_{\tau \in U_m \times \Gamma_n} \log_{\hat{E}}(c_{m,n}^\tau)\phi(\tau) = \sum_{\tau \in U_m \times \Gamma_n} (d_m^{u^{-n-1}})^\tau \mathrm{Tr}(\zeta_{p^{n+1}}^\tau)\phi(\tau) \\ = \mathfrak{g}(\phi|_\Gamma)\phi(u)^{n+1} \sum_{\tau \in U_m} d_m^\tau \phi(\tau),$$

which immediately yields the result. □

4. Heegner point main conjecture

In this section we construct plus/minus Heegner classes for rational elliptic curves at good supersingular primes and formulate an analogue of Perrin-Riou's Heegner point main conjecture for them.

Throughout, we let $E/\mathbf{Q}$ be an elliptic curve of conductor N, with associated newform $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$. We also let K be an imaginary quadratic field satisfying hypothesis (gen-H) and $p > 3$ be a prime of good supersingular reduction for E.

4.1. **The plus/minus Heegner classes.** Let X_{N^+,N^-} be the Shimura curve over $\mathbf{Q}$ (with cusps added, if $N^- = 1$) attached to the rational quaternion algebra B of discriminant N^- and an Eichler order $R \subset \mathcal{O}_B$ of level N^+. Let $\mathrm{Jac}(X_{N^+,N^-})/\mathbf{Q}$ be the Jacobian variety of X_{N^+,N^-} and choose a modular parametrization

$$\pi : \mathrm{Jac}(X_{N^+,N^-}) \to E.$$

For every positive integer S we let $\mathcal{O}_S = \mathbf{Z} + S\mathcal{O}_K$ be the order of K of conductor S, and let $K[S]$ be ring class field of K conduction S, so that $\mathrm{Gal}(K[S]/K) \simeq \mathrm{Pic}(\mathcal{O}_S)$ by the Artin map.

Proposition 4.1. *There is a collection of Heegner points $x_S \in E(K[S])\otimes \mathbf{Z}_p$ indexed by positive integers S prime to ND_K such that*

$$\mathrm{Tr}_{K[\ell S]/K[S]}(x_{\ell S}) = \begin{cases} a_\ell x_S & \text{if } \ell \nmid S \text{ is inert in } K, \\ a_\ell x_S - x_S^{\sigma_\ell} - x_S^{\sigma_\ell^*} & \text{if } \ell \nmid S \text{ splits in } K, \\ a_\ell x_S - x_{S/\ell} & \text{if } \ell \mid S, \end{cases}$$

where $\sigma_\ell, \sigma_\ell^* \in \mathrm{Gal}(K[S]/K)$ are the Frobenius elements at the primes above ℓ.

Proof. Fix a prime $q \nmid Np$ and consider the embedding

$$\iota_{N^+,N^-} : X_{N^+,N^-} \to \mathrm{Jac}(X_{N^+,N^-}), \quad x \mapsto (T_q - q - 1)(x),$$

where T_q is the q-th Hecke correspondence on X_{N^+,N^-}. By [How04b, Prop. 1.2.1] there is a collection of CM points $h_S \in X_{N^+,N^-}$ defined over $K[S]$ and such that

$$\mathrm{Norm}_{K[\ell S]/K[S]}(h_{\ell S}) = \begin{cases} T_\ell(h_S) & \text{if } \ell \nmid S \text{ is inert in } K, \\ T_\ell(h_S) - h_S^{\sigma_\ell} - h_S^{\sigma_\ell^*} & \text{if } \ell \nmid S \text{ splits in } K, \\ T_\ell(h_S) - h_{S/\ell} & \text{if } \ell \mid S \end{cases}$$

as divisors on $X_{N^+,N^-}(\mathbf{C})$. Choosing q as above with the additional property that $a_q - q - 1$ is a p-adic unit, the result follows by setting

$$x_S := \iota_{N^+,N^-}(h_S) \otimes (a_q - q - 1)^{-1} \in E(K[S]) \otimes \mathbf{Z}_p$$

(note that the $G_{\mathbf{Q}}$-representation $E[p]$ is irreducible by [Edi92], so such q exists). □

Let $T = T_pE$ be the p-adic Tate module of E, and denote by $z[S] \in \mathrm{H}^1(K[S], T)$ the image of x_S under the Kummer map

$$E(K[S]) \otimes \mathbf{Z}_p \to \mathrm{H}^1(K[S], T).$$

Since $a_p = 0$, letting Cor_n^{n+1} denote the corestriction map for the extension $K[Sp^{n+1}]/K[Sp^n]$, the norm-compatibility in Proposition 4.1 yields

$$\mathrm{Cor}_n^{n+1}(z[Sp^{n+1}]) = -z[Sp^{n-1}] \tag{4.1}$$

for all $n > 0$.

The anticyclotomic $\mathbf{Z}_p$-extension K_∞^{ac}/K is contained in $K[p^\infty] = \cup_{k\geqslant 0} K[p^k]$, and the Galois group $\mathrm{Gal}(K[p^\infty]/K)$ decomposes as

$$\mathrm{Gal}(K[p^\infty]/K) \simeq \Gamma^{\mathrm{ac}} \times \Delta$$

with $\Delta = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}}$ a finite group. Let $L \subset K[p^\infty]$ be the fixed field of Γ^{ac} and for each n let L_{n+1} be the subfield of $K[p^\infty]$ fixed by $(\Gamma^{\mathrm{ac}})^{p^n}$. Then

$$\tilde{\Gamma}_n := \mathrm{Gal}(L_{n+1}/K) \simeq \Delta \times \mathrm{Gal}(K_n^{\mathrm{ac}}/K), \tag{4.2}$$

where K_n^{ac} is the subextension of K_∞^{ac} of degree p^n over K. Note that there exists a non-negative integer δ such that $L_{n+1+\delta} = K[p^n]$ for $n \gg 0$, with $\delta = 0$ when the class number of K is coprime to p.

Consider the modules

$$\tilde{\mathbf{T}} = T\hat{\otimes}_{\mathbf{Z}_p}\mathbf{Z}_p[\![\mathrm{Gal}(K[p^\infty]/K)]\!], \quad \mathbf{T}^{\mathrm{ac}} = T\hat{\otimes}_{\mathbf{Z}_p}\Lambda^{\mathrm{ac}}$$

equipped with the diagonal G_K-action, with G_K acting on the right factors via the tautological characters. In particular, similarly as in (3.10), there is a $\mathbf{Z}_p[\![\mathrm{Gal}(K[p^\infty]/K)]\!]$-module isomorphism

$$\mathrm{H}^1(K, \tilde{\mathbf{T}}) \simeq \varprojlim_n \mathrm{H}^1(K[p^n], T)$$

given by Shapiro's lemma.

For any field extension L/K, denote by $L[S]$ the compositum of L and the ring class field $K[S]$. Our construction of plus/minus Heegner classes hinges on the next two lemmas.

Lemma 4.2. *Let S be a positive integer prime to Np. For every $n > 0$ the class $z[Sp^n]$ lies in the image of the natural map*

$$\mathrm{H}^1(K[S], \tilde{\mathbf{T}}) \to \mathrm{H}^1(K[Sp^n], T).$$

Proof. It suffices to show the result holds for all n sufficiently large. Note that (4.1) yields

$$\mathrm{Cor}_n^{n+2k}(z[Sp^{n+2k}]) = \pm p^k z[Sp^n] \tag{4.3}$$

for all k. Let $\gamma \in \Gamma^{\mathrm{ac}}$ be a topological generator, and set $\gamma_n = \gamma|_{K_n^{\mathrm{ac}}} \in \mathrm{Gal}(K_n^{\mathrm{ac}}/K)$. From the G_K-module exact sequence $0 \to \tilde{\mathbf{T}} \xrightarrow{\gamma_n - 1} \tilde{\mathbf{T}} \to T \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\tilde{\Gamma}_n] \to 0$ we obtain the exact sequence.

$$\mathrm{H}^1(K[S], \tilde{\mathbf{T}}) \to \mathrm{H}^1(L_{n+1}[S], T) \xrightarrow{\alpha_n} \mathrm{H}^2(K[S], \tilde{\mathbf{T}})^{\Gamma_n} \to 0.$$

Note that under the maps α_n, the corestriction $\mathrm{H}^1(L_{n+1}[S], T) \to \mathrm{H}^1(L_n[S], T)$ corresponds to the trace $\mathrm{H}^2(K[S], \tilde{\mathbf{T}})^{\Gamma_n} \to \mathrm{H}^2(K[S], \tilde{\mathbf{T}})^{\Gamma_{n-1}}$. Since $\mathrm{H}^2(K[S], \tilde{\mathbf{T}})$ is finitely generated over Λ^{ac}, the modules $M_n := \mathrm{H}^2(K[S], \tilde{\mathbf{T}})^{\Gamma_n}$ stabilize for $n \gg 0$, so there is some n_0 such that $M_n = M_{n_0}$ for all $n \geqslant n_0$. In particular, the trace map $\mathrm{Tr}_n^{n+1} : M_{n+1} \to M_n$ is given by multiplication by p on $M_{n_0} = \lim_{n\to\infty} M_n$ for all $n \geqslant n_0$. Combined with (4.3) we thus see that

$$\begin{aligned} \pm p^k \alpha_n(z[Sp^n]) &= \alpha_n(\mathrm{Cor}_n^{n+2k}(z[Sp^{n+2k}])) \\ &= \mathrm{Tr}_n^{n+2k}(\alpha_{n+2k}(z[Sp^{n+2k}])) = p^{2k}\alpha_{n+2k}(z[Sp^{n+2k}]) \end{aligned}$$

for all $n \geqslant n_0$ and $k \geqslant 0$. Letting $k \to \infty$, this shows that $\alpha_n(z[Sp^n])$ is divisible by arbitrarily high powers of p, and hence $\alpha_n(z[Sp^n]) = 0$, yielding the result. □

In the following, we identify Λ^{ac} with the the one variable power series ring $\mathbf{Z}_p[\![Y]\!]$ setting $Y = \gamma^{\mathrm{ac}} - 1$ for a fixed topological generator $\gamma^{\mathrm{ac}} - 1$.

Lemma 4.3. *Let S be a positive integer prime to p. Then $\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})$ is free over Λ^{ac}.*

Proof. As we recall in Lemma 6.6 below, $E[p]$ is absolutely irreducible as a G_K-module, and using this the result can be shown by arguing similarly as in [Kat04, §13.8]. Here we give a slightly different argument.

It suffices to show that $M_S := \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})$ is free over $\Lambda^{\mathrm{ac}} \simeq \mathbf{Z}_p[\![Y]\!]$. We claim that the maps

$$\alpha_Y : M_S \xrightarrow{\times Y} M_S, \quad \alpha_p : M_S/YM_S \xrightarrow{\times p} M_S/YM_S \tag{4.4}$$

are both injective. Indeed, the irreducibly of $E[p]$ as a $G_{\mathbf{Q}_p}$-module implies that $E(K)[p] = 0$, which gives $\mathrm{H}^0(K_\infty, T) = 0$. By [PR00, §1.3.3], it follows that the Λ^{ac}-torsion submodule of M_S is trivial, and so α_Y is injective. On the other hand, in light of the natural inclusion

$$M_S/YM_S \hookrightarrow \mathrm{H}^1(K[S], T),$$

to check the injectivity of α_p it suffices to check that multiplication by p is injective on $\mathrm{H}^1(K[S], T)$, but this follows easily again by the irreducibility of $E[p]$.

By the structure theorem, the injectivity of (4.4) implies that M_S injects into a free Λ^{ac}-module F with finite quotient N:

$$0 \to M_S \to F \to N \to 0.$$

If $N \neq 0$, then $\mathrm{Tor}_1^{\Lambda^{\mathrm{ac}}}(N, \Lambda^{\mathrm{ac}}/Y\Lambda^{\mathrm{ac}})$ is a nonzero $\mathbf{Z}_p$-torsion module injecting into M_S/YM_S, but this is impossible by injectivity of α_p. Thus $N = 0$, and this concludes the proof. □

To ease notation, in the next result we let Cor_n be the corestriction map for $K[Sp^{n+1-\delta}]/K_n^{\mathrm{ac}}[S]$.

Proposition 4.4. *Let $\epsilon = (-1)^n$. There exists a unique class*

$$z_n[S]^\epsilon \in \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})/\omega_n^\epsilon(Y)\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}}) \tag{4.5}$$

such that $\tilde{\omega}_n^{-\epsilon}(Y) z_n[S]^\epsilon = \mathrm{Cor}_n(z[Sp^{n+1-\delta}])$. Moreover, the sequences

$$\{(-1)^{n/2} z_n[S]^+\}_{n \text{ even}}, \quad \{(-1)^{(n+1)/2} z_n[S]^-\}_{n \text{ odd}}$$

are compatible under the natural maps

$$\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})/\omega_n^\epsilon(Y)\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}}) \to \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})/\omega_{n-2}^\epsilon(Y)\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}}).$$

Proof. By Lemma 4.2 the class $z[Sp^{n+1-\delta}]$ is in the image of the natural embedding

$$\mathrm{H}^1(K[S], \tilde{\mathbf{T}})/\omega_n(Y)\mathrm{H}^1(K[S], \tilde{\mathbf{T}}) \hookrightarrow \mathrm{H}^1(K[Sp^{n+1-\delta}], T).$$

With a slight abuse of notation, denote by $z[Sp^{n+1-\delta}]$ the natural image of this class under the map

$$\mathrm{H}^1(K[S], \tilde{\mathbf{T}})/\omega_n(Y)\mathrm{H}^1(K[S], \tilde{\mathbf{T}}) \to \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})/\omega_n(Y)\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})$$

given by corestriction. Using (4.1), the same calculation as in Corollary 3.5 shows that $\omega_n^\epsilon(Y) z[Sp^{n+1-\delta}] = 0$. In light of the freeness result in Lemma 4.3,

this implies the existence of a unique class $z_n[S]^\epsilon$ as in (4.5) such that $\tilde{\omega}_n^{-\epsilon}(Y)z_n[S]^\epsilon = \mathrm{Cor}_n(z[Sp^{n+1-\delta}])$ in the image of the map

$$\mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}})/\omega_n^\epsilon(Y)\mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}}) \xrightarrow{\sim} \tilde{\omega}_n^\epsilon(Y)\mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}})/\omega_n(Y)\mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}}) \hookrightarrow \mathrm{H}^1(K_n[S],T),$$

where the first arrow is the isomorphism given by multiplication by $\tilde{\omega}_n^{-\epsilon}(Y)$. This shows the first part of the lemma, and the second is shown by the same argument as in the proof of Proposition 3.11. □

In light of the last part of Proposition 4.4, we can make the following.

Definition 4.5. For every sign $\epsilon \in \{\pm\}$ and positive integer S prime to Np we define the *ϵ-Heegner point* of conductor S to be the class $\mathbf{z}_\infty[S]^\epsilon \in \mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}})$ given by

$$\mathbf{z}_\infty[S]^\epsilon := \{z_n[S]^\epsilon\}_n \in \varprojlim_n \mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}})/\omega_n^\epsilon(Y)\mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}}) \simeq \mathrm{H}^1(K[S],\mathbf{T}^{\mathrm{ac}}),$$

where the limit is over the positive integers n of parity ϵ.

Note that since $\{\omega_n^\epsilon(Y)\}_{n\equiv\epsilon \bmod 2}$ forms a basis for the topology of Λ^{ac}, the class $\mathbf{z}_\infty[S]^\epsilon$ is well-defined.

4.2. **The main conjecture.** In this section we formulate the supersingular analogue of Perrin-Riou's Heegner point main conjecture (see [PR87, Conj. B] for the ordinary case) in terms of the signed Heegner classes $\mathbf{z}_\infty[S]^\pm$.

Assume that

$$(p) = \mathfrak{p}\bar{\mathfrak{p}} \text{ splits in } K. \tag{spl}$$

Recall that $\Gamma^{\mathrm{ac}} = \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)$ is the Galois group of the anticyclotomic $\mathbf{Z}_p$-extension of K, and $\mathbf{\Gamma} = \mathrm{Gal}(K_\infty/K)$ is the Galois group of the unique $\mathbf{Z}_p^2$-extension of K. Let v be a prime of K above p, and let $v_1,\dots,v_{p^t}$ be the primes of K_∞^{ac} lying above v. Since each v_i is totally ramified in $K_\infty/K_\infty^{\mathrm{ac}}$, by abuse of notation we shall also denote by $v_1,\dots,v_{p^t}$ the primes of K_∞ lying above v. Fix v_1, let $\Gamma_{v_1}^{\mathrm{ac}}$ (resp. $\mathbf{\Gamma}_{v_1}$) be the decomposition group of v_1 in Γ^{ac} (resp. $\mathbf{\Gamma}$) and let $\gamma_1 = \mathrm{id}, \gamma_2, \dots, \gamma_{p^t} \in \Gamma^{\mathrm{ac}}$ be such that $v_i = \gamma_i v_1$.

Identifying $K_v = \mathbf{Q}_p$, we then have $\mathbf{\Gamma}_{v_1} \simeq \mathrm{Gal}(\mathbf{Q}_{p,\infty}^{\mathrm{ur}}/\mathbf{Q}_p)$, as considered in §3. Set

$$\mathbf{T}_{v_1}^{\mathrm{ac}} = T\hat{\otimes}_{\mathbf{Z}_p}\mathbf{Z}_p[\![\Gamma_{v_1}^{\mathrm{ac}}]\!]$$

with G_{K_v} acting on the second factor by the character $G_{K_v} \twoheadrightarrow \Gamma_{v_1}^{\mathrm{ac}} \hookrightarrow \mathbf{Z}_p[\![\Gamma_{v_1}^{\mathrm{ac}}]\!]^\times$, and define $\mathbf{T}_{v_1}$ similarly.

Definition 4.6. Let $\mathrm{H}^1_\pm(K_v,\mathbf{T}_{v_1}^{\mathrm{ac}})$ be the image of $\mathrm{H}^1_\pm(K_v,\mathbf{T}_{v_1}) \simeq \mathrm{H}^1_\pm(\mathbf{Q}_p,\mathbf{T}_p)$ under the map induced by the the projection $\mathbf{\Gamma} \twoheadrightarrow \Gamma^{\mathrm{ac}}$, and set

$$\mathrm{H}^1_\pm(K_v,\mathbf{T}^{\mathrm{ac}}) := \bigoplus_{i=1}^{p^t} \gamma_i.\mathrm{H}^1_\pm(K_v,\mathbf{T}_{v_1}^{\mathrm{ac}}). \tag{4.6}$$

Let $\mathbf{z}_\infty^\pm \in \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}})$ denote the image of the class $\mathbf{z}_\infty[1]^\pm$ under the corestriction map $\mathrm{H}^1(K[1], \mathbf{T}^{\mathrm{ac}}) \to \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}})$.

Lemma 4.7. *For each prime v of K above p we have* $\mathrm{loc}_v(\mathbf{z}_\infty^\pm) \in \mathrm{H}^1_\pm(K_v, \mathbf{T}^{\mathrm{ac}})$.

Proof. Since $\mathrm{H}^1_\pm(\mathbf{Q}_p, \mathbf{T}_p) \simeq \varprojlim_{m,n} \ker(P^\pm_{m,n})$ and the image of $P^\pm_{m,n}$ is contained in $\tilde{\omega}^\mp_{m,n}\Lambda_{m,n}$ (see §3.2), the result follows immediately from the isotropy of points under the local Tate pairing and the construction of $\mathbf{z}_\infty^\pm$. □

Now let $\mathcal{F}^\pm$ be the Selmer structure on $\mathbf{T}^{\mathrm{ac}}$ defined by

$$\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}}) = \begin{cases} \mathrm{H}^1_\pm(K_v, \mathbf{T}^{\mathrm{ac}}) & \text{if } v \mid p, \\ \mathrm{H}^1(K_v, \mathbf{T}^{\mathrm{ac}}) & \text{if } v \nmid p, \end{cases}$$

and let $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ be the associated Selmer group:

$$\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}}) := \ker\left\{ \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}) \to \prod_v \frac{\mathrm{H}^1(K_v, \mathbf{T}^{\mathrm{ac}})}{\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}})} \right\}, \tag{4.7}$$

where the product is over all places v of K.

Setting $\mathbf{A}^{\mathrm{ac}} := T \hat{\otimes}_{\mathbf{Z}_p} \mathrm{Hom}_{\mathbf{Z}_p}(\Lambda^{\mathrm{ac}}, \mathbf{Q}_p/\mathbf{Z}_p)$ equipped with the natural G_K-action, we let $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{A}^{\mathrm{ac}}) \subset \mathrm{H}^1(K_v, \mathbf{A}^{\mathrm{ac}})$ be the orthogonal complement of $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}})$ under local duality, and define $\mathrm{Sel}^\pm(K, \mathbf{A}^{\mathrm{ac}})$ by the same recipe as in (4.7). Let

$$X^\pm = \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}^\pm(K, \mathbf{A}^{\mathrm{ac}}), \mathbf{Q}_p/\mathbf{Z}_p)$$

be the Pontryagin dual. Note that it follows from Lemma 4.7 that $\mathbf{z}_\infty^\pm$ lands in $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$. As a natural extension of [PR87, Conj. B], we conjecture the following.

Conjecture 4.8 (Plus/minus Heegner point main conjecture)**.**

(1) *The class $\mathbf{z}_\infty^\pm$ is not Λ^{ac}-torsion.*
(2) *The modules $X^\pm$ and $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ both have Λ^{ac}-rank one.*
(3) *We have*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(X^\pm_{\mathrm{tors}}\right) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_\infty^\pm}\right)^2,$$

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

Remark 4.9. Like its counterpart for ordinary primes, Conjecture 4.8 might be seen as a Λ^{ac}-adic analogue[3] of Kolyvagin's result [Kol88] showing that when the Heegner point $y_K \in E(K)$ is non-torsion, the p-primary part of the Tate–Shafarevich group $Ш(E/K)$ is finite, of order essentially given by square of the index $[E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p y_K]$.

[3]In connection with this analogy, we note that building on the results in this paper towards Conjecture 4.8, Lei–Lim–Müller [LLM23] have obtained a new proof of a result originally due to Çiperiani [Ç09] showing that for supersingular primes p, the Tate–Shafarevich group $Ш(E/K_\infty)[p^\infty]$ is Λ^{ac}-cotorsion.

5. Greenberg main conjecture for $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$

Keeping the setting from Section 2, we now consider certain variants of the Selmer groups $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ and $\mathrm{Sel}^{\pm}(K,\mathbf{A}^{\mathrm{ac}})$ obtained by changing their conditions at the primes above p. Recall the Selmer structure $\mathcal{F}^{\pm}$ introduced in §4.2.

Definition 5.1. Let M denote either $\mathbf{T}^{\mathrm{ac}}$ or $\mathbf{A}^{\mathrm{ac}}$. For $v \in \{\mathfrak{p},\overline{\mathfrak{p}}\}$ and $\mathscr{L}_v \in \{\mathrm{rel},\pm,\mathrm{str}\}$, set

$$\mathrm{H}^1_{\mathscr{L}_v}(K_v,M) = \begin{cases} \mathrm{H}^1(K_v,M) & \text{if } \mathscr{L}_v = \mathrm{rel}, \\ \mathrm{H}^1_{\pm}(K_v,M) = \mathrm{H}^1_{\mathcal{F}^{\pm}}(K_v,M) & \text{if } \mathscr{L}_v = \pm, \\ 0 & \text{if } \mathscr{L}_v = \mathrm{str}. \end{cases}$$

Then for $\mathscr{L} = \{\mathscr{L}_{\mathfrak{p}},\mathscr{L}_{\overline{\mathfrak{p}}}\}$ we define the modified Selmer group $\mathrm{Sel}^{\mathscr{L}}(K,M)$ by

$$\mathrm{Sel}^{\mathscr{L}}(K,M) := \ker\left\{ \mathrm{H}^1(K,M) \to \prod_{v\in\{\mathfrak{p},\overline{\mathfrak{p}}\}} \frac{\mathrm{H}^1(K_v,M)}{\mathrm{H}^1_{\mathscr{L}_v}(K_v,M)} \times \prod_{v\nmid p} \frac{\mathrm{H}^1(K_v,M)}{\mathrm{H}^1_{\mathcal{F}^{\pm}}(K_v,M)} \right\}.$$

We also let $X^{\mathscr{L}}$ denote the Pontryagin dual of $\mathrm{Sel}^{\mathscr{L}}(K,\mathbf{A}^{\mathrm{ac}})$, and for Σ a finite set of places of K away from p, let $X^{\mathscr{L},\Sigma}$ denote the Pontryagin dual of Selmer group obtained as above by relaxing the local conditions at the primes $w \in \Sigma$. Thus in particular $\mathrm{Sel}^{\mathrm{rel,str}}(K,\mathbf{A}^{\mathrm{ac}})$ consists of classes which are trivial at $\overline{\mathfrak{p}}$ and satisfy no condition at $\mathfrak{p}$, and $\mathrm{Sel}^{\pm,\pm}(K,\mathbf{A}^{\mathrm{ac}})$ recovers the Selmer module $\mathrm{Sel}^{\pm}(K,\mathbf{A}^{\mathrm{ac}})$ of §4.2.

Note that for any character $\hat{\chi}$ in the interpolation range for the square-root p-adic L-function $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ in Proposition 2.1, the p-adic representation $V_pE\otimes\mathrm{Ind}_K^{\mathbf{Q}}(\hat{\chi})$ satisfies the *Panchishkin condition* introduced by Greenberg [Gre94]. The following Conjecture 5.2 may thus be viewed as an instance of the Iwasawa main conjectures formulated in *op. cit.* for $L_{\mathfrak{p}}^{\mathrm{BDP}} = (\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}})^2$.

Conjecture 5.2 (Iwasawa–Greenberg main conjecture)**.** *The module $X^{\mathrm{rel,str}}$ is Λ^{ac}-torsion, and*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)\Lambda^{\mathrm{ur}} = \big(L_{\mathfrak{p}}^{\mathrm{BDP}}\big)$$

as ideals in Λ^{ur}.

An important consequence of the main result of the authors with Zheng Liu [CLW22] is the following divisibility towards Conjecture 5.2.

Theorem 5.3 ([CLW22])**.** *Assume that:*

(i) *N is squarefree,*
(ii) *some prime $\ell \mid N$ is non-split in K,*
(iii) *if N is odd, then 2 splits in K.*

Then

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)\Lambda^{\mathrm{ur}} \subset \big(L_{\mathfrak{p}}^{\mathrm{BDP}}\big)$$

in $\Lambda^{\mathrm{ur}}[1/p]$. *If in addition* $E[p]$ *is ramified at every prime* $\ell \mid N^-$, *then the divisibility holds in* Λ^{ur}.

Proof. We first need to introduce some more notations. Denote by $\Psi : \mathbf{\Gamma} \to \mathbf{\Lambda}^\times$ the tautological character, and by ε the p-adic cyclotomic character. For Σ a finite set of primes of K not containing any prime above p, define the Σ-imprimitive p-adic L-function $L_{\mathfrak{p}}^{\mathrm{RS},\Sigma} \in \mathbf{\Lambda}^{\mathrm{ur}}$ by

$$L_{\mathfrak{p}}^{\mathrm{RS},\Sigma} := L_{\mathfrak{p}}^{\mathrm{RS}} \times \prod_{w\in\Sigma} P_w(\varepsilon^{-1}\Psi(\mathrm{Frob}_w)), \tag{5.1}$$

where $P_w(X) = \det(1-\mathrm{Frob}_w X)$ gives the Euler factor at w of the L-function of E.

Part (1) of [CLW22, Thm. 8.2.1] yields the divisibility as fractional ideals in $\mathbf{\Lambda}^{\mathrm{ur}} \otimes_{\mathbf{Z}_p[\![\mathbf{\Gamma}^+]\!]} \mathrm{Frac}(\mathbf{Z}_p[\![\mathbf{\Gamma}^+]\!])$:

$$\mathrm{char}_{\mathbf{\Lambda}}\big(\mathbf{X}^{\mathrm{rel,str},\Sigma}\big)\mathbf{\Lambda}^{\mathrm{ur}} \subset \big(L_{\mathfrak{p}}^{\mathrm{RS},\Sigma}\big), \tag{5.2}$$

where Σ is any finite set of primes of K away from p containing all primes dividing ND_K and $\mathbf{X}^{\mathrm{rel,str},\Sigma}$ is defined in the same manner as $X^{\mathrm{rel,str},\Sigma}$ with $\mathbf{A} := T\hat{\otimes}_{\mathbf{Z}_p}\mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{\Lambda}, \mathbf{Q}_p/\mathbf{Z}_p)$ in place of $\mathbf{A}^{\mathrm{ac}}$.

Letting $\gamma^+ \in \mathbf{\Gamma}^+$ be a topological generator, the natural inclusion $\Lambda^{\mathrm{ac}} \to \mathbf{\Lambda}$ identifies Λ^{ac} with $\mathbf{\Lambda}/I^+\mathbf{\Lambda}$, where $I^+ = (\gamma^+ - 1)$, and induces an isomorphism

$$\mathbf{X}^{\mathrm{rel,str},\Sigma}/I^+\mathbf{X}^{\mathrm{rel,str},\Sigma} \simeq X^{\mathrm{rel,str},\Sigma} \tag{5.3}$$

as Λ^{ac}-modules (see [SU14, Prop. 3.9]). Since I^+ generates the kernel of the projection $\mathrm{pr}_{\Gamma^{\mathrm{ac}}} : \mathbf{\Lambda} \to \Lambda^{\mathrm{ac}}$, combining (5.2) and (5.3) with Proposition 2.7 we conclude that

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str},\Sigma}\big)\Lambda^{\mathrm{ur}}[1/p] \subset \big(\mathrm{pr}_{\Gamma^{\mathrm{ac}}}\big(L_{\mathfrak{p}}^{\mathrm{RS},\Sigma}\big)\big) \tag{5.4}$$

as ideals in $\Lambda^{\mathrm{ur}}[1/p]$. Without loss of generality, assume that $X^{\mathrm{rel,str}}$ is Λ^{ac}-torsion (otherwise the characteristic ideal of $X^{\mathrm{rel,str}}$ is (0) by definition, and there is nothing to show). Then by [PW11, Lem. A.2] for any $\Sigma' \subset \Sigma$ we have an exact sequence

$$0 \to \mathrm{Sel}^{\mathrm{rel,str},\Sigma'}(K, \mathbf{A}^{\mathrm{ac}}) \to \mathrm{Sel}^{\mathrm{rel,str},\Sigma}(K, \mathbf{A}^{\mathrm{ac}}) \to \prod_{w\in\Sigma\smallsetminus\Sigma'} \mathrm{H}^1(K_w, \mathbf{A}^{\mathrm{ac}}) \to 0.$$

By a simple adaptation of [GV00, Prop. 2.4], it follows that

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str},\Sigma}\big) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str},\Sigma'}\big) \cdot \prod_{w\in\Sigma\smallsetminus\Sigma'} P_w(\varepsilon^{-1}\Psi^{-1}(\mathrm{Frob}_w)),$$

and hence combined with (5.1) it follows that the divisibility (5.4) also holds for $\Sigma = \emptyset$. Together with Proposition 2.7, this shows that

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)\Lambda^{\mathrm{ur}}[1/p] \subset \big(L_{\mathfrak{p}}^{\mathrm{BDP}} \cdot \alpha(f, f_B)\big) \tag{5.5}$$

as ideals in $\Lambda^{\mathrm{ur}}[1/p]$, yielding the first claim in the theorem.

Finally, if $E[p]$ is ramified at every prime $\ell \mid N^-$ then by [Pra06, p. 912] the term $\alpha(f, f_B)$ is a p-adic unit (indeed, this condition ensures that f is

not congruent mod p to any weight 2 newform of level dividing N/ℓ for any prime $\ell \mid N^-$); since $\mu(L_{\mathfrak{p}}^{\mathrm{BDP}}) = 0$ by Theorem 2.3, it follows that in this case the divisibility (5.5) holds in Λ^{ur}. □

Remark 5.4. At the referee's request, we note that assumption (iii) in Theorem 5.3 is used in *op. cit.* to simplify the choice of test vectors for which the corresponding local triple product integrals can be shown to be nonzero.

6. Main results

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ the newform associated with E, $p > 3$ a prime of good supersingular reduction for E, and K an imaginary quadratic field satisfying hypotheses (gen-H) and (spl).

6.1. **Explicit reciprocity law.** In this section we give a new construction of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ in terms of the signed Heegner classes $\mathbf{z}_{\infty}^{\pm}$ and the signed logarithm maps. This explicit reciprocity law will be the key ingredient allowing us to bring the Iwasawa–Greenberg main conjecture for $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ to bear on Conjecture 4.8.

Let H_K be the Hilbert class field of K, let $L_0 := K_{\infty}^{\mathrm{ac}} \cap H_K$, and denote by L_m the subextension of K_{∞}^{ac} with $[L_m \colon L_0] = p^m$ (so $L_m = K_{m+M}^{\mathrm{ac}}$ for some fixed $M \geqslant 0$). As in §4.2, for every prime v of K above p we have $\mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}) \simeq \mathrm{H}^1_{\pm}(\mathbf{Q}_p, \mathbf{T}_p)$, which is generated as $\mathbf{Z}_p[\![\mathbf{\Gamma}_{v_1}]\!]$-module by the element $\boldsymbol{b}^{\pm} = \{b^{\pm}_{m,n}\}$ from Proposition 3.11. Letting p^a be the inertial degree of $v_1 \cap L_0$ over v, we have $L_{m,v_1} \subset k_{m+a,m}$. Set

$$a_m^{\pm} := \mathrm{Cor}_{k_{m+a,m}/L_{m,v_1}}(\tilde{b}^{\pm}_{m+a,m}) \in \mathrm{H}^1_{\pm}(L_{m,v_1}, T),$$

where $\tilde{b}^{\pm}_{m+a,m}$ is an arbitrary lift of $b^{\pm}_{m+a,m}$ to $\mathrm{H}^1(k_{m+a,m}, T)$. This defines $a_m^{\pm} \in \mathrm{H}^1(K_{m,v_1}^{\mathrm{ac}}, T)$ for $m \geqslant M$ and setting $a_m^{\pm} := \mathrm{Cor}_{K_{M,v_1}^{\mathrm{ac}}/K_{m,v_1}^{\mathrm{ac}}}(a_m) \in \mathrm{H}^1(K_{m,v_1}^{\mathrm{ac}}, T)$ for $0 \leqslant m < M$ we obtain a system

$$\boldsymbol{a}^{\pm} = \{a_m^{\pm}\}_m \in \varprojlim_m \mathrm{H}^1_{\pm}(K_{m,v_1}^{\mathrm{ac}}, T) \simeq \mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}^{\mathrm{ac}})$$

which by Proposition 3.11 generates $\mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}^{\mathrm{ac}})$ as a free rank one $\mathbf{Z}_p[\![\Gamma_{v_1}^{\mathrm{ac}}]\!]$-module.

Definition 6.1. For v a prime of K above p, define $\mathrm{Log}^{\pm}_{v,1} : \mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}^{\mathrm{ac}}) \to \mathbf{Z}_p[\![\Gamma_{v_1}^{\mathrm{ac}}]\!]$ by

$$\boldsymbol{x} = \mathrm{Log}^{\pm}_{v,1}(\boldsymbol{x})\boldsymbol{a}^{\pm}$$

for all $\boldsymbol{x} \in \mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}^{\mathrm{ac}})$. Using $\Lambda^{\mathrm{ac}} = \bigoplus_{i=1}^{p^t} \gamma_i.\mathbf{Z}_p[\![\Gamma_{v_1}^{\mathrm{ac}}]\!]$ and the decompositions (4.6), we also define

$$\mathrm{Log}^{\pm}_{v} : \mathrm{H}^1_{\pm}(K_v, \mathbf{T}^{\mathrm{ac}}) \to \Lambda^{\mathrm{ac}}$$

by $\mathrm{Log}^{\pm}_{v}(\boldsymbol{y}) = \sum_i \gamma_i.\mathrm{Log}^{\pm}_{v,1}(\boldsymbol{y}_i))$, writing $\boldsymbol{y} = \sum_i \gamma_i.\boldsymbol{y}_i$ with $\boldsymbol{y}_i \in \mathrm{H}^1_{\pm}(K_v, \mathbf{T}_{v_1}^{\mathrm{ac}})$.

Recall the element $d = \{d_m\}_m \in \mathcal{O}_\infty = \varprojlim_m \mathbf{Z}_{p^m}$ chosen in the proof of Lemma 3.4 (and on which the construction of $\mathrm{Log}_v^\pm$ depends). As explained in [LZ14, §3], for varying m the maps

$$y_m : \mathbf{Z}_{p^m} \to \mathbf{Z}_{p^m}[\mathrm{Gal}(\mathbf{Q}_{p^m}/\mathbf{Q}_p)]$$

defined by $y_m(x) = \sum_{\sigma\in\mathrm{Gal}(\mathbf{Q}_{p^m}/\mathbf{Q}_p)} x^\sigma\sigma^{-1}$ assemble to yield in the limit an isomorphism between $\mathcal{O}_\infty$ and the subring of $\mathbf{Z}_p^{\mathrm{ur}}[\![U]\!]$ consisting of elements $f \in \mathbf{Z}_p^{\mathrm{ur}}[\![U]\!]$ such that

$$f^u = u.f \text{ for all } u \in U,$$

where the action of u on the left-hand side (resp. the right-hand side) is on the coefficients (resp. by multiplication as group-like elements). Let

$$\Xi_d := \varprojlim_m \sum_{\sigma\in\mathrm{Gal}(\mathbf{Q}_{p^m}/\mathbf{Q}_p)} d_m^\sigma\sigma^{-1} \in \mathbf{Z}_p^{\mathrm{ur}}[\![U]\!]$$

be the image of d under this isomorphism. Since d is a $\mathbf{Z}_p[\![U]\!]$-module generator of $\mathcal{O}_\infty$, the element Ξ_d is invertible.

Recall that by Lemma 4.7 for every prime v of K above p we have $\mathrm{loc}_v(\mathbf{z}_\infty^\pm) \in \mathrm{H}^1_\pm(K_v, \mathbf{T}^{\mathrm{ac}})$, and hence $\mathrm{Log}_v^\pm$ may be evaluated on $\mathrm{loc}_v(\mathbf{z}_\infty^\pm)$.

Theorem 6.2. *The following equality holds:*

$$\frac{\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}}{\Xi_d} = \sigma_{-1,\mathfrak{p}} \cdot \mathrm{Log}_{\mathfrak{p}}^\pm(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}_\infty^\pm)),$$

where $\sigma_{-1,\mathfrak{p}} = \mathrm{rec}_{\mathfrak{p}}(-1)|_{K_\infty^{\mathrm{ac}}} \in \Gamma^{\mathrm{ac}}$.

Proof. We just give the proof in the plus case, as the proof in the minus case is the same. Let $\hat\chi : \Gamma^{\mathrm{ac}} \to \mu_{p^\infty}$ be a non-trivial character factoring through a primitive character on $\mathrm{Gal}(K_n^{\mathrm{ac}}/K)$ for some even n. Viewing $\hat\chi$ as a character on $\tilde\Gamma$ via (4.2), the calculation in [CH18, pp. 598-9] (as adapted in [BCK21, Thm. 4.4] to the case $N^- \neq 1$) gives

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(\hat\chi^{-1}) = p^{-n}\mathfrak{g}(\chi_{\mathfrak{p}}^{-1})\chi_{\mathfrak{p}}(u^{-n}) \sum_{\sigma\in\tilde\Gamma_n} \hat\chi(\sigma)\log_{\hat E}(\sigma z[p^{n+1-\delta}]),$$

where $\chi_{\mathfrak{p}}$ denotes the component at $\mathfrak{p}$ of the Hecke character corresponding to $\hat\chi$ by (2.1). Combined with the definition of $z_n[1]^+$ (see Proposition 4.4) and $\mathbf{z}_\infty^+$, and Proposition 3.14, we thus obtain

$$\begin{aligned}
\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(\hat\chi^{-1}) &= \frac{\chi_{\mathfrak{p}}(-1)}{\mathfrak{g}(\chi_{\mathfrak{p}})\chi_{\mathfrak{p}}(u^n)} \cdot (-1)^{n/2}\hat\chi(\tilde\omega_n^-(X)) \sum_{\sigma\in\tilde\Gamma_n} \hat\chi(\sigma)\log_{\hat E}(\sigma z_n[1]^+) \\
&= \chi_{\mathfrak{p}}(-1)\cdot\hat\chi^{-1}(\mathrm{Log}_{\mathfrak{p}}^+(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}_\infty^+)))\cdot \sum_{\sigma\in U_{n+a}} \hat\chi(\sigma)d_{n+a}^\sigma \\
&= \hat\chi^{-1}\big(\sigma_{-1,\mathfrak{p}}\cdot\mathrm{Log}_{\mathfrak{p}}^+(\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}_\infty^+))\cdot\Xi_d\big).
\end{aligned}$$

Letting $\hat\chi$ as above vary, we obtain the result. □

Remark 6.3. Note that Theorem 6.2 shows that the period Ξ_d encodes all the $\Lambda^{\mathrm{ur}}/\Lambda$-transcendence of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$.

Corollary 6.4. *The class* $\mathrm{loc}_{\mathfrak{p}}(\mathbf{z}_{\infty}^{\pm})$ *is not* Λ^{ac}*-torsion.*

Proof. Immediate from Theorem 6.2 and the non-vanishing result for $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$ in Theorem 2.3. □

6.2. **Relating main conjectures.** The main result of this section is Theorem 6.8, connecting Conjecture 4.8 and Conjecture 5.2.

Let $\mathfrak{P} \neq p\Lambda^{\mathrm{ac}}$ be a height one prime of Λ^{ac}, denote by $S_{\mathfrak{P}}$ the integral closure of $\Lambda^{\mathrm{ac}}/\mathfrak{P}$, and let $\Phi_{\mathfrak{P}}$ be the field of fractions of $S_{\mathfrak{P}}$. Let also $\pi_{\mathfrak{P}} \in S_{\mathfrak{P}}$ be a uniformizer and $\mathfrak{m}_{\mathfrak{P}} = \pi_{\mathfrak{P}} S_{\mathfrak{P}}$ be the maximal ideal of $S_{\mathfrak{P}}$. Consider the $S_{\mathfrak{P}}$-modules

$$T_{\mathfrak{P}} := \mathbf{T}^{\mathrm{ac}} \otimes_{\Lambda^{\mathrm{ac}}} S_{\mathfrak{P}}, \quad V_{\mathfrak{P}} := T_{\mathfrak{P}} \otimes_{S_{\mathfrak{P}}} \Phi_{\mathfrak{P}}, \quad A_{\mathfrak{P}} := V_{\mathfrak{P}}/T_{\mathfrak{P}}. \tag{6.1}$$

As in [How04a, Prop. 2.2.4] the Weil pairing induces a perfect G_K-equivariant pairing

$$e_{\Lambda} : \mathbf{T}^{\mathrm{ac}} \times \mathbf{A}^{\mathrm{ac}} \to \mu_{p^\infty} \tag{6.2}$$

satisfying $e_{\Lambda}(\lambda \cdot t, a) = e_{\Lambda}(t, \lambda^{\iota} \cdot a)$ for all $t \in \mathbf{T}^{\mathrm{ac}}$, $a \in \mathbf{A}^{\mathrm{ac}}$, and $\lambda \in \Lambda^{\mathrm{ac}}$, where λ^{ι} denotes the image of λ under the involution $\iota : \Lambda^{\mathrm{ac}} \to \Lambda^{\mathrm{ac}}$ given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma^{\mathrm{ac}}$. Letting $\mathfrak{P}^{\iota}$ denote the image of $\mathfrak{P}$ under ι, this gives rise to a G_K-equivariant pairing $e_{\mathfrak{P}} : T_{\mathfrak{P}^{\iota}} \times A_{\mathfrak{P}} \to \mu_{p^\infty}$ satisfying $e_{\mathfrak{P}}(\lambda \cdot x, y) = e_{\mathfrak{P}}(x, \lambda^{\iota} \cdot y)$, which together with (6.2) allows us to dualize the natural map $\mathbf{T}^{\mathrm{ac}}/\mathfrak{P}^{\iota}\mathbf{T}^{\mathrm{ac}} \to T_{\mathfrak{P}^{\iota}}$ to a G_K and Λ^{ac}-equivariant map $A_{\mathfrak{P}} \to \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}]$.

Using $\mathbf{T}^{\mathrm{ac}} \to \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}} \to T_{\mathfrak{P}}$, we define

$$\mathrm{Sel}^{\pm}(K, T_{\mathfrak{P}}) \subset \mathrm{H}^1(K, T_{\mathfrak{P}}), \quad \mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}}) \subset \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}})$$

from $\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}})$ by propagation (i.e., defining the local conditions cutting out $\mathrm{Sel}^{\pm}(K, T_{\mathfrak{P}})$ to be the pushforward of those for $\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}})$ via the above map $\mathbf{T}^{\mathrm{ac}} \to T_{\mathfrak{P}}$), and similarly define $\mathrm{Sel}^{\pm}(K, A_{\mathfrak{P}})$ and $\mathrm{Sel}^{\pm}(K, \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}])$ from $\mathrm{Sel}^{\pm}(K, \mathbf{A}^{\mathrm{ac}})$ by propagation (i.e., pulling back the local conditions) via $A_{\mathfrak{P}} \to \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}] \to \mathbf{A}^{\mathrm{ac}}$.

Lemma 6.5. *There is a finite set* Σ_{Λ} *of height one primes* $\mathfrak{P} \subset \Lambda^{\mathrm{ac}}$*, with* $p\Lambda^{\mathrm{ac}} \in \Sigma_{\Lambda}$*, such that for* $\mathfrak{P} \notin \Sigma_{\Lambda}$ *the composite natural maps*

$$\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}})/\mathfrak{P}\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}}) \to \mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}}) \to \mathrm{Sel}^{\pm}(K, T_{\mathfrak{P}}),$$

$$\mathrm{Sel}^{\pm}(K, A_{\mathfrak{P}}) \to \mathrm{Sel}^{\pm}(K, \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}]) \to \mathrm{Sel}^{\pm}(K, \mathbf{A}^{\mathrm{ac}})[\mathfrak{P}]$$

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

Proof. As in the proof of [How04a, Prop. 2.2.8], it suffices to show (thanks to [MR04, Lem. 5.3.13]) that for all height one primes $\mathfrak{P} \subset \Lambda^{\mathrm{ac}}$ with $\mathfrak{P} \neq p\Lambda^{\mathrm{ac}}$, and for every place v of K, the natural maps

$$\mathrm{H}^1_{\mathcal{F}^{\pm}}(K_v, A_{\mathfrak{P}}) \to \mathrm{H}^1_{\mathcal{F}^{\pm}}(K_v, \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}]), \tag{6.3}$$

$$\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}}/\mathfrak{P}\mathbf{T}^{\mathrm{ac}}) \to \mathrm{H}^1_{\mathcal{F}^\pm}(K_v, T_{\mathfrak{P}}), \tag{6.4}$$

have finite kernel and cokernel which are bounded by a constant depending only on $[S_{\mathfrak{P}} : \Lambda^{\mathrm{ac}}/\mathfrak{P}]$, which for primes $v \nmid p$ is shown in [MR04, Lem. 5.3.13]. For $v \mid p$, that the map (6.3) has the desired property is shown in the proof of [Kim07, Prop. 4.18] (see also the discussion preceding it). On the other hand, since the natural map $\mathrm{H}^1(K_v, A_{\mathfrak{P}}) \to \mathrm{H}^1(K_v, \mathbf{A}^{\mathrm{ac}}[\mathfrak{P}])$ clearly has finite kernel and cokernel with a bound of the desired sort, we deduce that so does the induced map

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

from where the desired property for (6.4) follows by local duality. □

Lemma 6.6. *For every k the natural maps $T_{\mathfrak{P}}/\pi_{\mathfrak{P}}^k T_{\mathfrak{P}} \simeq A_{\mathfrak{P}}[\pi_{\mathfrak{P}}^k] \hookrightarrow A_{\mathfrak{P}}$ induce isomorphisms*

$$\mathrm{H}^1_{\mathcal{F}^\pm}(K, T_{\mathfrak{P}}/\pi_{\mathfrak{P}}^k T_{\mathfrak{P}}) \simeq \mathrm{H}^1_{\mathcal{F}^\pm}(K, A_{\mathfrak{P}}[\pi_{\mathfrak{P}}^k]) \simeq \mathrm{H}^1_{\mathcal{F}^\pm}(K, A_{\mathfrak{P}})[\pi_{\mathfrak{P}}^k].$$

Proof. This follows from Lemmas 3.5.3 and 3.5.4 in [MR04]. □

Lemma 6.7. *The following hold:*

1. *The modules $X^\pm$ and $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ have the same Λ^{ac}-rank.*
2. *$\mathrm{rank}_{\Lambda^{\mathrm{ac}}}(X^{\mathrm{rel},\pm}) = 1 + \mathrm{rank}_{\Lambda^{\mathrm{ac}}}(X^{\pm,\mathrm{str}})$ and*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel},\pm}_{\mathrm{tors}}\big) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm,\mathrm{str}}_{\mathrm{tors}}\big),$$

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

Proof. For part (1), it suffices to show that for every height one prime $\mathfrak{P} \neq p\Lambda^{\mathrm{ac}}$ outside a finite set Σ_Λ the modules

$$X^\pm/\mathfrak{P}X^\pm = \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}^\pm(K, \mathbf{A}^{\mathrm{ac}})[\mathfrak{P}], \mathbf{Q}_p/\mathbf{Z}_p), \quad \mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})/\mathfrak{P}\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$$

have the same $\mathbf{Z}_p$-rank. Since Lemma 6.6 gives that $\mathrm{Sel}^\pm(K, T_{\mathfrak{P}})$ is the $\pi_{\mathfrak{P}}$-adic Tate module of $\mathrm{Sel}^\pm(K, A_{\mathfrak{P}})$, the $\mathbf{Z}_p$-corank of $\mathrm{Sel}^\pm(K, A_{\mathfrak{P}})$ is the same as the $\mathbf{Z}_p$-rank of $\mathrm{Sel}^\pm(K, T_{\mathfrak{P}})$, which by Lemma 6.5 implies the result.

For the proof of part (2), we need some more preparation. For any height one prime $\mathfrak{P} \neq p\Lambda^{\mathrm{ac}}$, let $T_{\mathfrak{P}}$ be as in (6.1). As explained in the proof of [How04a, Lem. 2.1.1], the Weil pairing $e : T \times T \to \mu_{p^\infty}$ gives rise to a perfect symmetric $S_{\mathfrak{P}}$-bilinear pairing

$$e_{\mathfrak{P}} : T_{\mathfrak{P}} \times T_{\mathfrak{P}} \to S_{\mathfrak{P}}(1) \tag{6.5}$$

satisfying $e_{\mathfrak{P}}(s^\sigma, t^{\tau\sigma\tau})$ for all $s, t \in T_{\mathfrak{P}}$ and $\sigma \in G_K$, where $\tau \in G_{\mathbf{Q}}$ is any complex conjugation. Letting $\mathrm{Tw}(T_{\mathfrak{P}})$ denote the G_K-module given by T with G_K acting through the automorphism given by conjugation by τ, the pairing (6.5) becomes a G_K-equivariant pairing

$$e_{\mathfrak{P}} : T_{\mathfrak{P}} \times \mathrm{Tw}(T_{\mathfrak{P}}) \to S_{\mathfrak{P}}(1),$$

and by [Kim07, Prop. 4.11] the local conditions $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, T_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}^k T_\mathfrak{P})$, obtained by propagating $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, T_\mathfrak{P})$ via the quotient $T_\mathfrak{P} \to T_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}^k T_\mathfrak{P}$, are orthogonal complements under the induced local pairing

$$\mathrm{H}^1(K_v, T_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}^k T_\mathfrak{P}) \times \mathrm{H}^1(K_{\bar{v}}, T_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}^k T_\mathfrak{P}) \to S_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}^k. \tag{6.6}$$

Now set $\mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P}) := \mathrm{Sel}^{\pm,\mathrm{str}}(K, A_\mathfrak{P})$, and $\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})$ to be

$$\ker\left\{\mathrm{H}^1(K, A_\mathfrak{P}) \to \frac{\mathrm{H}^1(K_\mathfrak{p}, A_\mathfrak{P})}{\mathrm{H}^1(K_\mathfrak{p}, A_\mathfrak{P})_{\mathrm{div}}} \times \frac{\mathrm{H}^1(K_{\bar{\mathfrak{p}}}, A_\mathfrak{P})}{\mathrm{H}^1_\pm(K_{\bar{\mathfrak{p}}}, A_\mathfrak{P})} \times \prod_{v\nmid p} \frac{\mathrm{H}^1(K_v, A_\mathfrak{P})}{\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, A_\mathfrak{P})}\right\},$$

where the subscript div denotes the maximal divisible submodule. (Thus $\mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P})$ and $\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})$ are the propagation of $\mathrm{H}^1_{\pm,\mathrm{str}}(K, V_\mathfrak{P})$ and $\mathrm{H}^1_{\mathrm{rel},\pm}(K, V_\mathfrak{P})$ under $V_\mathfrak{P} \to A_\mathfrak{P}$ and $V_\mathfrak{P} \to A_\mathfrak{P}$, respectively.) By Lemma 6.6 and [MR04, Thm. 4.1.13], for every k there is a non-canonical isomorphism

$$\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})[p^k] \simeq (\Phi_\mathfrak{P}/S_\mathfrak{P})^r[p^k] \oplus \mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P})[p^k], \tag{6.7}$$

where r is the *core rank* (in the sense of [MR04, Def. 4.1.11]) of the Selmer conditions defining $\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})$, which by [DDT94, Thm. 2.18] is computed by

$$\mathrm{corank}_{S_\mathfrak{P}} \mathrm{H}^1(K_\mathfrak{p}, A_\mathfrak{P}) + \mathrm{corank}_{S_\mathfrak{P}} \mathrm{H}^1_\pm(K_{\bar{\mathfrak{p}}}, A_\mathfrak{P}) - \mathrm{corank}_{S_\mathfrak{P}} \mathrm{H}^0(K_w, A_\mathfrak{P}), \tag{6.8}$$

where w denotes the infinite place of K. By Proposition 3.8, the first two terms in (6.8) are equal to 2 and 1, respectively, and the third term is clearly equal to 2. Thus $r = 1$ in (6.7) and letting $k \to \infty$ we conclude that

$$\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P}) \simeq (\Phi_\mathfrak{P}/S_\mathfrak{P}) \oplus \mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P}). \tag{6.9}$$

Hence the $S_\mathfrak{P}$-coranks of $\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})$ and $\mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P})$ differ by one, and their quotient by the maximal divisible submodule have the same order. The argument in the proof of [AH06, Lem. 1.2.6] (taking also care of the prime $\mathfrak{P} = p\Lambda^{\mathrm{ac}}$ by approximating it by $\mathfrak{Q} = (Y + p^m) \subset \Lambda^{\mathrm{ac}} \simeq \mathbf{Z}_p[\![Y]\!]$ as $m \to \infty$) now allows us to conclude the proof of part (2), once we show that for $\mathfrak{P}$ outside a finite set Σ_Λ, the natural maps

$$\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P}) \to \mathrm{Sel}^{\mathrm{rel},\pm}(K, \mathbf{A}^{\mathrm{ac}})[\mathfrak{P}], \tag{6.10}$$

$$\mathrm{H}^1_{\pm,\mathrm{str}}(K, A_\mathfrak{P}) \to \mathrm{Sel}^{\pm,\mathrm{str}}(K, \mathbf{A}^{\mathrm{ac}})[\mathfrak{P}], \tag{6.11}$$

have finite kernel and cokernel, of order bounded by a constant depending only on the degree $[S_\mathfrak{P} : \Lambda^{\mathrm{ac}}/\mathfrak{P}]$. For (6.11), this is shown in Lemma 6.5, and for (6.10), it suffices to note that $\mathrm{H}^1_{\mathrm{rel},\pm}(K, A_\mathfrak{P})$ injects into $\mathrm{Sel}^{\mathrm{rel},\pm}(K, A_\mathfrak{P})$ with quotient contained in $\mathrm{H}^0(K_\mathfrak{p}, A_\mathfrak{P})/\mathrm{H}^0(K_\mathfrak{p}, A_\mathfrak{P})_{\mathrm{div}}$, which has a bound of the desired sort, and apply Lemma 6.5 again. This completes the proof. □

With the explicit reciprocity law of Theorem 6.2 and the preceding three lemmas in hand, we are now ready to establish the link Conjecture 4.8 and Conjecture 5.2.

Theorem 6.8. *The following are equivalent:*

(i) *Both* $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ *and* $X^{\pm}$ *have* Λ^{ac}*-rank one, and the following divisibility holds in* Λ^{ac}*:*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm}_{\mathrm{tors}}\big) \subset \mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}^{\pm}_{\infty}}\right)^2.$$

(ii) *Both* $\mathrm{Sel}^{\mathrm{str,rel}}(K,\mathbf{T}^{\mathrm{ac}})$ *and* $X^{\mathrm{rel,str}}$ *are* Λ^{ac}*-torsion, and the following divisibility holds in* Λ^{ur}*:*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)\Lambda^{\mathrm{ur}} \subset \big(L_{\mathfrak{p}}^{\mathrm{BDP}}\big).$$

The same result holds for the opposite divisibilities. In particular, Conjectures 4.8 and 5.2 are equivalent.

Proof. Note that $E(K)[p]=0$ (since $E[p]$ is irreducible as a $G_{\mathbf{Q}_p}$-module and p splits in K), and hence $E(K_\infty)[p^\infty]=0$, which by [PR00, §1.3.3] implies that the Λ^{ac}-torsion submodule of $\mathrm{H}^1(K,\mathbf{T}^{\mathrm{ac}})$ is trivial. Global duality yields the following exact sequence

$$\begin{aligned} 0 \to \mathrm{Sel}^{\mathrm{str,rel}}(K,\mathbf{T}^{\mathrm{ac}}) \to \mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} \mathrm{H}^1_{\pm}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}}) \\ \to X^{\mathrm{rel,str}} \to X^{\pm,\mathrm{str}} \to 0. \end{aligned} \tag{6.12}$$

Since $\mathrm{H}^1_{\pm}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}}) \simeq \Lambda^{\mathrm{ac}}$ (see Proposition 3.8), by Theorem 6.2 the equivalence between ranks in parts (i) and (ii) follows easily from (6.12). Indeed, if both $X^{\mathrm{rel,str}}$ and $\mathrm{Sel}^{\mathrm{str,rel}}(K,\mathbf{T}^{\mathrm{ac}})$ are Λ^{ac}-torsion, then (6.12) shows that $\mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$ has Λ^{ac}-rank one, and since by Lemma 4.7 and Corollary 6.4 the submodule $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}}) \subset \mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$ contains the non-torsion class $\mathbf{z}^{\pm}_{\infty}$, it follows that $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ has rank one, and therefore so does $X^{\pm}$ by Lemma 6.7(1). The other implication for Λ^{ac}-ranks is similar.

As for the relation between divisibilities in (i) and (ii), note that it follows from the preceding paragraph that either of the rank hypotheses in (i) or (ii) implies that both $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ and $\mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$ have Λ^{ac}-rank one, and hence $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}}) = \mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})$, since the quotient $\mathrm{Sel}^{\pm,\mathrm{rel}}(K,\mathbf{T}^{\mathrm{ac}})/\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ injects into $\mathrm{H}^1(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})/\mathrm{H}^1_{\pm}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})$, which has trivial Λ^{ac}-torsion by Proposition 3.8. The map $\mathrm{loc}_{\mathfrak{p}}$ in (6.12) is therefore the same as the one in the exact sequence

$$\begin{aligned} 0 \to \mathrm{Sel}^{\mathrm{str},\pm}(K,\mathbf{T}^{\mathrm{ac}}) \to \mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} \mathrm{H}^1_{\pm}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}}) \\ \to X^{\mathrm{rel},\pm} \to X^{\pm} \to 0. \end{aligned} \tag{6.13}$$

Since $\mathrm{H}^1(K,\mathbf{T}^{\mathrm{ac}})$ has trivial Λ^{ac}-torsion, the non-vanishing of $\mathrm{loc}_{\mathfrak{p}}$ and the equality $\mathrm{rank}_{\Lambda^{\mathrm{ac}}}(\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})) = 1$ implies that $\mathrm{Sel}^{\mathrm{str},\pm}(K,\mathbf{T}^{\mathrm{ac}}) = 0$, since it is of Λ^{ac}-rank zero. From (6.13) we thus obtain

$$0 \to \frac{\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}^{\pm}_{\infty}} \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} \frac{\mathrm{H}^1_{\pm}(K_{\mathfrak{p}},\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathrm{loc}(\mathbf{z}^{\pm}_{\infty})} \to \mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}) \to 0,$$

which by Theorem 6.2 yields the relation

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_{\infty}^{\pm}}\right)\cdot\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})\big)\Lambda^{\mathrm{ur}}=(\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}). \tag{6.14}$$

On the other hand, taking Λ^{ac}-torsion in the short exact sequence $0\to\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})\to X^{\mathrm{rel},\pm}\to X^{\pm}\to 0$ deduced from (6.13) and using Lemma 6.7(2) (noting that $X^{\pm,\mathrm{str}}$ is Λ^{ac}-torsion) we obtain

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm,\mathrm{str}}\big)=\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm}_{\mathrm{tors}}\big)\cdot\mathrm{char}_{\Lambda^{\mathrm{ac}}}(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})). \tag{6.15}$$

Similarly, the short exact sequence $0\to\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})\to X^{\mathrm{rel,str}}\to X^{\pm,\mathrm{str}}\to 0$ from (6.12) yields

$$\begin{aligned}\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)&=\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm,\mathrm{str}}\big)\cdot\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}})\big)\\&=\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm}_{\mathrm{tors}}\big)\cdot\mathrm{char}_{\Lambda^{\mathrm{ac}}}(\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}))^2,\end{aligned}$$

using (6.15) for the second equality. Combined with (6.14) we thus obtain

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\mathrm{rel,str}}\big)\cdot\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_{\infty}^{\pm}}\right)\Lambda^{\mathrm{ur}}=\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm}_{\mathrm{tors}}\big)\cdot\big(\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}\big)^2.$$

The equivalence between the divisibilities in the statement of the proposition is now clear. □

6.3. **A p-converse to Gross–Zagier and Kolyvagin for supersingular primes.** In this section we prove a p-converse to a theorem of Gross–Zagier and Kolyvagin for supersingular primes (Theorem 6.11).

The key step in our proof is the following result towards Conjecture 4.8.

Theorem 6.9. *Assume that:*

(i) *N is squarefree,*
(ii) *some prime $\ell\mid N$ is non-split in K,*
(iii) *if N is odd, then 2 splits in K.*

Then both $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ and $X^{\pm}$ have Λ^{ac}-rank one, and we have the equality

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}\big(X^{\pm}_{\mathrm{tors}}\big)=\mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_{\infty}^{\pm}}\right)^2$$

as ideals in $\Lambda^{\mathrm{ac}}[1/p]$. If in addition $E[p]$ is ramified at every prime $\ell\mid N^-$, then the equality holds in Λ^{ac}.

Proof. In the Appendix we explain how to adapt the methods of [How04a] to deduce from Corollary 6.4 that both $X^{\pm}$ and $\mathrm{Sel}^{\pm}(K,\mathbf{T}^{\mathrm{ac}})$ have Λ^{ac}-rank one, see Theorem A.5, and that we have the divisibility "$\subseteq$" in Λ^{ac} in the claimed equality of characteristic ideals. In light of the equivalences in Theorem 6.8 (whose proof applies without change for the Iwasawa algebras with p inverted), the result follows from Theorem 5.3. □

Let x_1 be the Heegner point of conductor one (see Proposition 4.1), and set

$$y_K = \mathrm{Tr}_{K[1]/K}(x_1) \in E(K) \otimes \mathbf{Z}_p.$$

It is immediate from the definitions that $\mathrm{Sel}^+(K, E[p^\infty]) = \mathrm{Sel}_{p^\infty}(E/K)$ and $\mathrm{Sel}^+(K,T)$ is identified with the pro-p Selmer group

$$\check{S}_p(E/K) = \varprojlim_m \mathrm{Sel}_{p^m}(E/K).$$

In the next result we recall all our running hypotheses for the convenience of the reader.

Theorem 6.10. *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, $p > 3$ a prime of good supersingular reduction for E, and K an imaginary quadratic field satisfying hypotheses* (gen-H) *and* (spl)*. Assume that:*

(i) *N is squarefree,*
(ii) *some prime $\ell \mid N$ is non-split in K,*
(iii) *if N is odd, then 2 splits in K.*

If $\mathrm{Sel}_{p^\infty}(E/K)$ has $\mathbf{Z}_p$-corank one, then y_K is non-torsion.

Proof. Let $\mathfrak{P}_0 = \ker(\Lambda^{\mathrm{ac}} \to \mathbf{Z}_p)$ be the augmentation ideal. Since $\mathbf{A}^{\mathrm{ac}}[\mathfrak{P}_0] = E[p^\infty]$ and $\mathbf{T}^{\mathrm{ac}}/\mathfrak{P}_0\mathbf{T}^{\mathrm{ac}} = T$, by Lemma 6.5 there are natural maps with finite kernel and cokernel:

$$\begin{aligned} X^+/\mathfrak{P}_0 X^+ &\to \mathrm{Sel}^+(K, E[p^\infty]) = \mathrm{Sel}_{p^\infty}(E/K), \\ \mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})/\mathfrak{P}_0\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}}) &\to \mathrm{Sel}^+(K,T) = \check{S}_p(E/K). \end{aligned} \tag{6.16}$$

By Theorem A.5 we have a Λ^{ac}-module pseudo-isomorphism $X^+ \sim \Lambda^{\mathrm{ac}} \oplus M \oplus M$ for some finitely generated torsion Λ^{ac}-module M, and Theorem 6.9 gives the equality[4]

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}(M) = \mathrm{char}_{\Lambda^{\mathrm{ac}}}\left(\frac{\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}})}{\Lambda^{\mathrm{ac}}\mathbf{z}_\infty^+}\right)$$

as ideals in $\Lambda^{\mathrm{ac}}[1/p]$. Thus the assumption that $\mathrm{Sel}_{p^\infty}(E/K)$ has $\mathbf{Z}_p$-corank 1 implies that $\mathrm{char}_{\Lambda^{\mathrm{ac}}}(\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})/\Lambda^{\mathrm{ac}}\mathbf{z}_\infty^+)$ is not divisible by $\mathfrak{P}_0$, and hence, denoting by $\mathbf{z}_0^+$ the image of $\mathbf{z}_\infty^+$ in $\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})/\mathfrak{P}_0\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})$, it follows that $\mathbf{z}_0$ generates a $\mathbf{Z}_p$-submodule of $\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})/\mathfrak{P}_0\mathrm{Sel}^+(K, \mathbf{T}^{\mathrm{ac}})$ of finite index. Since $\check{S}_p(E/K)$ has $\mathbf{Z}_p$-rank one by hypothesis, and by construction the class $\mathbf{z}_0^+$ is sent to the Kummer image of y_K in $\check{S}_p(E/K)$ under the second map in (6.16), the result follows. □

We conclude with the proof of Theorem A in the Introduction.

Theorem 6.11. *Let $E/\mathbf{Q}$ be a semistable elliptic curve, and $p > 3$ a prime of good supersingular reduction for E. Then*

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

[4]Note that only the divisibility "$\subseteq$" coming from Theorem 5.3 is needed for this proof.

Proof. By Ribet's level lowering [Rib90, Thm. 1.1], the representation $E[p]$ is ramified at some prime q dividing N. Fix one such prime q, and choose an imaginary quadratic field K of discriminant D_K such that:

(a) hypothesis (gen-H) holds,
(b) q is non-split in K,
(c) hypothesis (spl) holds,
(d) if N is odd, then 2 splits in K,
(e) $L(E^K, 1) \neq 0$.

The existence of such K follows easily from the non-vanishing result [FH95, Thm. B]. Indeed, if N is divisible by another prime $q' \neq q$, we require q, q' to be both inert in K and every prime factor of N/qq' to split in K; while if $N = q$, we consider K ramified at q. Any such K satisfies conditions (a) and (b); in particular, the root number of E/K is $w(E/K) = -1$. Since $\mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}) = 1 \implies w(E/\mathbf{Q}) = -1$ by [Kim07, Thm. 4.30], it follows that $w(E^K/\mathbf{Q}) = +1$, and since (a) through (d) impose only finitely many congruence conditions on the discriminant of K, condition (e) can also be arranged by [FH95, Thm. B].

Having fixed K as above, by work of Kolyvagin [Kol88] and Kato [Kat04], the non-vanishing of $L(E^K, 1)$ implies that

$$\mathrm{rank}_{\mathbf{Z}} E^K(\mathbf{Q}) = 0, \quad \#Ш(E^K/\mathbf{Q})[p^\infty] < \infty.$$

Thus

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

and so the Heegner point y_K is non-torsion by Theorem 6.10. By the Gross–Zagier formula [GZ86, YZZ13], it follows that $\mathrm{ord}_{s=1}L(E/K, s) = 1$, which by (e) implies that $\mathrm{ord}_{s=1}L(E, s) = 1$. □

Appendix A. Kolyvagin system argument

In this Appendix we explain how to derive a Kolyvagin system from the set of plus/minus Heegner classes constructed in §4.1, and use it to prove Theorem A.5 below towards Conjecture 4.8.

We place ourselves in the setting of §6. We begin by briefly recalling the ingredients from the theory of Kolyvagin systems that we need, referring the reader to [MR04, How04a] for more details. Let $\mathcal{L}$ denote the set of rational primes ℓ satisfying:

- $\ell \nmid Np$,
- ℓ is inert in K,
- $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$, where $a_\ell = \ell + 1 - \#\tilde{E}(\mathbf{F}_\ell)$,

and denote by $\mathcal{N}$ the set of squarefree products of primes $\ell \in \mathcal{L}$, with the convention that $1 \in \mathcal{N}$. For each $\ell \in \mathcal{L}$, let $I_\ell \subset \mathbf{Z}_p$ be the ideal generated by a_ℓ and $\ell + 1$, and for $S = \ell_1 \cdots \ell_r \in \mathcal{N}$ set $I_S = \sum_{i=1}^r I_{\ell_i}$, with $I_S = 0$ when $S = 1$.

For any G_K-module M and v a finite prime of K, define the *unramified* local condition $\mathrm{H}^1_{\mathrm{f}}(K_v, M)$ by

$$\mathrm{H}^1_{\mathrm{f}}(K_v, M) := \ker\big\{\mathrm{H}^1(K_\ell, M) \to \mathrm{H}^1(K_\ell^{\mathrm{ur}}, M)\big\},$$

and the *singular quotient* $\mathrm{H}^1_{\mathrm{s}}(K_v, M)$ by the exactness of the sequence

$$0 \to \mathrm{H}^1_{\mathrm{f}}(K_v, M) \to \mathrm{H}^1(K_v, M) \to \mathrm{H}^1_{\mathrm{s}}(K_v, M) \to 0.$$

Then for $\ell \in \mathcal{L}$, letting λ be the prime of K above ℓ, there is a *finite-singular comparison map*

$$\phi_\ell^{\mathrm{fs}} = \mathrm{Ev}_{\sigma_\ell}^{-1} \circ \mathrm{ev}_\lambda : \mathrm{H}^1_{\mathrm{f}}(K_\lambda, \mathbf{T}^{\mathrm{ac}}/I_\ell) \simeq \mathbf{T}^{\mathrm{ac}}/I_\ell \simeq \mathrm{H}^1_{\mathrm{s}}(K_\lambda, \mathbf{T}^{\mathrm{ac}}/I_\ell), \tag{A.1}$$

where ev_λ is given by evaluation at a Frobenius element at λ, and $\mathrm{Ev}_{\sigma_\ell}$ is given by evaluation at a fixed generator σ_ℓ of $G(\ell) := \mathrm{Gal}(K[\ell]/K[1])$, viewed as an element in the Galois group of the totally tamely ramified extension $K[\ell]_{\lambda'}/K_\lambda$, where λ' is the unique prime of $K[\ell]$ above λ.

For each $S = \ell_1 \cdots \ell_r \in \mathcal{N}$ set

$$\mathcal{G}(S) := \mathrm{Gal}(K[S]/K), \quad G(S) := \mathrm{Gal}(K[S]/K[1]) \simeq G(\ell_1) \times \cdots \times G(\ell_r),$$

and note that since the primes ℓ_i are inert, each $G(\ell_i)$ is cyclic order $\ell_i + 1$. Fix generators $\sigma_{\ell_i} \in G(\ell_i)$, and define the *Kolyvagin derivative operator* $D_S \in \mathbf{Z}[G(S)] \simeq \mathbf{Z}[G(\ell_1)] \otimes \cdots \otimes \mathbf{Z}[G(\ell_r)]$ by

$$D_S := D_{\ell_1} \cdots D_{\ell_r}, \quad \text{where } D_{\ell_i} := \sum_{j=1}^{\ell_i} j\sigma_{\ell_i}^j \in \mathbf{Z}[G(\ell_i)].$$

Tracing through the construction of $\mathbf{z}_\infty[S]^\pm$ in §4.1, [How04a, Lem. 1.7.1] implies that the natural image of

$$\tilde{\kappa}_S^\pm := \sum_{\sigma \in \mathcal{G}(S)/G(S)} \sigma D_S \mathbf{z}_\infty[S]^\pm \in \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}})$$

in $\mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$ is fixed under $\mathcal{G}(S)$.

In what follows we shall use repeatedly the fact that $E(K)[p] = 0$, which (as already noted in the body of the paper) is immediate from the fact that $E[p]$ is an irreducible $G_{\mathbf{Q}_p}$-module and p splits in K.

Lemma A.1. *For every $S \in \mathcal{N}$ the restriction map*

$$\mathrm{res}_S : \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}}) \to \mathrm{H}^1(K[S], \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})^{\mathcal{G}(S)}$$

is an isomorphism.

Proof. This follows readily from the inflation-restriction exact sequence, noting that $\mathrm{H}^0(K[S], \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}}) \simeq \varprojlim_n \mathrm{H}^0(K_n^{\mathrm{ac}}[S], E[I_S])$ vanishes, since $E(K_\infty)[p^\infty] = 0$ and $\mathbf{Q}(E[p^\infty]) \cap K[S] = \mathbf{Q}$. □

In light of Lemma A.1, we let $\kappa_S^\pm \in \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$ be the unique class satisfying $\mathrm{res}_S(\kappa_S^\pm) = \tilde{\kappa}_S^\pm$. To describe its local properties, for $\ell \in \mathcal{L}$ define the *transverse* local condition $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, M)$ by

$$\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, M) := \ker\left\{\mathrm{H}^1(K_\lambda, M) \to \mathrm{H}^1(K[\ell]_{\lambda'}, M)\right\},$$

where λ' is the unique prime of $K[\ell]$ above λ. Letting $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}}/I)$ be the propagation of $\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}})$ under a quotient map $\mathbf{T}^{\mathrm{ac}} \twoheadrightarrow \mathbf{T}^{\mathrm{ac}}/I$, for $S \in \mathcal{N}$ define the S-transverse Selmer group $\mathrm{H}^1_{\mathcal{F}^\pm(S)}(K, \mathbf{T}^{\mathrm{ac}}/I\mathbf{T}^{\mathrm{ac}})$ to be

$$\ker\left\{\mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}/I) \to \prod_{v\nmid S} \frac{\mathrm{H}^1(K_v, \mathbf{T}^{\mathrm{ac}}/I)}{\mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}}/I)} \times \prod_{v\mid S} \frac{\mathrm{H}^1(K_v, \mathbf{T}^{\mathrm{ac}}/I)}{\mathrm{H}^1_{\mathrm{tr}}(K_v, \mathbf{T}^{\mathrm{ac}}/I)}\right\}.$$

Lemma A.2. *Let $S \in \mathcal{N}$. Then we have $p^d \cdot \kappa_S^\pm \in \mathrm{H}^1_{\mathcal{F}^\pm(S)}(K, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$ for some $d \geqslant 0$ independent of S.*

Proof. Let $\lambda \mid \ell \mid S$ be a prime, and as before let λ' be the unique prime of $K[\ell]$ above λ. Then for every n the prime λ' splits completely in $K_n^{\mathrm{ac}}[S]$, and fixing a prime λ'' of $K_n^{\mathrm{ac}}[S]$ above λ' we have $K[\ell]_{\lambda'} = K_n^{\mathrm{ac}}[S]_{\lambda''}$. Hence from the construction of $\mathbf{z}_\infty[S]^\pm$ in Proposition 4.4, to show that $\kappa_S^\pm$ satisfies the transverse local condition at ℓ is suffices to check that $\sum_{\sigma\in\mathcal{G}(S)/G(S)} \sigma D_S z_n[S]$ has trivial restriction to $\mathrm{H}^1(K_n^{\mathrm{ac}}[S]_{\lambda''}, T/I_S T)$, which is checked in the proof of [How04a, Lem. 1.7.3]. On the other hand, for primes $v \nmid S$ the only non-trivial condition to check is that at the primes $v \mid p$ and at the primes $v \mid N$. In the former case, that the class $\kappa_S^\pm$ satisfies $\mathrm{loc}_v(\kappa_S^\pm) \in \mathrm{H}^1_{\mathcal{F}^\pm}(K_v, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$ follows immediately from Lemma 4.7. And in the latter case, the existence of some $d \geqslant 0$ such that $p^d \cdot \mathrm{loc}_v(\kappa_S^\pm) \in \mathrm{H}^1_{\mathcal{F}^\pm(S)}(K_v, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})$ (for all $v \mid N$ and all S) is shown by the same argument as in the proof of the inclusion (15) in [How04b, Prop. 3.4.1]. □

Lemma A.3. *For all $\ell S \in \mathcal{N}$, we have $\phi_\ell^{\mathrm{fs}}\big(\mathrm{loc}_\lambda(p^d \cdot \kappa_S^\pm)\big) = \mathrm{loc}_\lambda(p^d \cdot \kappa_{\ell S}^\pm)$.*

Proof. This follows from [How04a, Prop. 1.7.4] similarly as in the proof of Lemma A.2. □

In terms of [How04a, Def. 1.2.3], the preceding Lemmas A.2 and A.3 show that the collection of classes $\{p^d \cdot \kappa_S^\pm\}_{S\in\mathcal{N}}$ forms a *Kolyvagin system* for the triple $(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}^\pm, \mathcal{L})$. Letting $\mathbf{KS}(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}^\pm, \mathcal{L})$ denote the Λ^{ac}-module of such systems, we have thus shown the following.

Theorem A.4. *There exists a collection of cohomology classes*

$$\boldsymbol{\kappa}^\pm = \{\kappa_n^\pm \in \mathrm{H}^1(K, \mathbf{T}^{\mathrm{ac}}/I_S\mathbf{T}^{\mathrm{ac}})\}_{n\in\mathcal{N}}$$

with $\kappa_1^\pm = \mathbf{z}_\infty^\pm$ such that $p^d \cdot \boldsymbol{\kappa}^\pm := \{p^d \cdot \kappa_n^\pm\}_{n\in\mathcal{N}} \in \mathbf{KS}(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}^\pm, \mathcal{L})$.

Since $\mathbf{z}_\infty^\pm$ is not Λ^{ac}-torsion by Corollary 6.4, the Kolyvagin system $p^d \cdot \boldsymbol{\kappa}^\pm$ of Theorem A.4 is non-trivial. From the methods of Mazur–Rubin [MR04], as extended by Howard [How04a, How04b] to the anticyclototomic setting of Heegner points, we thus obtain:

Theorem A.5. *Assume that N is squarefree. Then the module $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ has Λ^{ac}-rank one, and there is a finitely generated Λ^{ac}-module M such that:*

(i) $X^\pm \sim \Lambda^{\mathrm{ac}} \oplus M \oplus M$,

(ii) *We have the divisibility*

$$\mathrm{char}_{\Lambda^{\mathrm{ac}}}(M) \supset \mathrm{char}_{\Lambda^{\mathrm{ac}}}(\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}})/\Lambda^{\mathrm{ac}}\mathbf{z}_{\infty}^{\pm})$$

in Λ^{ac}.

Proof. Let $\mathfrak{P}$ be a height one prime of Λ^{ac} with $\mathfrak{P} \neq p\Lambda^{\mathrm{ac}}$, let $S_{\mathfrak{P}}$ be the integral closure of $\Lambda^{\mathrm{ac}}/\mathfrak{P}$, and let $T_{\mathfrak{P}} := \mathbf{T}^{\mathrm{ac}} \otimes_{\Lambda^{\mathrm{ac}}} S_{\mathfrak{P}}$, endowed with the diagonal Galois action G_K-action. Let $\Phi_{\mathfrak{P}}$ be the field of fractions of $S_{\mathfrak{P}}$, and set $V_{\mathfrak{P}} := T_{\mathfrak{P}} \otimes_{S_{\mathfrak{P}}} \Phi_{\mathfrak{P}}$, $A_{\mathfrak{P}} := V_{\mathfrak{P}}/T_{\mathfrak{P}}$. Letting $\mathcal{F}_{\mathrm{ss}}^{\pm}$ denote the Selmer structure on $T_{\mathfrak{P}}$ obtained by propagation, specialization at $\mathfrak{P}$ yields a map

$$\mathbf{KS}(\mathbf{T}^{\mathrm{ac}}, \mathcal{F}^{\pm}, \mathcal{L}) \to \mathbf{KS}(T_{\mathfrak{P}}, \mathcal{F}_{\mathrm{ss}}^{\pm}, \mathcal{L}).$$

Denoting by $p^d \cdot \boldsymbol{\kappa}^{\pm,(\mathfrak{P})} = \{p^d \cdot \kappa_n^{\pm,(\mathfrak{P})}\}_{n\in\mathcal{N}}$ the image of $p^d \cdot \boldsymbol{\kappa}^{\pm}$ under this map, it follows from Lemma 6.5 and the non-triviality of $\mathbf{z}_{\infty}^{\pm}$ that the class $\kappa_1^{\pm,(\mathfrak{P})}$ is non-torsion for all but finitely many $\mathfrak{P}$. Since by [Kim07, Prop. 4.11] the local conditions $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ss}}^{\pm}}(K_v, T_{\mathfrak{P}})$ for $v \mid p$ are self-dual under the local Tate pairing and by [Edi97, Prop. 2.1] our assumption that N is squarefree and p is supersingular (so in particular, $E[p]$ is an irreducible $G_{\mathbf{Q}}$-module) implies that the $G_{\mathbf{Q}}$-action of $E[p]$ is surjective[5], by [How04b, Thm. 2.2.2] it follows that for all but finitely many $\mathfrak{P}$ we have $\kappa_1^{\pm,(\mathfrak{P})} \in \mathrm{H}^1_{\mathcal{F}_{\mathrm{ss}}^{\pm}}(K, T_{\mathfrak{P}})$, that $\mathrm{H}^1_{\mathcal{F}_{\mathrm{ss}}^{\pm}}(K, T_{\mathfrak{P}})$ is a free, rank one $S_{\mathfrak{P}}$-module, and that

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{ss}}^{\pm}}(K, A_{\mathfrak{P}}) \simeq (\Phi_{\mathfrak{P}}/S_{\mathfrak{P}}) \oplus M_{\mathfrak{P}} \oplus M_{\mathfrak{P}},$$

with $M_{\mathfrak{P}}$ a finite $S_{\mathfrak{P}}$-module satisfying

$$\mathrm{length}(M_{\mathfrak{P}}) \leq \mathrm{length}(\mathrm{H}^1_{\mathcal{F}_{\mathrm{ss}}^{\pm}}(K, T_{\mathfrak{P}})/S_{\mathfrak{P}} \cdot \kappa_1^{\pm,(\mathfrak{P})}).$$

The same argument as in [How04a, Thm. 2.2.10] then yields the result. □

References

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

[BCK21] Ashay Burungale, Francesc Castella, and Chan-Ho Kim, *A proof of Perrin-Riou's Heegner point main conjecture*, Algebra Number Theory **15** (2021), no. 7, 1627–1653.

[BCST22] Ashay Burungale, Francesc Castella, Christopher Skinner, and Ye Tian, *p^∞-Selmer groups and rational points on CM elliptic curves*, Ann. Math. Qué. **46** (2022), no. 2, 325–346.

[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.

[BST21] Ashay Burungale, Christopher Skinner, and Ye Tian, *Elliptic curves and Beilinson–Kato elements: rank one aspects*, preprint (2021).

[BSZ14] Manjul Bhargava, Christopher Skinner, and Wei Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, preprint, arXiv:1407.1826.

[5]We thank the anonymous referee for bringing this result to our attention.

[BT20] Ashay A. Burungale and Ye Tian, *p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin*, Invent. Math. **220** (2020), no. 1, 211–253.

[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.

[Ç09] Mirela Çiperiani, *Tate-Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes*, Compos. Math. **145** (2009), no. 2, 293–308.

[CGLS22] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner, *On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes*, Invent. Math. **227** (2022), no. 2, 517–580.

[CH18] Francesc Castella and Ming-Lun Hsieh, *Heegner cycles and p-adic L-functions*, Math. Ann. **370** (2018), no. 1-2, 567–628.

[CLW22] Francesc Castella, Zheng Liu, and Xin Wan, *Iwasawa-Greenberg main conjecture for nonordinary modular forms and Eisenstein congruences on GU(3,1)*, Forum Math. Sigma **10** (2022), Paper No. e110, 90.

[CW15] Francesc Castella and Xin Wan, *Iwasawa main conjecture for Heegner points: supersingular case*, (not for publication), arXiv:1506.02538.

[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.

[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.

[dS87] Ehud de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987.

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

[Edi97] ———, *Serre's conjecture*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 209–242.

[FH95] Solomon Friedberg and Jeffrey Hoffstein, *Nonvanishing theorems for automorphic L-functions on* GL(2), Ann. of Math. (2) **142** (1995), no. 2, 385–423.

[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.

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

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[HB15] Ernest Hunter Brooks, *Shimura curves and special values of p-adic L-functions*, Int. Math. Res. Not. IMRN (2015), no. 12, 4177–4241.

[Hid88] Haruzo Hida, *A p-adic measure attached to the zeta functions associated with two elliptic modular forms. II*, Ann. Inst. Fourier (Grenoble) **38** (1988), no. 3, 1–83.

[Hid10] ———, *The Iwasawa μ-invariant of p-adic Hecke L-functions*, Ann. of Math. (2) **172** (2010), no. 1, 41–137.

[How04a] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.

[How04b] ———, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45.

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

[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)

[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.

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

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

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

[Kim14] ———, *Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field*, Canad. J. Math. **66** (2014), no. 4, 826–843.

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

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and Sha(E,$\mathbf{Q}$) for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.

[Kri20] Daniel Kriz, *Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture*, preprint, arXiv:2002.04767.

[LLM23] Antonio Lei, Meng Fai Lim, and Katharina Müller, *Asymptotic formula for the Tate–Shafarevich groups of p-supersingular elliptic curves over anticyclotomic extensions*, preprint, arXiv:2302.06553.

[LLZ15] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for modular forms over imaginary quadratic fields*, Compos. Math. **151** (2015), no. 9, 1585–1625.

[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.

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

[PR87] Bernadette Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.

[PR94] ———, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161, With an appendix by Jean-Marc Fontaine.

[PR00] ———, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, Providence, RI, 2000.

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

[PW11] Robert Pollack and Tom Weston, *On anticyclotomic μ-invariants of modular forms*, Compos. Math. **147** (2011), no. 5, 1353–1381.

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[Ser98] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Ski20] Christopher Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, Ann. of Math. (2) **191** (2020), no. 2, 329–354.

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

[Wal85] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242.

[Wan20] Xin Wan, *Iwasawa main conjecture for Rankin-Selberg p-adic L-functions*, Algebra Number Theory **14** (2020), no. 2, 383–483.

[Wan21a] ———, *Heegner Point Kolyvagin System and Iwasawa Main Conjecture*, Acta Math. Sin. (Engl. Ser.) **37** (2021), no. 1, 104–120.

[Wan21b] ———, *Iwasawa Main Conjecture for Supersingular Elliptic Curves and BSD Conjecture*, preprint, arXiv:1411.6352v8.

[Wan23] Haining Wang, *Indivisibility of Heegner cycles over Shimura curves and Selmer groups*, J. I. Math. Jussieu, to appear (2023), to appear.

[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.

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

Conflicts of interest. None.

Data availability. Not applicable.

Department of Mathematics, University of California Santa Barbara, CA 93106, USA

Email address: castella@ucsb.edu

Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Science, No. 55 Zhongguancun East Road, Beijing, 100190, China

Email address: xwan@math.ac.cn