DERIVED p-ADIC HEIGHTS AND THE LEADING COEFFICIENT OF THE BERTOLINI–DARMON–PRASANNA p-ADIC L-FUNCTION

FRANCESC CASTELLA, CHI-YUN HSU, DEBANJANA KUNDU, YU-SHENG LEE, AND ZHENG LIU

Abstract. Let $E/\mathbf{Q}$ be an elliptic curve and let p be an odd prime of good reduction for E. Let K be an imaginary quadratic field satisfying the classical Heegner hypothesis and in which p splits. The goal of this paper is two-fold:

(1) We formulate a p-adic BSD conjecture for the p-adic L-function $L_{\mathfrak{p}}^{\rm BDP}$ introduced by Bertolini–Darmon–Prasanna [BDP13].
(2) For an algebraic analogue $F_{\overline{\mathfrak{p}}}^{\rm BDP}$ of $L_{\mathfrak{p}}^{\rm BDP}$, we show that the "leading coefficient" part of our conjecture holds, and that the "order of vanishing" part follows from the expected "maximal non-degeneracy" of an anticyclotomic p-adic height.

In particular, when the Iwasawa–Greenberg Main Conjecture $(F_{\overline{\mathfrak{p}}}^{\rm BDP}) = (L_{\mathfrak{p}}^{\rm BDP})$ is known, our results determine the leading coefficient of $L_{\mathfrak{p}}^{\rm BDP}$ at $T=0$ up to a p-adic unit. Moreover, by adapting the approach of Burungale–Castella–Kim [BCK21], we prove the main conjecture for supersingular primes p under mild hypotheses.

In the p-ordinary case, and under some additional hypotheses, similar results were obtained by Agboola–Castella [AC21], but our method is new and completely independent from theirs, and apply to all good primes.

Contents

1. Introduction

1.1. **The BDP p-adic L-function.** Let $E/\mathbf{Q}$ be an elliptic curve of conductor N and let p be an odd prime of good reduction for E. Set $f\in S_2(\Gamma_0(N))$ to denote the newform associated with E. Let K be an imaginary quadratic field of discriminant prime to Np, and assume the classical *Heegner hypothesis*, i.e., that

(Heeg) $$\text{every prime factor of } N \text{ splits in } K.$$

Fix an embedding $\iota_p:\overline{\mathbf{Q}}\hookrightarrow\overline{\mathbf{Q}}_p$, and assume also that

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

Date: December 10, 2024.
2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11R23, 11G16.

with $\mathfrak{p}$ the prime of K above p induced by ι_p. Let K_∞/K be the anticyclotomic $\mathbf{Z}_p$-extension, and put

$$\Gamma = \mathrm{Gal}(K_\infty/K), \qquad \Lambda = \mathbf{Z}_p[\![\Gamma]\!], \qquad \Lambda_{\widehat{\mathcal{O}}} = \Lambda\widehat{\otimes}_{\mathbf{Z}_p}\widehat{\mathcal{O}},$$

where $\widehat{\mathcal{O}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$.

In a seminal paper [BDP13], Bertolini–Darmon–Prasanna introduced a p-adic L-function

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}} \in \Lambda_{\widehat{\mathcal{O}}}$$

whose square $L_{\mathfrak{p}}^{\mathrm{BDP}} = (\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}})^2$ interpolates central critical values of the complex L-function of f/K twisted by infinite order characters of Γ. The main result in *op. cit.*, asserts that the value of $L_{\mathfrak{p}}^{\mathrm{BDP}}$ at the trivial character $\mathbb{1}$ of Γ (which lies outside the range of interpolation) is given by

$$\text{(BDP)} \qquad L_{\mathfrak{p}}^{\mathrm{BDP}}(\mathbb{1}) = \frac{1}{u_K^2 c_E^2}\cdot\left(\frac{1-a_p(E)+p}{p}\right)^2\cdot\log_{\omega_E}(z_K)^2.$$

Here, $a_p(E) := p+1-\#E(\mathbf{F}_p)$, $u_K := \frac{1}{2}\#\mathcal{O}_K^\times$, $z_K \in E(K)$ is a Heegner point arising from a modular parametrisation

$$\varphi_E : X_0(N) \to E$$

with associated Manin constant[1] $c_E \in \mathbf{Z}_{>0}\cap\mathbf{Z}_{(p)}$ (so $z_K\otimes c_E^{-1} \in E(K)\otimes\mathbf{Z}_p$ is independent of the choice of φ_E), and

$$\log_{\omega_E} : E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p \to \mathbf{Z}_p$$

is the formal group logarithm associated with a Néron differential $\omega_E \in \Omega^1(E/\mathbf{Z}_{(p)})$.

The above formula (BDP) has been a key ingredient in recent progress over the past decade towards the Birch–Swinnerton-Dyer conjecture when the analytic rank of E is ≤ 1: [JSW17], [Ski20], etc. (see [Bur22] and the references therein).

The goal of this paper is to formulate and study a p-adic analogue of the Birch–Swinnerton-Dyer conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$ for *all good primes* $p > 2$, predicting:

(i) the "order of vanishing" of $L_{\mathfrak{p}}^{\mathrm{BDP}}$ at the trivial character $\mathbb{1}$;
(ii) a formula for the "leading coefficient" of $L_{\mathfrak{p}}^{\mathrm{BDP}}$ at $\mathbb{1}$.

In the p-ordinary case, this task was first carried out by Agboola–Castella [AC21] drawing from the methods of Bertolini–Darmon [BD95]. The formulation of the conjecture in [AC21] imposed some technical hypotheses required for the existence of a "perfect control theorem": $p \nmid c_\ell$ for the Tamagawa numbers c_ℓ of $E/\mathbf{Q}_\ell$ for all primes $\ell \mid N$, and $p \nmid \#E(\mathbf{F}_p)$. Such control theorem is well-known to fail in the supersingular case. Moreover, it was also assumed that $\#Ш(E/K)[p^\infty] < \infty$.

The new approach in this paper allows us to give a formulation of a p-adic BSD conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$ without any of those additional hypotheses and for all good primes $p > 2$. Moreover, modulo the expected "maximal non-degeneracy" of an anticyclotomic p-adic height pairing, we prove our conjecture for an algebraic analogue of $L_{\mathfrak{p}}^{\mathrm{BDP}}$.

1.2. **p-adic analogue of BSD for $L_{\mathfrak{p}}^{\mathrm{BDP}}$.** For the formulation of our conjecture, we assume that the triple (E, K, p) satisfies the following additional hypotheses:

$$\text{(h0)} \qquad E(K)[p] = 0,$$

and that for every $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ the restriction map

$$\text{(h1)} \qquad \mathrm{res}_{\mathfrak{q}} : \check{S}_p(E/K) \to E(K_{\mathfrak{q}})\otimes\mathbf{Z}_p$$

[1] using [Maz78] for the inclusion $c_E \in \mathbf{Z}_{(p)}$.

has non-torsion image, where $\check{S}_p(E/K) = \varprojlim_k \mathrm{Sel}_{p^k}(E/K)$ is the usual compact Selmer group. (Note that (h1) is implied by the finiteness of $Ш(E/K)[p^\infty]$, since by the p-parity conjecture [Nek01, Kim07], hypothesis (Heeg) implies that the Selmer group $\check{S}_p(E/K)$ has odd $\mathbf{Z}_p$-rank.)

Denote by $E(K_\mathfrak{q})_{/\mathrm{tor}}$ the quotient of $E(K_\mathfrak{q})$ by its torsion submodule, and let $\mathrm{res}_{\mathfrak{q}/\mathrm{tor}}$ be the composition of $\mathrm{res}_\mathfrak{q}$ with the projection $E(K_\mathfrak{q}) \otimes \mathbf{Z}_p \to E(K_\mathfrak{q})_{/\mathrm{tor}} \otimes \mathbf{Z}_p$. Let

$$T = \varprojlim_k E[p^k]$$

be the p-adic Tate module of E, and set $\mathrm{Sel}_\mathfrak{q}(K,T) = \ker(\mathrm{res}_{\mathfrak{q}/\mathrm{tor}})$.

In Section 3, building on Howard's theory of derived p-adic heights [How04], we construct a filtration

$$\mathrm{Sel}_\mathfrak{q}(K,T) \supset \underleftarrow{\mathfrak{S}}_\mathfrak{q}^{(1)} \supset \underleftarrow{\mathfrak{S}}_\mathfrak{q}^{(2)} \supset \cdots \supset \underleftarrow{\mathfrak{S}}_\mathfrak{q}^{(i)} \supset \cdots,$$

with $\underleftarrow{\mathfrak{S}}_\mathfrak{p}^{(i)} = \{0\}$ for $i \gg 0$, equipped with a sequence of "derived" p-adic height pairings

$$h_\mathfrak{p}^{(i)} : \underleftarrow{\mathfrak{S}}_\mathfrak{p}^{(i)} \times \underleftarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)} \to J^i/J^{i+1}, \tag{1.1}$$

where $J \subset \Lambda$ is the augmentation ideal. Using these pairings, we define a p-adic regulator

$$\mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \in \big((J^\sigma/J^{\sigma+1}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p\big)/\mathbf{Z}_p^\times,$$

where $\sigma = \sum_{i\geq 1} i \cdot \mathrm{rank}_{\mathbf{Z}_p}(\underleftarrow{\mathfrak{S}}_\mathfrak{p}^{(i)}/\underleftarrow{\mathfrak{S}}_\mathfrak{p}^{(i+1)})$. By construction, $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ is *always* nonzero.

Set

$$r := \mathrm{rank}_{\mathbf{Z}_p}\check{S}_p(E/K).$$

Under hypotheses (h0)-(h1), the Selmer groups $\mathrm{Sel}_\mathfrak{q}(K,T) \subset \check{S}_p(E/K)$ are free $\mathbf{Z}_p$-modules of rank $r-1$ and r, respectively. Let $(s_1, \dots, s_{r-1})$ be a $\mathbf{Z}_p$-basis for $\mathrm{Sel}_\mathfrak{p}(K,T)$, and extend it to a $\mathbf{Z}_p$-basis $(s_1, \dots, s_{r-1}, s_\mathfrak{p})$ for $\check{S}_p(E/K)$. In particular, $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}(s_\mathfrak{p}) \neq 0$.

The following is our p-adic BSD conjecture for $L_\mathfrak{p}^{\mathrm{BDP}}$.

Conjecture 1.1 (p-adic BSD conjecture for $L_\mathfrak{p}^{\mathrm{BDP}}$)**.** *Assume* (h0)-(h1).

(i) (Leading Coefficient Formula) *Let*

$$\varrho_{\mathrm{an}} = \mathrm{ord}_J L_\mathfrak{p}^{\mathrm{BDP}} := \max\{i \geq 0 : \ L_\mathfrak{p}^{\mathrm{BDP}} \in J^i\},$$

and denote by $\overline{L_\mathfrak{p}^{\mathrm{BDP}}}$ *the natural image of* $L_\mathfrak{p}^{\mathrm{BDP}}$ *in* $J^{\varrho_{\mathrm{an}}}/J^{\varrho_{\mathrm{an}}+1}$*. Then, up to a p-adic unit*

$$\overline{L_\mathfrak{p}^{\mathrm{BDP}}} = \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \log_\mathfrak{p}(s_\mathfrak{p})^2 \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \cdot \#Ш_{\mathrm{BK}}(K,W) \cdot \prod_{\ell \mid N} c_\ell^2.$$

(ii) (Order of Vanishing) *Let* $r^\pm$ *denote the* $\mathbf{Z}_p$*-rank of the* $\pm$*-eigenspace of* $\check{S}_p(E/K)$ *under the action of complex conjugation. Then,*

$$\varrho_{\mathrm{an}} = 2(\max\{r^+, r^-\} - 1).$$

Here c_ℓ is the Tamagawa number of $E/\mathbf{Q}_\ell$, $W = E[p^\infty]$, and $Ш_{\mathrm{BK}}(K,W) = \mathrm{Sel}_{p^\infty}(E/K)_{/\mathrm{div}}$ is the Bloch–Kato Tate–Shafarevich group, i.e., the quotient of the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ by its maximal divisible submodule. Also,

$$\log_\mathfrak{p} : \check{S}_p(E/K) \to \mathbf{Z}_p$$

denotes the composition $\log_{\omega_E} \circ \mathrm{res}_{\mathfrak{p}/\mathrm{tor}}$.

Remark 1.2. In the p-ordinary case, a variant of Conjecture 1.1 was formulated in [AC21], with a regulator defined using the theory of derived p-adic heights by Bertolini–Darmon [BD95]. An important advantage of the present formulation in comparison with the formulation of [AC21, Conj. 4.2] is that the latter requires a hypothesis on the derived p-adic heights amounting to the requirement that $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} = 0$ for $i \geq p$ for the definition of their derived p-adic regulator in [*op. cit.*, Def. 4.1], whereas our formulation of Conjecture 1.1 is completely unconditional.

Remark 1.3. Assuming $\#Ш(E/K)[p^\infty] < \infty$ for the usual Tate–Shafarevich group $Ш(E/K)$, it is possible to remove the ambiguity by a p-adic unit in the formulation of Conjecture 1.1(i). Indeed, following an observation from [BD95, Rem. 2.21], this can be achieved as follows: in this case

$$\check{S}_p(E/K) \simeq E(K) \otimes \mathbf{Z}_p = (E(K)/E(K)_{\mathrm{tor}}) \otimes \mathbf{Z}_p \simeq \mathbf{Z}_p^r,$$

using (h0) for the middle equality. Let M be an endomorphism of $\check{S}_p(E/K)$ sending a $\mathbf{Z}$-basis $(P_1, \ldots, P_r)$ of $E(K)/E(K)_{\mathrm{tor}} \simeq \mathbf{Z}^r$ to $(s_1, \ldots, s_{r-1}, s_{\mathfrak{p}})$. Then it suffices to replace $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ in the right-hand side of Conjecture 1.1(i) by the modification

$$\det(M)^{-2} \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}},$$

which is a well-defined element in $(J^\sigma/J^{\sigma+1}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and is independent of the choice of M.

Remark 1.4. When $\mathrm{ord}_{s=1} L(E/K, s) = 1$, Conjecture 1.1(ii) follows immediately from (BDP) and the work of Gross–Zagier and Kolyvagin. In this case, $\varrho_{\mathrm{an}} = 0$, and the Leading Coefficient Formula in Conjecture 1.1(i) is *equivalent* to the p-part of the Birch–Swinnerton-Dyer formula for $L'(E/K, 1)$ (see Proposition 4.4).

1.3. **Main results.** By the Iwasawa–Greenberg Main Conjecture (see Conjecture 2.4), $L_{\mathfrak{p}}^{\mathrm{BDP}}$ should generate the characteristic ideal of a Λ-adic Selmer group denoted $X_{\overline{\mathfrak{p}}} = \mathrm{Sel}_{\overline{\mathfrak{p}}}(K_\infty, W)^\vee$ in the body of the paper. This module is known to be Λ-torsion under hypothesis (h0) (see Proposition 2.5).

The main result of this paper is the following.

Theorem 1.5. *Let $F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}} \in \Lambda$ be a generator of $\mathrm{char}_\Lambda(X_{\overline{\mathfrak{p}}})$, and put*

$$\varrho_{\mathrm{alg}} = \mathrm{ord}_J F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}} := \max\{i \geq 0 : \ F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}} \in J^i\}.$$

(i) *Let $\overline{F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}}$ be the natural image of $F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}$ in $J^{\varrho_{\mathrm{alg}}}/J^{\varrho_{\mathrm{alg}}+1}$. Then, up to a p-adic unit*

$$\overline{F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}} = \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2 \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \cdot \#Ш_{\mathrm{BK}}(K, W) \cdot \prod_{\ell | N} c_\ell^2.$$

(ii) *Furthermore,*

$$\varrho_{\mathrm{alg}} \geq 2(\max\{r^+, r^-\} - 1),$$

with equality if and only if $\mathrm{rank}_{\mathbf{Z}_p} \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(2)} = |r^+ - r^-| - 1$ *and* $\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)} = 0$ *for* $i \geq 3$.

Set $h_{\mathfrak{p}} := h_{\mathfrak{p}}^{(1)}$. We say that $h_{\mathfrak{p}}$ is *maximally non-degenerate* when the condition for equality in the last part of Theorem 1.5 holds. In the p-ordinary case, conjectures due to Mazur and Bertolini–Darmon ([BD95, §3]) imply that $h_{\mathfrak{p}}$ is maximally non-degenerate (see Remark 6.14), and we expect this condition to hold for all good primes $p > 2$. (For the second assertion in Theorem 1.5(ii), note that hypothesis (Heeg) and the p-parity conjecture imply that r^+ and r^- have different parities, and so $|r^+ - r^-| - 1 \geq 0$.)

As a consequence, when the Iwasawa–Greenberg Main Conjecture

$$(F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}) \stackrel{?}{=} (L_{\mathfrak{p}}^{\mathrm{BDP}}) \tag{1.2}$$

is known, Theorem 1.5 implies Conjecture 1.1(i) (up to a p-adic unit). For ordinary primes, a proof of the Main Conjecture (1.2) was obtained in [BCK21]. In Section 7 we extend their methods to the supersingular case, leading to the following result.

Theorem 1.6. *Let $p > 2$ be a prime of good supersingular reduction for E, and let K be an imaginary quadratic field satisfying* (Heeg) *and* (spl). *Assume in addition that:*

(i) *N is square-free.*
(ii) *$E[p]$ is ramified at every prime $\ell \mid N^+$.*
(iii) *$E[p]$ is ramified at every prime $\ell \mid N^-$ with $\ell \equiv \pm 1 \pmod p$.*
(iv) *Every prime above p is totally ramified in K_∞/K.*

Then $X_{\bar{\mathfrak{p}}}$ is Λ-torsion, with

$$\mathrm{char}_\Lambda\big(X_{\bar{\mathfrak{p}}}\big) = \big(L_{\mathfrak{p}}^{\mathrm{BDP}}\big).$$

In other words, the Iwasawa–Greenberg Main Conjecture (1.2) *holds.*

Hence (together with the proof of (1.2) in [BCK21] in the p-ordinary case, since Theorem 1.5 also applies to this case), our results in this paper determine (up to a p-adic unit) the leading coefficient of $L_{\mathfrak{p}}^{\mathrm{BDP}}$ at $T = 0$ for all primes $p > 2$ of good reduction, and reduce a full proof of Conjecture 1.1 to the expected maximal non-degeneracy of $h_{\mathfrak{p}}$.

1.4. **Relation to prior work.** In the p-ordinary case, a version of Theorem 1.5 was obtained in [AC21, Thm. 6.12] under some additional hypotheses, including:

(i) $a_p(E) \not\equiv 1 \pmod p$,
(ii) $p \nmid c_\ell$ for all primes $\ell \mid N$,
(iii) $\#Ш(E/K)[p^\infty] < \infty$.

As noted in [*op. cit.*, §6.2], their proof is largely based on an adaptation of the arguments from [BD95], and hypotheses (i) and (ii) are essential to their method. Our proof, building on the approach to derived p-adic heights later developed by Howard [How04], is completely different from and independent of [AC21], and we are able to dispense with hypotheses (i)–(iii) (and obtain a result also in the p-supersingular case).

Back to the p-ordinary case, Sano [San23] has also given a new proof of [AC21, Thm. 6.12] removing hypotheses (i) and (ii) by building on an extension of Nekovář's descent formalism [Nek06, §11.6] using "derived" Bockstein maps; his methods are also different from ours.

Finally we note that for supersingular primes $p > 2$, the results of Theorem 1.5 is new for all cases $\varrho_{\mathrm{alg}} > 0$; on the other hand, the case $\varrho_{\mathrm{alg}} = 0$ of Theorem 1.5 (in which case $\mathrm{Sel}_{\mathfrak{q}}(K,T) = 0$ and p-adic heights make no appearance) can be deduced from the "anticyclotomic control theorem" of Jetchev–Skinner–Wan [JSW17], but our results also give a new proof in this case.

1.5. **Method of proof.** In a series of papers culminating in [PR92] (see also [Col00]), Perrin-Riou developed a method for computing the leading coefficient of algebraic p-adic L-functions in terms of arithmetic invariants. In the setting of this paper, her methods allow one to determine a formula for ϱ_{alg} and the image $\overline{F_{\bar{\mathfrak{p}}}^{\mathrm{BDP}}} \in J^{\varrho_{\mathrm{alg}}}/J^{\varrho_{\mathrm{alg}}+1}$ (up to a p-adic unit) precisely when the sequence

$$0 \to \mathfrak{S}_{\mathfrak{p}}^{(\infty)} \otimes \mathbf{Q}_p \to \mathrm{Sel}_{\mathfrak{p}}(K,V) \xrightarrow{h_{\mathfrak{p}}} \mathrm{Hom}(\mathrm{Sel}_{\bar{\mathfrak{p}}}(K,V),\mathbf{Q}_p) \to \mathrm{Hom}\big(\mathfrak{S}_{\bar{\mathfrak{p}}}^{(\infty)} \otimes \mathbf{Q}_p,\mathbf{Q}_p\big) \to 0$$

is exact, where $V = T \otimes \mathbf{Q}_p$ is the rational p-adic Tate module, $\mathfrak{S}_{\mathfrak{q}}^{(\infty)} \otimes \mathbf{Q}_p = \cap_{i\geq 1}\mathfrak{S}_{\mathfrak{q}}^{(i)} \otimes \mathbf{Q}_p$ is the space of universal norms in $\mathrm{Sel}_{\mathfrak{q}}(K,V)$, and the middle arrow is defined by the p-adic height pairing $h_{\mathfrak{p}}$ (see [PR92, Thm. 3.3.4]). However, in the setting of this paper one can show that

$$\mathfrak{S}_{\mathfrak{q}}^{(\infty)} = 0,$$

(see Proposition 2.5 and Corollary 3.11(ii)), and therefore exactness of (1.3) amounts to the *non-degeneracy* of $h_{\mathfrak{p}}$, which in the anticyclotomic setting fails as long as $|r^+ - r^-| > 1$ (see Proposition 6.11).

The key technical innovation of this paper is the development of an extension of the results of [PR92] applicable to $X_{\overline{\mathfrak{p}}}$, building on Howard's theory of derived p-adic heights [How04] to account for the systematic degeneracies of $h_{\mathfrak{p}}$ in the anticyclotomic setting.

1.6. **Outline of the paper.** In Section 2 we introduce some of our Selmer groups of interest, and state the Iwasawa–Greenberg Main Conjecture (1.2). In Section 3, we extend the results we need from [How04] to our setting, yielding the groundwork for the definition of the derived regulator $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ in the formulation of our conjectures in Section 4. In Section 5, we state our main results toward the p-adic Birch–Swinnerton-Dyer conjectures for $L_{\mathfrak{p}}^{\mathrm{BDP}}$, and Sections 6-7 are devoted to the proofs. In particular, we refer the reader to the start of Section 6 for an outline of the proof of our main Theorem 1.5.

1.7. **Acknowledgements.** This work began at the APAW Collaborative Research Workshop held at the University of Oregon in the summer of 2022. The authors would like to thank the organisers of this workshop, and especially Ellen Eischen, for creating such a stimulating and thought-provoking event. We would also like to thank Takamichi Sano for sending us a copy of his recent preprint and for a number of helpful exchanges, and the anonymous referee for some useful comments and suggestions.

During the preparation of this paper, F.C. was partially supported by the NSF grant DMS-2101458, C.-Y.H. was partially supported by Agence Nationale de Recherche ANR-18-CE40-0029 in the project *Galois representations, automorphic forms and their L-functions (GALF)*, D.K. was partially supported by a PIMS postdoctoral fellowship, and Z.L. was partially supported by the NSF grant DMS-2001527.

This work was partially supported by Ellen Eischen's NSF CAREER grant DMS-1751281, and by the NSF grant DMS-1928930 while some of the authors (F.C., Y.-S.L., and Z.L.) were in residence at MSRI/SLMath during the spring of 2023 for the program "Algebraic Cycles, L-Values, and Euler Systems".

2. Selmer groups

We keep the notation from the Introduction, and assume that the triple (E, K, p) satisfies hypotheses (Heeg) and (spl). For every $n > 0$, we write K_n for the subextension of the anticyclotomic $\mathbf{Z}_p$-extension K_∞/K with $\mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}$.

Let Σ be a finite set of places of K containing the archimedean place ∞ and the primes dividing Np. Denote by Σ_f the set of finite places in Σ, and assume that all primes in Σ_f split in K. For every number field F containing K, let $G_{F,\Sigma} = \mathrm{Gal}(F^\Sigma/F)$ be the Galois group of the maximal algebraic extension of F unramified outside the places above Σ. Recall that T denotes the p-adic Tate module of E, and put

$$V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \qquad W = V/T \simeq E[p^\infty].$$

Definition 2.1. Suppose $F \supset K$ is a field extension, and let $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ be any of the primes of K above p. We define the $\mathfrak{q}$-*strict Selmer group* of V by

$$\mathrm{Sel}_{\mathfrak{q}}(F, V) := \ker\left\{\mathrm{H}^1(G_{F,\Sigma}, V) \to \prod_{w \in \Sigma_f} \frac{\mathrm{H}^1(F_w, V)}{\mathrm{H}^1_{\mathfrak{q}}(F_w, V)}\right\}, \tag{2.1}$$

where

$$\mathrm{H}^1_{\mathfrak{q}}(F_w, V) = \begin{cases} \mathrm{H}^1(F_w, V) & \text{if } w \mid \overline{\mathfrak{q}}, \\ 0 & \text{else.} \end{cases}$$

Similarly, letting $\mathrm{H}^1_{\mathrm{str}}(F_w,V)$ and $\mathrm{H}^1_{\mathrm{rel}}(F_w,V)$ be defined by

$$\mathrm{H}^1_{\mathrm{str}}(F_w,V)=0 \quad \text{for all } w\in\Sigma_f,$$

and

$$\mathrm{H}^1_{\mathrm{rel}}(F_w,V)=\begin{cases}\mathrm{H}^1(F_w,V) & \text{if } w\mid p,\\ 0 & \text{else,}\end{cases}$$

we define the Selmer groups $\mathrm{Sel}_{\mathrm{str}}(F,V)$ and $\mathrm{Sel}_{\mathrm{rel}}(F,V)$ by replacing $\mathrm{H}^1_{\mathfrak{q}}(F_w,V)$ by $\mathrm{H}^1_{\mathrm{str}}(F_w,V)$ and $\mathrm{H}^1_{\mathrm{rel}}(F_w,V)$, respectively, in (2.1).

For $?\in\{\mathfrak{q},\mathrm{str},\mathrm{rel}\}$, let $\mathrm{H}^1_?(F_w,T)$ and $\mathrm{H}^1_?(F_w,W)$ be the pre-image and image, respectively, of $\mathrm{H}^1_?(F_w,V)$ under the natural exact sequence

$$\mathrm{H}^1(F_w,T)\to\mathrm{H}^1(F_w,V)\to\mathrm{H}^1(F_w,W),$$

and define the Selmer groups $\mathrm{Sel}_?(F,T)$ and $\mathrm{Sel}_?(F,W)$ by the same recipe as in Definition 2.1.

Let $\mathrm{Sel}_{p^k}(E/F)\subset\mathrm{H}^1(G_{F,\Sigma},E[p^k])$ be the Selmer group fitting into the p^k-descent exact sequence

$$0\to E(F)/p^kE(F)\to\mathrm{Sel}_{p^k}(E/F)\to Ш(E/F)[p^k]\to 0,$$

where $Ш(E/F)[p^k]$ denotes the p^k-torsion in the Tate–Shafarevich group of E/F. Set

$$\mathrm{Sel}_{p^\infty}(E/F)=\varinjlim_k\mathrm{Sel}_{p^k}(E/F),\qquad\qquad \check{S}_p(E/F)=\varprojlim_k\mathrm{Sel}_{p^k}(E/F),$$

where the limits are with respect to the inclusion $E[p^k]\to E[p^{k+1}]$ and the multiplication-by-p map $E[p^{k+1}]\to E[p^k]$, respectively. Finally, set $K_p:=K\otimes\mathbf{Q}_p\simeq K_{\mathfrak{p}}\oplus K_{\overline{\mathfrak{p}}}$.

Lemma 2.2. *Assume* (h0)-(h1). *Then for every* $\mathfrak{q}\in\{\mathfrak{p},\overline{\mathfrak{p}}\}$

$$\mathrm{Sel}_{\mathfrak{q}}(K,T)=\ker(\mathrm{res}_{\mathfrak{q}/\mathrm{tor}}),$$

where $\mathrm{res}_{\mathfrak{q}/\mathrm{tor}}$ *is the composition*

$$\check{S}_p(E/K)\xrightarrow{\mathrm{res}_{\mathfrak{q}}}E(K_{\mathfrak{q}})\otimes\mathbf{Z}_p\to E(K_{\mathfrak{q}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p.$$

In particular,

$$\mathrm{rank}_{\mathbf{Z}_p}\mathrm{Sel}_{\mathfrak{q}}(K,T)=\mathrm{rank}_{\mathbf{Z}_p}\check{S}_p(E/K)-1.$$

Proof. It follows from global duality and Tate's global Euler characteristic formula that the image of the restriction map

$$\mathrm{Sel}_{\mathrm{rel}}(K,T)\to\mathrm{H}^1(K_p,T):=\mathrm{H}^1(K_{\mathfrak{p}},T)\oplus\mathrm{H}^1(K_{\overline{\mathfrak{p}}},T)$$

has $\mathbf{Z}_p$-rank 2 (see [Ski20, Lem. 2.3.1]). By global duality we also have the exact sequence

$$\begin{aligned}0\to\mathrm{Sel}_{\mathrm{str}}(K,T)\to\check{S}_p(E/K)\xrightarrow{\mathrm{res}_{p/\mathrm{tor}}}&(E(K_{\mathfrak{p}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p)\oplus(E(K_{\overline{\mathfrak{p}}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p)\\ &\to\mathrm{Sel}_{\mathrm{rel}}(K,W)^\vee\to\mathrm{Sel}_{p^\infty}(E/K)^\vee\to 0.\end{aligned}\tag{2.2}$$

Note that by assumption, the $\mathbf{Z}_p$-rank of the image of the map $\mathrm{res}_{p/\mathrm{tor}}=\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}\oplus\mathrm{res}_{\overline{\mathfrak{p}}/\mathrm{tor}}$ is either 1 or 2. In the former case, it follows from [Ski20, Lem. 2.3.2] that

$$\mathrm{Sel}_{\mathfrak{p}}(K,T)=\mathrm{Sel}_{\mathrm{str}}(K,T)=\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T)\tag{2.3}$$

and this yields the conclusion of the lemma. If the image of $\mathrm{res}_{p/\mathrm{tor}}$ has $\mathbf{Z}_p$-rank 2, we see from (2.2) that $\mathrm{Sel}_{p^\infty}(E/K)$ is contained in $\mathrm{Sel}_{\mathrm{rel}}(K,W)$ with finite index, and the conclusion again follows. □

Remark 2.3. A discussion of the case where $\mathrm{im}(\mathrm{res}_{p/\mathrm{tor}})$ has $\mathbf{Z}_p$-rank 2 is missing in the proof of [AC21, Lem. 2.2]. Hence the statement of that lemma needs to be corrected as in Lemma 2.2.

For $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ set

$$\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W) = \varinjlim_n \mathrm{Sel}_{\mathfrak{q}}(K_n, W).$$

As is well-known, $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$ is a cofinitely generated Λ-module, i.e., its Pontryagin dual $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)^\vee$ is finitely generated over Λ.

Conjecture 2.4 (Iwasawa–Greenberg Main Conjecture). *$\mathrm{Sel}_{\overline{\mathfrak{p}}}(K_\infty, W)$ is Λ-cotorsion and*

$$\mathrm{char}_\Lambda(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K_\infty, W)^\vee)\Lambda_{\widehat{\mathcal{O}}} = (L_{\mathfrak{p}}^{\mathrm{BDP}}).$$

Here, as in the Introduction, $L_{\mathfrak{p}}^{\mathrm{BDP}} = (\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}})^2$ denotes the square of the p-adic L-function

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}} \in \Lambda_{\widehat{\mathcal{O}}}$$

introduced in [BDP13] and further studied in [Bra11] (where it was shown to be an element in the Iwasawa algebra) and [CH18a] (where it was also shown to be non-zero).

The first claim in Conjecture 2.4 is now known under a mild hypothesis.

Proposition 2.5. *Assume* (h0). *Then* $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$ *is Λ-cotorsion.*

Proof. In the p-ordinary case, this follows from [CGLS22, Thm. 4.2.2] and [CGS23, Thm. 5.53]. Note that the proof of these results is based on Kolyvagin's methods applied to the anticyclotomic Euler system of Heegner points on E/K and a Λ-adic extension of the formula (BDP) of Bertolini–Darmon–Prasanna obtained in [CH18a, Thm. 5.1]. For supersingular primes p (and assuming $a_p = 0$ when $p = 3$), the result similarly follows from an adaptation of the argument in [CGLS22, Thm. 3.4.1] applied to (signed) Heegner point Kolyvagin system constructed in [CW24, Thm. A.4] (which is non-trivial by [CW24, Cor. 6.4] and in a similar relation to $L_{\mathfrak{q}}^{\mathrm{BDP}}$ as in the p-ordinary case by virtue of [CW24, Thm. 6.2]). Finally, when $p = 3$ is supersingular for E but a_3 is not necessarily zero, the result follows from the analogues of the aforementioned results from [CW24] developed in [CÇSS18, §4]. □

We conclude this section by recalling the following basic result which will be useful in some of our arguments.

Proposition 2.6. *Assume* (h0). *Then* $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$ *has no proper finite index Λ-submodules.*

Proof. As shown in [HL19, Prop. 3.12], this can be deduced from Greenberg's general results [Gre16]. □

3. Howard's derived p-adic heights and the derived regulator

We keep the setting from Section 2, and assume in addition that (h0) holds. In this section, we recall Howard's general construction of derived p-adic heights [How04], and extend some of his results in *op. cit.* to our setting to obtain derived p-adic heights on $\mathrm{Sel}_{\mathfrak{q}}(K, T)$. Then we define the regulator $\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma}$ appearing in the formulation of our conjectures.

3.1. **Λ_k-adic Selmer groups.** Fix a topological generator $\gamma \in \Gamma$. Adopting the notations in [How04], for any k we set

$$\mathcal{O}_k = \mathbf{Z}_p/p^k\mathbf{Z}_p, \qquad \Lambda_k = \mathcal{O}_k[\![\Gamma]\!].$$

Let $\mathcal{K}_k$ be the localisation of Λ_k at all elements of the form $g_n = \frac{\gamma^{p^n}-1}{\gamma-1}$ for some n, and define $\mathcal{P}_k$ by the exactness of the sequence

$$0 \to \Lambda_k \to \mathcal{K}_k \to \mathcal{P}_k \to 0. \tag{3.1}$$

Let $S^{(k)} = E[p^k]$, and put

$$S_{\mathrm{Iw}}^{(k)} := \varprojlim_n \mathrm{Ind}_{K_n/K} S^{(k)}, \qquad S_\infty^{(k)} := \varinjlim_n \mathrm{Ind}_{K_n/K} S^{(k)},$$

where the limits are with respect to the natural corestriction and restriction maps, respectively.

By Shapiro's lemma, we have a canonical $\Lambda_k[G_{K,\Sigma}]$-module isomorphism $S^{(k)}_{\mathrm{Iw}} \simeq S^{(k)} \otimes_{\mathcal{O}_k} \Lambda_k$, where the $G_{K,\Sigma}$-action on Λ_k is given by the inverse of the tautological character $G_{K,\Sigma} \twoheadrightarrow \Gamma \hookrightarrow \Lambda_k^\times$ (see [How04, Lem. 1.4]). There is also an isomorphism $S^{(k)} \otimes_{\mathcal{O}_k} \mathcal{P}_k \simeq S^{(k)}_\infty$ ([How04, Lem. 1.5]) depending on the choice of γ. Tensoring (3.1) over $\mathcal{O}_k$ with $S^{(k)}$, we then obtain

$$0 \to S^{(k)}_{\mathrm{Iw}} \to S^{(k)}_{\mathcal{K}} \to S^{(k)}_\infty \to 0, \tag{3.2}$$

dropping the subscripts in $\mathcal{K}_k$ for the ease of notation.

For $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, let $\mathcal{F}_{\mathfrak{q}}$ be the Selmer structure on $S^{(k)}_{\mathcal{K}}$ given by

$$\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_{\mathcal{K}}) = \begin{cases} \mathrm{H}^1_{\mathrm{unr}}(K_w, S^{(k)}_{\mathcal{K}}) & \text{if } w \nmid p\infty, \\ \mathrm{H}^1(K_{\overline{\mathfrak{q}}}, S^{(k)}_{\mathcal{K}}) & \text{if } w = \overline{\mathfrak{q}}, \\ 0 & \text{if } w = \mathfrak{q}. \end{cases} \tag{3.3}$$

Let $\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_{\mathcal{K}})$ be the associated Selmer group:

$$\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_{\mathcal{K}}) := \ker\left\{ \mathrm{H}^1(G_{K,\Sigma}, S^{(k)}_{\mathcal{K}}) \to \prod_{w \in \Sigma_f} \frac{\mathrm{H}^1(K_w, S^{(k)}_{\mathcal{K}})}{\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_{\mathcal{K}})} \right\}.$$

The short exact sequence (3.2) induces the natural exact sequence

$$\mathrm{H}^1(K_w, S^{(k)}_{\mathrm{Iw}}) \to \mathrm{H}^1(K_w, S^{(k)}_{\mathcal{K}}) \to \mathrm{H}^1(K_w, S^{(k)}_\infty).$$

Taking the image (resp. inverse image) of $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_{\mathcal{K}})$, we obtain the local condition $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_\infty)$ (resp. $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_{\mathrm{Iw}})$). Following [MR04], we refer to these local conditions as being *propagated* from $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_{\mathcal{K}})$ (or $S^{(k)}_{\mathcal{K}}$) via (3.2). The Selmer groups they define will be denoted $\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_\infty)$ and $\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_{\mathrm{Iw}})$, respectively. (Similar definitions of local conditions "by propagation" will be made below.)

Definition 3.1. For every $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, denote by $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)})$ the local conditions obtained from $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)}_\infty)$ by propagation via $S^{(k)} \to S^{(k)}_\infty$, and let

$$\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}) := \ker\left\{ \mathrm{H}^1(G_{K,\Sigma}, S^{(k)}) \to \prod_{w \in \Sigma_f} \frac{\mathrm{H}^1(K_w, S^{(k)})}{\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w, S^{(k)})} \right\}$$

be the resulting Selmer group.

Note that by condition (h0), the natural surjective map $\mathrm{H}^1(G_{K,\Sigma}, S^{(k)}) \twoheadrightarrow \mathrm{H}^1(G_{K,\Sigma}, S^{(k)}_\infty)[J]$ is an isomorphism; since the local conditions on $\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)})$ are propagated from $S^{(k)}_\infty$, this restricts to an isomorphism

$$\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}) \simeq \mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_\infty)[J]. \tag{3.4}$$

3.2. **Howard's derived p-adic heights.** For every $i \geq 1$, let $\mathfrak{S}^{(i)}_{\mathfrak{q},k} \subset \mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)})$ be the submodule mapping to $J^{i-1}\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}_\infty)[J]$ under the isomorphism (3.4). We have a filtration

$$\mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}) = \mathfrak{S}^{(1)}_{\mathfrak{q},k} \supset \mathfrak{S}^{(2)}_{\mathfrak{q},k} \supset \cdots \supset \mathfrak{S}^{(i)}_{\mathfrak{q},k} \supset \cdots .$$

Theorem 3.2 (Howard)**.** *For $i \geq 1$, there is a sequence of canonical symmetric i-th "derived" height pairings*

$$h^{(i)}_{\mathfrak{q},k} : \mathfrak{S}^{(i)}_{\mathfrak{q},k} \times \mathfrak{S}^{(i)}_{\overline{\mathfrak{q}},k} \to \mathcal{O}_k$$

such that the kernel on the left (resp. right) is $\mathfrak{S}^{(i+1)}_{\mathfrak{q},k}$ (resp. $\mathfrak{S}^{(i+1)}_{\overline{\mathfrak{q}},k}$).

Proof. By definition (3.3), the local conditions cutting out $\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\mathcal{K}}^{(k)})$ and $\mathfrak{Sel}_{\overline{\mathfrak{q}}}(K, S_{\mathcal{K}}^{(k)})$, are everywhere exact orthogonal complements under the pairing

$$\mathrm{H}^1(K_w, S_{\mathcal{K}}^{(k)}) \times \mathrm{H}^1(K_w, S_{\mathcal{K}}^{(k)}) \to \mathrm{H}^2(K_w, \mathcal{K}(1)) \simeq \mathcal{K}$$

induced by the Weil pairing $S^{(k)} \times S^{(k)} \to \mathcal{O}_k(1)$. Therefore, by [How04, Thm. 1.11] there is a canonical symmetric *height pairing*

$$\tilde{h}_{\mathfrak{q},k} : \mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)}) \times \mathfrak{Sel}_{\overline{\mathfrak{q}}}(K, S_{\infty}^{(k)}) \to \mathcal{O}_k.$$

(As written here, the pairing $\tilde{h}_{\mathfrak{q},k}$ depends on the choice of a topological generator $\gamma \in \Gamma$, but the J/J^2-valued pairing $(\gamma - 1) \cdot \tilde{h}_{\mathfrak{q},k}$ is independent of γ, as one checks immediately from [How04, Lem. 1.10(b)].) Note that $J^{i-1}\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J]$ is the image of the injection

$$\phi_{i,\gamma} : \frac{\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J^i]}{\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J^{i-1}]} \hookrightarrow \mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J] \tag{3.5}$$

given by multiplication by $(\gamma - 1)^{i-1}$. Thus we may define

$$\tilde{h}_{\mathfrak{q},k}^{(i)} : J^{i-1}\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J] \times J^{i-1}\mathfrak{Sel}_{\overline{\mathfrak{q}}}(K, S_{\infty}^{(k)})[J] \to \mathcal{O}_k$$

by $\tilde{h}_{\mathfrak{q},k}^{(i)}(s,t) := \tilde{h}_{\mathfrak{q},k}(\phi_{i,\gamma}^{-1}(s), t)$. In particular, $\tilde{h}_{\mathfrak{q},k}^{(1)}$ is the restriction of $\tilde{h}_{\mathfrak{q},k}$ to $\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J] \times \mathfrak{Sel}_{\overline{\mathfrak{q}}}(K, S_{\infty}^{(k)})[J]$. By [How04, Lem. 2.3], the left kernel (resp. right kernel) of $\tilde{h}_{\mathfrak{q},k}^{(i)}$ is exactly $J^i\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J]$ (resp. $J^i\mathfrak{Sel}_{\overline{\mathfrak{q}}}(K, S_{\infty}^{(k)})[J]$). Since (3.4) restricts to an isomorphism

$$\mathfrak{S}_{\mathfrak{q},k}^{(i)} \simeq J^{i-1}\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})[J],$$

we can transfer $\tilde{h}_{\mathfrak{q},k}^{(i)}$ to $\mathfrak{S}_{\mathfrak{q},k}^{(i)} \times \mathfrak{S}_{\overline{\mathfrak{q}},k}^{(i)}$ via this isomorphism. Thus, we get a sequence of pairings $h_{\mathfrak{q},k}^{(i)}$ with the stated properties. □

3.3. **Control theorems.** We now compare the Selmer groups $\mathfrak{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})$ (and limits thereof) of the preceding section with the Selmer groups $\mathrm{Sel}_{\mathfrak{q}}(K, T)$ and $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$ (see Corollary 3.6 and Corollary 3.9). This will allow us to deduce from Theorem 3.2 a construction of p-adic height pairings for $\mathrm{Sel}_{\mathfrak{q}}(K, T)$, and to relate their degeneracies to the Λ-module structure of $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$.

Let $\mathrm{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)})$ be the Selmer group cut out by the local conditions

$$\mathrm{H}^1_{\mathfrak{q}}(K_w, S_{\infty}^{(k)}) = \begin{cases} \mathrm{H}^1_{\mathrm{unr}}(K_w, S_{\infty}^{(k)}) & \text{if } w \nmid p\infty, \\ \mathrm{H}^1(K_{\overline{\mathfrak{q}}}, S_{\infty}^{(k)}) & \text{if } w = \overline{\mathfrak{q}}, \\ 0 & \text{if } w = \mathfrak{q}. \end{cases}$$

Putting $S_\infty = \varinjlim_k S_{\infty}^{(k)}$, we also consider the $\Lambda = \mathbf{Z}_p[\![\Gamma]\!]$-module

$$\mathrm{Sel}_{\mathfrak{q}}(K, S_\infty) := \varinjlim_k \mathrm{Sel}_{\mathfrak{q}}(K, S_{\infty}^{(k)}),$$

where the limit is with respect to the maps induced by the inclusion $S^{(k)} \to S^{(k+1)}$.

Lemma 3.3. *For every $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ there is a canonical Λ-module isomorphism*

$$\mathrm{Sel}_{\mathfrak{q}}(K, S_\infty) \simeq \mathrm{Sel}_{\mathfrak{q}}(K_\infty, W).$$

Proof. By Shapiro's lemma, we have $\mathrm{H}^1(G_{K,\Sigma}, S_\infty) \simeq \mathrm{H}^1(G_{K_\infty,\Sigma}, W)$. We check that under the above isomorphism, the Selmer groups in the statement are cut out by the same local conditions. For the primes w above p, this is clear. For the primes $w \in \Sigma_f \setminus \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, we need to check that $\varinjlim_k \mathrm{H}^1_{\mathrm{unr}}(K_w, S_\infty^{(k)}) = 0$, but this follows from [How04, Lem. 1.7], since by our assumption on Σ these primes are split in K, so they are finitely decomposed in K_∞/K. $\square$

Remark 3.4. In light of Lemma 3.3, we shall henceforth write $\mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)$ and $\mathrm{Sel}_{\mathfrak{q}}(K_\infty, W)$ interchangeably.

Directly from the definitions we have the inclusion $\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)}) \subset \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})$. On the other hand, the natural surjection

$$\mathrm{H}^1(G_{K,\Sigma}, S_\infty^{(k)}) \to \mathrm{H}^1(G_{K,\Sigma}, S_\infty)[p^k] \tag{3.6}$$

induces a map $\alpha_{\mathfrak{q}} : \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)}) \to \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)[p^k]$.

Proposition 3.5. *For every $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, the composition*

$$\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)}) \xrightarrow{\subset} \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)}) \xrightarrow{\alpha_{\mathfrak{q}}} \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)[p^k]$$

is injective with finite cokernel of bounded order as $k \to \infty$.

Proof. By (h0), the map (3.6) is an injection, and therefore so is $\alpha_{\mathfrak{q}}$. To bound the cokernel of the map in the statement, we bound the cokernel of each of the two maps in the composition.

From the definitions, we see that the quotient $\mathrm{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})/\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})$ injects into

$$\frac{\mathrm{H}^1(K_{\overline{\mathfrak{q}}}, S_\infty^{(k)})}{\mathrm{im}\big\{\mathrm{H}^1(K_{\overline{\mathfrak{q}}}, S_{\mathcal{K}}^{(k)}) \to \mathrm{H}^1(K_{\overline{\mathfrak{q}}}, S_\infty^{(k)})\big\}} \simeq \ker\big\{\mathrm{H}^2(K_{\overline{\mathfrak{q}}}, S_{\mathrm{Iw}}^{(k)}) \to \mathrm{H}^2(K_{\overline{\mathfrak{q}}}, S_{\mathcal{K}}^{(k)})\big\}. \tag{3.7}$$

By local duality, this is bounded by the size of $\bigoplus_{\eta|\overline{\mathfrak{q}}} E(K_{\infty,\eta})[p^k]$. Since $\bigoplus_{\eta|\overline{\mathfrak{q}}} E(K_{\infty,\eta})[p^\infty]$ is finite by [KO20, Lem. 2.7], the above quotient has the desired bound.

On the other hand, for the primes $w \in \Sigma_f \setminus \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, [How04, Lem. 1.7] gives

$$\mathrm{H}^1_{\mathrm{unr}}(K_w, S_\infty^{(k)}) = \mathrm{H}^1_{\mathrm{unr}}(K_w, S_\infty) = 0.$$

Therefore, by the snake lemma we see that the cokernel of $\alpha_{\mathfrak{q}}$ is bounded by the kernel of the restriction map

$$(r_w)_w : \bigoplus_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} \mathrm{H}^1(K_w, S_\infty^{(k)}) \to \bigoplus_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} \mathrm{H}^1(K_w, S_\infty)[p^k]. \tag{3.8}$$

From the cohomology long exact sequence associated with multiplication by p^k we see that $\ker(r_w) = \mathrm{H}^0(K_w, S_\infty)/p^k\mathrm{H}^0(K_w, S_\infty)$, and this is bounded by

$$\prod_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} \#((B_w)_{/\mathrm{div}}), \quad \text{where } B_w := \bigoplus_{\eta|w} E(K_{\infty,\eta})[p^\infty], \tag{3.9}$$

which is clearly finite and independent of k. Thus $\#\mathrm{coker}(\alpha_{\mathfrak{q}})$ has bounded order as $k \to \infty$, whence the result. $\square$

Corollary 3.6. *With notation as above, the following equality of Λ-modules holds*

$$\varinjlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)}) = \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty).$$

Proof. By Proposition 3.5, $\varinjlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})$ is contained in $\mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)$ with finite index, so the result follows from Proposition 2.6. $\square$

The next result is a variant of Mazur's control theorem for our $\mathfrak{q}$-strict Selmer groups.

Proposition 3.7. *The map $W \to S_\infty$ induces an injection*

$$\beta_{\mathfrak{q}} : \mathrm{Sel}_{\mathfrak{q}}(K, W) \to \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)[J]$$

with finite cokernel.

Proof. The map $\beta_{\mathfrak{q}}$ is the restriction of the natural map $\mathrm{H}^1(G_{K,\Sigma}, W) \to \mathrm{H}^1(G_{K,\Sigma}, S_\infty)$ induced by $W \to S_\infty$. This natural map is part of the cohomology long exact sequence induced by

$$0 \to W \to S_\infty \xrightarrow{\gamma-1} S_\infty \to 0,$$

and by (h0), it induces an isomorphism $\mathrm{H}^1(G_{K,\Sigma}, W) \simeq \mathrm{H}^1(G_{K,\Sigma}, S_\infty)[J]$. The injectivity of $\beta_{\mathfrak{q}}$ follows from this. On the other hand, from the definitions and a direct application of the snake lemma, we see that the cokernel of $\beta_{\mathfrak{q}}$ is bounded by the kernel of the restriction map

$$(r_{\overline{\mathfrak{q}}}, (r_w)_w) : \frac{\mathrm{H}^1(K_{\overline{\mathfrak{q}}}, W)}{\mathrm{H}^1(K_{\overline{\mathfrak{q}}}, W)_{\mathrm{div}}} \times \prod_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} \mathrm{H}^1(K_w, W) \to \{0\} \times \prod_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} \prod_{\eta | w} \mathrm{H}^1(K_{\infty,\eta}, W). \tag{3.10}$$

For $w = \overline{\mathfrak{q}}$, we compute

$$\begin{aligned} \ker(r_{\overline{\mathfrak{q}}}) &= \mathrm{H}^1(K_{\overline{\mathfrak{q}}}, T)_{\mathrm{tors}} \quad \text{by local Tate duality} \\ &= \ker\{\mathrm{H}^1(K_{\overline{\mathfrak{q}}}, T) \to \mathrm{H}^1(K_{\overline{\mathfrak{q}}}, V)\} \\ &= \mathrm{coker}\{\mathrm{H}^0(K_{\overline{\mathfrak{q}}}, V) \to \mathrm{H}^0(K_{\overline{\mathfrak{q}}}, W)\}, \end{aligned} \tag{3.11}$$

where the last equality follows from the cohomology long exact sequence associated to $T \hookrightarrow V \twoheadrightarrow W$. Since $\mathrm{H}^0(K_{\overline{\mathfrak{q}}}, V) = 0$, this shows that

$$\#\ker(r_{\overline{\mathfrak{q}}}) = \#\mathrm{H}^0(K_{\overline{\mathfrak{q}}}, W) = \#E(\mathbf{Q}_p)[p^\infty]. \tag{3.12}$$

For $w = \mathfrak{q}$, we have

$$\ker(r_{\mathfrak{q}}) = B_{\mathfrak{q}}/(\gamma - 1)B_{\mathfrak{q}},$$

where $B_{\mathfrak{q}}$ is as in (3.9), and therefore finite by [KO20, Lem. 2.7]. Finally, for $w \in \Sigma_f \setminus \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ we have $\ker(r_w) = B_w/(\gamma - 1)B_w$. From the exact sequence

$$0 \to E(K_w)[p^\infty] \to B_w \xrightarrow{\gamma-1} B_w \to B_w/(\gamma - 1)B_w \to 0$$

and the finiteness of $E(K_w)[p^\infty]$, we see that

$$(B_w)_{\mathrm{div}} \subset (\gamma - 1)B_w,$$

and so $\#\ker(r_w)$ is bounded by $[B_w : (B_w)_{\mathrm{div}}]$. Since all primes $w \in \Sigma_f$ are finitely decomposed in K_∞/K by our assumption on Σ, this concludes the proof. □

Remark 3.8. When $\#\mathrm{Sel}_{\mathfrak{q}}(K, W) < \infty$, adapting the arguments in [Gre99, §4], one can determine the exact size of the cokernel of the restriction map $\beta_{\mathfrak{q}}$ in Proposition 3.7, resulting in the formula

$$\#\mathrm{coker}(\beta_{\mathfrak{q}}) = (\#E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w|N} c_w^{(p)},$$

where $c_w^{(p)}$ is the p-part of the Tamagawa number of E/K_w (see [JSW17, Thm. 3.3.1]). However, Greenberg's arguments rely crucially on the surjectivity of the global-to-local map

$$\mathrm{H}^1(G_{K,\Sigma}, W) \to \prod_{w \in \Sigma_f} \frac{\mathrm{H}^1(K_w, W)}{\mathrm{H}^1_{\mathfrak{q}}(K_w, W)},$$

which fails when $\mathrm{Sel}_{\mathfrak{q}}(K, W)$ is infinite. In our approach, when $\mathrm{Sel}_{\mathfrak{q}}(K, W)$ is not necessarily finite, a result playing the role of an exact control on $\#\mathrm{coker}(\beta_{\mathfrak{q}})$ will be obtained in §6.3 (see Corollary 6.8).

Corollary 3.9. *The generalised Selmer group* $\varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})[J]$ *is contained in* $\mathrm{Sel}_{\mathfrak{q}}(K, T)$ *with finite index.*

Proof. By (h0), the natural surjection $\mathrm{H}^1(G_{K,\Sigma}, S^{(k)}) \to \mathrm{H}^1(G_{K,\Sigma}, W)[p^k]$ is an isomorphism. Since the local conditions defining $\mathrm{Sel}_{\mathfrak{q}}(K,T)$ and $\mathrm{Sel}_{\mathfrak{q}}(K,W)$ are propagated from $\mathrm{H}^1_{\mathfrak{q}}(K_w, V)$, we have

$$\mathrm{Sel}_{\mathfrak{q}}(K,T) \simeq \varprojlim_k \mathrm{Sel}_{\mathfrak{q}}(K,W)[p^k]. \tag{3.13}$$

On the other hand, it follows from the proof of Proposition 3.7 that for every k there is a natural injection

$$\mathrm{Sel}_{\mathfrak{q}}(K,W)[p^k] \to \mathrm{Sel}_{\mathfrak{q}}(K,S_\infty)[J + p^k\Lambda]$$

with cokernel bounded by the size of

$$\Bigg(E(\mathbf{Q}_p)[p^\infty] \times \prod_{w \in \Sigma_f \setminus \{\overline{\mathfrak{q}}\}} B_w/(\gamma-1)B_w\Bigg)[p^k].$$

Since this is finite (even before taking p^k-torsion) and the transition maps are given by multiplication by p, its inverse limit with respect to k vanishes. Therefore,

$$\varprojlim_k \mathrm{Sel}_{\mathfrak{q}}(K,W)[p^k] \simeq \varprojlim_k \mathrm{Sel}_{\mathfrak{q}}(K,S_\infty)[J+p^k\Lambda]. \tag{3.14}$$

Since Proposition 3.5 implies that $\varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})[J]$ is contained in $\varprojlim_k \mathrm{Sel}_{\mathfrak{q}}(K,S_\infty)[J+p^k\Lambda]$ with finite index, the result follows from (3.13) and (3.14). $\square$

Definition 3.10. For every $i \geq 1$, put

$$\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} = \varprojlim_k \mathfrak{S}_{\mathfrak{q},k}^{(i)},$$

where the limit is with respect to the multiplication-by-p maps $S^{(k+1)} \to S^{(k)}$.

Thus we obtain a filtration

$$\varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K,S^{(k)}) = \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(1)} \supset \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(2)} \supset \cdots \supset \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} \supset \cdots \supset \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(\infty)}, \tag{3.15}$$

where $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(\infty)} := \cap_{i\geq 1}\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)}$. The pairings $h_{\mathfrak{q},k}^{(i)}$ of Theorem 3.2 are compatible as k varies, and in the limit they give rise to a sequence of "derived" p-adic height pairings

$$h_{\mathfrak{q}}^{(i)} : \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} \times \underleftarrow{\mathfrak{S}}_{\overline{\mathfrak{q}}}^{(i)} \to \mathbf{Z}_p \tag{3.16}$$

such that the kernel on the left (resp. right) is $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i+1)}$ (resp. $\underleftarrow{\mathfrak{S}}_{\overline{\mathfrak{q}}}^{(i+1)}$).

Corollary 3.11. *Let $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$. Using $\sim$ to denote Λ-module pseudo-isomorphism, write*

$$\mathrm{Sel}_{\mathfrak{q}}(K,S_\infty)^\vee \sim \Lambda^{e_\infty} \oplus (\Lambda/J)^{e_1} \oplus (\Lambda/J^2)^{e_2} \oplus \cdots \oplus (\Lambda/J^i)^{e_i} \oplus \cdots \oplus M$$

with M a torsion Λ-module with characteristic ideal prime to J. Then

(i) $e_i = \mathrm{rank}_{\mathbf{Z}_p}(\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i+1)})$.

(ii) $e_\infty = \mathrm{rank}_{\mathbf{Z}_p}(\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(\infty)}) = \mathrm{rank}_{\mathbf{Z}_p}(\mathrm{Sel}_{\mathfrak{q}}(K,T)^u)$, *where*

$$\mathrm{Sel}_{\mathfrak{q}}(K,T)^u := \bigcap_n \mathrm{cor}_{K_n/K}(\mathrm{Sel}_{\mathfrak{q}}(K_n,T))$$

is the space of universal norms in $\mathrm{Sel}_{\mathfrak{q}}(K,T)$.

Remark 3.12. Proposition 2.5 says that $\mathrm{Sel}_{\mathfrak{q}}(K,S_\infty)^\vee$ is Λ-torsion, so $e_\infty = 0$.

Proof. The argument leading to the proof of [How04, Cor. 4.3] (for the usual Selmer group) applies *verbatim* to our setting, replacing the use of Proposition 3.5 and Lemma 4.1 in *op. cit.* by Proposition 3.5 and (the proof of) Proposition 3.7 above, respectively. $\square$

3.4. **The derived regulator.** Note that by Corollary 3.9 and (3.4), the Selmer group

$$\varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S^{(k)}) = \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(1)}$$

is contained in $\mathrm{Sel}_{\mathfrak{q}}(K,T)$ with finite index.

Definition 3.13. For $i \geq 1$, define

$$\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(i)} := \big(\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p\big) \cap \mathrm{Sel}_{\mathfrak{q}}(K,T)$$

to be the p-adic saturation of $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)}$ in $\mathrm{Sel}_{\mathfrak{q}}(K,T)$. In particular, $\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(1)} = \mathrm{Sel}_{\mathfrak{q}}(K,T)$.

By linearity, the pairings (3.16) extend to $\mathbf{Q}_p$-valued pairings

$$h_{\mathfrak{q}}^{(i)} : \overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(i)} \times \overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{q}}}^{(i)} \to \mathbf{Q}_p, \tag{3.17}$$

whose kernel on the left (resp. right) is $\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(i+1)}$ (resp. $\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{q}}}^{(i+1)}$) by virtue of Theorem 3.2.

By definition, for every $i \geq 1$ the quotients $\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i+1)}$ and $\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i+1)}$ are free $\mathbf{Z}_p$-modules, and since the action of complex conjugation defines an isomorphism $\mathrm{Sel}_{\mathfrak{p}}(K,S_\infty) \simeq \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,S_\infty)$, by Corollary 3.11(i) the $\mathbf{Z}_p$-ranks of these quotients are equal. Hence for every $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ we have

$$\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{q}}^{(i+1)} \simeq \mathbf{Z}_p^{e_i} \tag{3.18}$$

for some integers $e_i \geq 0$ (the same for both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$). By Corollary 3.11(ii) and Proposition 2.5 we know that $e_i = 0$ for $i \gg 0$.

Note that the i-th derived p-adic heights $h_{\mathfrak{q}}^{(i)}$ depend on the choice of a topological generator γ, but the $(J^i/J^{i+1}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$-valued pairings $(\gamma-1)^i \cdot h_{\mathfrak{q}}^{(i)}$ are independent of this choice. We record the dependence on γ in the following definition.

Definition 3.14. Let $(x_{1,1}, \ldots, x_{1,e_1}; \cdots; x_{i,1}, \ldots, x_{i,e_i}; \cdots)$ be a $\mathbf{Z}_p$-basis for $\mathrm{Sel}_{\mathfrak{p}}(K,T)$ adapted to the filtration

$$\mathrm{Sel}_{\mathfrak{p}}(K,T) = \overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(1)} \supset \overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(2)} \supset \cdots \supset \overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i)} \supset \cdots,$$

so that for every $i \geq 1$ the elements $x_{i,1}, \ldots, x_{i,e_i}$ project to a $\mathbf{Z}_p$-basis for $\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i+1)}$. Let $(y_{1,1}, \ldots, y_{1,e_1}; \cdots; y_{i,1}, \ldots, y_{i,e_i}; \cdots)$ be a $\mathbf{Z}_p$-basis for $\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T)$ defined in the same manner. Define the *i-th partial regulator* by

$$R_{\mathfrak{p},\gamma}^{(i)} := \det\big(h_{\mathfrak{p}}^{(i)}(x_{i,j}, y_{i,j'})\big)_{1 \leq j,j' \leq e_i},$$

and the *derived regulator* by $\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} := \prod_{i \geq 1} R_{\mathfrak{p},\gamma}^{(i)}$.

Remark 3.15. By definition, the partial regulators $R_{\mathfrak{p},\gamma}^{(i)}$ are non-zero, and they are well-defined up to a p-adic unit. So, we have

$$\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \in \mathbf{Q}_p^\times/\mathbf{Z}_p^\times.$$

Replacing $h_{\mathfrak{p}}^{(i)}$ by $(\gamma-1)^i \cdot h_{\mathfrak{p}}^{(i)}$ and writing $\sigma = \sum_{i \geq 1} ie_i$, the above definition gives a non-zero derived regulator

$$\mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \in \big((J^\sigma/J^{\sigma+1}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p\big)/\mathbf{Z}_p^\times$$

which is independent of γ.

4. BSD conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$

In this section, we formulate our p-adic analogue of the Birch–Swinnerton-Dyer conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$, extending the formulation given in [AC21] in the p-ordinary case.

We keep the setting from Section 2, and assume in addition that (h0) and (h1) hold.

By Lemma 2.2, we have

$$\mathrm{Sel}_{\mathfrak{p}}(K,T)=\ker(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}})\simeq \mathbf{Z}_p^{r-1},$$

where $r=\mathrm{rank}_{\mathbf{Z}_p}\check{S}_p(E/K)$. Let $(s_1,\dots,s_{r-1})$ be a $\mathbf{Z}_p$-basis for $\mathrm{Sel}_{\mathfrak{p}}(K,T)$, and extend it to a $\mathbf{Z}_p$-basis $(s_1,\dots,s_{r-1},s_{\mathfrak{p}})$ for $\check{S}_p(E/K)$. In particular, $\mathrm{res}_{\mathfrak{p}}(s_{\mathfrak{p}})\in E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p$ is non-torsion. Henceforth, we let

$$\log_{\mathfrak{p}}:\check{S}_p(E/K)\to\mathbf{Z}_p$$

be the composition of the map $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}$ with the formal group logarithm $E(K_{\mathfrak{p}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p\to\mathbf{Z}_p$ associated with a Néron differential $\omega_E\in\Omega^1(E/\mathbf{Z}_{(p)})$. Also, let $Ш_{\mathrm{BK}}(K,W)=\mathrm{Sel}_{p^\infty}(E/K)_{/\mathrm{div}}$ be the Bloch–Kato Tate–Shafarevich group, and for every prime $\ell\mid N$ write c_ℓ to denote the Tamagawa number of $E/\mathbf{Q}_\ell$.

In the following, we shall interchangeably view $L_{\mathfrak{p}}^{\mathrm{BDP}}$ as an element in $\widehat{\mathcal{O}}[\![T]\!]$ via the identification $\Lambda_{\widehat{\mathcal{O}}}\simeq\widehat{\mathcal{O}}[\![T]\!]$ defined by $T=\gamma-1$ for our fixed topological generator $\gamma\in\Gamma$. Thus T corresponds to a generator of the augmentation ideal $J\subset\Lambda_{\widehat{\mathcal{O}}}$.

Conjecture 4.1 (p-adic BSD conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$)**.** *The following assertions hold:*

(i) (Leading Coefficient Formula) *Let $\varrho_{\mathrm{an}}:=\mathrm{ord}_J L_{\mathfrak{p}}^{\mathrm{BDP}}$. Then, up to a p-adic unit,*

$$\frac{1}{\varrho_{\mathrm{an}}!}\frac{d^{\varrho_{\mathrm{an}}}}{dT^{\varrho_{\mathrm{an}}}}L_{\mathfrak{p}}^{\mathrm{BDP}}\Big|_{T=0}=\left(\frac{1-a_p(E)+p}{p}\right)^2\cdot\log_{\mathfrak{p}}(s_{\mathfrak{p}})^2$$
$$\times\,\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma}\cdot\#Ш_{\mathrm{BK}}(K,W)\cdot\prod_{\ell\mid N}c_\ell^2.$$

(ii) (Order of Vanishing) *Set $r^\pm$ to denote the $\mathbf{Z}_p$-corank of the $\pm$-eigenspace of $\check{S}_p(E/K)$ under the action of complex conjugation. Then*

$$\varrho_{\mathrm{an}}=2(\max\{r^+,r^-\}-1).$$

Remark 4.2. We observe that Conjecture 4.1 is a reformulation (depending on γ) of Conjecture 1.1 in the Introduction.

Remark 4.3. As noted in the Introduction (see Remark 1.2), Conjecture 4.1 extends to all good primes $p>2$ and with an unconditional definition of $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ the p-adic Birch–Swinnerton-Dyer conjecture formulated in [AC21, Conj. 4.2]. That their p-adic heights (deduced from the construction in [BD95]) agree with ours (deduced from the construction in [How04]) when both apply, follows from the height comparisons in [Nek95, §11] and [BMC24, §10].

By the works of Kolyvagin, Gross–Zagier, and Bertolini–Darmon–Prasanna, Conjecture 4.1 enjoys the following compatibility with the classical Birch–Swinnerton-Dyer for $L(E/K,s)$.

Proposition 4.4. *Assume* $\mathrm{ord}_{s=1}L(E/K,s)=1$*. Then:*

(i) *Conjecture 4.1(i) is equivalent to the p-part of the Birch–Swinnerton-Dyler formula for $L'(E/K,1)$.*

(ii) $\varrho_{\mathrm{an}}=0$*, and Conjecture 4.1(ii) holds.*

Proof. By the Gross–Zagier formula [GZ86], the Heegner point $z_K\in E(K)$ in formula (BDP) is non-torsion. Therefore, $\mathrm{rank}_{\mathbf{Z}}E(K)=1$ and $\#Ш(E/K)<\infty$ by Kolyvagin's work [Kol88], and $\varrho_{\mathrm{an}}=0$ by formula (BDP). In particular, Conjecture 4.1(ii) holds.

The above also shows that $\text{Ш}_{\mathrm{BK}}(K,W) = \text{Ш}(E/K)[p^\infty]$ and $\mathrm{rank}_{\mathbf{Z}_p}\check{S}_p(E/K) = 1$. Together with Lemma 2.2, it follows that $\mathrm{Sel}_{\mathfrak{p}}(K,T) = 0$, and so $\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} = 1$. Therefore, if $s_{\mathfrak{p}}$ is any element of $\check{S}_p(E/K) \simeq E(K)\otimes\mathbf{Z}_p$ satisfying $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}(s_{\mathfrak{p}}) \neq 0$, Conjecture 4.1(i) now reads

$$L_{\mathfrak{p}}^{\mathrm{BDP}}(0) \sim_p \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2 \cdot \#\text{Ш}(E/K)[p^\infty] \cdot \prod_{\ell|N} c_\ell^2. \tag{4.1}$$

We can write $z_K \otimes 1 = m \cdot s_{\mathfrak{p}}$, with $m \in \mathbf{Z}_p$ satisfying

$$\mathrm{ord}_p(m) = \mathrm{ord}_p\big([E(K):\mathbf{Z}z_K]\big),$$

and formula (BDP) can then be rewritten as

$$L_{\mathfrak{p}}^{\mathrm{BDP}}(0) \sim_p \frac{m^2}{u_K^2 c_E^2} \cdot \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2. \tag{4.2}$$

Combining (4.1) and (4.2), we thus see that Conjecture 4.1(i) is equivalent to

$$[E(K):\mathbf{Z}z_K]^2 \sim_p u_K^2 c_E^2 \cdot \#\text{Ш}(E/K) \cdot \prod_{\ell|N} c_\ell^2. \tag{4.3}$$

By the Gross–Zagier formula, (4.3) is equivalent to the p-part of the Birch–Swinnerton-Dyer formula for $L'(E/K,1)$ (see e.g. [Zha14, Lem. 10.1]), so this concludes the proof. □

5. Main result

We shall say that the p-adic height pairing $h_{\mathfrak{p}} := h_{\mathfrak{p}}^{(1)}$ is *maximally non-degenerate* if, letting e_i be as in (3.18), we have

$$e_i = \begin{cases} |r^+ - r^-| - 1 & \text{if } i = 2,\\ 0 & \text{if } i \geq 3, \end{cases}$$

where $r^\pm = \mathrm{rank}_{\mathbf{Z}_p}(\check{S}_p(E/K)^\pm)$ for the $\pm$-eigenspace $\check{S}_p(E/K)^\pm$ of $\check{S}_p(E/K)$ under the action of complex conjugation.

The main result of this paper is the following.

Theorem 5.1. *In the setting of §4, let $F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}} \in \Lambda$ be a generator of $\mathrm{char}_\Lambda(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K_\infty,W)^\vee)$. Put $\varrho_{\mathrm{alg}} := \mathrm{ord}_J F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}$.*

(i) *Up to a p-adic unit,*

$$\frac{1}{\varrho_{\mathrm{alg}}!}\frac{d^{\varrho_{\mathrm{alg}}}}{dT^{\varrho_{\mathrm{alg}}}}F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}\Big|_{T=0} = \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2 \times \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot \#\text{Ш}_{\mathrm{BK}}(K,W) \cdot \prod_{\ell|N} c_\ell^2.$$

(ii) *The following inequality holds*

$$\varrho_{\mathrm{alg}} \geq 2(\max\{r^+,r^-\}-1).$$

Furthermore, equality is attained if and only if $h_{\mathfrak{p}}$ is maximally non-degenerate.

Combined with progress towards the Iwasawa–Greenberg Main Conjecture (Conjecture 2.4), we deduce the following result towards the p-adic Birch–Swinnerton-Dyer conjecture for $L_{\mathfrak{p}}^{\mathrm{BDP}}$.

Corollary 5.2. *Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E[p])$ be the mod p representation associated with E. If p is ordinary, assume that:*

(1a) *Either N is square-free or there are at least two primes $\ell \| N$.*
(1b) *$\overline{\rho}$ is ramified at every prime $\ell \| N$.*

(1c) *$\overline{\rho}$ is surjective.*
(1d) *$a_p(E) \not\equiv 1 \pmod{p}$.*
(1e) *$p > 3$.*

If p is supersingular, assume that:

(2a) *N is square-free.*
(2b) *$\overline{\rho}$ is ramified at every prime $\ell \mid N$.*
(2c) *Every prime above p is totally ramified in K_∞/K.*
(2d) *$p > 3$, which implies $a_p(E) = 0$.*

Then,

(i) *The Leading Coefficient Formula of Conjecture 4.1(i) holds.*
(ii) *The following inequality holds*
$$\mathrm{ord}_J L_{\mathfrak{p}}^{\mathrm{BDP}} \geq 2(\max\{r^+, r^-\} - 1).$$
Equality is attained, and hence Conjecture 4.1(ii) holds, if and only if $h_{\mathfrak{p}}$ is maximally non-degenerate.

Proof. In the p-ordinary case, the Iwasawa–Greenberg Main Conjecture (Conjecture 2.4) was proved in [BCK21, Thm. B] under hypotheses (1a)–(1e); in the p-supersingular case, a proof of the same conjecture under hypotheses (2a)–(2d) is given in Corollary 7.2. The result thus follows from Theorem 5.1. □

6. Proof of Theorem 5.1

Before delving into the details, we give a brief outline of the proof of the Leading Coefficient Formula in part (i) of Theorem 5.1. The much shorter proof of part (ii) is given in §6.6.

The proof is divided into four steps. Our starting point is Lemma 6.1, giving an expression for the leading coefficient at $T = 0$ of the characteristic power series F_X of a torsion Λ-module X, where $\Lambda = \mathbf{Z}_p[\![T]\!]$. The formula is in terms of the orders of the flanking terms in the exact sequence
$$0 \to T^r X[T] \to T^r X \xrightarrow{T} T^r X \to T^r X/T^{r+1}X \to 0$$
for any $r \geq \mathrm{ord}_T F_X$. Together with the results from Section 3, this lemma applied to $X_{\overline{\mathfrak{p}}} = \mathrm{Sel}_{\overline{\mathfrak{p}}}(K_\infty, W)^\vee$ leads to a proof of the equality up to a p-adic unit
$$\text{(Step 1)} \qquad \frac{1}{\varrho_{\mathrm{alg}}!}\frac{d^{\varrho_{\mathrm{alg}}}}{dT^{\varrho_{\mathrm{alg}}}} F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}\Big|_{T=0} \sim_p \#\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)}\big)$$
for any $r \geq \varrho_{\mathrm{alg}}$. Passing to the limit in k, the $\mathcal{O}_k$-valued derived height pairings $h_{\mathfrak{p},k}^{(i)}$ give rise to a collection of exact sequences
$$(6.1) \qquad 0 \to \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)} \to \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)} \xrightarrow{h_{\mathfrak{p}}^{(i)}} \mathrm{Hom}_{\mathbf{Z}_p}\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)}, \mathbf{Q}_p/\mathbf{Z}_p\big) \to \mathrm{Hom}_{\mathbf{Z}_p}\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i+1)}, \mathbf{Q}_p/\mathbf{Z}_p\big) \to 0$$
for $i \geq 1$, where $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} = \varprojlim_k \mathfrak{S}_{\mathfrak{q},k}^{(i)}$ and $\underrightarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} = \varinjlim_k \mathfrak{S}_{\mathfrak{q},k}^{(i)}$.

We find the derived regulator $\mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma}$ appearing naturally from an iterative computation using (6.1) for $i = 1, \ldots, r$, leading to a proof of the equality
$$\text{(Step 2)} \qquad \#\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)}\big) \sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot \big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(1)}\big] \cdot \#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{/\mathrm{div}}\big)$$
for any $r \geq \varrho_{\mathrm{alg}}$.

Next we study the local conditions cutting out the Selmer groups $\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(1)}$ and $\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)}$, arriving at a five-term exact sequence from which we can deduce the relation
$$\text{(Step 3)} \quad \big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(1)}\big] \cdot \#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{/\mathrm{div}}\big) = \#(E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w \mid N} c_w^{(p)} \cdot \#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}).$$

Finally, using global duality and a computation using $\log_{\mathfrak{p}}$ we obtain (Step 4)

$$\#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}) \sim_p \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2 \cdot \#\text{Ш}_{\mathrm{BK}}(K,W) \cdot \frac{1}{(\#E(K_{\mathfrak{p}})[p^\infty])^2},$$

which in combination with the previous steps yields the Leading Coefficient Formula in part (i) of Theorem 5.1.

6.1. **Step 1: Non-semisimple torsion Λ-modules and augmentation filtration.** Let X be a Λ-module, where $\Lambda = \mathbf{Z}_p[\![T]\!]$. For every $r \geq 0$, denote by

$$\beta_X^{(r)} : T^rX \to T^rX$$

the map given by multiplication by T, and put $h(\beta_X^{(r)}) = \#\mathrm{coker}(\beta_X^{(r)})/\#\mathrm{ker}(\beta_X^{(r)})$ whenever both terms in the right-hand side are finite.

Lemma 6.1. *Let X be a finitely generated torsion Λ-module, and let $F_X \in \Lambda$ be a generator of* $\mathrm{char}_\Lambda(X)$*. Put*

$$\varrho_X := \mathrm{ord}_T F_X.$$

For any $r \geq \varrho_X$, the sub-quotients $T^rX/T^{r+1}X$ and $T^rX[T]$ are both finite. In addition,

$$\frac{1}{\varrho_X!}\frac{d^{\varrho_X}}{dT^{\varrho_X}}F_X\bigg|_{T=0} \sim_p h(\beta_X^{(r)}) = \frac{\#\big(T^rX/T^{r+1}X\big)}{\#(T^rX[T])},$$

where $\sim_p$ denotes equality up to a p-adic unit.

Proof. Suppose first that X is an elementary module, in the sense that

$$X = \Lambda/(f),$$

where $f = a_nT^n + a_{n+1}T^{n+1} + \cdots \in \Lambda$ with $a_n \neq 0$ (so $n = \varrho_X$). Then for any $r \geq n$ we find

$$\begin{aligned} X[T^r] &= (T^{-n}f)/(f), \\ T^rX &= (T^r,f)/(f) \simeq (T^r)/(T^r)\cap(f) = (T^r)/(T^{r-n}f), \end{aligned}$$

Therefore,for any $r \geq \varrho_X$ we have that $T^rX[T] \simeq X[T^{r+1}]/X[T^r]$ is trivial and

$$T^rX/T^{r+1}X \simeq (T^r)/(T^{r+1},T^{r-n}f) \simeq \mathbf{Z}_p/(a_n)$$

so the result is true in this case.

In general, by the structure theorem there exists a Λ-module homomorphism

$$\phi : X \to Y$$

with finite kernel and cokernel, where Y is a direct sum of elementary modules as above. Since X and Y have the same characteristic ideal and by the above argument the result is true for Y, it remains to show that $h(\beta_X^{(r)}) = h(\beta_Y^{(r)})$ for any $r \geq \varrho_X = \varrho_Y$.

For any Λ-module homomorphism $\beta : M \to M$ with finite kernel and cokernel, put $h(\beta) = \#\mathrm{coker}(\beta)/\#\mathrm{ker}(\beta)$. Note that if $0 \to A \to B \to C \to 0$ is a Λ-module exact sequence, and any two of the multiplication-by-T maps $T_A : A \to A$, $T_B : B \to B$, $T_C : C \to C$ have finite kernel and cokernel, then from an easy application of the snake lemma we see that $h(T_A)$, $h(T_B)$, $h(T_C)$ are all defined, with

$$h(T_B) = h(T_A)\cdot h(T_C). \tag{6.2}$$

For any $r > 0$, ϕ induces maps $\phi_r : T^rX \to T^rY$ with finite kernel and cokernel. Applying (6.2) to the tautological exact sequence $0 \to \mathrm{im}(\phi_r) \to T^rY \to \mathrm{coker}(\phi_r) \to 0$, we obtain

$$h(\beta_Y^{(r)}) = h(T_{\mathrm{im}(\phi_r)})\cdot h(T_{\mathrm{coker}(\phi_r)}) = h(T_{\mathrm{im}(\phi_r)}) \tag{6.3}$$

for any $r \geq \varrho_X$, using that $h(T_{\mathrm{coker}(\phi_r)}) = 1$ (since $\#\mathrm{coker}(\phi_r) < \infty$) for the last equality. On the other hand, applied to $0 \to \ker(\phi_r) \to T^r X \to \mathrm{im}(\phi_r) \to 0$, (6.2) similarly gives

$$h(\beta_X^{(r)}) = h(T_{\ker(\phi_r)}) \cdot h(T_{\mathrm{im}(\phi_r)}) = h(T_{\mathrm{im}(\phi_r)}) \tag{6.4}$$

for any $r \geq \varrho_X$. Combining (6.3) and (6.4), the result follows. □

Remark 6.2. When the action of T on X is "semi-simple" (i.e., when up to pseudo-isomorphism X is of the form $\oplus_i \Lambda/(f_i)$ with $f_i \in \Lambda$ satisfying $\mathrm{ord}_T(f_i) \leq 1$ for all i), Lemma 6.1 recovers a well-known result (see e.g. [PR93, §1.4, Lemme]).

For the rest of this section, we let $\Lambda = \mathbf{Z}_p[\![\Gamma]\!]$ be the anticyclotomic Iwasawa algebra and $J \subset \Lambda$ the augmentation ideal. We shall often identify Λ (resp. J) with the one variable power series ring $\mathbf{Z}_p[\![T]\!]$ (resp. (T)) setting $T = \gamma - 1$ for a fixed choice of topological generator $\gamma \in \Gamma$.

Proposition 6.3. *Let $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$. Let $F_{\mathfrak{q}}^{\mathrm{BDP}} \in \Lambda$ be a generator of the characteristic ideal of $X_{\mathfrak{q}} = \mathrm{Sel}_{\mathfrak{q}}(K, S_\infty)^\vee$, and put $\varrho_{\mathrm{alg}} = \mathrm{ord}_J F_{\mathfrak{q}}^{\mathrm{BDP}}$. Then*

$$\frac{1}{\varrho_{\mathrm{alg}}!} \frac{d^{\varrho_{\mathrm{alg}}}}{dT^{\varrho_{\mathrm{alg}}}} F_{\mathfrak{q}}^{\mathrm{BDP}} \Big|_{T=0} \sim_p \#\big(\underrightarrow{\mathfrak{S}}_{\mathfrak{q}}^{(r+1)}\big)$$

for any $r \geq \varrho_{\mathrm{alg}}$.

Proof. After Lemma 6.1, it suffices to show that we have

$$\#(J^r X_{\mathfrak{q}} / J^{r+1} X_{\mathfrak{q}}) = \#\big(\underrightarrow{\mathfrak{S}}_{\mathfrak{q}}^{(r+1)}\big), \qquad J^r X_{\mathfrak{q}}[J] = 0. \tag{6.5}$$

for any $r \geq \varrho_{\mathrm{alg}}$. Consider the exact sequence

$$0 \to \frac{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^{r+1}]}{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^r]} \to \frac{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)}{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^r]} \to \frac{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)}{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^{r+1}]} \to 0,$$

Taking Pontryagin duals and noting that

$$\big(\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)/\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^r]\big)^\vee = \big(J^r \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)\big)^\vee = J^r X_{\mathfrak{q}},$$

using Corollary 3.6 for the last equality, we obtain the exact sequence

$$0 \to J^{r+1} X_{\mathfrak{q}} \to J^r X_{\mathfrak{q}} \to \mathrm{Hom}_{\mathbf{Z}_p}\bigg(\frac{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^{r+1}]}{\mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J^r]}, \mathbf{Q}_p/\mathbf{Z}_p\bigg) \to 0. \tag{6.6}$$

Via the maps $\phi_{r+1,\gamma}$ in (3.5) given by multiplication by $(\gamma - 1)^r$, the last term in this sequence is identified with the Pontryagin dual of $J^r \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty)[J] \simeq \underrightarrow{\mathfrak{S}}_{\mathfrak{q}}^{(r+1)}$, and so the first equality in (6.5) (for any $r \geq 0$) follows from (6.6).

On the other hand, since by Proposition 2.5 we know that $X_{\mathfrak{q}}$ is Λ-torsion, Corollary 3.11(ii) and our running hypothesis (h0) imply that the filtration (3.15) satisfies $\underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} = 0$ for $i \gg 0$. Let

$$i_0 = \max\{i \geq 1 : \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(i)} \neq 0\}.$$

Then by Corollary 3.11 we may fix a Λ-module pseudo-isomorphism

$$X_{\mathfrak{q}} \sim (\Lambda/J)^{e_1} \oplus (\Lambda/J^2)^{e_2} \oplus \cdots \oplus (\Lambda/J^{i_0})^{e_{i_0}} \oplus M \tag{6.7}$$

with M a torsion Λ-module with characteristic ideal prime to J, and therefore $\#(M[J]) < \infty$. In particular

$$\varrho_{\mathrm{alg}} = e_1 + 2e_2 + \cdots + i_0 e_{i_0}, \tag{6.8}$$

which shows that $r \geq i_0$ for any $r \geq \varrho_{\mathrm{alg}}$. From (6.7), we thus see that for any $r \geq \varrho_{\mathrm{alg}}$ (in fact, $r \geq i_0$ suffices), the Λ-submodule $J^r X_{\mathfrak{q}}[J]$ of $X_{\mathfrak{q}}$ is finite, and so by Proposition 2.6 the second equality in (6.5) follows, whence the result. □

6.2. **Step 2: Derived p-adic regulator.** We begin with a basic algebraic lemma.

Lemma 6.4. *Let $0 \to A \xrightarrow{h} B \to C \to 0$ be an exact sequence of finitely generated modules over $\mathbf{Z}_p$. Then*

$$\#(A_{\mathrm{tor}}) \cdot \#(C_{\mathrm{tor}}) \sim_p \det{}^* h \cdot \#(B_{\mathrm{tor}}),$$

where $\det^* h$ is the product of the non-zero entries in the Smith normal form of $A_{/\mathrm{tor}} \xrightarrow{h} B_{/\mathrm{tor}}$.

Proof. This follows upon noting the relations $\#(C_{\mathrm{tor}}) = \#\big(B_{/\mathrm{tor}}/h(A_{/\mathrm{tor}})\big)_{\mathrm{tor}} \cdot \#(B_{\mathrm{tor}}/h(A_{\mathrm{tor}}))$ and $\#\big(B_{/\mathrm{tor}}/h(A_{/\mathrm{tor}})\big)_{\mathrm{tor}} \sim_p \det^* h$. $\square$

For $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, put

$$\mathfrak{Sel}_{\mathfrak{q}}(K,T) := \underleftarrow{\mathfrak{S}}_{\mathfrak{q}}^{(1)} = \varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K, S_\infty^{(k)})[J], \qquad \mathfrak{Sel}_{\mathfrak{q}}(K,W) := \underrightarrow{\mathfrak{S}}_{\mathfrak{q}}^{(1)}.$$

In particular, we have seen in Corollary 3.9 that $\mathfrak{Sel}_{\mathfrak{q}}(K,T)$ is contained in the $\mathfrak{q}$-strict Selmer groups $\mathrm{Sel}_{\mathfrak{q}}(K,T)$ with finite index.

Proposition 6.5. *For any $r \geq \varrho_{\mathrm{alg}} := \mathrm{ord}_J F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}$, we have*

$$\#\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)}\big) \sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot \big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \mathfrak{Sel}_{\mathfrak{p}}(K,T)\big] \cdot \#\big(\mathfrak{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}\big).$$

Proof. Passing to the limit in k, the $\mathcal{O}_k$-valued i-th derived height pairings $h_{\mathfrak{p},k}^{(i)}$ of Theorem 3.2 induce a pairing

$$\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)} \times \underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)} \to \mathbf{Q}_p/\mathbf{Z}_p.$$

By the descriptions of the kernels of $h_{\mathfrak{p},k}^{(i)}$ in Theorem 3.2, this gives rise to the exact sequence

$$0 \to \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)} \xrightarrow{\alpha^{(i)}} \mathrm{Hom}_{\mathbf{Z}_p}\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)}, \mathbf{Q}_p/\mathbf{Z}_p\big) \to \mathrm{Hom}_{\mathbf{Z}_p}\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i+1)}, \mathbf{Q}_p/\mathbf{Z}_p\big) \to 0.$$

We also have the tautological exact sequence

$$0 \to \underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)} \xrightarrow{\beta^{(i)}} \mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)} \to \mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)} \to 0.$$

Applying Lemma 6.4 to the above two exact sequences gives

$$\frac{\#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i+1)})_{/\mathrm{div}}\big)}{\#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{/\mathrm{div}}\big)} \sim_p \frac{\det^* \alpha^{(i)}}{\#\big((\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)})_{\mathrm{tor}}\big)},$$
$$\#\big((\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)})_{\mathrm{tor}}\big) \sim_p \frac{\det^* \beta^{(i)} \cdot \#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)}\big)_{\mathrm{tor}}}{\#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}\big)_{\mathrm{tor}}},$$

from which we get

$$\frac{\#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i+1)})_{/\mathrm{div}}\big)}{\#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{/\mathrm{div}}\big)} \sim_p \frac{\det^* \alpha^{(i)}}{\det^* \beta^{(i)}} \cdot \frac{\#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}\big)_{\mathrm{tor}}}{\#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)}\big)_{\mathrm{tor}}}. \tag{6.9}$$

For any $r \geq \varrho_{\rm alg}$, using that $\#(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)}) < \infty$ (and so $\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(r+1)} = 0$) and taking the product of (6.9) for $i = 1, \ldots, r$, we arrive at

$$
\begin{aligned}
\#\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)}\big) &= \#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(r+1)})_{/\rm div}\big) \\
&\sim_p \prod_{i=1}^{\varrho_{\rm alg}} \frac{\det^* \alpha^{(i)}}{\det^* \beta^{(i)}} \cdot \frac{\#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(1)}\big)_{\rm tor}}{\#\big(\mathrm{Sel}_{\mathfrak{p}}(K,T)/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(r+1)}\big)_{\rm tor}} \cdot \#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{/\rm div}\big) \\
&\sim_p \prod_{i=1}^{\varrho_{\rm alg}} \frac{\det^* \alpha^{(i)}}{\det^* \beta^{(i)}} \cdot \big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \mathfrak{Sel}_{\mathfrak{p}}(K,T)\big] \cdot \#\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{/\rm div}\big).
\end{aligned} \tag{6.10}
$$

Thus we are reduced to showing that

$$
\frac{\det^* \alpha^{(i)}}{\det^* \beta^{(i)}} = R_{\mathfrak{p},\gamma}^{(i)}, \tag{6.11}
$$

where $R_{\mathfrak{p},\gamma}^{(i)}$ is the partial regulator in Definition 3.14.

By Corollary 3.6, we note that Proposition 3.7 amounts to the statement that $\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)$ is contained in $\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)} \simeq \mathfrak{Sel}_{\overline{\mathfrak{p}}}(K,S_\infty)[J]$ with finite index. Therefore, $(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{\rm div} = \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{\rm div}$. It follows from the definition of $\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T)$ and $\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)$ by propagating the local conditions $\mathrm{H}^1_{\overline{\mathfrak{p}}}(K_w,V)$ that

$$
\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{\rm div}. \tag{6.12}
$$

From this, it follows that for every $i \geq 1$ we have

$$
\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)} \otimes \mathbf{Q}_p/\mathbf{Z}_p \simeq (\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{\rm div}. \tag{6.13}
$$

(Indeed, because $\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)}$ is defined as the saturation of $\underleftarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)}$ inside $\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T)$, the composite map

$$
\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)} \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T) \otimes \mathbf{Q}_p/\mathbf{Z}_p \simeq (\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(1)})_{\rm div}
$$

is injective with image $\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{\rm div}$.) From (6.13) we deduce

$$
\mathrm{Hom}_{\mathbf{Z}_p}\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{\rm div}, \mathbf{Q}_p/\mathbf{Z}_p\big) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)}, \mathbf{Z}_p), \tag{6.14}
$$

for all $i \geq 1$. Note that the composition

$$
\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)} \xrightarrow{\alpha^{(i)}} \mathrm{Hom}_{\mathbf{Z}_p}\big(\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)}, \mathbf{Q}_p/\mathbf{Z}_p\big) \to \mathrm{Hom}_{\mathbf{Z}_p}\big((\underrightarrow{\mathfrak{S}}_{\overline{\mathfrak{p}}}^{(i)})_{\rm div}, \mathbf{Q}_p/\mathbf{Z}_p\big) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)}, \mathbf{Z}_p)
$$

is induced by the pairing $h_{\mathfrak{p}}^{(i)}$. Hence,

$$
\begin{aligned}
\det^* \alpha^{(i)} &= \mathrm{disc}\Big(h_{\mathfrak{p}}^{(i)}|_{\big(\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)}\big)_{/\rm tor} \times \overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\overline{\mathfrak{p}}}^{(i+1)}}\Big) \\
&= R_{\mathfrak{p},\gamma}^{(i)} \cdot \Big[\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i)}/\overline{\underleftarrow{\mathfrak{S}}}_{\mathfrak{p}}^{(i+1)} \colon \big(\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i)}/\underleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(i+1)}\big)_{/\rm tor}\Big] \\
&= R_{\mathfrak{p},\gamma}^{(i)} \cdot \det^* \beta^{(i)}.
\end{aligned}
$$

This shows (6.11), which together with (6.10) yields the result. □

6.3. **Step 3: Local universal norms.** Note that by definition, we have

$$\mathfrak{Sel}_{\mathfrak{q}}(K,T)=\varprojlim_k \mathfrak{Sel}_{\mathfrak{q}}(K,S^{(k)}),\qquad \mathfrak{Sel}_{\mathfrak{q}}(K,W)=\varinjlim_k \mathfrak{Sel}_{\mathfrak{q}}(K,S^{(k)}),$$

where $\mathfrak{Sel}_{\mathfrak{q}}(K,S^{(k)})$ is as in Definition 3.1.

Proposition 6.6. *For every $w\in\Sigma_f$, the local conditions $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w,S^{(k)})$ and $\mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_w,S^{(k)})$ are exact orthogonal complements under the local Tate pairing*

$$\mathrm{H}^1(K_w,S^{(k)})\times\mathrm{H}^1(K_w,S^{(k)})\to\mathcal{O}_k \tag{6.15}$$

induced by the Weil pairing $e: S^{(k)}\times S^{(k)}\to\mathcal{O}_k(1)$.

Proof. We begin by considering the case $w=\mathfrak{q}$. From the definitions, we have

$$\begin{aligned}\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_{\mathfrak{q}},S^{(k)})&=\mathrm{im}\bigl\{\mathrm{H}^0(K_{\mathfrak{q}},S^{(k)}_\infty)_\Gamma\hookrightarrow\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})\bigr\},\\ \mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_{\mathfrak{q}},S^{(k)})&=\mathrm{im}\bigl\{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})_\Gamma\hookrightarrow\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})\bigr\}.\end{aligned}\tag{6.16}$$

To see the second equality, we note that the propagation to $S^{(k)}$ of

$$\mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_{\mathfrak{q}},S^{(k)}_\infty):=\mathrm{im}\bigl\{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_{\mathcal{K}})\to\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_\infty)\bigr\}=\ker\{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_\infty)\to\mathrm{H}^2(K_{\mathfrak{q}},S^{(k}_{\mathrm{Iw}})\}$$

equals the kernel of the composition $\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})\to\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_\infty)\to\mathrm{H}^2(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})$, which is the same as the connecting homomorphism for the exact sequence

$$0\to S^{(k)}_{\mathrm{Iw}}\xrightarrow{\gamma-1}S^{(k)}_{\mathrm{Iw}}\to S^{(k)}\to 0. \tag{6.17}$$

Hence,

$$\mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_{\mathfrak{q}},S^{(k)}_\infty)=\ker\{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})\to\mathrm{H}^2(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})\}=\mathrm{im}\bigl\{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})_\Gamma\hookrightarrow\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})\bigr\}.$$

Now, since we have

$$\frac{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)})}{\mathrm{H}^1(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})_\Gamma}\simeq\mathrm{H}^2(K_{\mathfrak{q}},S^{(k)}_{\mathrm{Iw}})[J]\simeq\bigl(\mathrm{H}^0(K_{\mathfrak{q}},S^{(k)}_\infty)_\Gamma\bigr)^\vee \tag{6.18}$$

from the cohomology long exact sequence associated with (6.17) and Tate's local duality, the orthogonality assertion for $w=\mathfrak{q}$ follows. The argument for $w=\overline{\mathfrak{q}}$ is the same.

Next we consider the case $w\in\Sigma_f\setminus\{\mathfrak{p},\overline{\mathfrak{p}}\}$. In this case, $\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w,S^{(k)}_\infty)=\mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_w,S^{(k)}_\infty)=0$, and therefore

$$\begin{aligned}\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w,S^{(k)})=\mathrm{H}^1_{\mathcal{F}_{\overline{\mathfrak{q}}}}(K_w,S^{(k)})&=\ker\bigl\{\mathrm{H}^1(K_w,S^{(k)})\to\mathrm{H}^1(K_w,S^{(k)}_\infty)\bigr\}\\&=\mathrm{im}\bigl\{\mathrm{H}^0(K_w,S^{(k)}_\infty)_\Gamma\hookrightarrow\mathrm{H}^1(K_w,S^{(k)})\bigr\}.\end{aligned}$$

From the short exact sequence

$$0\to\mathrm{H}^1(K_w,S^{(k)}_{\mathrm{Iw}})_\Gamma\to\mathrm{H}^1(K_w,S^{(k)})\to\mathrm{H}^2(K_w,S^{(k)}_{\mathrm{Iw}})[J]\simeq\bigl(\mathrm{H}^0(K_w,S^{(k)}_\infty)_\Gamma\bigr)^\vee\to 0 \tag{6.19}$$

induced by (6.17) and local Tate duality, we see that

$$\mathrm{H}^1_{\mathcal{F}_{\mathfrak{q}}}(K_w,S^{(k)})=\bigl(\mathrm{im}\{\mathrm{H}^1(K_w,S^{(k)}_{\mathrm{Iw}})_\Gamma\hookrightarrow\mathrm{H}^1(K_w,S^{(k)})\}\bigr)^\perp,$$

where the superscript $\perp$ denotes the orthogonal complement under (6.15). Thus it suffices to establish the equality

$$\mathrm{H}^0(K_w,S^{(k)}_\infty)_\Gamma=\mathrm{H}^1(K_w,S^{(k)}_{\mathrm{Iw}})_\Gamma \tag{6.20}$$

inside $\mathrm{H}^1(K_w, S^{(k)})$. Consider the commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{H}^0(K_w, S_\infty^{(k)})_{/\mathcal{K}} \arrow[r] \arrow[d, "\gamma-1"] & \mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)}) \arrow[r] \arrow[d, "\gamma-1"] & \mathrm{im}\{\mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)}) \to \mathrm{H}^1(K_w, S_{\mathcal{K}}^{(k)})\} \arrow[r] \arrow[d, "\gamma-1"] & 0 \\ 0 \arrow[r] & \mathrm{H}^0(K_w, S_\infty^{(k)})_{/\mathcal{K}} \arrow[r] & \mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)}) \arrow[r] & \mathrm{im}\{\mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)}) \to \mathrm{H}^1(K_w, S_{\mathcal{K}}^{(k)})\} \arrow[r] & 0, \end{tikzcd}$$

where the rows are induced by (3.2) and the subscript $/\mathcal{K}$ denotes the quotient by the natural image of $\mathrm{H}^0(K_w, S_{\mathcal{K}}^{(k)})$ in $\mathrm{H}^0(K_w, S_\infty^{(k)})$. Using the fact that multiplication by $\gamma-1$ is invertible in $S_{\mathcal{K}}^{(k)}$, the snake lemma applied to this diagram yields an injection

$$\mathrm{H}^0(K_w, S_\infty^{(k)})_\Gamma \hookrightarrow \mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)})_\Gamma. \tag{6.21}$$

On the other hand, we can compute

$$\#\mathrm{H}^0(K_w, S_\infty^{(k)})_\Gamma = \#\Big(\bigoplus_{\eta\mid w} E(K_{\infty,\eta})[p^k]\Big)_\Gamma = \#\Big(\bigoplus_{\eta\mid w} E(K_{\infty,\eta})[p^k]\Big)[J] = \#E(K_w)[p^k], \tag{6.22}$$

using the finiteness of $E(K_{\infty,\eta})[p^k]$ and the fact that w is finitely decomposed in K_∞/K (since it splits in K) for the second equality. From (6.19), we similarly find

$$\big[\mathrm{H}^1(K_w, S^{(k)}) : \mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)})_\Gamma\big] = \#\mathrm{H}^2(K_w, S_{\mathrm{Iw}}^{(k)})[J] = \#E(K_w)[p^k]. \tag{6.23}$$

Since $\#\mathrm{H}^1(K_w, S^{(k)}) = (\#E(K_w)[p^k])^2$ by Tate's local Euler characteristic formula and Tate's local duality, the desired equality (6.20) now follows from the combination of (6.21), (6.22), and (6.23), thereby concluding the proof. $\square$

From the analysis in the proof of Proposition 6.6, we deduce the following two key results.

Corollary 6.7. *We have*

$$\mathfrak{Sel}_{\mathfrak{q}}(K,T) \simeq \ker\Bigg\{\mathrm{H}^1(G_{K,\Sigma}, T) \to \mathrm{H}^1(K_{\mathfrak{q}}, T) \times \prod_{w\in\Sigma_f\setminus\{\mathfrak{q}\}} \frac{\mathrm{H}^1(K_w, T)}{\mathrm{H}^1(K_w, T)^u}\Bigg\},$$

where $\mathrm{H}^1(K_w, T)^u := \varprojlim_k \mathrm{im}\big\{\mathrm{H}^1(K_w, S_{\mathrm{Iw}}^{(k)})_\Gamma \to \mathrm{H}^1(K_w, S^{(k)})\big\}$.

Proof. By (6.16) and the equality (6.20) established in the proof of Proposition 6.6, the local conditions cutting out $\mathfrak{Sel}_{\mathfrak{q}}(K,T)$ are given by $\mathrm{H}^1(K_w, T)^u$ for $w \in \Sigma_f \setminus \{\mathfrak{q}\}$. Restricted to $\mathfrak{q}$, the classes in $\mathfrak{Sel}_{\mathfrak{q}}(K,T)$ land in the image of $\varprojlim_k \mathrm{H}^0(K_{\mathfrak{q}}, S_\infty^{(k)})_\Gamma$ in $\mathrm{H}^1(K_{\mathfrak{q}}, T)$, and so their restriction to $\mathfrak{q}$ vanishes by the finiteness of $\bigoplus_{\eta\mid\mathfrak{q}} E(K_{\infty,\eta})[p^\infty]$. $\square$

Corollary 6.8. *We have a five-term exact sequence*

$$0 \to \mathfrak{Sel}_{\mathfrak{q}}(K,T) \to \mathrm{Sel}_{\mathfrak{q}}(K,T) \to \mathcal{L} \to \mathfrak{Sel}_{\overline{\mathfrak{q}}}(K,W)^\vee \to \mathrm{Sel}_{\overline{\mathfrak{q}}}(K,W)^\vee \to 0$$

with

$$\#\mathcal{L} = (\#E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w\mid N} c_w^{(p)},$$

where $c_w^{(p)}$ is the p-part of the Tamagawa number of E/K_w.

Proof. In light of Proposition 6.6 and Corollary 6.7, Poitou–Tate duality gives rise to a five-term exact sequence as in the statement with

$$\mathcal{L} = \mathrm{H}^1_{\mathfrak{q}}(K_{\mathfrak{q}}, T) \times \prod_{w\in\Sigma_f\setminus\{\mathfrak{q}\}} \frac{\mathrm{H}^1_{\mathfrak{q}}(K_w, T)}{\mathrm{H}^1(K_w, T)^u}. \tag{6.24}$$

It remains to compute the size of each the factors in the right-hand side.

For the first factor, Definition 2.1 gives $\mathrm{H}^1_{\mathfrak{q}}(K_{\mathfrak{q}},T)=\mathrm{H}^1(K_{\mathfrak{q}},T)_{\mathrm{tor}}$, and from the combination of (3.11) and (3.12) we have

$$\#\mathrm{H}^1_{\mathfrak{q}}(K_{\mathfrak{q}},T)=\#\mathrm{H}^1(K_{\mathfrak{q}},T)_{\mathrm{tor}}=\#E(\mathbf{Q}_p)[p^\infty]. \tag{6.25}$$

For $w=\overline{\mathfrak{q}}$, the numerator in the second factor is $\mathrm{H}^1_{\mathfrak{q}}(K_{\overline{\mathfrak{q}}},T)=\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)$, and from (6.18) we have

$$\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)/\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)^u\simeq\Big(\varinjlim_k \mathrm{H}^0(K_{\overline{\mathfrak{q}}},S_\infty^{(k)})_\Gamma\Big)^\vee.$$

Since $\varinjlim_k \mathrm{H}^0(K_{\overline{\mathfrak{q}}},S_\infty^{(k)})$ is finite by [KO20, Lem. 2.7], it follows that

$$\#\big(\mathrm{H}^1_{\mathfrak{q}}(K_{\overline{\mathfrak{q}}},T)/\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)^u\big)=\#\big(\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)/\mathrm{H}^1(K_{\overline{\mathfrak{q}}},T)^u\big)=\#E(\mathbf{Q}_p)[p^\infty]. \tag{6.26}$$

It remains to consider the case $w\nmid p$. In this case, we have

$$\mathrm{H}^1_{\mathfrak{q}}(K_w,T)=\mathrm{H}^1(K_w,T)_{\mathrm{tor}}=\mathrm{H}^1(K_w,T),$$

using Tate's local Euler characteristic formula for the second equality. Therefore,

$$\begin{aligned}\#\big(\mathrm{H}^1_{\mathfrak{q}}(K_w,T)/\mathrm{H}^1(K_w,T)^u\big)&=\#\big(\mathrm{H}^1(K_w,T)/\mathrm{H}^1(K_w,T)^u\big)\\&=\#\big(\varinjlim_k \mathrm{H}^0(K_w,S^{(k)})_\Gamma\big)=\#\big(B_w/(\gamma-1)B_w\big),\end{aligned} \tag{6.27}$$

where the second equality is shown in the proof of Proposition 6.6, and B_w is as in (3.9). Now recall that $c_w^{(p)}=\#\mathrm{H}^1_{\mathrm{unr}}(K_w,W)$, where

$$\mathrm{H}^1_{\mathrm{unr}}(K_w,W):=\ker\left\{\mathrm{H}^1(K_w,W)\to\mathrm{H}^1(K_w^{\mathrm{unr}},W)\right\}.$$

Since for every $\eta\mid w$ the restriction map $\mathrm{H}^1(K_{\infty,\eta},W)\to\mathrm{H}^1(K_w^{\mathrm{unr}},W)$ is injective (this follows from the fact that $\mathrm{Gal}(K_w^{\mathrm{unr}}/K_{\infty,\eta})$ has trivial pro-p-part), we deduce that

$$\begin{aligned}\mathrm{H}^1_{\mathrm{unr}}(K_w,W)&=\ker\{\mathrm{H}^1(K_w,W)\to\bigoplus_{\eta\mid w}\mathrm{H}^1(K_{\infty,\eta},W)\}\\&\simeq B_w/(\gamma-1)B_w.\end{aligned} \tag{6.28}$$

From (6.27) and (6.28), we conclude that $\#\big(\mathrm{H}^1_{\mathfrak{q}}(K_w,T)/\mathrm{H}^1(K_w,T)^u\big)=c_w^{(p)}$ for $w\nmid p$. Together with (6.25) and (6.26), this gives the stated formula for $\#\mathcal{L}$. $\square$

6.4. **Step 4: p-adic logarithm.** The last step is to relate $\#\big(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}\big)$ to $\#Ш_{\mathrm{BK}}(K,W)$ and some of the other terms appearing in our Leading Coefficient Formula.

Proposition 6.9. *Assume hypotheses* (h0)-(h1). *Then*

$$\#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}})=\#Ш_{\mathrm{BK}}(K,W)\cdot(\#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}))^2,$$

where $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}$ *is the composition* $\check{S}_p(E/K)\xrightarrow{\mathrm{res}_{\mathfrak{p}}}E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p\to E(K_{\mathfrak{p}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p$.

Proof. By Lemma 2.2 we have

$$\mathrm{Sel}_{\mathfrak{p}}(K,T)=\ker(\mathrm{res}_{\mathfrak{p}})\simeq\mathbf{Z}_p^{r-1},$$

where $r=\mathrm{rank}_{\mathbf{Z}_p}\check{S}_p(E/K)$. Let $s_1,\ldots,s_{r-1}$ be a $\mathbf{Z}_p$-basis for $\mathrm{Sel}_{\mathfrak{p}}(K,T)$ and extend it to a $\mathbf{Z}_p$-basis $s_1,\ldots,s_{r-1},s_{\mathfrak{p}}$ for $\check{S}_p(E/K)$, so we have

$$\check{S}_p(E/K)\simeq\mathrm{Sel}_{\mathfrak{p}}(K,T)\oplus\mathbf{Z}_ps_{\mathfrak{p}}. \tag{6.29}$$

The map $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}$ gives an injection $\mathbf{Z}_ps_{\mathfrak{p}}\hookrightarrow E(K_{\mathfrak{p}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p$, and defining U by the exactness of the sequence

$$0\to\mathbf{Z}_ps_{\mathfrak{p}}\to E(K_{\mathfrak{p}})_{/\mathrm{tor}}\otimes\mathbf{Z}_p\to U\to 0, \tag{6.30}$$

we see that U is finite, with $\#U = \#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}})$. Tensoring (6.30) with $\mathbf{Q}_p/\mathbf{Z}_p$ gives

$$0 \to U' \to (\mathbf{Q}_p/\mathbf{Z}_p)s_{\mathfrak{p}} \to E(K_{\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to 0 \tag{6.31}$$

for a certain finite module U' with $\#U' = \#U$.

Noting that $\mathrm{Sel}_{\mathfrak{p}}(K,T) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{\mathfrak{p}}(K,W)_{\mathrm{div}}$ (see (6.12)) and similarly $\check{S}_p(E/K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{p^\infty}(E/K)_{\mathrm{div}}$, from (6.29) and (6.31) it follows that

$$\ker\left\{\mathrm{Sel}_{p^\infty}(E/K)_{\mathrm{div}} \xrightarrow{\mathrm{res}_{\mathfrak{p}}} E(K_{\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p\right\} \simeq \mathrm{Sel}_{\mathfrak{p}}(K,W)_{\mathrm{div}} \oplus U'. \tag{6.32}$$

Moreover, we know that

$$\#U' = \#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}). \tag{6.33}$$

Denote by $\mathrm{Sel}_{\mathrm{rel,fin}}(K,V)$ the Selmer group obtained by relaxing the condition at $\mathfrak{p}$ in the usual Bloch–Kato Selmer group $\mathrm{Sel}(K,V)$, and let $\mathrm{Sel}_{\mathrm{rel,fin}}(K,W)$ be the Selmer group obtained by propagation. Then from Poitou–Tate duality we have the exact sequence

$$\begin{aligned} 0 \to \mathrm{Sel}_{p^\infty}(E/K) \to \mathrm{Sel}_{\mathrm{rel,fin}}(K,W) \xrightarrow{\mathrm{res}_{\mathfrak{p}/\mathrm{fin}}} \frac{\mathrm{H}^1(K_{\mathfrak{p}},W)_{\mathrm{div}}}{E(K_{\mathfrak{p}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p} \simeq (E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p)^\vee \\ \xrightarrow{(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}})^\vee} \check{S}_p(E/K)^\vee, \end{aligned}$$

and it follows from our assumption that the map $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}$ has finite cokernel. Hence the map $\mathrm{res}_{\mathfrak{p}/\mathrm{fin}}$ has finite image, with

$$\#\mathrm{im}(\mathrm{res}_{\mathfrak{p}/\mathrm{fin}}) = \#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}). \tag{6.34}$$

We thus deduce the following commutative diagram with exact rows

$$\begin{tikzcd} & \mathrm{Sel}_{p^\infty}(E/K)_{\mathrm{div}} \arrow[r, "\simeq"] \arrow[d, hook] & \mathrm{Sel}_{\mathrm{rel,fin}}(K,W)_{\mathrm{div}} \arrow[d, hook] & & \\ 0 \arrow[r] & \mathrm{Sel}_{p^\infty}(E/K) \arrow[r] & \mathrm{Sel}_{\mathrm{rel,fin}}(K,W) \arrow[r] & \mathrm{im}(\mathrm{res}_{\mathfrak{p}/\mathrm{fin}}) \arrow[r] & 0, \end{tikzcd} \tag{6.35}$$

from where, together with (6.34), we conclude that

$$\#(\mathrm{Sel}_{\mathrm{rel,fin}}(K,W)_{/\mathrm{div}}) = \#Ш_{\mathrm{BK}}(K,W) \cdot \#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}). \tag{6.36}$$

On the other hand, from (6.32) and the isomorphism in (6.35) we also have the commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{\mathrm{div}} \oplus U' \arrow[r] \arrow[d, hook] & \mathrm{Sel}_{\mathrm{rel,fin}}(K,W)_{\mathrm{div}} \arrow[r, "\mathrm{res}_{\overline{\mathfrak{p}}}"] \arrow[d, hook] & E(K_{\overline{\mathfrak{p}}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W) \arrow[r] & \mathrm{Sel}_{\mathrm{rel,fin}}(K,W) \arrow[r, "\mathrm{res}_{\overline{\mathfrak{p}}}"] & E(K_{\overline{\mathfrak{p}}}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r] & 0, \end{tikzcd}$$

from where we conclude that

$$\#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}) = \#(\mathrm{Sel}_{\mathrm{rel,fin}}(K,W)_{/\mathrm{div}}) \cdot \#U'.$$

Together with (6.33) and (6.36), this last formula yields the result. □

Recall that we use $\log_{\mathfrak{p}} : \check{S}_p(E/K) \to \mathbf{Z}_p$ to denote the composition of $\mathrm{res}_{\mathfrak{p}/\mathrm{tor}} : \check{S}_p(E/K) \to E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p$ with the formal group logarithm associated with a fixed Néron differential $\omega_E \in \Omega^1(E/\mathbf{Z}_{(p)})$.

Proposition 6.10. *Let the hypotheses be as in Proposition 6.9. Then*

$$\#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}) \sim_p \left(\frac{1-a_p(E)+p}{p}\right) \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}}) \cdot \frac{1}{\#E(K_{\mathfrak{p}})[p^\infty]},$$

where $s_{\mathfrak{p}}$ is any generator of $\check{S}_p(E/K)/\ker(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}) \simeq \mathbf{Z}_p$ and $a_p(E) := p+1-\#E(\mathbf{F}_p)$.

Proof. As shown in the proof of Proposition 6.9 (see (6.30)), we have

$$\#(\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}})) = [E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p : \mathbf{Z}_p s_{\mathfrak{p}}]. \tag{6.37}$$

Let $E_1(K_{\mathfrak{p}})$ be the kernel of the reduction map modulo $\mathfrak{p}$, so we have the exact sequence

$$0 \to E_1(K_{\mathfrak{p}}) \to E(K_{\mathfrak{p}}) \to E(\mathbf{F}_p) \to 0.$$

The formal group logarithm defines an isomorphism

$$\log_{\mathfrak{p}} : E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \xrightarrow{\simeq} p\mathbf{Z}_p,$$

and this extends to an injection $E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p \hookrightarrow \mathbf{Z}_p$. Hence from (6.37) we find

$$\begin{aligned}
\#(\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}})) &= \frac{[\mathbf{Z}_p : \log_{\mathfrak{p}}(s_{\mathfrak{p}})\mathbf{Z}_p]}{[\mathbf{Z}_p : \log_{\mathfrak{p}}(E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p)]}\\
&= \frac{[\mathbf{Z}_p : \log_{\mathfrak{p}}(s_{\mathfrak{p}})\mathbf{Z}_p]}{[\mathbf{Z}_p : p\mathbf{Z}_p]} \cdot [E(K_{\mathfrak{p}})_{/\mathrm{tor}} \otimes \mathbf{Z}_p : E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p]\\
&\sim_p \frac{\log_{\mathfrak{p}}(s_{\mathfrak{p}})}{p} \cdot \frac{[E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p : E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p]}{\#E(K_{\mathfrak{p}})[p^\infty]}.
\end{aligned}$$

Since by definition $\#(E(\mathbf{F}_p) \otimes \mathbf{Z}_p) \simeq \#\mathbf{Z}_p/(1-a_p(E)+p)\mathbf{Z}_p$, this yields the result. □

6.5. **Leading Coefficient Formula.**

Proof of Theorem 5.1(i). Let $r \geq \varrho_{\mathrm{alg}} = \mathrm{ord}_J F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}$. From Proposition 6.3 and Proposition 6.5 we have the equalities up to a p-adic unit:

$$\begin{aligned}
\frac{1}{\varrho_{\mathrm{alg}}!}\frac{d^{\varrho_{\mathrm{alg}}}}{dT^{\varrho_{\mathrm{alg}}}} F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}\Big|_{T=0} &\sim_p \#\big(\mathfrak{S}_{\rightarrow\overline{\mathfrak{p}}}^{(r+1)}\big)\\
&\sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot \big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \mathfrak{Sel}_{\mathfrak{p}}(K,T)\big] \cdot \#\big(\mathfrak{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}\big).
\end{aligned} \tag{6.38}$$

Since from Corollary 6.8 we have the relation

$$\big[\mathrm{Sel}_{\mathfrak{p}}(K,T) \colon \mathfrak{Sel}_{\mathfrak{p}}(K,T)\big] \cdot \#\big(\mathfrak{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}\big) = \#(E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w|N} c_w^{(p)} \cdot \#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}}),$$

continuing from (6.38) we deduce that

$$\begin{aligned}
&\frac{1}{\varrho_{\mathrm{alg}}!}\frac{d^{\varrho_{\mathrm{alg}}}}{dT^{\varrho_{\mathrm{alg}}}} F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}\Big|_{T=0}\\
&\qquad \sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot (\#E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w|N} c_w^{(p)} \cdot \#(\mathrm{Sel}_{\overline{\mathfrak{p}}}(K,W)_{/\mathrm{div}})\\
&\qquad \sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot (\#E(\mathbf{Q}_p)[p^\infty])^2 \cdot \prod_{w|N} c_w^{(p)} \cdot \#Ш_{\mathrm{BK}}(K,W) \cdot (\#\mathrm{coker}(\mathrm{res}_{\mathfrak{p}/\mathrm{tor}}))^2\\
&\qquad \sim_p \mathrm{Reg}_{\mathfrak{p},\mathrm{der},\gamma} \cdot \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\mathfrak{p}}(s_{\mathfrak{p}})^2 \cdot \prod_{w|N} c_w^{(p)} \cdot \#Ш_{\mathrm{BK}}(K,W),
\end{aligned}$$

using Proposition 6.9 and Proposition 6.10 for the middle and the last equality, respectively. Noting that $\prod_{w|N} c_w = \prod_{\ell|N} c_\ell^2$ as a consequence of (Heeg), this finishes the proof. □

6.6. **Order of Vanishing.** In this section we give the proof of Theorem 5.1(ii). Since $\overleftarrow{\overline{\mathfrak{S}}}_{\mathfrak{q}}^{(1)} = \mathrm{Sel}_{\mathfrak{q}}(K,T)$, from (3.17) we have a p-adic height pairing

$$h_{\mathfrak{p}} = h_{\mathfrak{p}}^{(1)} : \mathrm{Sel}_{\mathfrak{p}}(K,T) \times \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T) \to \mathbf{Q}_p$$

whose kernel on the left is given by $\overleftarrow{\overline{\mathfrak{S}}}_{\mathfrak{p}}^{(2)}$ (and whose $\mathbf{Z}_p$-rank is the same as that of $\overleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(2)}$).

Proposition 6.11. *Set* $r^{\pm} = \mathrm{rank}_{\mathbf{Z}_p} \check{S}_p(E/K)^{\pm}$. *Then*

$$\mathrm{rank}_{\mathbf{Z}_p} \overleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(2)} \geq \left| r^+ - r^- \right| - 1.$$

Proof. Note that complex conjugation acts on $\mathrm{Sel}_{\mathrm{str}}(K,T) = \mathrm{Sel}_{\mathfrak{p}}(K,T) \cap \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T)$. Let

$$h_{\mathrm{str}} : \mathrm{Sel}_{\mathrm{str}}(K,T) \times \mathrm{Sel}_{\mathrm{str}}(K,T) \to \mathbf{Q}_p \tag{6.39}$$

be the pairing obtained from $h_{\mathfrak{p}}$ by restriction. By [How04, Rem. 1.12], we have

$$h_{\mathrm{str}}(x^{\tau}, y^{\tau}) = -\check{h}_p(x,y),$$

for all $x, y \in \mathrm{Sel}_{\mathrm{str}}(K,T)$, where τ is complex conjugation. Writing $r_{\mathrm{str}}^{\pm}$ to denote the $\mathbf{Z}_p$-rank of the τ-eigenspace $\mathrm{Sel}_{\mathrm{str}}(K,T)^{\pm}$, it follows that

$$\mathrm{rank}_{\mathbf{Z}_p} \ker(h_{\mathrm{str}}) \geq \left| r_{\mathrm{str}}^+ - r_{\mathrm{str}}^- \right|. \tag{6.40}$$

We distinguish two cases according to the $\mathbf{Z}_p$-rank of the image of the restriction map res_p in the proof of Lemma 2.2.

Case (i): $\mathrm{rank}_{\mathbf{Z}_p} \mathrm{im}(\mathrm{res}_p) = 1$. By (2.3), we have $h_{\mathrm{str}} = h_{\mathfrak{p}}$ and

$$(r_{\mathrm{str}}^+, r_{\mathrm{str}}^-) \in \{(r^+ - 1, r^-), (r^+, r^- - 1)\}.$$

Thus $\left| r_{\mathrm{str}}^+ - r_{\mathrm{str}}^- \right| \geq |r^+ - r^-| - 1$, and the result follows from (6.40).

Case (ii): $\mathrm{rank}_{\mathbf{Z}_p} \mathrm{im}(\mathrm{res}_p) = 2$. Consider a non-zero element $z \in \check{S}_p(E/K)$ satisfying $\mathrm{res}_{\mathfrak{p}}(z) = \mathrm{res}_{\overline{\mathfrak{p}}}(z^{\tau}) = 0$ and $\mathrm{res}_{\overline{\mathfrak{p}}/\mathrm{tor}}(z) \neq 0$. Then

$$\check{S}_p(E/K) = \mathrm{Sel}_{\mathrm{str}}(K,T) \oplus \mathbf{Z}_p z^+ \oplus \mathbf{Z}_p z^-, \tag{6.41}$$

where $z^{\pm} = \frac{1}{2}(z \pm z^{\tau})$. With this notation, we can write

$$\mathrm{Sel}_{\mathfrak{p}}(K,T) = \mathrm{Sel}_{\mathrm{str}}(K,T) \oplus \mathbf{Z}_p z, \qquad \mathrm{Sel}_{\overline{\mathfrak{p}}}(K,T) = \mathrm{Sel}_{\mathrm{str}}(K,T) \oplus \mathbf{Z}_p z^{\tau}.$$

Now, we immediately see that

$$(\text{left kernel of } h_{\mathfrak{p}}) \supset \bigcap_s \ker(h_{\mathrm{str}}(-,s)) \cap \ker(h_{\mathfrak{p}}(-,z^{\tau})),$$

where s runs over all the elements in $\mathrm{Sel}_{\mathrm{str}}(K,T)$. Thus we conclude that

$$\begin{aligned} \mathrm{rank}_{\mathbf{Z}_p} \overleftarrow{\mathfrak{S}}_{\mathfrak{p}}^{(2)} &\geq \mathrm{rank}_{\mathbf{Z}_p} \ker(h_{\mathrm{str}}) - 1 \\ &\geq \left| r_{\mathrm{str}}^+ - r_{\mathrm{str}}^- \right| - 1 \\ &= \left| r^+ - r^- \right| - 1, \end{aligned}$$

using (6.40) and (6.41) for the second inequality and the last equality, respectively. □

Remark 6.12. Conjecturally, *Case (i)* in the proof of Proposition 6.11 only occurs when either r^+ or r^- is 0. Indeed, let $E^K/\mathbf{Q}$ be the twist of E by the quadratic character corresponding to $K/\mathbf{Q}$. If both r^+ and r^- are positive, then the finiteness of $Ш(E/K)[p^{\infty}] = Ш(E/\mathbf{Q})[p^{\infty}] \oplus Ш(E^K/\mathbf{Q})[p^{\infty}]$ implies that the restriction map

$$\mathrm{res}_p = (\mathrm{res}_p^+, \mathrm{res}_p^-) : \check{S}_p(E/K) \to E(K_p) \otimes \mathbf{Z}_p = (E(\mathbf{Q}_p) \otimes \mathbf{Z}_p) \oplus (E^K(\mathbf{Q}_p) \otimes \mathbf{Z}_p)$$

satisfies $\mathrm{rank}_{\mathbf{Z}_p} \mathrm{im}(\mathrm{res}_p^{\pm}) = 1$, so the $\mathbf{Z}_p$-rank of $\mathrm{im}(\mathrm{res}_p)$ is 2.

The following is Theorem 5.1(ii):

Corollary 6.13. *Let* $\varrho_{\mathrm{alg}} = \mathrm{ord}_J F_{\overline{\mathfrak{p}}}^{\mathrm{BDP}}$. *Then*

$$\varrho_{\mathrm{alg}} \geq 2(\max\{r^+, r^-\} - 1),$$

where $r^{\pm} = \mathrm{rank}_{\mathbf{Z}_p} \check{S}_p(E/K)^{\pm}$, *with equality if and only if* $h_{\mathfrak{p}}$ *is maximally non-degenerate.*

Proof. With the notation from (6.8), we have

$$\begin{aligned} \varrho_{\mathrm{alg}} &= e_1 + 2e_2 + \cdots + i_0 e_{i_0} \\ &\geq (e_1 + e_2 + \cdots + e_{i_0}) + (e_2 + \cdots + e_{i_0}) \\ &\geq (r-1) + (\left|r^+ - r^-\right| - 1) \\ &= 2(\max\{r^+, r^-\} - 1), \end{aligned}$$

using Proposition 6.11 for the second inequality. These inequalities are equalities if and only if $e_i = 0$ for $i \geq 3$ and $e_2 = |r^+ - r^-| - 1$, as was to be shown. □

Remark 6.14. Assume that p is ordinary for E. Applied to the usual (compact) Selmer group $\check{S}_p(E/K)$, Howard's work produces a filtration

$$\check{S}_p(E/K) \otimes \mathbf{Q}_p = S_p^{(1)} \supset S_p^{(2)} \supset \cdots \supset S_p^{(i)} \supset \cdots$$

and a sequence of pairings $\check{h}_p^{(i)} : S_p^{(i)} \times S_p^{(i)} \to \mathbf{Q}_p$ such that $S_p^{(i+1)}$ is the kernel of $S_p^{(i)}$ ([How04, Thm. 4.2]). In this setting, a conjecture due to Mazur and Bertolini–Darmon predicts that

$$\dim_{\mathbf{Q}_p} S_p^{(i)} \overset{?}{=} \begin{cases} |r^+ - r^-| & \text{if } i = 2, \\ 1 & \text{if } i = 3, \end{cases} \tag{6.42}$$

and $S_p^{(i)} = 0$ for $i \geq 4$, and that $S_p^{(3)}$ spanned by the space of universal norms

$$\check{S}_p(E/K)^u = \bigcap_n \mathrm{cor}_{K_n/K}(\check{S}_p(E/K_n))$$

(see [How04, Conj. 4.4] and [BD95, Conj. 3.8]). Using Proposition 2.5 and Corollary 3.11, one easily checks (arguing similarly as in the proof of Proposition 6.11) that $\check{S}_p(E/K)^u \cap \mathrm{Sel}_{\mathfrak{p}}(K,T) = 0$. As a result, conjecture (6.42) implies that $h_{\mathfrak{p}}$ is maximally non-degenerate.

In the p-supersingular case the same conclusion should hold, building on the work of Benois [Ben21] to obtain (derived) anticyclotomic p-adic height pairings on $\check{S}_p(E/K) \otimes \mathbf{Q}_p$ compatible with our $h_{\mathfrak{p}}$.

7. Proof of anticyclotomic main conjectures: supersingular case

The purpose of this section is to give a proof of the signed Heegner point main conjecture formulated in [CW24] for supersingular primes p under mild hypotheses. By the equivalence between this conjecture and Conjecture 2.4 when $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K, we deduce a proof of the latter conjecture under the same hypotheses.

The formulation of the signed main conjecture in [CW24] is under a generalised Heegner hypothesis[2], and many cases were proved in *op. cit.* by building on the main result of [CLW22]. Unfortunately, due to the technical hypotheses from [CLW22], the classical Heegner hypothesis (Heeg), i.e. the case $N^- = 1$, was excluded from those results. To obtain a result under (Heeg), here we adapt the approach of [BCK21] to the supersingular setting[3].

[2]Allowing N to be divisible by any square-free product N^- of an even number of primes inert in K.

[3]After a first draft of this Appendix was written, similar results were announced in [BLV23].

7.1. **Statement of the main results.** We begin by introducing the setting, which is slightly more general than what is needed for the application in Corollary 5.2.

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, and let $p > 2$ be a prime of good supersingular reduction for E. We assume that

$$\text{(non-ord)} \qquad a_p(E) = 0$$

(which by the Hasse bounds is automatic for $p > 3$). Let K be an imaginary quadratic field of discriminant prime to N such that

$$\text{(spl)} \qquad p = \mathfrak{p}\overline{\mathfrak{p}} \text{ splits in } K.$$

Writing $N = N^+N^-$ with N^+ (resp. N^-) divisible only by primes that split (resp. remain inert) in K, assume the following *generalised Heegner hypothesis*:

$$\text{(gen-Heeg)} \qquad N^- \text{ is the square-free product of an even number of primes.}$$

As in the main text, we let Γ be the Galois group of the anticyclotomic $\mathbf{Z}_p$-extension K_∞/K, and let $\Lambda = \mathbf{Z}_p[\![\Gamma]\!]$ be the anticyclotomic Iwasawa algebra.

For any triple (E, K, p) satisfying (non-ord), (spl), and (gen-Heeg) as above, an analogue of Perrin-Riou's Heegner point main conjecture [PR87] was formulated in [CW24, Conj. 4.8]. Letting $\mathcal{S}^\pm$ and $\mathcal{X}^\pm$ be the compact Selmer groups over K_∞/K denoted by $\mathrm{Sel}^\pm(K, \mathbf{T}^{\mathrm{ac}})$ and $\mathrm{Sel}^\pm(K, \mathbf{A}^{\mathrm{ac}})^\vee$ in [CW24, §4.2], respectively, the conjecture predicts that both $\mathcal{S}^\pm$ and $\mathcal{X}^\pm$ have Λ-rank one, with the characteristic ideal of the Λ-torsion submodule $\mathcal{X}^\pm_{\mathrm{tors}} \subset \mathcal{X}^\pm$ being the same as $\mathrm{char}_\Lambda(\mathcal{S}^\pm/(\kappa^\pm_\infty))^2$ for the Λ-adic $\pm$-Heegner class

$$\kappa^\pm_\infty \in \mathcal{S}^\pm \tag{7.1}$$

constructed in [CW24, §4.1] (where it is denoted $\mathbf{z}^\pm_\infty = \mathrm{cor}_{K[1]/K}(\mathbf{z}_\infty[1]^\pm)$.

In this section we prove the following.

Theorem 7.1. *Let (E, K, p) be a triple as above, and assume in addition that:*

(i) *N is square-free.*
(ii) *$E[p]$ is ramified at every prime $\ell \mid N^+$.*
(iii) *$E[p]$ is ramified at every prime $\ell \mid N^-$ with $\ell \equiv \pm 1 \pmod p$.*
(iv) *Every prime above p is totally ramified in K_∞/K.*

Then $\mathcal{S}^\pm$ and $\mathcal{X}^\pm$ have Λ-rank one, and

$$\mathrm{char}_\Lambda(\mathcal{X}^\pm_{\mathrm{tors}}) = \mathrm{char}_\Lambda(\mathcal{S}^\pm/(\kappa^\pm_\infty))^2.$$

In other words, the $\pm$-Heegner point main conjecture in [CW24, Conj. 4.8] *holds.*

Corollary 7.2. *Let the hypotheses be as in Theorem 7.1. Then* [CW24, Conj. 5.2] *holds. In particular, in the case $N^- = 1$, Conjecture 2.4 in the body of the paper holds.*

Proof. This follows from Theorem 7.1 and the equivalence in [CW24, Thm. 6.8], noting that Conjecture 2.4 is the same as [CW24, Conj. 5.2] when $N^- = 1$. □

The remainder of this section is devoted to the proof of Theorem 7.1.

7.2. **Bipartite Euler system for non-ordinary primes.** Let $f = \sum_{n=1}^\infty a_n q^n \in S_2(\Gamma_0(N))$ be the newform corresponding to E, and denote by

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p)$$

the associated residual representation. Following [PW11], we say that the pair $(\overline{\rho}, N^-)$ satisfies *Condition CR* if:

- $\overline{\rho}$ is ramified at every prime $\ell \mid N^-$ with $\ell \equiv \pm 1 \pmod p$, and
- $\overline{\rho}$ is surjective[4].

[4] It follows from [Edi97, Prop. 2.1] that if E is semistable and p is supersingular for E, then $\overline{\rho}$ is surjective.

We refer the reader to [BD05, p. 18] for the definition of j-*admissible* primes (for any $j > 0$) relative to f. Denote by $\mathcal{L}_j$ the set of j-admissible primes, and by $\mathcal{N}_j$ the set of square-free products of primes $q \in \mathcal{L}_j$. When $j = 1$, we suppress it from the notations. We decompose

$$\mathcal{N}_j = \mathcal{N}_j^{\mathrm{ind}} \sqcup \mathcal{N}_j^{\mathrm{def}}$$

with $\mathcal{N}_j^{\mathrm{ind}}$ consisting of the square-free products of an even number of primes $q \in \mathcal{L}_j$.

Remark 7.3. By definition, admissible primes $q \in \mathcal{L}$ satisfy in particular $q \not\equiv \pm 1 \pmod p$. So, Condition CR allows for the existence, for any $m \in \mathcal{N}$, of m-new forms $g \in S_2(\Gamma_0(Nm))$ level-raising f (and whose existence follows from results of Ribet [Rib84] and Diamond–Taylor [DT94a, DT94b]; see [Zha14, Thm. 2.1]).

Let $T = \varprojlim_j E[p^j]$ be the p-adic Tate module of E, and put

$$\mathbf{T}_j := \varprojlim_n \mathrm{Ind}_{K_n/K}(T/p^jT), \qquad \mathbf{A}_j := \varinjlim_n \mathrm{Ind}_{K_n/K}(E[p^j]).$$

For every $m \in \mathcal{N}_j$ the "N^-m-ordinary" signed Selmer groups $\mathrm{Sel}^{\pm}_{N^-m}(K, \mathbf{T}_j)$, $\mathrm{Sel}^{\pm}_{N^-m}(K, \mathbf{A}_j)$ are defined as in [BCK21, p. 1634], with the local conditions at primes $v \mid p$ in *loc. cit.* replaced by the above local conditions $\mathrm{H}^1_{\pm}(K_v, \mathbf{T}_j)$ and $\mathrm{H}^1_{\pm}(K_v, \mathbf{A}_j)$ in [CW24, Def. 4.6].

In particular, at the primes $q \nmid N^-mp$, the classes $c \in \mathrm{Sel}^{\pm}_{N^-m}(K, \mathbf{T}_j)$ are unramified, i.e., $\mathrm{res}_q(c) \in \mathrm{H}^1_{\mathrm{unr}}(K_q, \mathbf{T}_j)$, while at the primes $q \mid N^-m$ they are required to land in the "ordinary" submodule $\mathrm{H}^1_{\mathrm{ord}}(K_q, \mathbf{T}_j)$. It is easy to see that for $q \in \mathcal{L}$, both $\mathrm{H}^1_{\mathrm{unr}}(K_q, \mathbf{T}_j)$ and $\mathrm{H}^1_{\mathrm{ord}}(K_q, \mathbf{T}_j)$ are free of rank 1 over $\Lambda/p^j\Lambda$ (see e.g. [BCK21, Lem. 2.1]).

Theorem 7.4 (Darmon–Iovita, Pollack–Weston)**.** *Suppose that*

(i) $a_p(E) = 0$.
(ii) *p splits in K.*
(iii) *Each prime above p is totally ramified in K_∞/K.*
(iv) *$(\bar{\rho}, N^-)$ satisfies Condition CR.*

Then for every choice of sign $\pm$ and every $j > 0$ there is a pair of systems

$$\boldsymbol{\kappa}_j^{\pm} = \{\kappa_j^{\pm}(m) \in \mathrm{Sel}^{\pm}_{N^-m}(K, \mathbf{T}_j) : \; m \in \mathcal{N}_j^{\mathrm{ind}}\},$$
$$\boldsymbol{\lambda}_j^{\pm} = \{\lambda_j^{\pm}(m) \in \Lambda/\wp^j\Lambda : \; m \in \mathcal{N}_j^{\mathrm{def}}\},$$

related by a system of "explicit reciprocity laws":

- *If $mq_1q_2 \in \mathcal{N}_j^{\mathrm{ind}}$ with $q_1, q_2 \in \mathcal{L}_j$ distinct primes, then*
$$\mathrm{loc}_{q_2}(\kappa_j^{\pm}(mq_1q_2)) = \lambda_j^{\pm}(mq_1)$$
under a fixed isomorphism $\mathrm{H}^1_{\mathrm{ord}}(K_{q_1}, \mathbf{T}_j) \simeq \Lambda/p^j\Lambda$.
- *If $mq \in \mathcal{N}_j^{\mathrm{def}}$ with $q \in \mathcal{L}_j$ prime, then*
$$\mathrm{loc}_q(\kappa_j^{\pm}(m)) = \lambda_j^{\pm}(mq)$$
under a fixed isomorphism $\mathrm{H}^1_{\mathrm{unr}}(K_q, \mathbf{T}_j) \simeq \Lambda/p^j\Lambda$.

Proof. This is shown in [DI08] (in particular, see [*op. cit.*, Prop. 4.4, Prop. 4.6] for the two explicit reciprocity laws) under hypotheses (i)–(iii) and an additional hypothesis that f is "p-isolated" in the sense of [BD05]. This last hypothesis was replaced by the weaker hypothesis (iv) above in [PW11] (see [*op. cit.*, §4.3]). □

For $m = 1$, the classes $\kappa_j^{\pm} := \kappa_j^{\pm}(1)$ exist for all $j > 0$ and are compatible under the natural maps $\mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{T}_{j+1}) \to \mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{T}_j)$, thereby defining the class

$$\varprojlim_j \kappa_j^{\pm} \in \mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{T}) := \varprojlim_j \mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{T}_j). \tag{7.2}$$

As in [BCK21, Lem. 2.2], we have natural isomorphisms

$$\mathcal{S}^{\pm} \simeq \varprojlim_{j} \mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{T}_j), \qquad \mathcal{X}^{\pm} \simeq \Big(\varinjlim_{j} \mathrm{Sel}^{\pm}_{N^-}(K, \mathbf{A}_j)\Big)^{\vee}$$

(note that the almost divisibility result of [HL19, Prop. 3.12] used in the proof can be shown in the same manner in the supersingular case, replacing the appeal to results from [Cas17] by their counterparts in [CW24], and using the equality $\mathrm{Sel}^{\pm}(K, \mathbf{T}^{\mathrm{ac}}) = \mathrm{Sel}^{\pm,\mathrm{rel}}(K, \mathbf{T}^{\mathrm{ac}})$ shown in the proof of [CW24, Thm. 6.8]). Moreover, comparing the construction of the classes $\kappa_j^{\pm}(m)$ in [DI08, §4][5] and the construction of the classes $\mathbf{z}_\infty[S]^{\pm}$ in [CW24, §4.1][6], we see that (7.2) is the same as the class $\kappa_\infty^{\pm}$ in (7.1).

Denote by $\mathfrak{m} \subset \Lambda$ the maximal ideal.

Theorem 7.5 (Howard)**.** *Let the notations and hypotheses be as in Theorem 7.4. Then both $\mathcal{S}^{\pm}$ and $\mathcal{X}^{\pm}$ have Λ-rank one, and the following divisibility holds in Λ:*

$$\mathrm{Char}_{\Lambda}(\mathcal{X}^{\pm}_{\mathrm{tors}}) \supset \mathrm{Char}_{\Lambda}(\mathcal{S}^{\pm}/(\kappa_\infty^{\pm}))^2.$$

Moreover, if for some $j > 0$ there exists $m \in \mathcal{N}_j^{\mathrm{def}}$ such that $\lambda_j^{\pm}(m)$ has non-zero image under the map

$$\Lambda/p^j\Lambda \to \Lambda/\mathfrak{m}\Lambda \simeq \mathbf{F}_p,$$

then the above divisibility is an equality.

Proof. The element $\kappa_\infty^{\pm}$ is non-torsion by Cornut–Vatsal [CV07] (alternatively, it follows from the explicit reciprocity law of [CW24, Thm. 6.2] and the non-vanishing of $\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}$). Suppose $j = j_0 > 0$ is such that the condition in the last part of the theorem holds. Then by [BCK21, Lem. 3.6][7] it follows that for all $j \geq j_0$ the system $\boldsymbol{\lambda}_j^{\pm}$ satisfies the following condition: for all height one primes $\mathfrak{P} \subset \Lambda$, the system $\boldsymbol{\lambda}_j^{\pm}$ contains an element with non-zero image in $\Lambda/(\mathfrak{P}, p)$. The result thus follows from [How06, Thm. 3.2.3] with $k = k(\mathfrak{P}) = 1$ and the ordinary Selmer condition at the primes above p replaced by the $\pm$-condition, noting that the self-duality of the latter is given by [Kim07, Prop. 4.11], and as shown in [CW24, Lem. 6.5] the analogue of the control theorem of [How06, Prop. 3.3.1] follows from [Kim07, Prop. 4.18]. $\square$

For the proof of Theorem 7.1, we shall verify the non-vanishing condition in the last statement of Theorem 7.5 building on progress towards the *cyclotomic* Iwasawa main conjecture.

7.3. **A consequence of the GL_2-Iwasawa main conjecture.** If $g \in S_2(\Gamma_0(M))$ is any cuspidal eigenform, we denote by $A_g/\mathbf{Q}$ a GL_2-type abelian variety in the isogeny class associated to g, and by $\mathscr{O} = \mathscr{O}_g$ the ring of integers of the completion of the Hecke field $\mathbf{Q}(\{a_n(g)\}_n)$ at the prime $\wp$ above p determined by our fixed embedding $\iota_p : \overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. We also let

$$\Omega_g^{\mathrm{cong}} \in \overline{\mathbf{Q}}_p^{\times}$$

be Hida's canonical period of g as defined in [SZ14, §9.3]. For any number field F and a finite prime w of F, let $t_w(A_g/F)$ denote the Tamagawa exponent as defined in [*op. cit.*,§9.1].

Theorem 7.6. *Let $g \in S_2(\Gamma_0(M))$ be a cuspidal eigenform, and let $\wp$ be a prime of $\mathscr{O}_g$ above $p \geq 3$. Suppose that*

(i) *$\wp$ is good non-ordinary for g.*
(ii) *M is square-free.*

[5] see esp. [DI08, Prop. 4.3].
[6] see esp. [CW24, Prop. 4.4].
[7] where $\wp$ should denote the maximal ideal $\mathfrak{m}$ of Λ.

Then $L(g/K,1)$ is non-zero if and only if $\mathrm{Sel}_{\wp^\infty}(A_g/K)$ is finite, in which case

$$\mathrm{ord}_{\wp}\left(\frac{L(g/K,1)}{\Omega_g^{\mathrm{cong}}}\right)=\mathrm{length}_{\mathscr{O}}\,\mathrm{Sel}_{\wp^\infty}(A_g/K)+\sum_{w|M}t_w(A_g/K).$$

Proof. Let g^K be the newform associated to the twist of g by the quadratic character corresponding to K. As a consequence of the Iwasawa Main Conjecture for $\mathrm{GL}_2/\mathbf{Q}$ for non-ordinary primes (see [CÇSS18, Thm. C], and also [FW21, Cor. 1.10]) we have that $L(g,1)$ is non-zero if and only if $\mathrm{Sel}_{\wp^\infty}(A_g/\mathbf{Q})$ is finite, in which case

$$\mathrm{ord}_{\wp}\left(\frac{L(g,1)}{-2\pi i\cdot\Omega_g^+}\right)=\mathrm{length}_{\mathscr{O}}\,\mathrm{Sel}_{\wp^\infty}(A_g/\mathbf{Q})+\sum_{\ell|M}t_\ell(A_g/\mathbf{Q}),\tag{7.3}$$

where Ω_g^+ is the canonical period of g (see [SZ14, §9.2]), and similarly[8] with g^K in place of g. By [SZ14, Cor. 9.2] we have

$$\sum_{w|M}t_w(A_g/K)=\sum_{\ell|M}t_\ell(A_g/\mathbf{Q})+\sum_{\ell|M}t_\ell(A_{g^K}/\mathbf{Q}),$$

and since $\overline{\rho}$ is irreducible as a consequence of hypothesis (i), by Lemmas 9.5 and 9.6 in *op. cit.* we have the period relation

$$\Omega_g^{\mathrm{cong}}\sim_p(2\pi i)^2\cdot\Omega_g^+\cdot\Omega_{g^K}^+.$$

The result thus follows from the combination of (7.3) for g and g^K. □

Remark 7.7. Note that the p-th Fourier coefficient of the non-ordinary form g in Theorem 7.6 is not assumed to be zero. In fact, the result will be applied to a suitable g satisfying $g\equiv f \pmod{\wp^j}$ for some $j>0$, where f is as in Theorem 7.1, and so *a priori* we only have

$$a_p(g)\equiv 0\pmod{\wp^j}.$$

Thus the Iwasawa theory of g underlying the proof of Theorem 7.6 is of $\sharp/\flat$-type (after Sprung and Lei–Loeffler–Zerbes), rather than $\pm$-type (after Kobayashi and Pollack).

Suppose now that $g\in S_2(\Gamma_0(M))$ is an eigenform of level $M=M^+M^-$ with M^- equal to the square-free product of an *odd* number of primes inert in K and such that every prime factor of M^+ splits in K. Further, suppose that the p-th Fourier coefficient of g satisfies $a_p(g)\equiv 0\pmod{\wp^j}$ for some $j>0$.

As explained in [CÇSS18, §4.3] (see also [BBL24, Thm. 3.5]), building on the results of [CH18b] one can associate to g a pair of theta elements $\Theta_\infty^\pm(g/K)\in\mathscr{O}[\![\Gamma]\!]$, and it follows from their construction and the interpolation formula in [CH18b, Prop. 4.3] that the image of

$$L_p^\pm(g/K):=\Theta_\infty^\pm(g/K)^2\tag{7.4}$$

under the augmentation map $\mathscr{O}[\![\Gamma]\!]\to\mathscr{O}$ is equal to

$$\frac{L(g/K,1)}{\Omega_g^{\mathrm{cong}}}\cdot\frac{1}{\eta_{g,M^+,M^-}}\in\mathscr{O}$$

up to a p-adic unit, where $\eta_{g,M^+,M^-}\in\mathscr{O}$ is as in [Zha14, Eq. (6.4)]. Moreover, one can easily check the implication if $g\equiv f \pmod{\wp^j}$, then

$$\Theta_\infty^\pm(g/K)\equiv\Theta_\infty^\pm(f/K)\pmod{\wp^j\mathscr{O}[\![\Gamma]\!]}$$

(see [BBL24, Lem. 3.7]). Therefore, from the construction of the elements $\lambda_j^\pm(m)$, it follows that if g is level-raising f at $m\in\mathcal{N}_j^{\mathrm{def}}$, then the image of $\Theta_\infty^\pm(g/K)$ under the map $\mathscr{O}[\![\Gamma]\!]\to\mathscr{O}[\![\Gamma]\!]/\wp^j\mathscr{O}[\![\Gamma]\!]$ is the same as $\lambda_j^\pm(m)$.

[8]Note that [CÇSS18, Thm. C] assumes square-free level as stated, but as explained in [JSW17, Rmk. 7.2.3] it also applies to quadratic twists such as g^K.

7.4. **Proof of Theorem 7.1.** By Theorem 7.5 and the construction of $\boldsymbol{\lambda}_j^{\pm}$ of Theorem 7.4, it suffices to show that there exists $m \in \mathcal{N}^{\mathrm{def}}$ and an m-new eigenform $g \in S_2(\Gamma_0(Nm))$ with $f \equiv g \pmod{\wp}$, for which the p-adic L-function $L_p^{\pm}(g/K)$ in (7.4) is invertible. Let

$$r = \dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K). \tag{7.5}$$

The surjectivity of $\overline{\rho}$ implies that the natural map $\mathrm{Sel}_p(E/K) \twoheadrightarrow \mathrm{Sel}_{p^\infty}(E/K)[p]$ is an isomorphism. By (gen-Heeg) and the p-parity conjecture we know that r is odd, say $r = 2s+1$. By a repeated application of the argument in the proof [Zha14, Thm. 9.1] (to drop the Selmer rank (7.5) down to 1 by adding distinct admissible primes $q_1, \dots, q_{2s}$ to the level of f) and the proof of Theorem 7.2 in *op. cit.*, there exists $m = q_1 \cdots q_{2s} q_r \in \mathcal{N}^{\mathrm{def}}$ and an m-new eigenform $g \in S_2(\Gamma_0(Nm))$ level-raising f with $\dim_{\mathscr{O}/\wp} \mathrm{Sel}_\wp(A_g/K) = 0$. In particular,

$$\mathrm{Sel}_{\wp^\infty}(A_g/K) = 0.$$

From Theorem 7.6, it follows that

$$\mathrm{ord}_\wp\left(\frac{L(g/K,1)}{\Omega_g^{\mathrm{cong}}}\right) = \sum_{w \mid Nm} t_w(A_g/K).$$

By the hypothesis that $E[p]$ is ramified at the primes $\ell \mid N^+$, we have $t_w(A_g/K) = 0$ for all $w \mid N^+$, and by [PW11, Thm. 6.8] (see also [Zha14, Thm. 6.4]) we have

$$\mathrm{ord}_\wp(\eta_{g,N^+,N^-m}) = \sum_{w \mid N^-m} t_w(A_g/K).$$

Therefore,

$$\frac{L(g/K,1)}{\Omega_g^{\mathrm{cong}}} \frac{1}{\eta_{g,N^+,N^-m}} \in \mathscr{O}^\times,$$

and this concludes the proof.

References

[AC21] Adebisi Agboola and Francesc Castella, *On anticyclotomic variants of the p-adic Birch and Swinnerton-Dyer conjecture*, J. Théor. Nombres Bordeaux **33** (2021), no. 3, part 1, 629–658.

[BBL24] Ashay Burungale, Kâzı m Büyükboduk, and Antonio Lei, *Anticyclotomic Iwasawa theory of abelian varieties of* GL_2*-type at non-ordinary primes*, Adv. Math. **439** (2024), Paper No. 109465, 63.

[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.

[BD95] Massimo Bertolini and Henri Darmon, *Derived p-adic heights*, Amer. J. Math. **117** (1995), no. 6, 1517–1554.

[BD05] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic* $\mathbb{Z}_p$*-extensions*, Ann. of Math. (2) **162** (2005), no. 1, 1–64.

[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.

[Ben21] Denis Benois, *p-adic heights and p-adic Hodge theory*, Mém. Soc. Math. Fr. (N.S.) (2021), no. 167, vi + 135.

[BLV23] Massimo Bertolini, Matteo Longo, and Rodolfo Venerucci, *The anticyclotomic main conjectures for elliptic curves*, preprint, available at `https://arxiv.org/abs/2306.17784`.

[BMC24] David Burns and Daniel Macias Castillo, *On refined conjectures of Birch and Swinnerton-Dyer type for Hasse-Weil-Artin L-series*, Mem. Amer. Math. Soc. **297** (2024), no. 1482, v+156.

[Bra11] Miljan Brakočević, *Anticyclotomic p-adic L-function of central critical Rankin-Selberg L-value*, Int. Math. Res. Not. **Issue 12** (2011).

[Bur22] Ashay Burungale, *A p-adic Waldspurger Formula and the Conjecture of Birch and Swinnerton-Dyer*, J. Indian Inst. Sci. (2022), 885–894.

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

[CÇSS18] Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On the Iwasawa main conjectures for modular forms at non-ordinary primes*, available at `https://arxiv.org/abs/1804.10993`.

[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.

[CGS23] Francesc Castella, Giada Grossi, and Christopher Skinner, *Mazur's main conjecture at Eisenstein primes*, available at `https://arxiv.org/abs/2303.04373`.

[CH18a] Francesc Castella and Ming-Lun Hsieh, *Heegner cycles and p-adic L-functions*, Math. Ann. **370** (2018), no. 1-2, 567–628.

[CH18b] Masataka Chida and Ming-Lun Hsieh, *Special values of anticyclotomic L-functions for modular forms*, J. Reine Angew. Math. **741** (2018), 87–131.

[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.

[Col00] Pierre Colmez, *Fonctions L p-adiques*, no. 266, 2000, Séminaire Bourbaki, Vol. 1998/99, pp. Exp. No. 851, 3, 21–58.

[CV07] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186.

[CW24] Francesc Castella and Xin Wan, *Perrin-Riou's main conjecture for elliptic curves at supersingular primes*, Math. Ann. **389** (2024), no. 3, 2595–2636.

[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.

[DT94a] Fred Diamond and Richard Taylor, *Lifting modular mod l representations*, Duke Math. J. **74** (1994), no. 2, 253–269.

[DT94b] ———, *Nonoptimal levels of mod l modular representations*, Invent. Math. **115** (1994), no. 3, 435–462.

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

[FW21] Olivier Fouquet and Xin Wan, *On the Iwasawa Main Conjecture for universal families of modular motives*, available at `https://arxiv.org/abs/2107.13726`.

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

[Gre16] ———, *On the structure of Selmer groups*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 225–252.

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

[HL19] Jeffrey Hatley and Antonio Lei, *Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms*, Math. Res. Lett. **26** (2019), no. 4, 1115–1144.

[How04] Benjamin Howard, *Derived p-adic heights and p-adic L-functions*, Amer. J. Math. **126** (2004), no. 6, 1315–1340.

[How06] ———, *Bipartite Euler systems*, J. Reine Angew. Math. **597** (2006), 1–25.

[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.

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

[KO20] Shinichi Kobayashi and Kazuto Ota, *Anticyclotomic main conjecture for modular forms and integral Perrin-Riou twists*, Development of Iwasawa theory—the centennial of K. Iwasawa's birth, Adv. Stud. Pure Math., vol. 86, Math. Soc. Japan, Tokyo, [2020] ©2020, pp. 537–594.

[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.

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

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

[Nek95] Jan Nekovář, *On the p-adic height of Heegner cycles*, Math. Ann. **302** (1995), no. 4, 609–686. MR 1343644 (96f:11073)

[Nek01] ———, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

[Nek06] ———, *Selmer complexes*, Astérisque (2006), no. 310, viii+559.

[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.

[PR92] ———, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.

[PR93] ———, *Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes)*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 203–220.

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

[Rib84] Kenneth A. Ribet, *Congruence relations between modular forms*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 503–514.

[San23] Takamichi Sano, *Derived Bockstein regulators and anticyclotomic p-adic Birch and Swinnerton-Dyer conjectures*, preprint.

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

[SZ14] Christopher Skinner and Wei Zhang, *Indivisibility of Heegner points in the multiplicative case*, available at `https://arxiv.org/abs/1407.1099`.

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

(Castella) Department of Mathematics, University of California Santa Barbara, CA 93106
Email address: castella@ucsb.edu

(Hsu) Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA
Email address: chsu6@scu.edu

(Kundu) Department of Mathematical and Statistical Sciences, UTRGV, 1201 W University Dr., Edinburg, TX 78539, USA
Email address: dkundu@math.toronto.edu

(Lee) Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
Email address: yushglee@umich.edu

(Liu) Department of Mathematics, University of California Santa Barbara, CA 93106, USA
Email address: zliu@math.ucsb.edu