ON ANTICYCLOTOMIC VARIANTS OF THE p-ADIC BIRCH AND SWINNERTON-DYER CONJECTURE

ADEBISI AGBOOLA AND FRANCESC CASTELLA

Abstract. We formulate analogues of the Birch and Swinnerton-Dyer conjecture for the p-adic L-functions of Bertolini, Darmon, and Prasanna attached to elliptic curves $E/\mathbf{Q}$ at primes p of good ordinary reduction. Using Iwasawa theory, we then prove, under mild hypotheses, one of the inequalities predicted by the "rank part" of our conjectures, as well as the predicted leading coefficient formula, up to a p-adic unit.

Our conjectures are very closely related to conjectures of Birch and Swinnerton-Dyer type formulated by Bertolini and Darmon in 1996 for Heegner distributions, and as application of our results we also obtain the proof of an inequality in the rank part of their conjectures.

Contents

1. Introduction

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, let $p > 2$ be a prime of good ordinary reduction for E, and let K be an imaginary quadratic field of discriminant prime to Np. Let K_∞/K be the anticyclotomic $\mathbf{Z}_p$-extension of K, and set $\Gamma_\infty = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \mathbf{Z}_p[[\Gamma_\infty]]$.

Assume that K satisfies the *Heegner hypothesis* relative to N, i.e., that

(Heeg) every prime factor of N splits in K.

This condition implies that the root number of E/K is -1. Assume in addition that

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

and let $\hat{\mathcal{O}}$ be the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$. Let $f \in S_2(\Gamma_0(N))$ be the newform associated with E. In [BDP13] (as later strengthened in [Bra11, CH18]), Bertolini–Darmon–Prasanna introduced a p-adic L-function

$$\mathscr{L}_{\mathfrak{p}}(f) \in \Lambda_{\hat{\mathcal{O}}} := \Lambda\hat{\otimes}_{\mathbf{Z}_p}\hat{\mathcal{O}}$$

with $L_{\mathfrak{p}}(f) := \mathscr{L}_{\mathfrak{p}}(f)^2$ interpolating the central critical values for the twists of f/K by certain infinite order characters of Γ_∞. In this paper we formulate and study analogues of the Birch and Swinnerton-Dyer conjecture for these p-adic L-functions.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11R23, 11G16.

F. Castella's research supported in part by National Science Foundation grant DMS-1946136.

Any continuous character $\chi : \Gamma_\infty \to \hat{\mathcal{O}}^\times$ extends to a map $\chi : \Lambda_{\hat{\mathcal{O}}} \to \hat{\mathcal{O}}$, and we write $L_\mathfrak{p}(f)(\chi)$ for $\chi(L_\mathfrak{p}(f))$. The trivial character $\mathbb{1}$ of Γ_∞ lies outside the range of p-adic interpolation for $L_\mathfrak{p}(f)$, and one of the main results of [BDP13] is a formula of p-adic Gross–Zagier type for this value:

$$L_\mathfrak{p}(f)(\mathbb{1}) = \frac{1}{u_K^2 c_E^2} \cdot \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \log_{\omega_E}(z_K)^2 \tag{1.1}$$

(see [BDP13, Thm. 5.13], as specialized in [BDP12, Thm. 3.12] to the case where f has weight $k = 2$). Here $a_p(E) := p + 1 - \#E(\mathbf{F}_p)$ and $u_K := \frac{1}{2}\#\mathcal{O}_K^\times$ as usual, $z_K \in E(K)$ is a Heegner point arising from a modular parametrization $\varphi : X_0(N) \to E$,

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

is the formal group logarithm associated with a Néron differential $\omega_E \in \Omega^1(E/\mathbf{Z}_{(p)})$, and $c_E \in \mathbf{Z}$ is such that $\varphi^*(\omega_E) = c_E \cdot 2\pi i f(\tau) d\tau$.

Formula (1.1) has been a key ingredient in recent progress towards the Birch and Swinnerton-Dyer conjecture. Most notably, for elliptic curves $E/\mathbf{Q}$ with $\mathrm{rank}_\mathbf{Z} E(\mathbf{Q}) = 1$ and $\#\text{Ш}(E/\mathbf{Q})_{p^\infty} < \infty$, it was used by Skinner [Ski20] (for a suitable choice of K) to prove a converse to the celebrated theorem of Gross–Zagier and Kolyvagin, and for elliptic curves $E/\mathbf{Q}$ with $\mathrm{ord}_{s=1} L(E, s) = 1$, it was used by Jetchev–Skinner–Wan [JSW17] (again, for suitably chosen K) to prove under mild hypotheses the p-part of the Birch and Swinnerton-Dyer formula.

However, when $\mathrm{rank}_\mathbf{Z} E(K) > 1$ the Heegner point z_K is torsion and formula (1.1) shows that $L_\mathfrak{p}(f)(\mathbb{1}) = 0$. In other words, in that case $L_\mathfrak{p}(f) \in J$, where

$$J := \ker(\epsilon : \Lambda_{\hat{\mathcal{O}}} \to \hat{\mathcal{O}})$$

is the augmentation ideal of $\Lambda_{\hat{\mathcal{O}}}$. The conjectures we formulate in this paper predict the largest power J^ν in which $L_\mathfrak{p}(f)$ lives (i.e., the "order of vanishing" of $L_\mathfrak{p}(f)$ at $\mathbb{1}$) in terms of the ranks of $E(\mathbf{Q})$ and $E(K)$, and a formula for the image of $L_\mathfrak{p}(f)$ in $J^\nu/J^{\nu+1}$ (i.e., the "leading coefficient" of $L_\mathfrak{p}(f)$ at $\mathbb{1}$) in terms of arithmetic invariants of E. For the sake of illustration, we now concentrate on a weaker form of our conjectures, whose refined formulation is given in Section 4.

Let $S_p(E/K)$ be the pro-p Selmer group of E fitting in the exact sequence

$$0 \to E(K) \otimes \mathbf{Z}_p \to S_p(E/K) \to T_p\text{Ш}(E/K) \to 0,$$

where $T_p\text{Ш}(E/K) = \varprojlim_m \text{Ш}(E/K)_{p^m}$ is the p-adic Tate module of the Tate–Shafarevich group of E over K. Assume that $\#\text{Ш}(E/K) < \infty$, so in particular $S_p(E/K) \simeq E(K) \otimes \mathbf{Z}_p$. The work of Mazur–Tate [MT83] produces a canonical symmetric p-adic height pairing

$$h_p^{\mathrm{MT}} : S_p(E/K) \times S_p(E/K) \to (J/J^2) \otimes \mathbf{Q}.$$

Our assumption also implies that the modified Selmer group

$$\mathfrak{Sel}_\mathfrak{p}(K, T) := \ker\{S_p(E/K) \to E(K_\mathfrak{p}) \otimes \mathbf{Z}_p\}$$

has $\mathbf{Z}_p$-rank $r - 1$, where $r = \mathrm{rank}_\mathbf{Z} E(K)$. Assume that $S_p(E/K)$ is torsion-free (this holds if e.g. E_p is irreducible as G_K-module), let $P_1, \ldots, P_r$ be an integral basis for $E(K) \otimes \mathbf{Q}$ and let M be an endomorphism of $E(K) \otimes \mathbf{Z}_p$ sending the basis $P_1, \ldots, P_r$ to a $\mathbf{Z}_p$-basis $x_1, \ldots, x_{r-1}, y_\mathfrak{p}$ for $S_p(E/K)$ with $x_1, \ldots, x_{r-1}$ generating $\mathfrak{Sel}_\mathfrak{p}(K, T)$. Set

$$t_M = \det(M) \cdot [E(K) \colon \mathbf{Z}P_1 + \cdots + \mathbf{Z}P_r].$$

The following is a special case of our Conjecture 4.2.

Conjecture 1.1. *Assume that $\#\text{Ш}(E/K) < \infty$ and that E_p is irreducible as G_K-module, and let $r = \mathrm{rank}_\mathbf{Z} E(K)$. Then:*

(i) $L_\mathfrak{p}(f) \in J^{r-1}$.

(ii) *Letting $\bar{L}_{\mathfrak{p}}(f)$ be the natural image of $L_{\mathfrak{p}}(f)$ in J^{r-1}/J^r, we have*

$$\bar{L}_{\mathfrak{p}}(f) = \left(\frac{1-a_p(E)+p}{p}\right)^2 \cdot \log_{\omega_E}(y_{\mathfrak{p}})^2 \cdot \mathrm{Reg}_{\mathfrak{p}} \cdot t_M^{-2} \cdot \#\text{Ш}(E/K) \cdot \prod_{\ell \mid N} c_\ell^2,$$

where $\mathrm{Reg}_{\mathfrak{p}} = \det(h_p^{\mathrm{MT}}(x_i, x_j))_{1 \leqslant i,j \leqslant r-1}$ *is the regulator of* h_p^{MT} *restricted to* $\mathrm{Sel}_{\mathrm{str}}(K,T)$*, and c_ℓ is the Tamagawa number of $E/\mathbf{Q}_\ell$.*

Remark 1.2. Suppose $\mathrm{rank}_{\mathbf{Z}} E(K) = 1$. Under the assumptions of Conjecture 1.1 we then have $\mathfrak{Sel}_{\mathfrak{p}}(K,T) = 0$, $\mathrm{Reg}_{\mathfrak{p}} = 1$ and $t_M^{-1} \cdot \log_{\omega_E}(y_{\mathfrak{p}}) = [E(K) : \mathbf{Z}.P]^{-1} \cdot \log_{\omega_E}(P)$, where $P \in E(K)$ is any non-torsion point. Hence in this case Conjecture 1.1 predicts that $L_{\mathfrak{p}}(f)(\mathbb{1}) \neq 0$, and by formula (1.1) the predicted expression for $L_{\mathfrak{p}}(f)(\mathbb{1})$ is equivalent to the equality

$$[E(K) : \mathbf{Z}.z_K]^2 = u_K^2 c_E^2 \cdot \#\text{Ш}(E/K) \cdot \prod_{\ell \mid N} c_\ell^2. \tag{1.2}$$

Note that (1.2) is also predicted by the classical Birch and Swinnerton-Dyer conjecture for E/K when combined with the Gross–Zagier formula (see [Gro91, Conj. 1.2]).

The p-adic L-function $L_{\mathfrak{p}}(f)$ is known to be nonzero ([CH18, Thm. 3.9]), and the Iwasawa–Greenberg main conjecture [Gre94] predicts that $L_{\mathfrak{p}}(f)$ generates the characteristic ideal of a certain Λ-torsion Selmer group $X_{\mathfrak{p}}$. Letting $F_{\mathfrak{p}}(f) \in \Lambda$ be a generator of the characteristic ideal of $X_{\mathfrak{p}}$, in this paper we prove the following result on the algebraic side, which can be viewed as an extension of the "anticyclotomic control theorem" of [JSW17, §3.3] to arbitrary ranks.

Theorem 1.3 (see Theorem 6.2 for a more general statement)**.** *Assume that $\#\text{Ш}(E/K)_{p^\infty} < \infty$ and that:*

(i) *$\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E_p)$ is surjective.*
(ii) *E_p is ramified at every prime $\ell \mid N$.*
(iii) *$p \nmid \#E(\mathbf{F}_p)$.*

Then $F_{\mathfrak{p}}(f) \in J^{r-1}$, where $r = \mathrm{rank}_{\mathbf{Z}} E(K)$, and letting $\bar{F}_{\mathfrak{p}}(f)$ be the natural image of $F_{\mathfrak{p}}(f)$ in J^{r-1}/J^r, we have

$$\bar{F}_{\mathfrak{p}}(f) = p^{-2} \cdot \log_{\omega_E}(y_{\mathfrak{p}})^2 \cdot \mathrm{Reg}_{\mathfrak{p}} \cdot \#\text{Ш}(E/K)_{p^\infty}$$

up to a p-adic unit.

Remark 1.4. Note that under hypotheses (ii) and (iii) in Theorem 1.3, the terms $1 - a_p(E) + p$ and c_ℓ in Conjecture 1.1 are all p-adic units.

Combined with the Iwasawa–Greenberg main conjecture for $L_{\mathfrak{p}}(f)$ (which is known under relatively mild hypotheses [BCK20]), Theorem 1.3 can be parlayed in terms $L_{\mathfrak{p}}(f)$ (see Corollary 6.4), yielding our main result towards Conjecture 1.1, or rather its refinement in Conjecture 4.2.

Let us now comment on the need for the aforementioned refinement of Conjecture 1.1. We continue to assume that $\#\text{Ш}(E/K) < \infty$, and let

$$r^{\pm} := \mathrm{rank}_{\mathbf{Z}} E(K)^{\pm}$$

be the rank of the $\pm$-eigenspaces of $E(K)$ under complex conjugation. Thus

$$r = \mathrm{rank}_{\mathbf{Z}} E(K) = r^+ + r^-.$$

From the Galois-equivariance properties of h_p^{MT}, one easily sees that $\mathrm{Reg}_{\mathfrak{p}} = 0$ when $|r^+ - r^-| > 1$. These systematic degeneracies of the p-adic height pairing in the anticyclotomic setting (which are in sharp contrast with the expected non-degeneracy of the p-adic height pairing in the cyclotomic setting) were understood by Bertolini–Darmon [BD94, BD95] as giving rise to canonical *derived* p-adic height pairings, in terms of which we will define a generalized p-adic regulator $\mathrm{Reg}_{\mathrm{der},\mathfrak{p}}$. This generalized regulator recovers $\mathrm{Reg}_{\mathfrak{p}}$ when $|r^+ - r^-| = 1$, but provides extra information when $|r^+ - r^-| > 1$. More precisely, the expected "maximal non-degeneracy" of the anticyclotomic p-adic height pairing leads to the prediction that $\mathrm{Reg}_{\mathrm{der},\mathfrak{p}}$ is a nonzero element in $J^{2\rho}/J^{2\rho+1}$, where

$$\rho = \max\{r^+, r^-\} - 1.$$

Conjecture 4.2 then predicts that $L_{\mathfrak{p}}(f)$ lands in $J^{2\rho}$ (note that $2\rho > r-1$ when $|r^+ - r^-| > 1$), and posits a formula for its natural image in $J^{2\rho}/J^{2\rho+1}$ in terms of $\mathrm{Reg}_{\mathrm{der},\mathfrak{p}}$. Our main result (see Theorem 6.2) is the analogue of Theorem 1.3 for this refined conjecture.

Remark 1.5. As will be clear to the reader, our conjectures are closely related to the conjectures of Birch and Swinnerton-Dyer type formulated by Bertolini–Darmon [BD96] for certain Heegner distributions. In fact, as application of our results towards the p-adic Birch–Swinnerton-Dyer conjecture for $L_{\mathfrak{p}}(f)$ formulated here, we will deduce under mild hypotheses the proof of an inequality in the rank part of their conjectures (see Corollary 6.5).

Here is an outline of the paper. After some preliminaries in Section 2, in Section 3 we recall the conjectures of Bertolini–Darmon for Heegner distributions. In Section 4 we formulate our conjectures of Birch and Swinnerton-Dyer type for the p-adic L-functions $L_{\mathfrak{p}}(f)$ and $\mathscr{L}_{\mathfrak{p}}(f)$, and in Section 5 we relate the rank part of our conjectures to the rank part of those of Bertolini–Darmon. Finally, in Section 6 we state and prove our main results towards these conjectures.

Acknowledgements. The authors thank Henri Darmon, Chris Skinner, and the anonymous referee for their comments on an earlier draft of this paper.

2. Selmer groups

We keep the notation from the Introduction. In particular, K_∞ denotes the anticyclotomic $\mathbf{Z}_p$-extension of K. For every n we write K_n for the subextension of K_∞ with

$$\Gamma_n := \mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}.$$

Let S be a finite set of places of $\mathbf{Q}$ containing ∞ and the primes dividing Np. For every finite extension $F/\mathbf{Q}$ let $\mathfrak{G}_{F,S} = \mathrm{Gal}(F^S/F)$ be the Galois group of the maximal algebraic extension of F unramified outside the places above S. Let $T = T_pE$ be the p-adic Tate module of E, and for each prime $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ set

$$\mathfrak{Sel}_{\mathfrak{q}}(K_n, T) := \ker\left\{\mathrm{H}^1(\mathfrak{G}_{K_n,S}, T) \to \prod_{w \nmid \mathfrak{q}} \mathrm{H}^1(K_{n,w}, T)\right\}.$$

Let $\mathfrak{Sel}_{\mathfrak{q}}(K_n, E_{p^\infty}) \subset \mathrm{H}^1(\mathfrak{G}_{K_n,S}, E_{p^\infty})$ be the Selmer group cut out by the local conditions given by the orthogonal complement under local Tate duality of the subspaces cutting out $\mathfrak{Sel}_{\mathfrak{q}}(K_n, T)$, and set

$$\mathfrak{Sel}_{\mathfrak{q}}(K_\infty, E_{p^\infty}) := \varinjlim_n \mathfrak{Sel}_{\mathfrak{q}}(K_n, E_{p^\infty}).$$

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

Conjecture 2.1 (Iwasawa–Greenberg main conjecture)**.** *$\mathfrak{Sel}_{\mathfrak{p}}(K_\infty, E_{p^\infty})$ is Λ-cotorsion and*

$$\mathrm{char}_\Lambda(\mathfrak{Sel}_{\mathfrak{p}}(K_\infty, E_{p^\infty})^\vee)\Lambda_{\hat{\mathcal{O}}} = (L_{\mathfrak{p}}(f))$$

as ideals in $\Lambda_{\hat{\mathcal{O}}}$.

Here $L_{\mathfrak{p}}(f) = \mathscr{L}_{\mathfrak{p}}(f)^2$ denotes the square of the p-adic L-function

$$\mathscr{L}_{\mathfrak{p}}^{\mathrm{BDP}}(f) \in \Lambda_{\hat{\mathcal{O}}}$$

constructed in [BCK20, §4] (following earlier constructions in [BDP13, CH18]).

The following lemma will be useful in the following. Let

$$\mathrm{Sel}_{\mathrm{str}}(K,T) := \ker\left\{ \mathrm{H}^1(\mathfrak{G}_{K,S},T) \to \prod_w \mathrm{H}^1(K_w,T)\right\}$$

be the strict Selmer group, which is clearly contained in $S_p(E/K)$.

Lemma 2.2. *Assume that $\#\text{Ш}(E/K)_{p^\infty} < \infty$. Then*

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

In particular, $\mathfrak{Sel}_{\mathfrak{p}}(K,T)$ and $\mathfrak{Sel}_{\overline{\mathfrak{p}}}(K,T)$ are both contained in $S_p(E/K)$ and have $\mathbf{Z}_p$-rank $r-1$, where $r = \mathrm{rank}_{\mathbf{Z}} E(K)$.

Proof. By our assumption on $\text{Ш}(E/K)$, hypothesis (Heeg) and the p-parity conjecture [Nek01] imply that $r = \mathrm{rank}_{\mathbf{Z}} E(K)$ is odd, so in particular $r > 0$. Thus the image of restriction map

$$S_p(E/K) \to \prod_{w|p} E(K_w) \otimes \mathbf{Z}_p \tag{2.1}$$

has $\mathbf{Z}_p$-rank one, and the result follows from [Ski20, Lem. 2.3.2]. □

3. Conjectures of Bertolini–Darmon

In this section, we recall some of the conjectures of Birch–Swinnerton-Dyer type formulated by Bertolini–Darmon in [BD96]. These conjectures will guide our formulation in §4 of analogous statements for the p-adic L-functions $L_{\mathfrak{p}}(f)$ and $\mathscr{L}_{\mathfrak{p}}(f)$ of Bertolini–Darmon–Prasanna.

As in the Introduction, we assume that the elliptic curve $E/\mathbf{Q}$ has good ordinary reduction at $p > 2$, and that K is an imaginary quadratic field of discriminant D_K prime to Np in which $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits. However, rather than hypothesis (Heeg) from the Introduction, we assume that writing N as the product

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

with N^+ (resp. N^-) divisible only by primes which are split (resp. inert) in K, we have

(gen-H) $\quad N^-$ is the squarefree product of an even number of primes.

This condition still guarantees that the root number of E/K is -1, as well as the presence of Heegner points on E defined over the different layers of the anticyclotomic $\mathbf{Z}_p$-extension K_∞/K.

More precisely, let X_{N^+,N^-} be the Shimura curve (with the cusps added when $N^- = 1$, so $X_{N,1} = X_0(N)$) attached to the quaternion algebra $B/\mathbf{Q}$ of discriminant N^- and an Eichler order $R \subset B$ of level N^+. The curve X_{N^+,N^-} has a canonical model over $\mathbf{Q}$, and we let $J(X_{N^+,N^-})_{/\mathbf{Q}}$ denote its Jacobian. By [BCDT01], we may fix a modular parametrization

$$\varphi : X_0(N) \to E.$$

This induces a map $J(X_0(N)) \to E$ by Albanese functoriality, which by the Jacquet–Langlands correspondence together with Faltings' isogeny theorem gives rise to a map

$$\varphi_* : J(X_{N^+,N^-}) \to E. \tag{3.1}$$

Similarly as in [BD96, p. 425], after possibly changing E within its isogeny class, we assume that E is an optimal quotient of $J(X_{N^+,N^-})$, meaning that the kernel of (3.1) is connected.

When $N^- \neq 1$, lacking the existence of a natural rational base point on X_{N^+,N^-}, we choose an auxiliary prime ℓ_0 and consider (following [JSW17, §4.2]) the embedding

$$\iota_{N^+,N^-} : X_{N^+,N^-} \to J(X_{N^-,N^-}) \tag{3.2}$$

given by $x \mapsto (T_{\ell_0} - \ell_0 - 1)[x]$.

Let $K[c]$ be the ring class field of K of conductor c. For integers c prime to ND_K, there are CM points $h_c \in X_{N^+,N^-}(K[c])$ satisfying the relations

$$\mathrm{Norm}_{K[c\ell]/K[c]}(h_c) = \begin{cases} T_\ell \cdot h_c & \text{if } \ell \nmid c \text{ is inert in } K, \\ T_\ell \cdot h_c - \sigma_\ell h_c - \sigma_\ell^* h_c & \text{if } \ell \nmid c \text{ splits in } K, \\ T_\ell \cdot h_c - h_{c/\ell} & \text{if } \ell \mid c, \end{cases} \tag{3.3}$$

where σ_ℓ and σ_ℓ^* denote the Frobenius elements of the primes in K above ℓ. (See e.g. [How04, Prop. 1.2.1].) Assume from now on that E_p is irreducible as a $G_{\mathbf{Q}}$-module, and choose the prime ℓ_0 in (3.2) so that $a_{\ell_0}(E) - \ell_0 - 1 \notin p\mathbf{Z}$. Define $y_n \in E(K[p^n]) \otimes \mathbf{Z}_p$ by

$$y_n := \frac{1}{a_{\ell_0}(E) - \ell_0 - 1} \cdot \varphi_*(\iota_{N^+,N^-}(h_{p^n})),$$

and letting α_p be the p-adic unit root of the polynomial $X^2 - a_p(E)X + p$, define the *regularized Heegner point* of conductor p^n by

$$z_n := \frac{1}{\alpha^n} \cdot y_n - \frac{1}{\alpha^{n+1}} \cdot y_{n-1}, \quad \text{if } n \geqslant 1,$$
$$z_0 := u_K^{-1} \cdot (1 - (\sigma_p + \sigma_p^*)\alpha^{-1} + \alpha^{-2}) \cdot y_0.$$

One immediately checks from (3.3) that the points z_n are norm-compatible. For each $n \geqslant 0$, we then set

$$\mathbf{z}_n := \mathrm{Norm}_{K[p^m]/K_n}(z_m), \tag{3.4}$$

where $m \gg 0$ is such that $K_n \subset K[p^m]$, and letting $Z_p := E(K_\infty) \otimes \mathbf{Z}_p$ we define $\theta_n \in Z_p[\Gamma_n]$ by

$$\theta_n := \sum_{\sigma \in \Gamma_n} \mathbf{z}_n^\sigma \otimes \sigma^{-1}.$$

These elements are compatible under the natural projections $Z_p[\Gamma_{n+1}] \to Z_p[\Gamma_n]$, and in the limit they define the "Heegner distribution"

$$\theta = \theta_\infty := \varprojlim_n \theta_n \in Z_p[[\Gamma_\infty]]. \tag{3.5}$$

Let J be the augmentation ideal of $\Lambda = \mathbf{Z}_p[[\Gamma_\infty]]$, and define the *order of vanishing* of θ by

$$\mathrm{ord}_J\theta := \max\left\{\rho \in \mathbf{Z}_{\geqslant 0} \, : \, \theta \in Z_p \otimes_{\mathbf{Z}_p} J^\rho\right\}.$$

Remark 3.1. We note that the work of Cornut–Vatsal [CV07] implies that θ is a nonzero element in $Z_p[[\Gamma_\infty]]$, and so its order of vanishing is well-defined.

Recall that $E(K)^\pm$ denotes the $\pm$-eigenspaces of $E(K)$ under the action of complex conjugation. The following conjecture is the "indefinite case" of [BD96, Conj. 4.1].

Conjecture 3.2 (Bertolini–Darmon). *We have*

$$\mathrm{ord}_J\theta = \max\{r^+, r^-\} - 1,$$

where $r^\pm := \mathrm{rank}_{\mathbf{Z}} E(K)^\pm$.

Let θ^* denote the image of θ under the involution of $Z_p[[\Gamma_\infty]]$ given by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma_\infty$, and set

$$\mathscr{L} := \theta \otimes \theta^* \in Z_p^{\otimes 2}[[\Gamma_\infty]].$$

Lemma 3.3. *Let $\rho = \mathrm{ord}_J\theta$. Then the natural image $\bar{\mathscr{L}}$ of $\mathscr{L}$ in $Z_p^{\otimes 2} \otimes_{\mathbf{Z}_p} (J^{2\rho}/J^{2\rho+1})$ is contained in the image of the map*

$$E(K)^{\otimes 2} \otimes (J^{2\rho}/J^{2\rho+1}) \to Z_p^{\otimes 2} \otimes_{\mathbf{Z}_p} (J^{2\rho}/J^{2\rho+1}).$$

Proof. This follows from the fact that the natural image of θ in $Z_p \otimes_{\mathbf{Z}_p} (J^{\rho}/J^{\rho+1})$ is fixed by Γ_∞ (see [BD96, Lem. 2.14]). □

Let $r = \mathrm{rank}_{\mathbf{Z}} E(K)$. Since clearly

$$2(\max\{r^+, r^-\} - 1) \geqslant r - 1,$$

by Lemma 3.3 we see that Conjecture 3.2 predicts in particular the inclusion $\bar{\mathscr{L}} \in E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$. The conjectures of Bertolini–Darmon also predict an expression for $\bar{\mathscr{L}}$ in terms of the following "enhanced" regulator associated to the Mazur–Tate anticyclotomic p-adic height pairing

$$h_p^{\mathrm{MT}} : E(K) \times E(K) \to (J/J^2) \otimes \mathbf{Q}.$$

Definition 3.4. Let $P_1, \dots, P_r$ be a basis for $E(K)/E(K)_{\mathrm{tors}}$ and set $t = [E(K)\colon \mathbf{Z}P_1 + \dots + \mathbf{Z}P_r]$. The *enhanced regulator* $\widetilde{\mathrm{Reg}}$ is the element of $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r) \otimes \mathbf{Q}$ defined by

$$\widetilde{\mathrm{Reg}} := \frac{1}{t^2} \sum_{i,j=1}^{r} (-1)^{i+j} P_i \otimes P_j \otimes R_{i,j},$$

where $R_{i,j}$ is the (i,j)-minor of the matrix $(h_p^{\mathrm{MT}}(P_i, P_j))_{1 \leqslant i,j \leqslant r}$.

The next remark will be important in the following.

Remark 3.5. The non-trivial automorphism $\tau \in \mathrm{Gal}(K/\mathbf{Q})$ acts as multiplication by -1 on Γ_∞. Viewing h_p^{MT} as valued in $\Gamma_\infty \otimes \mathbf{Q}$ via the natural identification $J/J^2 \simeq \Gamma_\infty$, the Galois-equivariance of h_p^{MT} implies that

$$h_p^{\mathrm{MT}}(\tau x, \tau y) = h_p^{\mathrm{MT}}(x, y)^\tau = -h_p^{\mathrm{MT}}(x, y).$$

It follows that the τ-eigenspaces $E(K)^\pm$ are isotropic for h_p^{MT}, and so the null-space of h_p^{MT} has rank at least $|r^+ - r^-|$.

The following is the "non-exceptional case" of [BD96, Conj. 4.5].

Conjecture 3.6 (Bertolini–Darmon)**.** *Let $\bar{\mathscr{L}}$ be the natural image of $\mathscr{L}$ in $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$. Then*

$$\bar{\mathscr{L}} = \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \widetilde{\mathrm{Reg}} \cdot \#\text{Ш}(E/K) \cdot \prod_{\ell \mid N^+} c_\ell^2,$$

where c_ℓ is the Tamagawa number of $E/\mathbf{Q}_\ell$.

As noted in [BD96, p. 447], when $|r^+ - r^-| > 1$ Conjecture 3.6 reduces to the prediction "$0 = 0$". Indeed, $2(\max\{r^+, r^-\} - 1)$ is then strictly larger than $r - 1$, and so by Conjecture 3.2 the image of $\mathscr{L}$ in $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$ should vanish, while on the other hand the isotropy of $E(K)^\pm$ under h_p^{MT} forces $\widetilde{\mathrm{Reg}}$ to also vanish in this case (see [BD96, Lem. 3.2]).

As explained below, a refinement of Conjecture 3.6, predicting a formula for the natural image of $\mathscr{L}$ in $E(K)^{\otimes 2} \otimes (J^{2\rho}/J^{2\rho+1})$, which should be thought of as the "leading coefficient" of $\mathscr{L}$, can be given in terms of the *derived* p-adic height pairings introduced by Bertolini–Darmon [BD94, BD95].

Remark 3.7. Such refinements of Conjecture 3.6 (namely Conjecture 3.11 and 3.16 below) seems to not have been explicitly stated in the literature. Even though the formulation of such refinements appears to be quite clear in light of the conjectures explicitly stated in [BD96] and [BD95], any inaccuracies in the conjectures below should be blamed only on the authors of this paper.

Assume from now on that $Ш(E/K)_{p^\infty}$ is finite and that:

(i) $\bar{\rho}_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E_p)$ is surjective.
(ii) $p \nmid \#E(\mathbf{F}_p)$.
(iii) E_p is ramified at every prime $\ell | N$.

Note that (ii) amounts to the condition $a_p(E) \not\equiv 1 \pmod{p}$, and condition (i) implies that E has no CM. In particular, these assumptions imply that $S_p(E/K) \simeq E(K) \otimes \mathbf{Z}_p$ is a free $\mathbf{Z}_p$-module of rank r, and the pair (E, K) is "generic" in the terminology of [Maz84].

By [BD95, §2.4], there is a filtration

$$S_p(E/K) = \bar{S}_p^{(1)} \supset \bar{S}_p^{(2)} \supset \cdots \supset \bar{S}_p^{(p)}, \tag{3.6}$$

and a sequence of "derived p-adic height pairings"

$$h_p^{(k)} : \bar{S}_p^{(k)} \times \bar{S}_p^{(k)} \to (J^k/J^{k+1}) \otimes \mathbf{Q}, \quad \text{for } 1 \leqslant k \leqslant p-1,$$

such that $\bar{S}_p^{(k+1)}$ is the null-space of $h_p^{(k)}$, with $h_p^{(1)} = h_p^{\mathrm{MT}}$. By Remark 3.5, $\bar{S}_p^{(2)}$ has $\mathbf{Z}_p$-rank at least $|r^+ - r^-|$, and by construction the subspace of universal norms

$$US_p(E/K) := \bigcap_{n \geqslant 1} \mathrm{cor}_{K_n/K}(S_p(E/K_n))$$

is contained in the null-space of all $h_p^{(k)}$. The work of Cornut–Vatsal implies that $US_p(E/K) \simeq \mathbf{Z}_p$.

The expected "maximal non-degeneracy" of h_p^{MT} predicts the following (see [BD95, Conj. 3.3, Conj. 3.8]).

Conjecture 3.8 (Mazur, Bertolini–Darmon)**.** *Under the above hypotheses we have*

$$\mathrm{rank}_{\mathbf{Z}_p} \bar{S}_p^{(k)} = \begin{cases} |r^+ - r^-| & \text{if } k = 2, \\ 1 & \text{if } k \geqslant 3, \end{cases}$$

and in fact $\bar{S}_p^{(3)} = US_p(E/K)$.

By construction, the successive quotients $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$ are free $\mathbf{Z}_p$-modules, say

$$\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)} \simeq \mathbf{Z}_p^{e_k}, \tag{3.7}$$

and Conjecture 3.8 predicts in particular that

$$e_1 = 2\min\{r^+, r^-\}, \quad e_2 = |r^+ - r^-| - 1,$$

and $e_k = 0$ for all $k \geqslant 3$.

Using derived p-adic height pairings, one can define an enhanced p-adic regulator extending Definition 3.4. Assume that $\bar{S}_p^{(p)} = US_p(E/K)$ (as Conjecture 3.8 predicts in particular). Let $P_1, \ldots, P_r$ be an integral basis for $E(K) \otimes \mathbf{Q}$, and let $M \in M_n(\mathbf{Z}_p)$ be an endomorphism of $S_p(E/K)$ sending $P_1, \ldots, P_r$ to a $\mathbf{Z}_p$-basis $x_1, \ldots, x_r$ for $S_p(E/K)$ compatible with the filtration (3.6), so for $1 \leqslant k \leqslant p-1$ the projection of say $x_{h_k+1}, \ldots, x_{h_k+e_k}$ to $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$ is a $\mathbf{Z}_p$-basis for $\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)}$ and $y := x_r$ generates $US_p(E/K)$. Set $t_M = \det(M) \cdot [E(K) \colon \mathbf{Z}P_1 + \cdots + \mathbf{Z}P_r]$.

Definition 3.9. Let $\varrho := \sum_{k=1}^{p-1} k e_k$. The *derived enhanced regulator* $\widetilde{\mathrm{Reg}}_{\mathrm{der}}$ is the element of $E(K)^{\otimes 2} \otimes (J^\varrho/J^{\varrho+1}) \otimes \mathbf{Q}$ defined by

$$\widetilde{\mathrm{Reg}}_{\mathrm{der}} := t_M^{-2} \cdot (y \otimes y) \otimes \prod_{k=1}^{p-1} R^{(k)},$$

where $R^{(k)} = \det(h_p^{(k)}(x_i, x_j))_{h_k+1 \leqslant i,j \leqslant h_k+e_k}$.

The relation between $\widetilde{\mathrm{Reg}}_{\mathrm{der}}$ and $\widetilde{\mathrm{Reg}}$ is readily described.

Lemma 3.10. *Assume Conjecture 3.8. If* $|r^+ - r^-| = 1$, *then* $\widetilde{\mathrm{Reg}}_{\mathrm{der}} = \widetilde{\mathrm{Reg}}$.

Proof. By our running assumption that $\#\text{Ш}(E/K)_{p^\infty} < \infty$, we may view h_p^{MT} as defined on $S_p(E/K)$. Denote by $R'_{i,j}$ the (i,j)-minor of the matrix $(h_p^{\mathrm{MT}}(x_i,x_j))_{1\leqslant i,j\leqslant r}$. Since universal norms are in the null-space of h_p^{MT}, we find that

$$\begin{aligned}\widetilde{\mathrm{Reg}} &= t_M^{-2}\sum_{1\leqslant i,j\leqslant r}(-1)^{i+j}x_i\otimes x_j\otimes R'_{i,j}\\ &= t_M^{-2}\cdot(y\otimes y)\otimes R'_{r,r},\end{aligned}$$

noting that for $(i,j)\neq(r,r)$ the minor $R'_{i,j}$ is the determinant of a matrix having either a row or a column consisting entirely of zeroes. Since our assumptions together with (3.7) imply that

$$\bar{S}_p^{(2)} = \bar{S}_p^{(3)} = \cdots = US_p(E/K),$$

we conclude that $\prod_{k=1}^{p-1}R^{(k)} = R^{(1)} = R'_{r,r}$, hence the result. □

In general, Conjecture 3.8 predicts that $\widetilde{\mathrm{Reg}}_{\mathrm{der}}$ is a nonzero element in $E(K)^{\otimes 2}\otimes(J^{\varrho}/J^{\varrho+1})\otimes\mathbf{Q}$, where

$$\begin{aligned}\varrho = e_1 + 2e_2 &= 2\min\{r^+,r^-\} + 2(|r^+-r^-|-1)\\ &= 2(\max\{r^+,r^-\}-1),\end{aligned}$$

which as already noted is strictly larger than $r-1$ when $|r^+-r^-|>1$. Thus, by Lemma 3.10 the following refines Conjecture 3.6.

Conjecture 3.11 (Bertolini–Darmon)**.** *Under the above hypotheses we have*

$$\mathrm{ord}_J\mathscr{L} = 2(\max\{r^+,r^-\}-1),$$

and letting $\bar{\mathscr{L}}$ *be the natural image of* $\mathscr{L}$ *in* $E(K)^{\otimes 2}\otimes(J^{2\rho}/J^{2\rho+1})$, *where* $\rho = \max\{r^+,r^-\}-1$, *we have*

$$\bar{\mathscr{L}} = \left(\frac{1-a_p(E)+p}{p}\right)^2\cdot\widetilde{\mathrm{Reg}}_{\mathrm{der}}\cdot\#\text{Ш}(E/K)\cdot\prod_{\ell\mid N^+}c_\ell^2.$$

It is also possible to formulate a leading term formula for the Heegner distribution θ, refining the "non-exceptional case" of [BD96, Conj. 4.6].

The subspace of universal norms $US_p(E/K)$ is stable under the action of $\mathrm{Gal}(K/\mathbf{Q})$, and therefore is contained in one of the eigenspaces $S_p(E/K)^\pm$.

Lemma 3.12. *Assume Conjecture 3.8. Letting* sign $US_p(E/K)$ *be the sign of the* τ*-eigenspace where* $US_p(E/K)$ *is contained, we have*

$$\mathrm{sign}\,US_p(E/K) = \begin{cases}1 & \text{if } r^+ > r^-,\\ -1 & \text{if } r^- > r^+.\end{cases}$$

In other words, $US_p(E/K)$ *is contained in the larger of the* τ*-eigenspaces* $S_p(E/K)^\pm$.

Proof. Viewing h_p^{MT} as defined on $S_p(E/K)$, Conjecture 3.8 predicts that the restriction

$$h_p^{\mathrm{MT}} : S_p(E/K)^+\times S_p(E/K)^-\to(J/J^2)\otimes\mathbf{Q}$$

is either left non-degenerate or right non-degenerate, depending on which of the τ-eigenspaces $S_p(E/K)^\pm\subset S_p(E/K)$ is larger. Since the universal norms are contained in the null-space of h_p^{MT}, it follows that $US_p(E/K)$ is contained in the τ-eigenspace of larger rank. □

Remark 3.13. The conclusion of Lemma 3.12 is predicted by the "sign conjecture" of Mazur–Rubin (see [MR03, Conj. 4.8]), and the fact that it follows from Conjecture 3.8 was already observed by them.

Let $s := \min\{r^+, r^-\}$ and recall that Conjecture 3.8 predicts that $e_1 := \mathrm{rank}_{\mathbf{Z}_p}\bar{S}_p^{(1)}/\bar{S}_p^{(2)} = 2s$. Order the first $2s$ elements of the basis $x_1, \ldots, x_r$ for $S_p(E/K)$ so that $x_1 =: y_1^+, \ldots, x_s =: y_s^+$ belong to $S_p(E/K)^+$ and $x_{s+1} =: y_1^-, \cdots, x_{2s} =: y_s^-$ belong to $S_p(E/K)^-$.

Lemma 3.14. *We have*

$$R^{(1)} = -(\det(h_p^{\mathrm{MT}}(y_i^+, y_j^-)_{1\leqslant i,j\leqslant s})^2.$$

Proof. This is immediate from the isotropic property of $S_p(E/K)^{\pm}$ under the pairing h_p^{MT} (see Remark 3.5). □

By Lemma 3.14, the first "partial regulator" $R^{(1)}$ is essentially a square. On the other hand, since for even k the pairing $h_p^{(k)}$ is alternating (see part (1) of [BD95, Thm. 2.18]), we have

$$R^{(2)} = \mathrm{pf}(h_p^{(2)}(x_i, x_j)_{e_1+1\leqslant i,j\leqslant e_1+e_2})^2,$$

where $\mathrm{pf}(M)$ denotes the Pfaffian of the matrix M. This motivates the following definition of a square-root of the regulator $\widetilde{\mathrm{Reg}}_{\mathrm{der}}$ in Definition 3.9.

Definition 3.15. Assume Conjecture 3.8 and let $\rho = \max\{r^+, r^-\} - 1$. The *square-root derived enhanced regulator* is the element of $E(K) \otimes (J^\rho/J^{\rho+1}) \otimes \mathbf{Q}$ given by

$$\begin{aligned}\widetilde{\mathrm{Reg}}_{\mathrm{der}}^{1/2} := t_M^{-1} \cdot y \otimes (&\det(h_p^{\mathrm{MT}}(y_i^+, y_j^-)_{1\leqslant i,j\leqslant s}) \\ &\times \mathrm{pf}(h_p^{(2)}(x_i, x_j)_{e_1+1\leqslant i,j\leqslant e_1+e_2}).\end{aligned}$$

Note that this is only well-defined up to sign.

The following refines [BD96, Conj. 4.6] in the cases where $|r^+ - r^-| > 1$, and complements Conjecture 3.2 with a leading coefficient formula. Of course, for its statement we assume that $Ш(E/K)$ is finite.

Conjecture 3.16 (Bertolini–Darmon)**.** *We have*

$$\mathrm{ord}_J\theta = \max\{r^+, r^-\} - 1,$$

and letting $\bar{\theta}$ be the natural image of θ in $(E(K_\infty) \otimes J^\rho/J^{\rho+1})^{\Gamma_\infty}$, where $\rho = \max\{r^+, r^-\} - 1$, the following equality holds:

$$\bar{\theta} = \pm\left(\frac{1 - a_p(E) + p}{p}\right) \cdot \widetilde{\mathrm{Reg}}_{\mathrm{der}}^{1/2} \cdot \sqrt{\#Ш(E/K)} \cdot \prod_{\ell | N^+} c_\ell.$$

Remark 3.17. Note that the sign ambiguity in the last part Conjecture 3.16 is unavoidable, as the term $\widetilde{\mathrm{Reg}}_{\mathrm{der}}^{1/2}$ is only well-defined up to sign.

4. Conjectures for $L_\mathfrak{p}(f)$ and $\mathscr{L}_\mathfrak{p}(f)$

We keep the hypotheses on the triple (E, p, K) from Section 3, and assume in addition that hypothesis (Heeg) from the Introduction.

By Lemma 2.2, the Selmer groups $\mathfrak{Sel}_\mathfrak{p}(K, T)$ and $\mathfrak{Sel}_{\bar{\mathfrak{p}}}(K, T)$ are both contained in $S_p(E/K)$ and they agree with the kernel $\mathrm{Sel}_{\mathrm{str}}(K, T)$ of the restriction map (2.1). Thus we can consider the pairing

$$h_\mathfrak{p} : \mathfrak{Sel}_\mathfrak{p}(K, T) \times \mathfrak{Sel}_{\bar{\mathfrak{p}}}(K, T) \to (J/J^2) \otimes \mathbf{Q}$$

obtained by restricting h_p^{MT}. The filtration in (3.6) induces a filtration

$$\mathfrak{Sel}_{\mathfrak{p}}(K,T) = \bar{\mathfrak{S}}_{\mathfrak{p}}^{(1)} \supset \bar{\mathfrak{S}}_{\mathfrak{p}}^{(2)} \supset \cdots \supset \bar{\mathfrak{S}}_{\mathfrak{p}}^{(p)} \tag{4.1}$$

defined by $\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)} := \bar{S}_p^{(k)} \cap \mathfrak{Sel}_{\mathfrak{p}}(K,T)$, with the filtered pieces equipped with corresponding derived p-adic height pairing

$$h_{\mathfrak{p}}^{(k)} : \bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)} \times \bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)} \to (J^k/J^{k+1}) \otimes \mathbf{Q}$$

obtained from $h_p^{(k)}$ by restriction.

Assume that $\bar{S}_p^{(p)} = US_p(E/K)$ and that $\mathfrak{Sel}_{\mathfrak{p}}(K_\infty, E_{p^\infty})$ is Λ-cotorsion. Then $\varprojlim_n \mathfrak{Sel}_{\mathfrak{p}}(K_n,T)$ vanishes (see e.g. [Cas17, Lem. A.3]), and therefore the subspace of universal norms $U\mathfrak{Sel}_{\mathfrak{p}}(K,T) \subset \mathfrak{Sel}_{\mathfrak{p}}(K,T)$ is trivial. It follows that

$$US_p(E/K) \cap \mathfrak{Sel}_{\mathfrak{p}}(K,T) = 0,$$

and so $\log_{\omega_E}(y) \neq 0$ for any generator $y \in US_p(E/K)$ viewed in $E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p$ by restriction. Thus the first $r-1$ elements in the $\mathbf{Z}_p$-basis $x_1, \ldots, x_r$ for $S_p(E/K)$ chosen for the definition of $\widetilde{\mathrm{Reg}}_{\mathrm{der}}$ yield a basis for $\mathfrak{Sel}_{\mathfrak{p}}(K,T)$ adapted to the filtration (4.1), with the image of $x_{h_k+1}, \ldots, x_{h_k+e_k}$ in

$$\bar{S}_p^{(k)}/\bar{S}_p^{(k+1)} \simeq \bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)}/\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k+1)} \simeq \mathbf{Z}_p^{e_k} \tag{4.2}$$

giving a basis for $\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)}/\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k+1)}$. Then the partial regulators of Definition 3.4 can be rewritten as

$$R^{(k)} = \det(h_{\mathfrak{p}}^{(k)}(x_i,x_j))_{h_k+1 \leqslant i,j \leqslant h_k+e_k} = \mathrm{disc}\big(h_{\mathfrak{p}}^{(k)}|_{\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k)}/\bar{\mathfrak{S}}_{\mathfrak{p}}^{(k+1)}}\big), \tag{4.3}$$

which we shall denote by $\mathcal{R}_{\mathfrak{p}}^{(k)}$ in the following.

We can now define the p-adic regulator appearing in the leading term formula of our p-adic Birch and Swinnerton-Dyer conjecture for $L_{\mathfrak{p}}(f)$. The map $\log_{\omega_E}$ gives rise to a map

$$\mathrm{Log}_{\mathfrak{p}} : (E(K) \otimes \mathbf{Z}_p)^{\otimes 2} \to (E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p)^{\otimes 2} \xrightarrow{\log_{\omega_E}^{\otimes 2}} \mathbf{Z}_p \otimes \mathbf{Z}_p \to \mathbf{Z}_p,$$

where the last arrow is given by multiplication. Choose a basis $x_1, \ldots, x_{r-1}$, x_r as before, with $x_r = y_{\mathfrak{p}}$ given by a generator for $US_p(E/K)$ with

$$p^{-1}\log_{\omega_E}(y_{\mathfrak{p}}) \not\equiv 0 \pmod{p}.$$

Definition 4.1. The *derived regulator* $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ is defined by

$$\mathrm{Reg}_{\mathfrak{p},\mathrm{der}} := \mathrm{Log}_{\mathfrak{p}}(\widetilde{\mathrm{Reg}}_{\mathrm{der}}) = t_M^{-2} \cdot \log_{\omega_E}(y_{\mathfrak{p}})^2 \cdot \prod_{k=1}^{p-1} \mathcal{R}_{\mathfrak{p}}^{(k)}.$$

Note that $\mathrm{Reg}_{\mathfrak{p},\mathrm{der}}$ is an element in $(J^{\varrho}/J^{\varrho+1}) \otimes \mathbf{Q}$, where $\varrho = \sum_{k=1}^{p-1} ke_k$, and Conjecture 3.8 predicts the equality $\varrho = 2(\max\{r^+, r^-\} - 1)$.

Conjecture 4.2. *We have*

$$\mathrm{ord}_J L_{\mathfrak{p}}(f) = 2(\max\{r^+, r^-\} - 1),$$

and letting $\bar{L}_{\mathfrak{p}}(f)$ *be the natural image of* $L_{\mathfrak{p}}(f)$ *in* $J^{2\rho}/J^{2\rho+1}$*, where* $\rho = \max\{r^+, r^-\} - 1$*, the following equality holds:*

$$\bar{L}_{\mathfrak{p}}(f) = \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \cdot \#\text{Ш}(E/K) \cdot \prod_{\ell \mid N} c_\ell^2.$$

Similarly as in Section 3, we can also formulate a version of Conjecture 4.2 for the "square-root" p-adic L-function $\mathscr{L}_{\mathfrak{p}}(f)$. Assume Conjecture 3.8, so that following Definition 3.15 we can define the *derived square-root regulator*

$$\mathrm{Reg}^{1/2}_{\mathfrak{p},\mathrm{der}} := t_M^{-1} \cdot \log_{\omega_E}(y_{\mathfrak{p}}) \cdot (\det(h_{\mathfrak{p}}(y_i^+, y_j^-)_{1\leqslant i,j\leqslant s}) \\ \times \mathrm{pf}(h_p^{(2)}(x_i, x_j)_{e_1+1\leqslant i,j\leqslant e_1+e_2}).$$

As before, note that $\mathrm{Reg}^{1/2}_{\mathfrak{p},\mathrm{der}}$ is only well-defined up to sign, and is contained in $(J^\rho/J^{\rho+1})\otimes\mathbf{Q}$, where $\rho = \max\{r^+, r^-\} - 1$.

Conjecture 4.3. *We have*

$$\mathrm{ord}_J \mathscr{L}_{\mathfrak{p}}(f) = \max\{r^+, r^-\} - 1,$$

and letting $\bar{\mathscr{L}_{\mathfrak{p}}}(f)$ be the natural image of $\mathscr{L}_{\mathfrak{p}}(f)$ in $J^\rho/J^{\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, the following equality holds:

$$\bar{\mathscr{L}_{\mathfrak{p}}}(f) = \pm\left(\frac{1 - a_p(E) + p}{p}\right) \cdot \mathrm{Reg}^{1/2}_{\mathfrak{p},\mathrm{der}} \cdot \sqrt{\#\text{Ш}(E/K)} \cdot \prod_{\ell | N} c_\ell.$$

5. A relation between the conjectures

In this section we explain a relation between Bertolini–Darmon's Conjecture 3.2 and the "rank part" of our Conjecture 4.3.

Recall that $Z_p := E(K_\infty) \otimes \mathbf{Z}_p$, and for each n define $\Psi_n : E(K_n) \otimes \mathbf{Z}_p \to Z_p[\Gamma_n]$ by

$$\Psi_n(P_n) = \sum_{\sigma\in\Gamma_n} P_n^\sigma \otimes \sigma^{-1}.$$

Letting $\pi_{n+1,n} : Z_p[\Gamma_{n+1}] \to Z_p[\Gamma_n]$ be the map induced by the projection $\Gamma_{n+1} \to \Gamma_n$, we see that for all $P_{n+1} \in E(K_{n+1}) \otimes \mathbf{Z}_p$ we have

$$\pi_{n+1,n}(\Psi_{n+1}(P_{n+1})) = \sum_{\tau\in\Gamma_n}\left(\sum_{\substack{\sigma\in\Gamma_{n+1}\\ \sigma|_{K_n}=\tau}} P_{n+1}^\sigma\right) \otimes \tau^{-1} = \Psi_n(\mathrm{Norm}_{K_{n+1}/K_n}(P_{n+1})).$$

It is also readily checked that Ψ_n is Γ_n-equivariant. Thus setting

$$\mathcal{U}(K_\infty/K) := \varprojlim_n E(K_n) \otimes \mathbf{Z}_p,$$

where the limit is with respect to the norm maps $\mathrm{Norm}_{K_{n+1}/K_n} : E(K_{n+1})\otimes\mathbf{Z}_p \to E(K_n)\otimes\mathbf{Z}_p$, we obtain a Λ-linear map

$$\Psi_\infty : \mathcal{U}(E/K_\infty) \to Z_p[[\Gamma_\infty]].$$

The regularized Heegner points $\mathbf{z}_n$ in (3.4) define an element $\mathbf{z}_\infty \in \mathcal{U}(E/K_\infty)$, and by definition the Heegner distribution $\theta = \theta_\infty$ in (3.5) is given by

$$\theta_\infty = \Psi_\infty(\mathbf{z}_\infty). \tag{5.1}$$

By a slight abuse of notation, in the next proposition we let J denote both the augmentation ideal of Λ and of $\Lambda_{\hat{\mathcal{O}}}$.

Proposition 5.1. *Assume that*

1. $p = \mathfrak{p}\bar{\mathfrak{p}}$ *splits in* K.
2. E_p *is irreducible as a* G_K*-module.*
3. $\#\text{Ш}(E/K_n)_{p^\infty} < \infty$ *for all* n.
4. E_p *is ramified for every prime* $\ell | N$.
5. $p \nmid N\varphi(ND_K)$.

Then we have the implication

$$\mathscr{L}_{\mathfrak{p}}(f) \in J^{\rho} \quad \Longrightarrow \quad \theta_{\infty} \in Z_p \otimes_{\mathbf{Z}_p} J^{\rho}.$$

Proof. In light of (5.1) and the Λ-linearity of Ψ_{∞}, it suffices to show the implication

$$\mathscr{L}_{\mathfrak{p}}(f) \in J^{\rho} \quad \Longrightarrow \quad \mathbf{z}_{\infty} \in J^{\rho}\mathcal{U}(E/K_{\infty}). \tag{5.2}$$

Suppose $\mathscr{L}_{\mathfrak{p}}(f) \in J^{\rho}$. By our assumption that $\#Ш(E/K_n)_{p^\infty} < \infty$ for all n, we may identify $\mathcal{U}(E/K_{\infty})$ with

$$\mathrm{Sel}(K_{\infty}, T) := \varprojlim_{n} S_p(E/K_n),$$

where the limit is with respect to the corestriction maps. Let $\gamma \in \Gamma_{\infty}$ be a topological generator. Using that $p \nmid \mathbf{z}_{\infty}$ by [Cor02, Thm. B] (taking $q = p$ in *loc. cit.*) and the Weierstrass preparation theorem, we see that it suffices to solve the equation

$$\mathbf{z}_{\infty} = (\gamma - 1)^{\rho} \cdot \mathbf{z}_{\infty}^{(\rho)}$$

in $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{Sel}(K_{\infty}, T)_{\hat{\mathcal{O}}}$, where $\mathrm{Sel}(K_{\infty}, T)_{\hat{\mathcal{O}}}$ denotes the extension of scalars to $\Lambda_{\hat{\mathcal{O}}}$ of the Λ-module $\mathrm{Sel}(K_{\infty}, T)$. By [CH18, Thm. 5.7] (see also the remarks in [Cas17, Thm. A.1]) and [Cas20, Lem. 6.4], there is an injective $\Lambda_{\hat{\mathcal{O}}}$-linear map

$$\mathfrak{L}_{\mathfrak{p}} : \mathrm{Sel}(K_{\infty}, T)_{\hat{\mathcal{O}}} \to \Lambda_{\hat{\mathcal{O}}}$$

with finite cokernel such that

$$\mathfrak{L}_{\mathfrak{p}}(\mathbf{z}_{\infty}) = -\mathscr{L}_{\mathfrak{p}}(f) \cdot \sigma_{-1,\mathfrak{p}}, \tag{5.3}$$

where $\sigma_{-1,\mathfrak{p}} \in \Gamma_{\infty}$ has order two. Thus $\mathfrak{L}_{\mathfrak{p}}$ becomes an isomorphism upon tensoring with $\mathbf{Q}_p$, and using the above observations the implication (5.2) follows immediately from (5.3). □

6. Main results

6.1. **Statements.** We make the following hypotheses on the triple (E, p, K), where we let $\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E_p)$ be the Galois representation of the p-torsion of E.

Hypotheses 6.1.

1. $p \nmid 2N$ is a prime of good ordinary reduction for E.
2. $\rho_{E,p}$ is ramified at every prime $\ell | N$.
3. Every prime $\ell | N$ splits in K.
4. $\rho_{E,p}$ is surjective.
5. $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K.
6. $a_p(E) \not\equiv 1 \pmod{p}$.

Among these hypotheses, (5) appears to be the most fundamental, as it is needed for the construction of $L_{\mathfrak{p}}(f) \in \Lambda_{\hat{\mathcal{O}}}$ in [CH18]. Under these hypotheses the module $\mathfrak{Sel}_{\mathfrak{p}}(K_{\infty}, E_{p^\infty})$ is known to be Λ-cotorsion, and we let $F_{\mathfrak{p}}(f) \in \Lambda$ be a characteristic power series for its Pontryagin dual $X_{\mathfrak{p}}$.

Theorem 6.2. *Assume Hypotheses 6.1 and that $\#Ш(E/K)_{p^\infty} < \infty$. Then*

$$\mathrm{ord}_J F_{\mathfrak{p}}(f) \geqslant 2(\max\{r^+, r^-\} - 1),$$

where $r^{\pm} = \mathrm{rank}_{\mathbf{Z}} E(K)^{\pm}$, and letting $\bar{F}_{\mathfrak{p}}(f)$ be the natural image of $F_{\mathfrak{p}}(f)$ in $J^{2\rho}/J^{2\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we have

$$\bar{F}_{\mathfrak{p}}(f) = p^{-2} \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \cdot \#Ш(E/K)_{p^\infty}$$

up to a p-adic unit.

Remark 6.3. If $\mathrm{rank}_{\mathbf{Z}} E(K) = 1$ and $\#Ш(E/K)_{p^\infty} < \infty$, then the Selmer group $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})$ is finite (see Lemma 2.2), and hence the image of $F_{\mathfrak{p}}(f)$ under the augmentation map

$$\epsilon : \Lambda_{\hat{\mathcal{O}}} \to \hat{\mathcal{O}}$$

is nonzero. It follows that in this case the inequality in Theorem 6.2 is an equality, and letting $F_{\mathfrak{p}}(f)(0) \in \hat{\mathcal{O}}$ denote the image of $F_{\mathfrak{p}}(f)$ under ϵ, the last part of Theorem 6.2 reduces to the equality, up to a p-adic unit,

$$F_{\mathfrak{p}}(f)(0) = p^{-2} \cdot \#Ш(E/K)_{p^\infty} \cdot \left(\frac{\log_{\omega_E}(y)}{[E(K) : \mathbf{Z}.y]} \right)^2,$$

where $y \in E(K)$ is a point of infinite order with $p^{-1} \log_{\omega_E}(y) \not\equiv 0 \pmod{p}$. Thus Theorem 6.2 gives an extension of the "anticyclotomic control theorem" in [JSW17, Thm. 3.3.1] to arbitrary ranks.

Under Hypotheses 6.1, and assuming that

$$(\star) \qquad \text{either } N \text{ is squarefree, or there are at least two primes } \ell \| N,$$

the Iwasawa–Greenberg main conjecture for $L_{\mathfrak{p}}(f)$ is proved in [BCK20] building on work of Howard [How06] and W. Zhang [Zha14] (see [BCK20, Thm. B]). Thus from Theorem 6.2 we can deduce the following result towards Conjecture 4.2.

Corollary 6.4. *Assume Hypotheses 6.1, that* $\#Ш(E/K)_{p^\infty} < \infty$*, and that* $(\star)$ *holds. Then*

$$\mathrm{ord}_J L_{\mathfrak{p}}(f) \geqslant 2(\max\{r^+, r^-\} - 1),$$

and letting $\bar{L}_{\mathfrak{p}}(f)$ *be the natural image of* $L_{\mathfrak{p}}(f)$ *in* $J^{2\rho}/J^{2\rho+1}$*, where* $\rho = \max\{r^+, r^-\} - 1$*, we have*

$$\bar{L}_{\mathfrak{p}}(f) = p^{-2} \cdot \mathrm{Reg}_{\mathfrak{p},\mathrm{der}} \cdot \#Ш(E/K)_{p^\infty}$$

up to a p-adic unit.

In particular, Corollary 6.4 shows the inclusion $\mathscr{L}_{\mathfrak{p}}(f) \in J^\rho$, where $\rho = \max\{r^+, r^-\} - 1$. In light of Proposition 5.1, this implies the following result, which yields one of the inequalities in the "rank part" of Bertolini–Darmon's Conjecture 3.16 (and therefore also in their Conjecture 3.11).

Corollary 6.5. *Assume Hypotheses 6.1, that* $\#Ш(E/K_n)_{p^\infty} < \infty$ *for all* n*, that* $p \nmid N\varphi(ND_K)$*, and that* $(\star)$ *holds. Then we have the inclusion*

$$\theta \in Z_p \otimes J^\rho,$$

where $\rho = \max\{r^+, r^-\} - 1$.

The remainder of this paper is devoted to the proof of Theorem 6.2.

6.2. **Proof of Theorem 6.2.** Note by (5) and (6) in Hypotheses 6.1 we have $p \nmid \#E(\mathbf{F}_v)$ for every prime v of K above p, where $\mathbf{F}_v = \mathbf{F}_p$ is the residue field of K at v, and by [Maz72, §4] and condition (1) this implies that the local norm maps

$$\mathrm{Norm}_v : E(K_{n,v}) \to E(K_v) \tag{6.1}$$

are surjective for all primes v of K and all finite extensions K_n/K contained in K_∞. (Here we let $E(K_{n,v})$ denote $\oplus_{w|v} E(K_{n,w})$, where the sum is over all places w of K_n lying above v; similar conventions for cohomology will be applied below.)

Define

$$\mathrm{H}^1_{\mathrm{fin}}(K_{n,v}, E_{p^m}) := E(K_{n,v})/p^m E(K_{n,v}),$$

$$\mathrm{H}^1_{\mathrm{sing}}(K_{n,v}, E_{p^m}) := \frac{\mathrm{H}^1(K_{n,v}, E_{p^m})}{\mathrm{H}^1_{\mathrm{fin}}(K_{n,v}, E_{p^m})} \simeq \mathrm{H}^1(K_{n,v}, E)_{p^m},$$

where the last identification follows from Tate's local duality.

Definition 6.6. As in [BD05], we say that a prime $q \nmid pN$ is *m-admissible* for E if

(1) q is inert in K,
(2) $q \not\equiv \pm 1 \pmod{p}$,
(3) p^m divides $q+1-a_q(E)$ or $q+1+a_q(E)$.

We say that a finite set of rational primes Σ is an *m-admissible set* for E if every $q \in \Sigma$ is an m-admissible prime for E and the restriction map

$$\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^m}) \to \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_q, E_{p^m})$$

is injective.

Remark 6.7. As shown in [BD94, Lem. 2.23] by an application of Čebotarev's density theorem, m-admissible sets for E always exist, and it follows from the argument in the proof given there that one can in fact always find m-admissible sets for E with $\#\Sigma = \dim_{\mathbf{F}_p}(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^m})\otimes\mathbf{F}_p)$.

Following the notations in Section 2, assume that the finite set S contains Σ, and let

$$\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m}) := \ker\left\{\mathrm{H}^1(\mathfrak{G}_{K_n,S}, E_{p^m}) \to \bigoplus_{q\in S\smallsetminus\Sigma} \mathrm{H}^1_{\mathrm{sing}}(K_{n,q}, E_{p^m})\right\}$$

be the Selmer group $\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^m})$ relaxed at the places in Σ.

Lemma 6.8. *Let Σ be an m-admissible set for E. Then for every n the modules*

$$\bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^m}), \quad \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{sing}}(K_{n,q}, E_{p^m}), \quad \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m})$$

are free $(\mathbf{Z}/p^m\mathbf{Z})[\Gamma_n]$-modules of rank $\#\Sigma$, and there is an exact sequence

$$\begin{aligned} 0 \to \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^m}) \to \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m}) \to \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{sing}}(K_{n,q}, E_{p^m}) \\ \xrightarrow{\delta} \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^m})^{\vee} \to 0, \end{aligned} \tag{6.2}$$

where δ is the dual to the natural restriction map.

Proof. This is well-known, but we recall the arguments for the convenience of the reader. Let q be an m-admissible prime for E, and denote by $\mathfrak{Q}$ the prime of K lying above q. Then E_{p^m} is unramified as a $G_{K_{\mathfrak{Q}}}$-module, and the action of a Frobenius element at $\mathfrak{Q}$ yields a decomposition

$$E_{p^m} \simeq (\mathbf{Z}/p^m\mathbf{Z}) \bigoplus (\mathbf{Z}/p^m\mathbf{Z})(1)$$

as $\mathrm{Gal}(K^{\mathrm{unr}}_{\mathfrak{Q}}/K_{\mathfrak{Q}})$-modules. From this an easy calculation shows that both $\mathrm{H}^1_{\mathrm{fin}}(K_q, E_{p^m})$ and $\mathrm{H}^1_{\mathrm{sing}}(K_q, E_{p^m})$ are free of rank one over $\mathbf{Z}/p^m\mathbf{Z}$ (see e.g. [BD05, Lem. 2.6]). Since $\mathfrak{Q}$ splits completely in K_n/K, the freeness claims for the first two modules follow.

By Poitou–Tate duality, to establish the exactness of (6.2) it suffices to establish injectivity of the restriction map

$$\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^m}) \to \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^m}) \tag{6.3}$$

(indeed, this implies surjectivity of δ). Arguing by contradiction, suppose that the kernel $\mathcal{K}$ of this restriction map is nonzero. Then we can find a nonzero element $s \in \mathcal{K}$ which is fixed by Γ_n, since Γ_n is a p-group. However, the surjectivity of the local norm maps in (6.1) implies that the restriction map

$$\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^m}) \to \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^m})^{\Gamma_n} \tag{6.4}$$

is an isomorphism (see [BD95, Lem. 1.4]), and so s gives rise a nonzero element in the kernel of $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^m}) \to \oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K, E_{p^m})$, contradicting the m-admissibility of Σ. Thus the exactness of (6.2) follows; the freeness claim for $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m})$ then follow by a counting argument as in [BD94, Thm. 3.2]. □

Recall that $F_{\mathfrak{p}}(f) \in \Lambda$ is a characteristic power series for the Pontryagin dual

$$X_{\mathfrak{p}} := \mathfrak{Sel}_{\mathfrak{p}}(K_\infty, E_{p^\infty})^\vee.$$

Denote by $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}}$ the quotient of $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})$ by its maximal divisible subgroup. The next result reduces the proof of Theorem 6.2 to the calculation of $\#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}}$.

Proposition 6.9. *Assume Hypotheses 6.1 and $\#Ш(E/K)_{p^\infty} < \infty$. Then*

$$\mathrm{ord}_J F_{\mathfrak{p}}(f) \geqslant 2(\max\{r^+, r^-\} - 1), \tag{6.5}$$

and letting $\bar{F}_{\mathfrak{p}}(f)$ be the natural image of $F_{\mathfrak{p}}(f)$ in $J^{2\rho}/J^{2\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we have

$$\bar{F}_{\mathfrak{p}}(f) = \#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}}) \cdot \prod_{k=1}^{p-1} \mathcal{R}^{(k)}_{\mathfrak{p}}$$

up to a p-adic unit.

For the proof of Proposition 6.9, which occupies the rest of this section, we shall adapt the arguments in [BD95, §2.5].

Define

$$\langle\ ,\ \rangle_{K_n/K,m} : \bigoplus_{q\in\Sigma} \mathrm{H}^1(K_{n,q}, E_{p^m}) \times \bigoplus_{q\in\Sigma} \mathrm{H}^1(K_{n,q}, E_{p^m}) \to (\mathbf{Z}/p^m\mathbf{Z})[\Gamma_n] \tag{6.6}$$

by the rule

$$\langle x, y\rangle_n := \sum_{\sigma\in\Gamma_n} \langle x, y^\sigma\rangle_{K_n,m} \cdot \sigma^{-1},$$

where $\langle\ ,\ \rangle_{K_n,m} : \oplus_{q\in\Sigma}\mathrm{H}^1(K_{n,q}, E_{p^m}) \times \oplus_{q\in\Sigma}\mathrm{H}^1(K_{n,q}, E_{p^m}) \to \mathbf{Z}/p^m\mathbf{Z}$ is the natural extension of the local Tate pairing.

Lemma 6.10. *The pairing $\langle\ ,\ \rangle_{K_n/K,m}$ is symmetric, non-degenerate, and Galois-equivariant. Moreover, the images of $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^m})$ and $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m})$ are isotropic for this pairing.*

Proof. All the claims except the last one follow from the corresponding properties of the local Tate pairing, while the isotropy of $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^m})$ follows from the global reciprocity law of class field theory. □

In what follows, we take $m = n$, and set

$$R_n := (\mathbf{Z}/p^n\mathbf{Z})[\Gamma_n], \qquad \langle\ ,\ \rangle_n := \langle\ ,\ \rangle_{K_n/K,n}$$

for ease of notation.

As shown in the proof of Lemma 6.8, the natural map $\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n}) \to \oplus_{q\in\Sigma}\mathrm{H}^1(K_{n,q}, E_{p^n})$ is injective, and we can write

$$\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n}) = \left(\bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})\right) \cap \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n}), \tag{6.7}$$

with the modules in the intersection being each free R_n-modules of rank $\#\Sigma$. By Lemma 6.10, $\langle\ ,\ \rangle_n$ restricts to a non-degenerate pairing

$$[\ ,\ ]_n : \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n}) \times \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{sing}}(K_{n,q}, E_{p^n}) \to R_n,$$

and with a slight abuse of notation we define

$$\langle\ ,\ \rangle_n : \bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n}) \times \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n}) \to R_n$$

by $\langle x, y\rangle_n := [x, \lambda(y)]_n$, where $\lambda : \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n}) \to \oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{sing}}(K_{n,q}, E_{p^n})$ is the natural map.

Lemma 6.11. *Let $\mu_n : \Lambda \to R_n$ be the map induced by the projection $\Gamma_\infty \to \Gamma_n$. Then*

$$\mu_n(F_{\mathfrak{p}}(f)) = \mathrm{Fitt}_{R_n}(\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})^\vee) = \det(\langle x_i, y_j\rangle_n)_{1\leqslant i,j\leqslant \#\Sigma},$$

where $x_1, \dots, x_{\#\Sigma}$ and $y_1, \dots, y_{\#\Sigma}$ are any R_n-bases for $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$ and $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$, respectively.

Proof. Letting $\gamma_n \in \Gamma_n$ be a generator, the first equality follows from the natural isomorphism

$$X_{\mathfrak{p}}/(\gamma_n - 1, p^n)X_{\mathfrak{p}} \simeq \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})^\vee$$

together with standard properties of Fitting ideals, and the second equality follows from the fact that by Lemma 6.8 we have a presentation

$$R_n^{\#\Sigma} \xrightarrow{M} R_n^{\#\Sigma} \to \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})^\vee \to 0$$

with M given by a matrix with entries $m_{i,j} = [x_i, \lambda(y_j)]_n = \langle x_i, y_j\rangle_n$ (see [BD95, Lemmas 2.25 and 2.26] for details). $\square$

Later in the proof we shall apply Lemma 6.11 for suitably chosen bases. Recall the filtration (4.1) of $\mathfrak{Sel}_{\mathfrak{p}}(K, T) = \bar{\mathfrak{S}}^{(1)}_{\mathfrak{p}}$ by the submodules $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p}}$. Letting $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p},n}$ be the image of $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p}}$ in $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n})$ we obtain a filtration

$$\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n}) \supset \bar{\mathfrak{S}}^{(1)}_{\mathfrak{p},n} \supset \bar{\mathfrak{S}}^{(2)}_{\mathfrak{p},n} \supset \cdots \supset \bar{\mathfrak{S}}^{(p)}_{\mathfrak{p},n} \tag{6.8}$$

with $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p},n}/\bar{\mathfrak{S}}^{(k+1)}_{\mathfrak{p},n} \simeq (\mathbf{Z}/p^n\mathbf{Z})^{e_k}$, for $1 \leqslant k \leqslant p-1$, and $\bar{\mathfrak{S}}^{(p)}_{\mathfrak{p},n} \simeq (\mathbf{Z}/p^n\mathbf{Z})^{d_p}$ for $d_p = \mathrm{rank}_{\mathbf{Z}_p}\bar{\mathfrak{S}}^{(p)}_{\mathfrak{p}}$.

From (6.7) (using that (6.4) is an isomorphism), we see that

$$\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n}) = \left(\bigoplus_{q\in\Sigma} \mathrm{H}^1_{\mathrm{fin}}(K_q, E_{p^n})\right) \cap \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n}) \tag{6.9}$$

with the modules in the intersection being free over $\mathbf{Z}/p^n\mathbf{Z}$ of rank $\#\Sigma$.

Let $\bar{x}_1, \dots, \bar{x}_{\#\Sigma}$ and $\bar{y}_1, \dots, \bar{y}_{\#\Sigma}$ be $\mathbf{Z}/p^n\mathbf{Z}$-bases for $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_q, E_{p^n})$ and $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n})$, respectively, adapted to the filtration (6.8), meaning that the first r vectors $\bar{x}_1, \dots, \bar{x}_r$ are a basis for $\bar{\mathfrak{S}}^{(1)}_{\mathfrak{p},n} \subset \mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n})$ with the images of $\bar{x}_{h_k}, \dots \bar{x}_{h_k+e_k}$ in $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p},n}/\bar{\mathfrak{S}}^{(k+1)}_{\mathfrak{p},n}$ giving a basis for $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p},n}/\bar{\mathfrak{S}}^{(k+1)}_{\mathfrak{p},n}$ ($1 \leqslant k \leqslant p-1$) and $\bar{x}_{h_p}, \dots, \bar{x}_{h_p+d_p}$ a basis for $\bar{\mathfrak{S}}^{(p)}_{\mathfrak{p},n}$, and similarly for $\bar{y}_1, \dots, \bar{y}_{\#\Sigma}$. On the other hand, let $x'_1, \dots, x'_{\#\Sigma}$ and $y'_1, \dots, y'_{\#\Sigma}$ be any R_n-bases for $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$ and $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$, respectively, and set

$$\bar{x}'_i := \mathrm{cor}_{K_n/K}(x'_i), \quad \bar{y}'_i := \mathrm{cor}_{K_n/K}(y'_i).$$

Let $\bar{M}$ and $\bar{N}$ be matrices in $\mathrm{GL}_{\#\Sigma}(\mathbf{Z}/p^n\mathbf{Z})$ taking $(\bar{x}'_1, \dots, \bar{x}'_{\#\Sigma})$ into $(\bar{x}_1, \dots, \bar{x}_{\#\Sigma})$ and $(\bar{y}'_1, \dots, \bar{y}'_{\#\Sigma})$ into $(\bar{y}_1, \dots, \bar{y}_{\#\Sigma})$, respectively. Let $M, N \in \mathrm{GL}_{\#\Sigma}(R_n)$ be any lifts of $\bar{M}, \bar{N}$ under the map $\mathrm{GL}_{\#\Sigma}(R_n) \to \mathrm{GL}_{\#\Sigma}(\mathbf{Z}/p^n\mathbf{Z})$ induced by the augmentation

$$\epsilon : R_n \to \mathbf{Z}/p^n\mathbf{Z}.$$

Then the images

$$(x_1, \dots, x_{\#\Sigma}) := (x'_1, \dots, x'_{\#\Sigma})M, \quad (y_1, \dots, y_{\#\Sigma}) := (y'_1, \dots, y'_{\#\Sigma})N$$

are R_n-bases for $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$ and $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$, respectively, with the property that

$$\mathrm{cor}_{K_n/K}(x_i) = \bar{x}_i, \quad \mathrm{cor}_{K_n/K}(y_i) = \bar{y}_i.$$

Lemma 6.12. *For $n \gg 0$, for any choice of R_n-bases $x_1, \dots, x_{\#\Sigma}$ and $y_1, \dots, y_{\#\Sigma}$ as above, we have*

$$\epsilon(\det(\langle x_i, y_j\rangle_n)_{r+1\leqslant i,j\leqslant \#\Sigma}) = u \cdot \#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}})$$

for some unit $u \in (\mathbf{Z}/p^n\mathbf{Z})^\times$.

Proof. Write

$$\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}} \simeq \mathbf{Z}/p^{s_1}\mathbf{Z} \bigoplus \cdots \bigoplus \mathbf{Z}/p^{s_k}\mathbf{Z}$$

Taking n from the outset to be sufficiently large, we may assume that $s_i < n$ for all i. Denote by $\mathfrak{X}^{\Sigma}_{\mathfrak{p}}(K, E)_{p^n}$ the image of $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n})$ under the natural map

$$\mathrm{H}^1(K, E_{p^n}) \to \mathrm{H}^1(K, E)_{p^n}.$$

Since the elements in $\bar{y}_1, \dots, \bar{y}_r$ are in $\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n})$ and $\bar{y}_1, \dots, \bar{y}_{\#\Sigma}$ is a basis for $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n})$, we see that the natural surjection $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n}) \twoheadrightarrow \mathfrak{X}^{\Sigma}_{\mathfrak{p}}(K, E)_{p^n}$ identifies $\mathfrak{X}^{\Sigma}_{\mathfrak{p}}(K, E)_{p^n}$ with the span of $\bar{y}_{r+1}, \dots \bar{y}_{\#\Sigma}$ and we have an exact sequence

$$0 \to \mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n}) \to \mathfrak{X}^{\Sigma}_{\mathfrak{p}}(K, E)_{p^n} \to \lambda(\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n})) \to 0.$$

Thus we find that

$$\lambda(\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K, E_{p^n})) \simeq p^{s_1}(\mathbf{Z}/p^n\mathbf{Z}) \bigoplus \cdots \bigoplus p^{s_k}(\mathbf{Z}/p^n\mathbf{Z}) \bigoplus (\mathbf{Z}/p^n\mathbf{Z})^{\#\Sigma - r - k},$$

and choosing the basis elements $\bar{x}_{r+1}, \dots, \bar{x}_{\#\Sigma}$ and $\bar{y}_{r+1}, \dots, \bar{y}_{\#\Sigma}$ so that $\langle \bar{x}_i, \bar{y}_j\rangle_{K,n} = p^{s_i}\delta_{ij}$, the result follows from the relation

$$\epsilon(\langle x_i, y_j\rangle_n) = -\langle \bar{x}_i, \bar{y}_j\rangle_{K,n},$$

which is immediate from the compatibility of the local Tate pairing with respect to corestriction (see [BD94, Prop. 2.10]). □

Fix a generator $\gamma_n \in \Gamma_n$, and set

$$\mathfrak{S}^{(k)}_{\mathfrak{p},n} := \mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^n}) \cap (\gamma_n - 1)^{k-1}\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n}) \tag{6.10}$$

and $\mathfrak{S}^{(k)}_{\mathfrak{p}} := \varprojlim_n \mathfrak{S}^{(k)}_{\mathfrak{p},n}$, where the limit is with respect to the maps induced by the multiplication-by-p map $E_{p^{n+1}} \to E_{p^n}$. Note that $\mathfrak{S}^{(1)}_{\mathfrak{p}} = \mathfrak{Sel}_{\mathfrak{p}}(K, T)$. By definition, the term $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p}}$ in the filtration (4.1) is the p-adic saturation of $\mathfrak{S}^{(k)}_{\mathfrak{p}}$ in $\mathfrak{S}^{(1)}_{\mathfrak{p}}$. Letting p^A be the maximum of the exponents of the finite groups $\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p}}/\mathfrak{S}^{(k)}_{\mathfrak{p}}$, for $1 \leqslant k \leqslant p$, we then have $p^A\bar{\mathfrak{S}}^{(k)}_{\mathfrak{p},n} \subset \mathfrak{S}^{(k)}_{\mathfrak{p},n}$ for all n. Using (6.10), let $\widetilde{x}_{h_k+1}, \dots, \widetilde{x}_{h_k+e_k}; \widetilde{y}_{h_k+1}, \dots, \widetilde{y}_{h_k+e_k} \in \mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})$ be such that

$$(\gamma_n - 1)^{k-1}\widetilde{x}_{h_k+i} = p^A\bar{x}_{h_k+i}, \quad (\gamma_n - 1)^{k-1}\widetilde{y}_{h_k+i} = p^A\bar{y}_{h_k+i}. \tag{6.11}$$

For $0 \leqslant k \leqslant p$, let $D^{(k)}_n \in R_n$ be the derivative operator

$$D^{(k)}_n := (-1)^k\gamma_n^{-k}\sum_{i=0}^{p^n-1}\binom{i}{k}\gamma_n^i$$

introduced in [Dar92, §3.1]. In particular, $D^{(0)}_n = \sum_{\gamma\in\Gamma_n}\gamma$ is the norm map.

Claim 6.13. For every $1 \leqslant k \leqslant p$, there exist elements $x'_{h_k+1}, \dots, x'_{h_k+e_k} \in \oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$ and $y'_{h_k+1}, \dots, y'_{h_k+e_k} \in \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$ satisfying

$$D^{(k-1)}_n(x'_{h_k+i}) = \widetilde{x}_{h_k+i}, \quad D^{(k-1)}_n(y'_{h_k+i}) = \widetilde{y}_{h_k+i}. \tag{6.12}$$

Indeed, note that by (6.9) and the definition of n-admissible set we may view the $\bar{x}_{h_k+i}$ as elements in $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_q, E_{p^n}) = (\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n}))^{\Gamma_n}$ and by injectivity of the restriction map (6.3), the equality in (6.11) may be seen as taking place in $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$. Hence by [BD95, Cor. 2.4] applied to $\oplus_{q\in\Sigma}\mathrm{H}^1_{\mathrm{fin}}(K_{n,q}, E_{p^n})$ (which is free over R_n by Lemma 6.8), the existence of elements x'_{h_k+i} satisfying (6.12) follows. The existence of elements y'_{h_k+i} satisfying (6.12) is seen similarly, viewing (6.11) as taking place in $\mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$ (which is also free over R_n by Lemma 6.8).

Setting $x'_i := p^A x_i$ and $y'_i := p^A y_i$ for $r+1 \leqslant i \leqslant \#\Sigma$, for x_i, y_i as in Lemma 6.12, an argument similar to the one preceding that lemma shows that, after possibly transforming the bases $x'_1, \ldots, x'_{\#\Sigma}$ and $y'_1, \ldots, y'_{\#\Sigma}$ by matrices in the kernel of the map $\mathrm{GL}_{\#\Sigma}(R_n) \to \mathrm{GL}_{\#\Sigma}(\mathbf{Z}/p^n\mathbf{Z})$ induced by the augmentation, we may assume

$$\operatorname{cor}_{K_n/K}(x'_i) = p^A \bar{x}_i, \quad \operatorname{cor}_{K_n/K}(y'_i) = p^A \bar{y}_i \tag{6.13}$$

for all i.

We can now conclude the proof of Proposition 6.9.

Proof of Proposition 6.9. Let $\sigma_p := e_1 + 2e_2 + \cdots + (p-1)e_{p-1} + d_p$. (Recall that e_k is given by (4.2), and $d_p := \operatorname{rank}_{\mathbf{Z}_p}\mathfrak{S}^{(p)}_{\mathfrak{p}}$.) To prove the inequality (6.5), it is enough to show the inclusion

$$\operatorname{Fitt}_{R_n}(\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})^{\vee}) \in J_n^{\sigma_p} \tag{6.14}$$

for all $n \geqslant 1$, where J_n is the augmentation ideal of R_n. Indeed, this implies that $\operatorname{ord}_J F_{\mathfrak{p}}(f) \geqslant \sigma_p$, and by Remark 3.5 we have

$$\begin{aligned}\sigma_p = \sum_{k=1}^{p} \operatorname{rank}_{\mathbf{Z}_p}\mathfrak{S}^{(k)}_{\mathfrak{p}} &\geqslant (r-1) + (|r^+ - r^-| - 1)\\ &= 2(\max\{r^+, r^-\} - 1).\end{aligned}$$

As noted earlier, we may choose the n-admissible sets Σ_n having cardinality $\#\Sigma_n$ independent of n; from now on we assume now that the preceding constructions of bases have been carried out with such Σ_n, which we shall just denote by Σ.

The Galois-equivariance property of $\langle\ ,\ \rangle_n$ together with (6.12) imply that for all $1 \leqslant i \leqslant e_k$ and $y \in \mathfrak{Sel}^{\Sigma}_{\mathfrak{p}}(K_n, E_{p^n})$ we have

$$D_n^{(k-1)}(\langle x'_{h_k+i}, y\rangle_n) = \langle D_n^{(k-1)}(x'_{h_k+i}), y\rangle_n = 0,$$

using Lemma 6.10 for the second equality. By [BD95, Cor. 2.5], it follows that $\langle x'_{h_k+i}, y\rangle_n \in J_n^k$. Since Lemma 6.11 shows that

$$(\det(\langle x'_i, y'_j\rangle_n)_{1\leqslant i,j\leqslant\#\Sigma}) = p^{2A\#\Sigma} \cdot \operatorname{Fitt}_{R_n}(\mathfrak{Sel}_{\mathfrak{p}}(K_n, E_{p^n})^{\vee}), \tag{6.15}$$

the inclusion (6.14) follows.

Finally, to prove the expression in Proposition 6.9 for the image of $F_{\mathfrak{p}}(f)$ in $J^{2\rho}/J^{2\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we may assume that $\sigma_p = 2\rho$ (otherwise the result is trivial, both terms in the formula being equal to 0). Then by Lemma 6.10 and Lemma 6.12 for $n \gg 0$ we get the equality

$$\begin{aligned}\det(\langle x'_i, y'_j\rangle_n)_{1\leqslant i,j\leqslant\#\Sigma} &= \det(\langle x'_i, y'_j\rangle_n)_{1\leqslant i,j\leqslant r}\\ &\qquad \times u_n \cdot p^{2(\#\Sigma-r)}\#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}})\end{aligned} \tag{6.16}$$

in $J_n^{2\rho}/J_n^{2\rho+1}$ for some unit $u_n \in (\mathbf{Z}/p^n\mathbf{Z})^{\times}$. In view of (6.11) and (6.12), by the definition of the derived pairing $h^{(k)}_{\mathfrak{p},n}$ (see [BD95, p. 1526]) we have

$$h^{(k)}_{\mathfrak{p},n}(p^A\bar{x}_i, p^A\bar{y}_j) = \langle x'_i, y'_j\rangle_n \in J_n^k/J_n^{k+1}$$

for all $h_k+1 \leqslant i,j \leqslant h_k+e_k$, and hence from the definition of $\mathcal{R}_{\mathfrak{p}}^{(k)}$ we get

$$p^{2Ar}\cdot\prod_{k=1}^{p-1}\mu_n(\mathcal{R}_{\mathfrak{p}}^{(k)})=\prod_{k=1}^{p-1}\det(\langle x_i',y_j'\rangle_n)_{h_k+1\leqslant i,j\leqslant h_k+e_k} \tag{6.17}$$

Since $\mu_n(F_{\mathfrak{p}}(f)) = \mathrm{Fitt}_{R_n}(\mathfrak{Sel}_{\mathfrak{p}}(K_n,E_{p^n})^\vee)$ (see Lemma 6.11), combining (6.15), (6.16), (6.17), and letting $n\to\infty$, the result follows. $\square$

6.3. **Calculation of $\#(\mathfrak{Sel}_{\mathfrak{p}}(K,E_{p^\infty})_{/\mathrm{div}})$.** The calculation in this section draws from the methods of [Agb07].

Define the $\bar{\mathfrak{p}}$-relaxed Tate–Shafarevich group by

$$Ш^{\{\bar{\mathfrak{p}}\}}(E/K) := \ker\Big\{\mathrm{H}^1(K,E)\to\prod_{w\neq\bar{\mathfrak{p}}}\mathrm{H}^1(K_w,E)\Big\},$$

and let $Ш^{\{\bar{\mathfrak{p}}\}}(E/K)_{p^\infty}$ denote its p-primary component. Recall that by hypothesis (Heeg) the root number of E/K is -1, so by the p-parity conjecture if $Ш(E/K)_{p^\infty}$ is finite then $E(K)$ has positive rank.

Lemma 6.14. *Assume that $\#Ш(E/K)_{p^\infty}<\infty$. Then $Ш^{\{\bar{\mathfrak{p}}\}}(E/K)_{p^\infty}$ is also finite, and*

$$\#Ш^{\{\bar{\mathfrak{p}}\}}(E/K)_{p^\infty} = \#Ш(E/K)_{p^\infty}\cdot\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}),$$

where $\mathrm{loc}_{\mathfrak{p}}: S_p(E/K)\to E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p$ is the restriction map.

Proof. Define B_∞ by the exactness of the sequence

$$0\to Ш(E/K)_{p^\infty}\to\mathrm{H}^1(K,E)_{p^\infty}\to\prod_w\mathrm{H}^1(K_w,E)_{p^\infty}\to B_\infty\to 0.$$

Then we have an induced exact sequence

$$0\to Ш(E/K)_{p^\infty}\to Ш^{\{\bar{\mathfrak{p}}\}}(E/K)_{p^\infty}\to\mathrm{H}^1(K_{\bar{\mathfrak{p}}},E)_{p^\infty}\xrightarrow{h_\infty}B_\infty. \tag{6.18}$$

By surjectivity of the top right arrow in the commutative

$$\begin{tikzcd}
E(K)\otimes\mathbf{Q}_p/\mathbf{Z}_p \arrow[r, hook] \arrow[d] & \mathrm{H}^1(K,E_{p^\infty}) \arrow[r, two heads] \arrow[d] \arrow[dr, "\partial"] & \mathrm{H}^1(K,E)_{p^\infty} \arrow[d] \\
\prod_w E(K_w)\otimes\mathbf{Q}_p/\mathbf{Z}_p \arrow[r, hook] & \prod_w\mathrm{H}^1(K_w,E_{p^\infty}) \arrow[r, two heads] & \prod_w\mathrm{H}^1(K_w,E)_{p^\infty},
\end{tikzcd}$$

we see that $\ker(h_\infty)$ is the same as the kernel of the map δ in the Cassels dual exact sequence

$$0\to\mathrm{Sel}_{p^\infty}(E/K)\to\mathrm{Sel}_{p^\infty}^{\{\bar{\mathfrak{p}}\}}(E/K)\to\mathrm{H}^1(K_{\bar{\mathfrak{p}}},E)_{p^\infty}\xrightarrow{\delta}S_p(E/K)^\vee,$$

where

$$\mathrm{Sel}_{p^\infty}^{\{\bar{\mathfrak{p}}\}}(E/K) := \ker\Big\{\mathrm{H}^1(K,E_{p^\infty})\to\prod_{w\nmid\bar{\mathfrak{p}}}\mathrm{H}^1(K_w,E)_{p^\infty}\Big\}.$$

Since $\mathrm{Hom}_{\mathrm{cts}}(E_{p^\infty},\mu_{p^\infty})\simeq T^\tau$ as G_K-modules, it follows that the kernel of h_∞ is dual to the cokernel of the map $\mathrm{loc}_{\mathfrak{p}}: S_p(E/K)\to E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p$, which is finite under our hypotheses. The result follows. $\square$

The following result is an analogue of [JSW17, Prop. 3.2.1] in arbitrary rank.

Proposition 6.15. *Suppose $\#Ш(E/K)_{p^\infty}<\infty$ and $a_p(E)\not\equiv 1 \pmod p$. Then*

$$\#(\mathfrak{Sel}_{\mathfrak{p}}(K,E_{p^\infty})_{/\mathrm{div}}) = \#Ш(E/K)_{p^\infty}\cdot(\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}))^2,$$

where $\mathrm{loc}_{\mathfrak{p}}: S_p(E/K)\to E(K_{\mathfrak{p}})\otimes\mathbf{Z}_p$ is the restriction map.

Proof. Let $y_1, \ldots, y_{r-1}$ be a $\mathbf{Z}_p$-basis for the kernel

$$E_{1,\mathfrak{p}}(K) := \ker\Big\{E(K) \otimes \mathbf{Z}_p \xrightarrow{\mathrm{loc}_\mathfrak{p}} E(K_\mathfrak{p}) \otimes \mathbf{Z}_p\Big\},$$

and extend it to a $\mathbf{Z}_p$-basis $y_1, \ldots, y_{r-1}, y_\mathfrak{p}$ for $E(K) \otimes \mathbf{Z}_p$, so

$$E(K) \otimes \mathbf{Z}_p = E_{1,\mathfrak{p}}(K) \bigoplus \mathbf{Z}_p.y_\mathfrak{p}. \tag{6.19}$$

Then the finite module U defined by the exactness of the sequence

$$0 \to \mathbf{Z}_p.y_\mathfrak{p} \to E(K_\mathfrak{p}) \otimes \mathbf{Z}_p \to U \to 0 \tag{6.20}$$

satisfies

$$\#U = [E(K_\mathfrak{p}) \otimes \mathbf{Z}_p \colon \mathrm{loc}_\mathfrak{p}(E(K) \otimes \mathbf{Z}_p)] = \#\mathrm{coker}(\mathrm{loc}_\mathfrak{p}), \tag{6.21}$$

using the finiteness assumption on $\text{Ш}(E/K)$ for the second equality. The hypothesis that $a_p(E) \not\equiv 1 \pmod p$ implies that $E(K_\mathfrak{p})$ has no p-torsion, and so $E(K_\mathfrak{p}) \otimes \mathbf{Z}_p$ is a free $\mathbf{Z}_p$-module of rank one. Tensoring (6.21) with $\mathbf{Q}_p/\mathbf{Z}_p$ therefore yields

$$0 \to V \to (\mathbf{Q}_p/\mathbf{Z}_p).y_\mathfrak{p} \to E(K_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to 0$$

with $\#V = \#U$, and from (6.19) we deduce that

$$\ker\Big\{E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\lambda_\mathfrak{p}} E(K_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p\Big\} = (E_{1,\mathfrak{p}}(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p) \bigoplus V. \tag{6.22}$$

Now consider the p-relaxed Tate–Shafarevich group defined by

$$\text{Ш}^{\{p\}}(E/K) := \ker\Big\{\mathrm{H}^1(K, E) \to \prod_{w \nmid p} \mathrm{H}^1(K_w, E)\Big\}.$$

It is immediately seen that its p-primary part fits into the exact sequence

$$0 \to E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}^{\{p\}}_{p^\infty}(E/K) \to \text{Ш}^{\{p\}}(E/K)_{p^\infty} \to 0,$$

where $\mathrm{Sel}^{\{p\}}_{p^\infty}(E/K) := \ker\{\mathrm{H}^1(K, E_{p^\infty}) \to \prod_{w \nmid p} \mathrm{H}^1(K_w, E)_{p^\infty}\}$. Consider also the commutative diagram

$$\begin{tikzcd}
E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r, hook] \arrow[d, "\lambda_\mathfrak{p}"] & \mathrm{Sel}^{\{p\}}_{p^\infty}(E/K) \arrow[r, two heads] \arrow[d] & \text{Ш}^{\{p\}}(E/K)_{p^\infty} \arrow[d] \\
E(K_\mathfrak{p}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r, hook] & \mathrm{H}^1(K_\mathfrak{p}, E_{p^\infty}) \arrow[r, two heads] & \mathrm{H}^1(K_\mathfrak{p}, E)_{p^\infty}
\end{tikzcd}$$

in which the unlabeled vertical maps are given by restriction. Since the map $\lambda_\mathfrak{p}$ is surjective by our assumptions, the Snake Lemma applied to this diagram yields the exact sequence

$$0 \to \ker(\lambda_\mathfrak{p}) \to \mathfrak{Sel}_\mathfrak{p}(K, E_{p^\infty}) \to \text{Ш}^{\{\overline{\mathfrak{p}}\}}(E/K)_{p^\infty} \to 0, \tag{6.23}$$

and hence from (6.23), (6.22), and (6.21) we conclude that

$$\begin{aligned}
\#(\mathfrak{Sel}_\mathfrak{p}(K, E_{p^\infty})_{/\mathrm{div}}) &= \#\text{Ш}^{\{\overline{\mathfrak{p}}\}}(E/K)_{p^\infty} \cdot \#V \\
&= \#\text{Ш}^{\{\overline{\mathfrak{p}}\}}(E/K)_{p^\infty} \cdot \#\mathrm{coker}(\mathrm{loc}_\mathfrak{p}) \\
&= \#\text{Ш}(E/K)_{p^\infty} \cdot \#(\mathrm{coker}(\mathrm{loc}_\mathfrak{p}))^2,
\end{aligned}$$

using Lemma 6.14 for the last equality. □

As in the proof of Proposition 6.15, let $y_1, \ldots, y_{r-1}$ be a $\mathbf{Z}_p$-basis for the kernel $\mathrm{Sel}_{\mathrm{str}}(K,T)$ of

$$\mathrm{loc}_{\mathfrak{p}} : E(K) \otimes \mathbf{Z}_p \to E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p,$$

and extend it to a $\mathbf{Z}_p$-basis $y_1, \ldots, y_{r-1}, y_{\mathfrak{p}}$ for $E(K) \otimes \mathbf{Z}_p$. We denote by $\log_{\omega_E} : E(K) \otimes \mathbf{Z}_p \to \mathbf{Z}_p$ the composition of $\mathrm{loc}_{\mathfrak{p}}$ with the formal group logarithm associated with a Néron differential $\omega_E \in \Omega^1(E/\mathbf{Z}_{(p)})$.

Proposition 6.16. *Suppose* $\#Ш(E/K)_{p^\infty} < \infty$ *and* $a_p(E) \not\equiv 1 \pmod{p}$. *Then*

$$\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}) = p^{-1}\#(\mathbf{Z}_p/\log_{\omega_E}(y_{\mathfrak{p}})).$$

Proof. Let $E_1(K_{\mathfrak{p}})$ be the kernel of reduction modulo $\mathfrak{p}$, so there is an exact sequence

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

Set

$$Y := \mathbf{Z}_p.y_{\mathfrak{p}}, \quad Y_{\mathfrak{p},1} := \mathrm{loc}_{\mathfrak{p}}(Y) \cap (E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p), \quad Z := Y/Y_{\mathfrak{p},1},$$

and note that Z is finite. We consider the commutative diagram

$$\begin{tikzcd}
Y_{\mathfrak{p},1} \arrow[r, hook] \arrow[d, "\lambda_{\mathfrak{p},1}"] & Y \arrow[r, two heads] \arrow[d, "\mathrm{loc}_{\mathfrak{p}}|_Y"] & Z \arrow[d] \\
E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \arrow[r, hook] & E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \arrow[r, two heads] & E(\mathbf{F}_p) \otimes \mathbf{Z}_p.
\end{tikzcd}$$

Since the middle vertical is injective by our choice of $y_{\mathfrak{p}}$ and $E(\mathbf{F}_p) \otimes \mathbf{Z}_p \simeq \mathbf{Z}_p/(1 - a_p(E) + p)$ is trivial by our assumption on $a_p(E)$, the Snake Lemma applied to this diagram yields

$$\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}|_Y) \cdot \#Z = \#\mathrm{coker}(\lambda_{\mathfrak{p},1}). \tag{6.24}$$

Noting that $\#Z \cdot y_{\mathfrak{p}}$ is a generator of $Y_{\mathfrak{p},1}$ and the formal group logarithm induces an isomorphism $\log_{\omega_E} : E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \simeq p\mathbf{Z}_p$ we find

$$\#\mathrm{coker}(\lambda_{\mathfrak{p},1}) = \frac{\#\mathbf{Z}_p/\log_{\omega_E}(\#Z \cdot y_{\mathfrak{p}})}{\#\mathbf{Z}_p/\log_{\omega_E}(E_1(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p)} = \#Z \cdot p^{-1}\#(\mathbf{Z}_p/\mathrm{loc}_{\omega_E}(y_{\mathfrak{p}})). \tag{6.25}$$

Since clearly $\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}|_Y) = [E(K_{\mathfrak{p}}) \otimes \mathbf{Z}_p \colon \mathrm{loc}_{\mathfrak{p}}(S_p(E/K))]$ by the definition of $y_{\mathfrak{p}}$, combining (6.24) and (6.25) the result follows. ☐

We can now conclude the proof of Theorem 6.2.

Proof of Theorem 6.2. By Proposition 6.9 we have $\mathrm{ord}_J F_{\mathfrak{p}}(f) \geqslant 2\rho$ with $\rho = \max\{r^+, r^-\} - 1$, and the equality

$$\bar{F}_{\mathfrak{p}}(f) = \#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}}) \cdot \prod_{k=1}^{p-1} \mathcal{R}_{\mathfrak{p}}^{(k)} \tag{6.26}$$

in $(J^{2\rho}/J^{2\rho+1}) \otimes \mathbf{Q}$ up to a p-adic unit.

On the other hand, combining Propositions 6.15 and 6.16 we obtain

$$\begin{aligned} \#(\mathfrak{Sel}_{\mathfrak{p}}(K, E_{p^\infty})_{/\mathrm{div}}) &= \#Ш(E/K)_{p^\infty} \cdot (\#\mathrm{coker}(\mathrm{loc}_{\mathfrak{p}}))^2 \\ &= \#Ш(E/K)_{p^\infty} \cdot p^{-2} \cdot \log_{\omega_E}(y_{\mathfrak{p}})^2, \end{aligned} \tag{6.27}$$

with the last equality holding up to a p-adic unit. The proof of Theorem 6.2 now follows from (6.26) and (6.27). ☐

References

[Agb07] A. Agboola, *On Rubin's variant of the p-adic Birch and Swinnerton-Dyer conjecture*, Compos. Math. **143** (2007), no. 6, 1374–1398.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BCK20] Ashay Burungale, Francesc Castella, and Chan-Ho Kim, *A proof of Perrin-Riou's Heegner point main conjecture*, Algebra Number Theory, to appear (2020).

[BD94] Massimo Bertolini and Henri Darmon, *Derived heights and generalized Mazur-Tate regulators*, Duke Math. J. **76** (1994), no. 1, 75–111.

[BD95] ———, *Derived p-adic heights*, Amer. J. Math. **117** (1995), no. 6, 1517–1554.

[BD96] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456.

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

[BDP12] M. Bertolini, H. Darmon, and K. Prasanna, *p-adic Rankin L-series and rational points on CM elliptic curves*, Pacific J. of Math. (2012), 261–303.

[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.

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

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

[Cas20] ———, *On the p-adic variation of Heegner points*, J. Inst. Math. Jussieu, to appear (2020).

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

[Cor02] Christophe Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523.

[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.

[Dar92] Henri Darmon, *A refined conjecture of Mazur-Tate type for Heegner points*, Invent. Math. **110** (1992), no. 1, 123–146.

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

[Gro91] Benedict H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[How04] Benjamin Howard, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45.

[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.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[Maz84] B. Mazur, *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 185–211.

[MR03] Barry Mazur and Karl Rubin, *Studying the growth of Mordell-Weil*, no. Extra Vol., 2003, Kazuya Kato's fiftieth birthday, pp. 585–607.

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237.

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

[Ski20] Christopher Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, Ann. of Math. (2) **191** (2020), no. 2, 329–354. MR 4076627

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

Department of Mathematics, University of California Santa Barbara, CA 93106, USA
Email address: agboola@ucsb.edu

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