ON ANTICYCLOTOMIC VARIANTS OF THE \(p\)-ADIC BIRCH–SWINNERTON-DYER CONJECTURE

ADEBISI AGBOOLA AND FRANCESC CASTELLA

Abstract. We formulate analogues of the Birch–Swinnerton-Dyer for the \(p\)-adic \(L\)-functions of Bertolini–Darmon–Prasanna attached to elliptic curves \(E/\mathbb{Q}\) 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 (modulo the expected “maximal non-degeneracy” of the anticyclotomic \(p\)-adic height pairing).

Contents

1. Introduction 1
2. The conjectures 4
3. Main result 10
References 19

1. Introduction

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

Assume that \(K\) satisfies the Heegner hypothesis relative to \(N\), i.e., that every prime factor of \(N\) splits in \(K\). This condition guarantees that the root number of \(E/K\) is \(-1\). Assume in addition that \(p = \mathfrak{p} \mathfrak{P}\) splits in \(K\), and let \(\hat{\mathcal{O}}\) be the completion of the ring of integers of the maximal unramified extension of \(\mathbb{Q}_p\). 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 interpolating the central critical values for the twists of \(f/K\) by certain infinite order characters of \(\Gamma_\infty\).

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 \(L_p(f)\) for \(\chi(L_p(f))\). The trivial character \(1\) of \(\Gamma_\infty\) lies outside the range of \(p\)-adic interpolation for \(L_p(f)\), and one of the main results of [BDP13] is a formula of \(p\)-adic Gross–Zagier type for this value:

\[
L_p(f)(1) = \left(\frac{1 - a_p(E) + p}{p}\right)^2 \log_{\omega_f}(z_K)^2
\]
(see [BDP13 Thm. 5.13], as specialized in [BDP12 Thm. 3.12] to the case where \( f \) has weight \( k = 2 \)). Here \( z_K \in E(K) \) is a Heegner point arising from a suitable modular parameterization \( \varphi : X_0(N) \to E \),

\[
\log_{\omega_f} : E(K_p) \otimes \mathbb{Z}_p \to \mathbb{Z}_p
\]

is the formal group logarithm associated with the differential \( \omega_f \in \Omega^1_{E/Q} \) defined by \( \varphi^*(\omega_f) = f(q)dq/q \), and \( \omega_p(E) := p + 1 - #E(F_p) \) as usual. If the \( p \)-torsion \( E_p \) is irreducible as \( G_Q \)-module, one can choose \( \varphi \) so that \( \omega_f \) generates \( \Omega^1_{E/Z_p} \), and in the following we assume that \( \varphi \) has been so chosen.

Formula [BDP] has been a key ingredient in recent progress on the Birch–Swinnerton-Dyer conjecture for elliptic curves \( E/Q \) of rank at most one. Most notably, by choosing \( K \) so that \( \text{rank}_{\mathbb{Z}}E(K) = 1 \), it was used by Skinner [Ski14] to prove a converse to the celebrated theorem of Gross–Zagier and Kolyvagin, and by choosing \( K \) so that \( \text{ord}_{s=1} L(E/K,s) = 1 \), it was used by Jetchev–Skinner–Wan [JSW17] to prove under relatively mild hypotheses the \( p \)-part of the Birch–Swinnerton-Dyer formula for semistable elliptic curves \( E/Q \) with \( \text{ord}_{s=1} L(E,s) = 1 \).

For elliptic curves \( E/Q \) with \( \text{rank}_{\mathbb{Z}}E(Q) \geq 2 \) and finite \( p \)-primary component of the Tate–Shafarevich group \( III(E/K) \) (so that the Heegner point \( z_K \) is torsion by [Ski14] and [GZ86]), formula [BDP] shows that \( L_p(f)(1) = 0 \), or equivalent, that \( L_p(f) \in J \), where

\[
J := \ker(\epsilon : \Lambda_{\hat{O}} \to \hat{O})
\]

is the augmentation ideal of \( \Lambda_{\hat{O}} \). The Birch–Swinnerton-Dyer type conjectures formulated in this paper predict the order of vanishing of \( L_p(f) \) at \( 1 \) (defined as the largest power of \( J \) where \( L_p(f) \) lives) in terms of the rank \( r \) of \( E(K) \), and a formula for the leading coefficient of \( L_p(f) \) at \( 1 \) in terms of arithmetic invariants of \( E \). For the sake of illustration, in the remainder of this Introduction we concentrate on a weaker form of these conjectures, referring the reader to Sections 3 for their actual form.

Let \( T \) be the \( p \)-adic Tate module of \( E \), and let \( S_p(E/K) \subset H^1(K,T) \) be the pro-\( p \) Selmer group of \( E \). We shall assume that \( \#III(E/K)_{p^\infty} < \infty \), so in particular \( S_p(E/K) \cong E(K) \otimes Z_p \).

By the work of Mazur–Tate [MT83], there is a canonical symmetric \( p \)-adic height pairing

\[
h_p^{\text{HT}} : S_p(E/K) \times S_p(E/K) \to (J/J^2) \otimes Q,
\]

The finiteness assumption on \( III(E/K)_{p^\infty} \) together with the \( p \)-parity conjecture [Nek01] also implies that the strict Selmer group defined by

\[
\text{Sel}_{\text{st}}(K,T) := \ker(S_p(E/K) \to E(K) \otimes Z_p)
\]

has \( Z_p \)-rank equal to \( r - 1 \), where \( r = \text{rank}_{\mathbb{Z}}E(K) \). Assume that \( S_p(E/K) \) is torsion-free (this holds if \( E_p \) is irreducible as \( G_K \)-module, for example), let \( P_1, \ldots, P_r \) be an integral basis for \( E(K) \otimes Q \) and let \( A \) be an endomorphism of \( E(K) \otimes Z_p \) sending \( P_1, \ldots, P_r \) to a \( Z_p \)-basis \( x_1, \ldots, x_r, y_p \) for \( S_p(E/K) \) with \( x_1, \ldots, x_r, y_p \) generating \( \text{Sel}_{\text{st}}(K,T) \). Set \( t = \text{det}(A) \).

The following is a special case of our Conjecture 2.21.

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

(i) \( L_p(f) \in J^{r-1} \).

(ii) Letting \( L_p(f) \) be the natural image of \( L_p(f) \) in \( J^{r-1}/J^r \), we have

\[
L_p(f) = \left( 1 - \frac{\omega_p(E)}{p} \right)^2 \cdot \log_{\omega_f}(y_p)^2 \cdot \text{Reg}_p \cdot t^{-2} \cdot \#III(E/K)_{p^\infty} \cdot \prod_{i=1}^{r} c_i^2,
\]

where \( \text{Reg}_p = \det(h^{\text{HT}}_p(x_i, x_j))_{1 \leq i, j \leq r - 1} \) is the regulator of \( h^{\text{HT}}_p \) restricted to \( \text{Sel}_{\text{st}}(K,T) \), and \( c_i \) is the \( p \)-part of the Tamagawa number of \( E/Q_i \).

\(^1\)In fact, in terms of the ranks of the eigenspaces of \( E(K) \) for the action of complex conjugation.
Remark 1.2. With the assumptions of Conjecture 1.1 when \( r = 1 \) we have \( \text{Sel}_{\text{str}}(K, T) = \{0\} \), \( \text{Reg}_p = 1 \), and \( t = [E(K) \otimes \mathbb{Z}_p : \mathbb{Z}_p \cdot y_K] \), where \( y_K \) is a generator of \( E(K) \otimes \mathbb{Q} \). Thus in this special case Conjecture 1.1 predicts that \( L_p(f)(1) \neq 0 \), and by formula (BDP) the predicted expression for \( L_p(f)(1) \) is equivalent to the equality
\[
[E(K) \otimes \mathbb{Z}_p : \mathbb{Z}_p \cdot y_K]^2 = \#\text{III}(E/K)_p \cdot \prod_{\ell \mid N} c_\ell^2,
\]
which is also predicted by the classical Birch and Swinnerton-Dyer conjecture when combined with the Gross–Zagier formula (see [Gro91, Conj. 1.2]).

The Iwasawa–Greenberg main conjecture [Gre94] predicts that \( L_p(f) \) is a generator of the characteristic ideal of a certain \( \Lambda \)-torsion Selmer group \( X_p \). Letting \( F_p(f) \in \Lambda \) be a generator of this characteristic ideal, in this paper we prove the following result towards Conjecture 1.1, which can be viewed simultaneously as a non-CM analogue of the result in [Agb07, Thm. B] towards Rubin’s variant of the \( p \)-adic Birch–Swinnerton-Dyer conjecture, and an extension of the anticyclotomic control theorem of [JSW17, §3.3] to arbitrary ranks.

**Theorem 1.3** ([cf. Theorem 3.3]). Assume that \( \#\text{III}(E/K)_{p^\infty} < \infty \), and that:

- \( E_p : \text{Gal}(\mathbb{Q}) \to \text{Aut}_{\text{p}}(E_p) \) is surjective.
- \( E_p \) is ramified at every prime \( \ell \mid N \).
- \( p \nmid \# E_p \).

Then \( F_p(f) \in J_p^{r-1} \), where \( r = \text{rank}_Z E(K) \), and letting \( \bar{F}_p(f) \) be the natural image of \( F_p(f) \) in \( J_p^{r-1}/J_p^r \), we have
\[
\bar{F}_p(f) = p^{-2} \cdot \log_{\omega_f}(y_p)^2 \cdot \text{Reg}_p \cdot t^{-2} \cdot \#\text{III}(E/K)_{p^\infty}
\]
up to a \( p \)-adic unit.

Combined with the aforementioned case of the Iwasawa–Greenberg main conjecture (which is known under relatively mild hypotheses [BCK19]), Theorem 1.3 can be rephrased in terms of \( L_p(f) \), yielding our main result towards Conjecture 1.1 (or rather its refinement in Conjecture 2.21; see Corollary 3.4).

We end this Introduction by commenting on the need for the refinement of Conjecture 1.1 given by Conjecture 2.21. We continue to assume that \( \#\text{III}(E/K)_{p^\infty} < \infty \), and let
\[
r := \text{rank}_Z E(K)^\pm
\]
be the rank of the \( \pm \)-eigenspace \( E(K)^\pm \subset E(K) \) under the action of complex conjugation, so \( r = r^+ + r^- \). From the Galois-equivariance properties of \( h_p^{\text{MT}} \), one sees that \( \text{Reg}_p = 0 \) when \( |r^+ - r^-| > 1 \). These systematic degeneracies of the \( p \)-adic height pairing in the anticyclotomic setting were understood by Bertolini–Darmon [BD94, BD95] as giving rise to canonical derived \( p \)-adic height pairings, with which one can define a generalized \( p \)-adic regulator \( \text{Reg}_{\text{der.p}} \). This regulator recovers the classical Mazur–Tate regulator \( \text{Reg}_p \) 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 (as conjectured by Mazur and Bertolini–Darmon) leads one to expect that \( \text{Reg}_{\text{der.p}} \) is a nonzero element in \( J_p^{2\rho}/J_p^{2\rho+1} \), where
\[
\rho = \max\{r^+, r^-\} - 1.
\]

Conjecture 2.21 predicts that \( L_p(f) \) lands in \( J_p^{2\rho} \) (note that \( 2\rho \geq r - 1 \), with equality if and only if \( |r^+ - r^-| = 1 \)), and posits a formula for its natural image in \( J_p^{2\rho}/J_p^{2\rho+1} \) in terms of \( \text{Reg}_{\text{der.p}} \). Our main result is the analogue of Theorem 1.3 for this refined conjecture.

**Remark 1.4.** As the reader will see, our conjectures are very closely related to the conjectures of Birch–Swinnerton-Dyer type formulated by Bertolini–Darmon [BD94] for certain “Heegner distributions”.

ON ANTICYCLOTOMIC VARIANTS OF THE \( p \)-ADIC BIRCH–SWINNERTON-DYER CONJECTURE 3
The remainder of this paper in organized as follows. In Section 2, after defining the relevant Selmer groups and recalling conjectures of Bertolini–Darmon (some of which are not explicitly stated in the literature), we formulate our conjectures of BSD type for the $p$-adic $L$-functions $L_p(f)$ and $L_p(f)$. In Section 3, we state and prove our main results in the direction of these conjectures.

2. The conjectures

2.1. Selmer groups. Let $S$ be a fixed finite set of places of $\mathbb{Q}$ containing $\infty$ and the primes dividing $Np$, and for every finite field extension $F/\mathbb{Q}$ let $G_{F,S}$ be the Galois group over $F$ of the maximal extension of $F$ unramified outside the places above $\Sigma$. For each prime $q \in \{p, \bar{p}\}$ and non-negative integer $n$, set

$$\text{Sel}_q(K_n, T) := \ker \left\{ H^1(G_{K_n,S}, T) \to \prod_{w | p, w \neq q} H^1(K_{n,w}, T) \right\}.$$ 

Let $\text{Sel}_q(K, T) := \varprojlim_n \text{Sel}_q(K_n, T)$.

2.1.1. Selmer groups. Let $S$ be a fixed finite set of places of $\mathbb{Q}$ containing $\infty$ and the primes dividing $Np$, and for every finite field extension $F/\mathbb{Q}$ let $G_{F,S}$ be the Galois group over $F$ of the maximal extension of $F$ unramified outside the places above $\Sigma$. For each prime $q \in \{p, \bar{p}\}$ and non-negative integer $n$, set

$$\text{Sel}_q(K_n, T) := \ker \left\{ H^1(G_{K_n,S}, T) \to \prod_{w | p, w \neq q} H^1(K_{n,w}, T) \right\}.$$

Let $\text{Sel}_q(K, E_{p, \infty}) \subset H^1(G_{K,S}, E_{p, \infty})$ be the Selmer group cut out by the local conditions determined by the orthogonal complement under local Tate duality of the subspaces cutting out $\text{Sel}_q(K_n, T)$, and set

$$\text{Sel}_q(K, E_{p, \infty}) := \varprojlim_n \text{Sel}_q(K_n, E_{p, \infty}).$$

As is well-known, $\text{Sel}_q(K, E_{p, \infty})$ is a cofinitely generated $\Lambda$-module, i.e., its Pontryagin dual $\text{Sel}_q(K, E_{p, \infty})^\vee$ is finitely generated over $\Lambda$.

Conjecture 2.1 (Iwasawa–Greenberg main conjecture). The module $\text{Sel}_p(K, E_{p, \infty})$ is $\Lambda$-cotorsion and

$$\text{char}_\Lambda(\text{Sel}_p(K, E_{p, \infty})^\vee)\Lambda_{\text{cyc}} = (L_p(f))$$

as ideals in $\Lambda_{\text{cyc}}$.

The following lemma will be useful in the following. Let

$$\text{Sel}_{\text{str}}(K, T) := \ker \left\{ H^1(G_K,S), T) \to \prod_{w} H^1(K_w, T) \right\}$$

be the strict Selmer group, which is clearly contained in the pro-$p$ Selmer group $S_p(E/K) = \varprojlim_m S_{p,m}(E/K)$ fitting in the descent exact sequence

$$0 \to E(K) \otimes \mathbb{Z}_p \to S_{p}(E/K) \to T_p \text{III}(E/K) \to 0,$$

where $T_p \text{III}(E/K) := \varprojlim_m \text{III}(E/K)_p m$ is the $p$-adic Tate module of $\text{III}(E/K)$.

Lemma 2.2. Assume that $\text{III}(E/K)_p m$ is finite. Then

$$\text{Sel}_p(K, T) = \text{Sel}_{\text{str}}(K, T) = \text{Sel}_p(K, T).$$

In particular, $\text{Sel}_p(K, T)$ and $\text{Sel}_{\text{str}}(K, T)$ are contained in $S_p(E/K)$ and have $\mathbb{Z}_p$-rank $r - 1$, where $r = \text{rank}_\mathbb{Z} E(K)$.

Proof. By our assumption on $\text{III}(E/K)$, hypothesis [Heeg] and the $p$-parity conjecture imply that $r$ is odd, so in particular positive. Thus the image of restriction map

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

has $\mathbb{Z}_p$-rank one, and the result follows from [Ski14, Lem. 2.3.2].
2.2. **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 of analogous statements for the $p$-adic $L$-functions $L_p(f)$ and $Z_p(f)$ of Bertolini–Darmon–Prasanna, which is given in §2.3.

As in the Introduction, assume that $E$ has good ordinary reduction at $p$ and that $K$ is an imaginary quadratic field of discriminant prime to $N_p$, but in this subsection we also allow $p$ to be inert in $K$. Moreover, 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 $\ell$ which are split (resp. inert) in $K$, we have

$$N^-\text{ is the squarefree product of an even number of primes.}$$

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 $K_n \subset K_\infty$ of the anticyclotomic $\mathbb{Z}_p$-extension $K_\infty/K$.

In [BD96] §2.7 Bertolini–Darmon constructed certain “Heegner distributions”

$$\theta \in \mathbb{Z}_p[[\Gamma_\infty]], \quad \text{where } Z_p := E(K_\infty) \otimes \mathbb{Z}_p,$$

and formulated analogues of the $p$-adic Birch–Swinnerton-Dyer conjecture for them. Let $J$ be the augmentation ideal of $\Lambda = \mathbb{Z}_p[[\Gamma_\infty]]$, and define the order of vanishing of $\theta$ by

$$\text{ord}_J \theta := \max \{ \rho \in \mathbb{Z}_{\geq 0} : \theta \in Z_p \otimes_{\mathbb{Z}_p} J^\rho \}.$$

Note that since the element $\theta$ is known to be nonzero by Cornut–Vatsal, its order of vanishing is a well-defined integer.

The following conjecture is the “indefinite case” of [BD96] Conj. 4.1, where we let $E(K)\pm$ be the $\pm$-eigenspaces of $E(K)$ under the action of complex conjugation.

**Conjecture 2.3** (Bertolini–Darmon). *We have*

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

*where $r^\pm := \text{rank}_\mathbb{Q} E(K)^\pm$.*

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

$$\mathcal{L} := \theta \otimes \theta^* \in \mathbb{Z}_p^{\otimes 2}[[\Gamma_\infty]].$$

Let $\rho = \text{ord}_J \theta$, so clearly $\mathcal{L} \in \mathbb{Z}_p^{\otimes 2} \otimes_{\mathbb{Z}_p} J^{2\rho}$.

**Lemma 2.4.** *The natural image $\bar{\mathcal{L}}$ of $\mathcal{L}$ in $\mathbb{Z}_p^{\otimes 2} \otimes_{\mathbb{Z}_p} (J^{2\rho}/J^{2\rho+1})$ is contained in the image of the map*

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

**Proof.** This follows from the fact that the natural image $\bar{\theta}$ of $\theta$ in $Z_p \otimes_{\mathbb{Z}_p} (J^\rho/J^{\rho+1})$ is fixed by $\Gamma_\infty$ (see [BD96] Lem. 2.14)).

Since $2(\max \{ r^+, r^- \} - 1) \geq r - 1$, we see from Lemma 2.4 that Conjecture 2.3 predicts in particular the inclusion $\bar{\mathcal{L}} \in E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$, where $r = \text{rank}_\mathbb{Q} E(K)$. The conjectures of Bertolini–Darmon also predict an expression for $\mathcal{L}$ in terms of the following “enhanced” regulator associated to the Mazur–Tate anticyclotomic $p$-adic height pairing

$$h^\text{MT}_p : E(K) \times E(K) \to (J/J^2) \otimes \mathbb{Q}.$$

The next remark will be important in the following.
Remark 2.5. Let $\tau$ be the non-trivial element of $\text{Gal}(K/\mathbb{Q})$, which by definition acts as multiplication by $-1$ on $\Gamma_\infty$. Viewing $h_p^\text{NT}$ as valued in $\Gamma_\infty \otimes \mathbb{Q}$ under the identification $J/J^2 \simeq \Gamma_\infty$, the Galois-equivariance property of $h_p^\text{NT}$ implies that

$$h_p^\text{NT}(\tau x, \tau y) = h_p^\text{NT}(x, y)^\tau = -h_p^\text{NT}(x, y).$$

It follows that the $\tau$-eigenspaces $E(K)^\pm$ are isotropic for $h_p^\text{NT}$, and so the null-space of $h_p^\text{NT}$ has rank at least $|r^+ - r^-|$ (which should always be positive, since by (gen-H) the rank $r = r^+ + r^-$ should be odd).

Definition 2.6. Let $P_1, \ldots, P_r$ be a basis for $(E(K)/E(K)_{\text{tors}}$. Then set $t = [E(K) : \mathbb{Z}P_1 + \cdots + \mathbb{Z}P_r]$. The enhanced regulator $\text{Reg}$ is the element of $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r) \otimes \mathbb{Q}$ defined by

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

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

The following is the “non-exceptional case” (meaning that $E/K$ has good ordinary or non-split multiplicative reduction at every prime above $p$) of [BD96 Conj. 4.5].

Conjecture 2.7 (Bertolini–Darmon). Let $\mathcal{L}$ be the natural image of $\mathcal{L}_p$ in $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$. Then

$$\mathcal{L} = \left(1 - a_p(E) + \frac{p}{p}\right)^2 \cdot \widetilde{\text{Reg}} \cdot \#\text{III}(E/K)^\infty \cdot \prod_{\ell | N^+} c_\ell^2,$$

where $c_\ell$ is the $p$-part of the Tamagawa number of $E/\mathbb{Q}_\ell$.

As noted in [BD96 p. 447], when $|r^+ - r^-| > 1$, Conjecture 2.7 reduces to the prediction “$0 = 0$”. Indeed, $2(\max\{r^+, r^-\} - 1)$ is then strictly larger than $r-1$, and so by Conjecture 2.3 the image of $\mathcal{L}$ in $E(K)^{\otimes 2} \otimes (J^{r-1}/J^r)$ should vanish, while on the other hand by the isotropy of $E(K)^\pm$ under $h_p^\text{NT}$ all the minors $R_{i,j}$ in the definition of $\text{Reg}$ should also vanish (see [BD96 Lem. 3.2]). A more satisfying refinement of Conjecture 2.7, predicting a formula for the natural image of $\mathcal{L}$ in $E(K)^{\otimes 2} \otimes (J^{2p}/J^{2p+1})$, which should be thought of as a “leading coefficient”, can be given in terms of the derived $p$-adic height pairings introduced by Bertolini–Darmon [BD94, BD95], accounting for the degeneracies of $h_p^\text{NT}$ in the anticyclotomic setting.

Remark 2.8. Such refinement of Conjecture 2.7 seems to not have been explicitly stated in the literature. Even though the formulation of such refinement 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 $\text{III}(E/K)^\infty$ is finite and that:

(i) $\bar{p}_{E,p} : G_{\mathbb{Q}} \to \text{Aut}_{\mathbb{F}_p}(E_p)$ is surjective.

(ii) $p \nmid \#E(F_v)$ for all $v | p$, where $F_v$ is the residue field of $K$ at $v$.

Note that (i) amounts to the condition $a_p(E) \neq 1 \pmod{p}$ when $p$ splits in $K$, and $a_p(E) \neq \pm 1 \pmod{p}$ when $p$ is inert in $K$, and that by (ii) the elliptic curve $E$ has no CM. In particular, these assumptions imply that $S_p(E/K) \simeq E(K) \otimes \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of rank $r$, and the pair $(E, K)$ is “generic” in the terminology of [Maz94].

By [BD95 §2.4], there is a filtration

$$S_p(E/K) = S_p^{(1)} \supseteq S_p^{(2)} \supseteq \cdots \supseteq S_p^{(p)},$$

and a sequence of “derived $p$-adic height pairings”

$$h_p^{(k)} : S_p^{(k)} \times \tilde{S}_p^{(k)} \to (J^k/J^{k+1}) \otimes \mathbb{Q}, \quad \text{for} \quad 1 \leq k \leq p - 1,$$
such that $S_p^{(k+1)}$ is the null-space of $h_p^{(k)}$, with $h_p^{(1)} = h_p^{\text{MT}}$. By Remark 2.5, $\bar{S}_p^{(2)}$ has $\mathbb{Z}_p$-rank at least $|r^+ - r^-|$, and by construction the subspace $US_p(E/K) \subset S_p(E/K)$ of universal norms for $K_{\infty}/K$, which is known to be a free $\mathbb{Z}_p$-module of rank one by Cornut–Vatsal, is contained in the null-space of all $h_p^{(k)}$.

The expected “maximal non-degeneracy” of $h_p^{\text{MT}}$ then leads to the following ([BD95 Conj. 3.3, Conj. 3.8]).

**Conjecture 2.9** (Mazur, Bertolini–Darmon). Assume that $\# \text{III}(E/K)_{p^{\infty}} < \infty$ and the pair $(E, K)$ is generic. Then

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

and in fact $S_p^{(3)}$ is the $p$-adic saturation of $US_p(E/K)$ in $S_p(E/K)$.

The successive quotients $\bar{S}_p^{(k)}/S_p^{(k+1)}$ are free $\mathbb{Z}_p$-modules, say

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

and Conjecture 2.9 predicts in particular that

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

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

With the notion of derived $p$-adic height pairings, one can naturally define an enhanced regulator extending $\text{Reg}$ in Definition 2.6. Assume that $S_p^{(p)}$ is the $p$-adic saturation of $US_p(E/K)$ in $S_p(E/K)$ (as predicted in particular by Conjecture 2.9). Let $P_1, \ldots, P_r$ be an integral basis for $E(K) \otimes \mathbb{Q}$, and let $A \in M_n(\mathbb{Z}_p)$ be an endomorphism of $S_p(E/K)$ sending $P_1, \ldots, P_r$ to a $\mathbb{Z}_p$-basis $x_1, \ldots, x_r$ for $S_p(E/K)$ compatible with the filtration (2.2), so for $1 \leq k \leq p-1$ the projection of say $x_{h_k+1}, \ldots, x_{h_k+e_k}$ to $S_p^{(k)}/S_p^{(k+1)}$ is a $\mathbb{Z}_p$-basis for $S_p^{(k)}/S_p^{(k+1)}$ and $y := x_r$ is a $\mathbb{Z}_p$-generator of $US_p(E/K)$.

**Definition 2.10.** Let $\varrho := \sum_{k=1}^{p-1} k e_k$. The derived enhanced regulator $\text{Reg}_\text{der}$ is the element of $E(K) \otimes^2 (J^0/J^{e+1}) \otimes \mathbb{Q}$ defined by

$$\text{Reg}_\text{der} := \det(A)^{-2} \cdot (y \otimes y) \otimes \prod_{k=1}^{p-1} R^{(k)},$$

where $R^{(k)} = \det(h_p^{(k)}(x_i, x_j))_{h_k+1 \leq i, j \leq h_k+e_k}$ is the $k$-th partial regulator.

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

**Lemma 2.11.** Assume Conjecture 2.9 and that $\text{III}(E/K)_{p^{\infty}}$ is finite. If $|r^+ - r^-| = 1$, then

$$\text{Reg}_\text{der} = \text{Reg}.$$
In general, Conjecture 2.9 predicts that \( \overline{\text{Reg}}_{\text{der}} \) is a nonzero element in \( E(K)^{\otimes 2} \otimes (J^\rho/J^{2\rho+1}) \otimes \mathbb{Q} \), where

\[
\rho = e_1 + 2e_2 = 2 \min\{r^+, r^-\} + 2(|r^+ - r^-| - 1) = 2(\max\{r^+, r^-\} - 1),
\]

which as already noted is strictly larger than \( r - 1 \) when \( |r^+ - r^-| > 1 \). Thus, by Lemma 2.11 the following refines Conjecture 2.7.

**Conjecture 2.12** (Bertolini–Darmon). Assume that \( III(E/K)_{p^\infty} \) is finite and the pair \((E, K)\) is generic. Then

\[
\text{ord}_{J} \mathcal{L} = 2(\max\{r^+, r^-\} - 1),
\]

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

\[
\tilde{\mathcal{L}} = \left( \frac{1 - a_p(E) + p}{p} \right)^2 \cdot \overline{\text{Reg}}_{\text{der}} \cdot \#III(E/K)_{p^\infty} \cdot \prod_{\ell \mid N^+} c_{\ell}^2.
\]

It is also possible to formulate a leading term formula for the Heegner distribution \( \theta \), 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 \( \text{Gal}(K/\mathbb{Q}) \), and therefore is contained in one of the \( \tau \)-eigenspaces \( S_\tau(E/K)^\pm \). Note that \( \text{rank}_{\mathbb{Z}} S_\tau(E/K)^\pm = r^\pm \), since we are assuming finiteness of \( III(E/K)_{p^\infty} \).

**Lemma 2.13.** Assume Conjecture 2.9. Letting sign \( US_p(E/K) \) be the sign of the \( \tau \)-eigenspace where \( US_p(E/K) \) is contained, we have

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

In other words, \( US_p(E/K) \) is contained in the larger of the \( \tau \)-eigenspaces \( S_\tau(E/K)^\pm \).

**Proof.** Viewing \( h^\text{MT}_p \) as defined on \( S_\tau(E/K) \), Conjecture 2.9 predicts that the restriction

\[
h^\text{MT}_p : S_\tau(E/K)^+ \times S_\tau(E/K)^- \rightarrow (J/J^2) \otimes \mathbb{Q}
\]

is either left non-degenerate or right non-degenerate, depending on which of the \( \tau \)-eigenspaces \( S_\tau(E/K)^\pm \subset S_\tau(E/K) \) is larger. Since the universal norms are contained in the null-space of \( h^\text{MT}_p \), it follows that \( US_p(E/K) \) is contained in the \( \tau \)-eigenspace of larger rank. \( \square \)

**Remark 2.14.** The conclusion of Lemma 2.13 is predicted by the “sign conjecture” of Mazur–Rubin [MR03] Conj. 4.8, and the fact that it follows from Conjecture 2.9 (although it might be substantially weaker) was already observed by them.

Let \( s := \min\{r^+, r^-\} \) and recall that Conjecture 2.9 predicts \( e_1 := \text{rank}_{\mathbb{Z}} \tilde{s}_p^{(1)}/\tilde{s}_p^{(2)} = 2s \). Order the first \( 2s \) elements of the basis \( x_1, \ldots, x_r \) for \( S_\tau(E/K) \) so that \( x_1 =: y_1^+, \ldots, x_s =: y_s^+ \) belong to \( S_\tau(E/K)^+ \) and \( x_{s+1} =: y_1^- , \ldots, x_{2s} =: y_s^- \) belong to \( S_\tau(E/K)^- \).

**Lemma 2.15.** We have

\[
R_1 = -\left( \det(h^\text{MT}_p(y_i^+, y_j^-))_{1 \leq i, j \leq s} \right)^2.
\]

**Proof.** This is immediate from the isotropic property of \( S_\tau(E/K)^\pm \) under the pairing \( h^\text{MT}_p \) (see Remark 2.5). \( \square \)

Thus \( R_1 \) is essentially a square. On the other hand, since for even values of \( \kappa \) the pairing \( h^k_p \) is alternating (see part (1) of [BD95] Thm. 2.18), we have

\[
R_2 = \text{pf}(h^2_p(x_i, x_j)_{e_1+1 \leq i, j \leq e_1+e_2})^2,
\]

where \( \text{pf}(M) \) denotes the Pfaffian of the matrix \( M \). This motivates the following.
Definition 2.16. Assume Conjecture 2.9. The square-root derived enhanced regulator is the element of \((J^p/J^{p+1}) \otimes \mathbb{Q}\), where \(p = \max\{r^+, r^-\} - 1\), defined by
\[
\tilde{\text{Reg}}_{\text{der}} := \det(A)^{-1} \cdot y \otimes (\det(h_p^{\text{MT}}(y_1, y_j))_{1 \leq i, j \leq s}) \cdot \text{pf}(h_p^{(2)}(x_i, x_j)_{e_1+1 \leq i, j \leq e_2}),
\]
where \(y = x_r\) is a \(\mathbb{Z}_p\)-generator of \(US_p(E/K) \simeq \mathbb{Z}_p\).

Remark 2.17. Note that \(\tilde{\text{Reg}}_{\text{der}}^{-1/2}\) is only well-defined up to sign.

The following refines [BD98, Conj. 4.6] in the cases where \(|r^+ - r^-| > 1\), and complements Conjecture 2.3 with a leading coefficient formula.

Conjecture 2.18. Assume that \(\text{III}(E/K)_{p^\infty}\) is finite and the pair \((E, K)\) is generic. Then
\[\text{ord}_j \theta = \max\{r^+, r^-\} - 1,\]
and letting \(\tilde{\theta}\) be the natural image of \(\theta\) in \((E(K_{\infty}) \otimes J^p/J^{p+1})_{K_{\infty}}\), where \(\rho = \max\{r^+, r^-\} - 1\), we have
\[\tilde{\theta} = \pm \left(1 - a_p(E) + p \right) \cdot \tilde{\text{Reg}}_{\text{der}}^{-1/2} \cdot \sqrt{\#\text{III}(E/K)_{p^\infty}} \cdot \prod_{l \mid N^+} c_l.\]

2.3. Conjectures for \(L_p(f)\). We assume now that the triple \((E, p, K)\) satisfies the hypotheses from the Introduction. In particular, hypotheses \([\text{Heeg}]\) and \([\text{spl}]\) hold. We also assume as in the preceding section that \(\text{III}(E/K)_{p^\infty}\) is finite, and that
\[(i) \ \tilde{\rho}_{E,q} : G_Q \to \text{Aut}_{p}(E_p)\]
\[(ii) a_p(E) \neq 1 \pmod{p}.

Remark 2.19. Hypothesis \([\text{spl}]\) will be essential in what follows, so that the \(p\)-adic \(L\)-function \(L_p(f)\) can be constructed as an element in \(A_{\tilde{\Delta}}\) (cf. [Kri18, AI19] when \(p\) is non-split in \(K\)). On the other hand, it should not be difficult to extend the construction of \(L_p(f)\) in [CH18] to the more general Heegner hypothesis \([\text{gen-H}]\) considered in the previous section.

By Lemma 2.2, the Selmer groups \(\mathcal{Sel}_p(K, T)\) and \(\mathcal{Sel}_p(K, T)\) are both contained in \(S_p(E/K)\) and they agree with the kernel \(\text{Sel}_{\text{str}}(K, T)\) of the restriction map \((2.1)\). In particular, we can consider the pairing
\[h_p : \mathcal{Sel}_p(K, T) \times \mathcal{Sel}_p(K, T) \to (J/J^2) \otimes \mathbb{Q}\]
on obtained by restricting \(h_p^{\text{MT}}\). The filtration in \((2.2)\) induces a filtration
\[(2.3) \quad \mathcal{Sel}_p(K, T) = \mathcal{S}_p^{(1)} \supset \mathcal{S}_p^{(2)} \supset \cdots \supset \mathcal{S}_p^{(p)}\]
defined by \(\mathcal{S}_p^{(k)} := S_p^{(1)} \cap \mathcal{Sel}_p(K, T)\), with the filtered pieces equipped with the corresponding derived \(p\)-adic height pairing
\[h_p^{(k)} : \mathcal{S}_p^{(k)} \times \mathcal{S}_p^{(k)} \to (J^k/J^{k+1}) \otimes \mathbb{Q}\]
on obtained from \(h_p^{(k)}\) by restriction.

Assume that \(\mathcal{S}_p^{(p)}\) is the \(p\)-adic saturation of \(US_p(E/K)\) in \(S_p(E/K)\) and that \(\mathcal{Sel}_p(K_{\infty}, E_{p^{\infty}})\)
is \(\Lambda\)-cotorsion, so the subspace of universal norms \(U\mathcal{Sel}_p(K, T) \subset \mathcal{Sel}_p(K, T)\) is trivial. It follows that
\[US_p(E/K) \cap \text{Sel}_{\text{str}}(K, T) = \{0\},\]
and so \(\log_{\omega_f}(y) \neq 0\) for any generator \(y \in US_p(E/K)\). Thus the first \(r-1\) elements in the basis \(x_1, \ldots, x_r\) for \(S_p(E/K)\) chosen for the definition of \(\text{Reg}_{\text{der}}\) yield a basis for \(\mathcal{Sel}_p(K, T)\) adapted to the filtration \(2.3\), with the image of \(x_{h_k+1}, \ldots, x_{h_k+e_{k+1}}\) in \(S_p^{(k)}/\mathcal{S}_p^{(k+1)}\) \(\simeq \mathcal{S}_p^{(k)}/\mathcal{S}_p^{(k+1)}\) giving a basis for \(\mathcal{S}_p^{(k)}/\mathcal{S}_p^{(k+1)}\). Then the partial regulators of Definition 2.6 can be rewritten as
\[(2.4) \quad R^{(k)} = \det(h_p^{(k)}(x_i, x_j))_{h_k+1 \leq i, j \leq h_k+e_k} = \text{disc}(h_p^{(k)}|\mathcal{S}_p^{(k)}/\mathcal{S}_p^{(k+1)})\),
which we shall now denote by $\mathcal{R}_p^{(k)}$ in the following.

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

$$\log_{\omega_f} : E(K) \otimes \mathbb{Q} \rightarrow E(K_p) \otimes E(K_p) \rightarrow \mathbb{Z}_p \otimes \mathbb{Z}_p \rightarrow \mathbb{Z}_p,$$

where the last arrow is given by multiplication. Choose a basis $x_1, \ldots, x_r, y_r$ as before, with $x_r = y_p$ given by a generator for $US_p(E/K)$ with $p^{-1}\log_{\omega_f}(y_p) \equiv 0 \pmod{p}$.

**Definition 2.20.** The derived regulator $\text{Reg}_{p,\text{der}}$ is defined by

$$\text{Reg}_{p,\text{der}} := \log_{\omega_f}(\text{Reg}_{\text{der}}) = \det(A)^{-2} \cdot \log_{\omega_f}(y_p)^2 \cdot \prod_{k=1}^{p-1} \mathcal{R}_p^{(k)}.$$ 

Note that $\text{Reg}_{p,\text{der}}$ is an element in $J^\rho / J^{\rho+1} \otimes \mathbb{Q}$, where $\rho = \sum_{k=1}^{p-1} ke_k$, and Conjecture 2.9 predicts the equality $\rho = \max\{r^+, r^-\} - 1$.

We are now in a position to formulate a $p$-adic Birch–Swinnerton-Dyer conjecture for $L_p(f)$, which is visibly a “shadow” of Bertolini–Darmon’s Conjecture 2.12.

**Conjecture 2.21.** Assume that $\text{III}(E/K)_{p^\infty}$ is finite and the pair $(E, K)$ is generic. Then

$$\text{ord}_f L_p(f) = 2(\max\{r^+, r^-\} - 1),$$

and letting $\tilde{L}_p(f)$ be the natural image of $L_p(f)$ in $J^\rho / J^{\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we have

$$\tilde{L}_p(f) = \left(1 - \frac{a_p(E) + p}{p}\right)^2 \cdot \text{Reg}_{p,\text{der}} \cdot \#\text{III}(E/K)_{p^\infty} \cdot \prod_{\ell | N} c_\ell^2.$$ 

2.4. **Conjectures for $\mathcal{L}_p(f)$.** Similarly as in Conjecture 2.18 we can also formulate a version of Conjecture 2.21 for the “square-roots” $p$-adic $L$-function $\mathcal{L}_p(f)$.

Assume Conjecture 2.9 so that we can define the derived square-root regulator by

$$\text{Reg}_{p,\text{der}}^{1/2} := \det(A)^{-1} \cdot \log_{\omega_f}(y_p) \cdot (\det(h_p(y_1^+, y_1^-)_{1 \leq i, j \leq s}) \cdot \prod_{(x_i, x_j, e_1+1 \leq i, j \leq e_1+e_2)}^f).$$

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

**Conjecture 2.22.** Assume that $\text{III}(E/K)_{p^\infty}$ is finite and the pair $(E, K)$ is generic. Then

$$\text{ord}_f \mathcal{L}_p(f) = \max\{r^+, r^-\} - 1,$$

and letting $\mathcal{L}_p(f)$ be the natural image of $\mathcal{L}_p(f)$ in $J^\rho / J^{\rho+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we have

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

3. **Main result**

3.1. **Statements.** We shall make the following hypotheses on the triple $(E, p, K)$, where we let $\rho_E : G_{\mathbb{Q}} \rightarrow \text{Aut}_{\mathbb{F}_p}(E_p)$ be the Galois representation of the $p$-torsion of $E$.

**Hypotheses 3.1.**

(a) $p \nmid 2N$ is a prime of good ordinary reduction for $E$.
(b) $\rho_{E,p}$ is ramified at every prime $\ell | N$.
(c) Every prime $\ell | N$ splits in $K$.
(d) $\rho_{E,p}$ is surjective.
(e) $p \equiv 1^\infty$ splits in $K$. 

reduces to the equality (up to a $p$-adic unit). It follows that in this case the inequality in Theorem A is an equality, and letting $p$ be a $p$-adic unit.

\[ F_p(f) = \left( 1 - a_p(E) + \frac{p}{\rho} \right)^2 \cdot \text{Reg}_{p,\text{der}} \cdot \# \text{III}(E/K)_{p^\infty} \cdot \prod_{\ell \mid N} c_\ell^2 \]

up to a $p$-adic unit.

**Remark 3.3.** If $\text{rank}_\mathbb{Z} E(K) = 1$, then the module $\text{Sel}_F(K, E_{p^\infty})$ is finite (see Lemma 2.2), and therefore the image of $F_p(f)$ under the augmentation map

\[ \epsilon : \Lambda \to \hat{O} \]

is nonzero. It follows that in this case the inequality in Theorem A is an equality, and letting $F_p(f)(0) \in \hat{O}$ denote the image of $F_p(f)$ under $\epsilon$, the leading term formula of Theorem A reduces to the equality (up to a $p$-adic unit)

\[ F_p(f)(0) = \left( 1 - a_p(E) + \frac{p}{\rho} \right)^2 \cdot \# \text{III}(E/K)_{p^\infty} \cdot \left( \frac{\log_{\omega_f}(y)}{E(K) : \mathbb{Z}y} \right)^2 \cdot \prod_{\ell \mid N} c_\ell^2, \]

where $y \in E(K)$ is any point of infinite order. Thus Theorem 3.2 extends the “anticyclotomic control theorem” in [JSW17, Thm. 3.3.1] to arbitrary ranks.

Under Hypotheses 3.1 (in fact, slightly weaker hypotheses suffice), and assuming that

\[(*) \text{ either } N \text{ is squarefree, or there are at least two primes } \ell \| N, \]

the Iwasawa–Greenberg main conjecture for $L_p(f)$ can be proved (see [BCK19, Cor. 7.7]) by building on work of Howard [How06] and W. Zhang [Zha14]. Thus Theorem 3.2 yields the following result towards Conjecture 2.21.

**Corollary 3.4.** Assume Hypotheses 3.1, that $\text{III}(E/K)_{p^\infty}$ is finite, and that \((*)\) holds. Then

\[ \text{ord}_L L_p(f) \geq 2(\max\{r^+, r^-\} - 1), \]

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

\[ L_p(f) = \left( 1 - a_p(E) + \frac{p}{\rho} \right)^2 \cdot \text{Reg}_{p,\text{der}} \cdot \# \text{III}(E/K)_{p^\infty} \cdot \prod_{\ell \mid N} c_\ell^2, \]

up to a $p$-adic unit.

3.2. **Proof of Theorem 3.2** Note by parts (e) and (f) of Hypotheses 3.1 we have $p \nmid \# E(F_p)$, and by [Maz72] §4 and condition (i) this implies that the local norm maps

\[ \text{Norm}_v : E(K_{n,v}) \to E(K_v) \]

are surjective for all primes $v$ of $K$ and all finite extensions $K_n \subset K_{\infty}$. (Here $E(K_{n,v})$ denotes $\bigoplus_{v \mid v} E(K_{n,v})$, where the sum runs over all places $w$ of $K_n$ lying above $v$.)

**Definition 3.5.** We say that a rational prime $q \nmid pN$ is $m$-admissible for $E$ if

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

And we say that a finite set of rational primes Σ is an m-admissible set for E if every q ∈ Σ is an m-admissible prime for E and the restriction map

\[ \mathcal{Sel}_p(K, E_{p^m}) \to \bigoplus_{q \in \Sigma} H^1_{\text{fin}}(K_q, E_{p^m}) \]

is injective.

Remark 3.6. As shown in [BD94, Lem. 2.23] (by a routine application of Čebotarev’s density theorem), m-admissible sets for E always exist, and it follows from the argument in the proof that one can in fact always find m-admissible sets for E with \#Σ = dim_{F_p}(\mathcal{Sel}_p(K, E_{p^m}) \otimes F_p).

The following important lemma underlies the usefulness of m-admissible sets (and sets).

Lemma 3.7. Let Σ be an m-admissible set for E. Then for every n the modules

\[ \bigoplus_{q \in \Sigma} H^1_{\text{fin}}(K_{n, q}, E_{p^m}), \quad \bigoplus_{q \in \Sigma} H^1_{\text{sing}}(K_{n, q}, E_{p^m}), \quad \mathcal{Sel}_p^\Sigma(K_n, E_{p^m}) \]

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

\[ 0 \to \mathcal{Sel}_p(K_n, E_{p^m}) \to \mathcal{Sel}_p^\Sigma(K_n, E_{p^m}) \to \bigoplus_{q \in \Sigma} H^1_{\text{sing}}(K_{n, q}, E_{p^m}) \to \mathcal{Sel}_p(K_n, E_{p^m})^\vee \to 0, \]

where δ is the dual to the natural restriction map.

Proof. Let q be an m-admissible prime for E, and denote by Ω the prime of K lying above q. Then \(E_{p^m}\) is unramified as \(G_{K_{n, q}}\)-module, and the action of the Frobenius element at Ω yields a decomposition

\[ E_{p^m} \simeq (\mathbb{Z}/p^m\mathbb{Z}) \oplus (\mathbb{Z}/p^m\mathbb{Z})(1) \]

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

By Poitou–Tate duality, to establish the exactness of (3.2) it suffices to establish injectivity of the restriction map

\[ \mathcal{Sel}_p(K_n, E_{p^m}) \to \bigoplus_{q \in \Sigma} H^1_{\text{fin}}(K_{n, q}, E_{p^m}) \]

(Indeed, this will imply surjectivity of δ). For contradiction, suppose that the kernel \(\mathcal{K}\) of this map is nonzero. Then we can find a nonzero element \(s \in \mathcal{K}\) which is fixed by \(\Gamma_n\), since \(\Gamma_n\) is a p-group. However, the surjectivity of the local norm maps in (3.1) implies that the restriction map

\[ \mathcal{Sel}_p(K, E_{p^m}) \to \mathcal{Sel}_p(K_n, E_{p^m})^{\Gamma_n} \]

is an isomorphism (see [BD94, Prop. 1.6]), and so \(s\) gives a nonzero element in the kernel of \(\mathcal{Sel}_p(K, E_{p^m}) \to \bigoplus_{q \in \Sigma} H^1_{\text{fin}}(K, E_{p^m})\), which is impossible by the m-admissibility of Σ. Thus the exactness of (3.2) follows, and with this the freeness claims for the module \(\mathcal{Sel}_p^\Sigma(K_n, E_{p^m})\) are shown in [BD94, Thm. 3.2].

Recall that \(F_p \in \Lambda\) is a characteristic power series for the Pontryagin dual \(X_p\) of \(\mathcal{Sel}_p(K_{p^\infty}, E_{p^\infty})\). The next result reduces the proof of Theorem 3.2 to the calculation of \(#(\mathcal{Sel}_p(K, E_{p^\infty})/\text{div,}\)

which is carried out in (3.3).
Proposition 3.8. Assume Hypotheses 3.7 and that $\text{III}(E/K)_{p^\infty}$ is finite. Then
\begin{equation}
\text{ord}_F(p(f)) \geq 2(\max\{r^+, r^-\} - 1),
\end{equation}
and letting $F_p(f)$ be the natural image of $F_p(f)$ in $J^{2p}/J^{2p+1}$, where $\rho = \max\{r^+, r^-\} - 1$, we have
\begin{equation}
F_p(f) = \#(\mathcal{E}(K, E_{p^\infty})/\text{div}) \cdot \det(A)^{-2} \cdot \prod_{k=1}^{p-1} \mathcal{R}^{(k)}_p
\end{equation}
up to a $p$-adic unit.

The rest of the section is devoted to the proof of Proposition 3.8, for which we shall suitably adapt the arguments in [BD95, §2.5].

Define
\begin{equation}
\langle \cdot, \cdot \rangle_{K_n/K_m} : \bigoplus_{q \in \Sigma} H^1(K_{n,q}, E_{p^m}) \times \bigoplus_{q \in \Sigma} H^1(K_{n,q}, E_{p^m}) \to (\mathbb{Z}/p^m\mathbb{Z})[\Gamma_n]
\end{equation}
by the rule
\begin{equation}
\langle x, y \rangle_n := \sum_{\sigma \in \Gamma_n} \langle x, y^\sigma \rangle_{K_n/m} \cdot \sigma^{-1},
\end{equation}
where $\langle \cdot, \cdot \rangle_{K_n/m} : \bigoplus_{q \in \Sigma} H^1(K_{n,q}, E_{p^m}) \times \bigoplus_{q \in \Sigma} H^1(K_{n,q}, E_{p^m}) \to \mathbb{Z}/p^m\mathbb{Z}$ is the natural extension of the local Tate pairing.

Lemma 3.9. The pairing $\langle \cdot, \cdot \rangle_{K_n/K_m}$ is symmetric, non-degenerate, and Galois-equivariant, and the images of $\bigoplus_{q \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^m})$ and $\mathcal{E}(K_n, E_{p^m})$ are isotropic for this pairing.

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

In the following, we take $m = n$, and set
\begin{equation}
R_n := (\mathbb{Z}/p^n\mathbb{Z})[\Gamma_n], \quad \langle \cdot, \cdot \rangle_n := \langle \cdot, \cdot \rangle_{K_n/K_n}
\end{equation}
for the ease of notation.

As shown in the proof of Lemma 3.7, the natural map $\mathcal{E}(K_n, E_{p^n}) \to \bigoplus_{q \in \Sigma} H^1(K_{n,q}, E_{p^n})$ is injective and we can write
\begin{equation}
\mathcal{E}(K_n, E_{p^n}) = \left( \bigoplus_{q \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n}) \right) \cap \mathcal{E}(K_n, E_{p^n}),
\end{equation}
with the modules in the intersection being each free $R_n$-modules of rank $\#\Sigma$. By Lemma 3.9 $\langle \cdot, \cdot \rangle_n$ restricts to a non-degenerate pairing
\begin{equation}
\langle \cdot, \cdot \rangle_n : \bigoplus_{q \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n}) \times \bigoplus_{q \in \Sigma} H^1_{\text{sing}}(K_{n,q}, E_{p^n}) \to R_n,
\end{equation}
and with a slight abuse of notation we define
\begin{equation}
\langle \cdot, \cdot \rangle_n : \bigoplus_{q \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n}) \times \mathcal{E}(K_n, E_{p^n}) \to R_n
\end{equation}
byp $\langle x, y \rangle_n := [x, \lambda(y)]_n$, where $\lambda$ is the natural map $\mathcal{E}(K_n, E_{p^n}) \to \bigoplus_{q \in \Sigma} H^1_{\text{sing}}(K_{n,q}, E_{p^n})$.

Lemma 3.10. Let $\mu_n : \Lambda \to R_n$ be the natural map. Then
\begin{equation}
\mu_n(F_p) = \text{Fitt}_{\Gamma_n}(\mathcal{E}(K_n, E_{p^n})^\vee) = \det((x_i, y_j)_{n, i,j \in \#\Sigma})
\end{equation}
where $x_1, \ldots, x_{\#\Sigma}$ and $y_1, \ldots, y_{\#\Sigma}$ are any $R_n$-bases for $\bigoplus_{q \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n})$ and $\mathcal{E}(K_n, E_{p^n})$, respectively.
Proof. The first equality follows from the natural isomorphism
\[ X_p/(\gamma_n - 1, p^n)X_p \simeq \mathcal{Sel}_p(K_n, E_{p^n})^\vee \]
together with standard properties of Fitting ideals, and the second equality follows from the fact that by Lemma 3.7 we have a presentation
\[ R_n^\# \Sigma \xrightarrow{A} R_n^\# \Sigma \to \mathcal{Sel}_p(K_n, E_{p^n})^\vee \to 0 \]
with \( A \) given by a matrix with entries \( a_{i,j} = [x_i, \lambda(y_j)]_n = \langle x_i, y_j \rangle_n \) (see [BD95] Lem. 2.25 and Lem. 2.26) for details).

Recall the filtration \( \mathcal{Sel}_p(K, T) = \mathcal{Sel}^{(1)}_p \supset \mathcal{Sel}^{(2)}_p \supset \cdots \) in (2.3). Letting \( \mathcal{Sel}^{(k)}_{p,n} \) be the natural image of \( \mathcal{Sel}^{(k)}_p \) in \( \mathcal{Sel}_p(K, E_{p^n}) \) we obtain a filtration
\[ \mathcal{Sel}_p(K, E_{p^n}) = \mathcal{Sel}^{(1)}_p \supset \mathcal{Sel}^{(2)}_p \supset \cdots \supset \mathcal{Sel}^{(p)}_p \]
with \( \mathcal{Sel}^{(k)}_{p,n}/\mathcal{Sel}^{(k+1)}_{p,n} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{e_k} \), for \( 1 \leq k \leq p - 1 \), and \( \mathcal{Sel}^{(p)}_p \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d_p} \) for \( d_p = \text{rank}_{\mathbb{Z}_p} \mathcal{Sel}^{(p)}_p \).

From (3.7) (using that (3.4) is an isomorphism), we see that
\[ \mathcal{Sel}_p(K, E_{p^n}) = \left( \bigoplus_{q \in \Sigma} H^1_{\text{et}}(K_q, E_{p^n}) \right) \cap \mathcal{Sel}^{(p)}_p(K, E_{p^n}) \]
with the modules in the intersection being free over \( \mathbb{Z}/p^n\mathbb{Z} \) of rank \#\( \Sigma \).

Let \( \bar{x}_1, \ldots, \bar{x}_{\#\Sigma} \) and \( \bar{y}_1, \ldots, \bar{y}_{\#\Sigma} \) be \( \mathbb{Z}/p^n\mathbb{Z} \)-bases for \( \bigoplus_{q \in \Sigma} H^1_{\text{et}}(K_q, E_{p^n}) \) and \( \mathcal{Sel}^{(p)}_p(K, E_{p^n}) \), respectively, which are adapted to the filtration (3.8), meaning that the first \( r \) vectors \( \bar{x}_1, \ldots, \bar{x}_r \) are a basis for \( \mathcal{Sel}_p(K, E_{p^n}) \) with the images of \( \bar{x}_{hr}, \ldots, \bar{x}_{hr+e_k} \) in \( \mathcal{Sel}^{(k)}_{p,n}/\mathcal{Sel}^{(k+1)}_{p,n} \) giving a basis for \( \mathcal{Sel}^{(k)}_{p,n}/\mathcal{Sel}^{(k+1)}_{p,n} \) (\( 1 \leq k \leq p - 1 \)) and \( \bar{x}_{hr}, \ldots, \bar{x}_{hr+e_k} \) a basis for \( \mathcal{Sel}^{(p)}_{p,n} \), and similarly for \( \bar{y}_1, \ldots, \bar{y}_{\#\Sigma} \). On the other hand, let \( x'_1, \ldots, x'_{\#\Sigma} \) and \( y'_1, \ldots, y'_{\#\Sigma} \) be any \( R_n \)-bases for \( \bigoplus_{q \in \Sigma} H^1_{\text{et}}(K_q, E_{p^n}) \) and \( \mathcal{Sel}^{(p)}_p(K, E_{p^n}) \), respectively, and set
\[ \bar{x}'_i := \text{cor}_{K_n/K}(x'_i), \quad \bar{y}'_i := \text{cor}_{K_n/K}(y'_i). \]

Then there exist matrices \( M \) and \( N \) in \( \text{GL}_{\#\Sigma}(\mathbb{Z}/p^n\mathbb{Z}) \) taking \( (\bar{x}'_1, \ldots, \bar{x}'_{\#\Sigma}) \mapsto (\bar{x}_1, \ldots, \bar{x}_{\#\Sigma}) \) and \( (\bar{y}'_1, \ldots, \bar{y}'_{\#\Sigma}) \mapsto (\bar{y}_1, \ldots, \bar{y}_{\#\Sigma}) \), respectively, and letting \( M, N \in \text{GL}_{\#\Sigma}(R_n) \) be any lifts of \( M, N \) under the map \( \text{GL}_{\#\Sigma}(R_n) \to \text{GL}_{\#\Sigma}(\mathbb{Z}/p^n\mathbb{Z}) \) induced by the augmentation
\[ \epsilon : R_n \to \mathbb{Z}/p^n\mathbb{Z}, \]
the images of \( (x'_1, \ldots, x'_{\#\Sigma}), (y'_1, \ldots, y'_{\#\Sigma}) \) under \( M, N \) are \( R_n \)-bases \( (x_1, \ldots, x_{\#\Sigma}), (y_1, \ldots, y_{\#\Sigma}) \) satisfying
\[ \text{cor}_{K_n/K}(x_i) = \bar{x}_i, \quad \text{cor}_{K_n/K}(y_i) = \bar{y}_i. \]

Lemma 3.11. With the above choice of \( R_n \)-bases \( x_1, \ldots, x_{\#\Sigma} \) and \( y_1, \ldots, y_{\#\Sigma} \), we have
\[ \epsilon(\text{det}([x_i, y_j]_n))_{r+1 \leq i,j \leq \#\Sigma}) = u \cdot \#(\mathcal{Sel}_p(K, E_{p^n})/\text{div}) \]
for some \( u \in (\mathbb{Z}/p^n\mathbb{Z})^\times \).

Proof. Write
\[ \mathcal{Sel}_p(K, E_{p^n})/\text{div} \simeq \mathbb{Z}/p^{s_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{s_r}\mathbb{Z} \]
Taking \( n \) from the outset to be sufficiently large, we may assume that \( s_i < n \) for all \( i \). Denote by \( X_p^{(p)}(K, E)_{p^n} \) the image of \( \mathcal{Sel}^{(p)}_p(K, E_{p^n}) \) under the natural map
\[ H^1(K, E_{p^n}) \to H^1(K, E_{p^n}). \]
Since the elements in $\bar{y}_1, \ldots, \bar{y}_r$ are in $\mathcal{S}\ell_p(K, E_{p^n})$ and $\bar{y}_1, \ldots, \bar{y}_\#\Sigma$ is a basis for $\mathcal{S}\ell_p^\Sigma(K, E_{p^n})$, we see that the natural surjection $\mathcal{S}\ell_p^\Sigma(K, E_{p^n}) \to \mathcal{X}_p^\Sigma(K, E)_{p^n}$ identifies $\mathcal{X}_p^\Sigma(K, E)_{p^n}$ with the span of $\bar{y}_{r+1}, \ldots, \bar{y}_\#\Sigma$ and we have an exact sequence

$$0 \to \mathcal{S}\ell_p(K, E_{p^n}) \to \mathcal{X}_p^\Sigma(K, E)_{p^n} \to \lambda(\mathcal{S}\ell_p^\Sigma(K, E_{p^n})) \to 0.$$ 

Thus we find that

$$\lambda(\mathcal{S}\ell_p^\Sigma(K, E_{p^n})) \cong p^{s_1}(\mathcal{Z}/p^n\mathcal{Z}) \oplus \cdots \oplus p^{s_k}(\mathcal{Z}/p^n\mathcal{Z}) \oplus (\mathcal{Z}/p^n\mathcal{Z})^{\#\Sigma-r-k},$$

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

$$\epsilon(\langle \bar{x}_i, \bar{y}_j \rangle_{\mathbb{K}}) = -\langle \bar{x}_i, \bar{y}_j \rangle_{\mathbb{K}},$$

which is immediate from the definitions and the compatibility of the local Tate pairing with corestriction (see [BD91, Prop. 2.10]).

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

$$\mathcal{S}\ell_p^{(k)} := \mathcal{S}\ell_p(K, E_{p^n}) \cap (\gamma_n - 1)^{k-1} \mathcal{S}\ell_p(K, E_{p^n}).$$

By definition, $\mathcal{S}\ell_p^{(k)}$ is the $p$-adic saturation of

$$\mathcal{S}\ell_p^{(k)} := \varprojlim \mathcal{S}\ell_p^{(k)}_n,$$

where the limit is with respect to the natural maps induced by the multiplication $E_{p^{n+1}} \to E_{p^n}$. Letting $p^A$ be the maximum of the exponents of the finite groups $\mathcal{S}\ell_p^{(k)} / \mathcal{S}\ell_p^{(0)}$ for $1 \leq k \leq p$, it follows that the elements $p^A \bar{x}_{h_k+1}, \ldots, p^A \bar{x}_{h_k+e_k}; p^A \bar{y}_{h_k+1}, \ldots, p^A \bar{y}_{h_k+e_k}$ belong to $\mathcal{S}\ell_p^{(k)}$. Let $\bar{x}_{h_k+1}, \ldots, \bar{x}_{h_k+e_k}; \bar{y}_{h_k+1}, \ldots, \bar{y}_{h_k+e_k} \in \mathcal{S}\ell_p(K, E_{p^n})$ be such that

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

For $0 \leq k \leq p$, the $D^{(k)}_n$ be the derivative operator

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

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

**Claim 3.12.** For every $1 \leq k \leq p$, there exist elements $x'_{h_k+i}, \ldots, x'_{h_k+e_k} \in \bigoplus_{\ell \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n})$ and $y'_{h_k+1}, \ldots, y'_{h_k+e_k} \in \mathcal{S}\ell_p(K, E_{p^n})$ satisfying the following two properties:

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

To see this, note that by (3.9) and the definition of $n$-admissible set we may view $p^A \bar{x}_{e_k+i}$ as elements in $\bigoplus_{\ell \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n}) = (\bigoplus_{\ell \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n}))^n$ and by injectivity of the restriction map (3.3) the equality in (3.10) may be seen as taking place in $\bigoplus_{\ell \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n})$. Hence by [BD99, Cor. 2.4] applied to $\bigoplus_{\ell \in \Sigma} H^1_{\text{lin}}(K_{n,q}, E_{p^n})$ (which is free over $R_n$ by Lemma 3.7), the existence of elements $x'_{h_k+i}$ satisfying (i) follows. The existence of elements $y'_{h_k+i}$ satisfying (ii) is seen similarly, viewing (3.10) as taking place in the $\mathcal{S}\ell_p^\Sigma(K, E_{p^n})$. By (3.10), the resulting elements $x'_1, \ldots, x'_r$ and $y'_1, \ldots, y'_r$ and $R_n$-linearly independent, and setting $x'_i := p^A x_i$ and $y'_i := p^A y_i$ for $r + 1 \leq i \leq \#\Sigma$ an argument as the one preceding Lemma 3.11 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 $\text{GL}_{\#\Sigma}(R_n) \to \text{GL}_{\#\Sigma}(\mathcal{Z}/p^n\mathcal{Z})$ induced by the augmentation, we may assume

$$\text{cor}_{K_{n,q}}(x'_i) = p^A x_i, \quad \text{cor}_{K_{n,q}}(y'_i) = p^A y_i.$$
for all $i$.

We can now conclude the proof of Proposition 3.8.

**Proof of Proposition 3.8.** Let $\sigma_r := e_1 + 2e_2 + \cdots + (p-1)e_{p-1} + d_p$. To prove the inequality (3.5), it is enough to show the inclusion

\[ (\text{3.13}) \quad \text{Fitt}_{R_n}(\mathfrak{Sel}_p(K_n, E_{p^n})) \in I_n^p \]

for all $n \geq 1$, where $I_n$ is the augmentation ideal of $R_n$.

As noted earlier, we may choose $n$-admissible sets $\Sigma = \Sigma_n$ with $\#\Sigma$ independent of $n$, and we assume now that the preceding constructions of bases have been done with such $\Sigma$.

The Galois-equivariance of $(\cdot, \cdot)_n$ together with (3.11) imply that for $1 \leq k \leq p-1$ we have

\[ (\text{3.14}) \quad \det((x'_{h_k+i}, y')_n) = 0 \]

for all $1 \leq i \leq e_k$ and $y \in \mathfrak{Sel}_p^\Sigma(K_n, E_{p^n})$, using Lemma 3.9 for the second equality. By [BD95, Cor. 2.5], it follows that $(x'_{h_k+i}, y')_n \in I_n^k$. Since (3.12) readily implies the equality

\[ (\text{3.15}) \quad \det((p^{A}x_i, p^{A}y_j)_n)_{1 \leq i, j \leq \#\Sigma} = \det((p^{A}x_i, p^{A}y_j)_n)_{1 \leq i, j \leq \#\Sigma}; \]

and by Lemma 4.8 we have

\[ (\text{3.16}) \quad \det((p^{A}x_i, p^{A}y_j)_n)_{1 \leq i, j \leq \#\Sigma} = p^{2A\#\Sigma} \cdot \text{Fitt}_{R_n}(\mathfrak{Sel}_p(K_n, E_{p^n})) \]

the inclusion (3.13) follows.

Finally, to prove the expression in Proposition 3.8 for the image of $F_p$ in $J^p/J^{p+1}$, we may assume that $\rho = \sigma_r$ (otherwise the result is trivial, both terms in the formula being equal to zero). Then by Lemma 3.9, (3.14), and Lemma 3.11 we get

\[ (\text{3.17}) \quad h_{p,n}^{(k)}(p^{A}x_i, p^{A}y_j) = (x'_i, y'_j)_n \in J_n^k/J_n^{k+1} \]

for all $h_k + 1 \leq i, j \leq h_k + e_k$, combining Lemma 3.10 with (3.14), (3.15), (3.16), and (3.17) we arrive at the equality

\[ (\text{3.18}) \quad \mu_n(F_p) = u_n \cdot \prod_{k=1}^{p-1} \det(h_{p,n}^{(k)}(x'_i, y'_j))_{h_k+1 \leq i, j \leq h_k + e_k} \]

in $J_n^p/J_n^{p+1}$, and letting $n \to \infty$ the result follows. \hfill $\square$

### 3.3. Calculation of $\#(\mathfrak{Sel}_p(K, E_{p^n})/\text{div})$. Define the $\bar{p}$-relaxed Tate–Shafarevich group by

\[ \text{III}^{[\bar{p}]}(E/K) := \ker \left\{ H^1(K, E) \to \coprod_{w \neq \bar{p}} H^1(K_w, E) \right\}, \]

and let $\text{III}^{[\bar{p}]}(E/K)_{p^n}$ denote its $p$-primary component.

**Lemma 3.13.** Assume that $\mathrm{rank}_Z E(K) > 0$ and $\text{III}(E/K)_{p^n}$ is finite. Then $\text{III}^{[\bar{p}]}(E/K)_{p^n}$ is also finite, and we have

\[ \#\text{III}^{[\bar{p}]}(E/K)_{p^n} = \#\text{III}(E/K)_{p^n} \cdot \#\mathrm{coker}(\mathrm{loc}_p), \]

where $\mathrm{loc}_p : S_p(E/K) \to E(K_p) \otimes \mathbb{Z}_p$ is the restriction map.
Proof. Define $B_{\infty}$ by the exactness of the sequence

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

which induces an exact sequence

$$(3.18) \quad 0 \to \text{III}(E/K)_{p^\infty} \to \text{III}^{[\mathfrak{p}]}(E_{p^\infty}/K) \to H^1(K_{\mathfrak{p}}, E)_{p^\infty} \xrightarrow{h_{\infty}} B_{\infty}.$$ By surjectivity of the top right arrow in the commutative diagram

$$\begin{array}{ccccccc}
0 & \to & E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & H^1(K, E_{p^\infty}) & \to & H^1(K, E)_{p^\infty} & \to & 0 \\
& & \downarrow & & \downarrow \delta & & \downarrow & \\
0 & \to & \prod_w E(K_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & \prod_w H^1(K_w, E_{p^\infty}) & \to & \prod_w H^1(K_w, E)_{p^\infty} & \to & 0
\end{array}$$

we see that $B_{\infty}$ is the kernel of the map $\delta$ in the Cassels dual exact sequence

$$0 \to \text{Sel}_{p^\infty}(E/K) \to H^1(K, E_{p^\infty}) \xrightarrow{\delta} \prod_w H^1(K_w, E)_{p^\infty}.$$ Thus using that $E_{p^\infty}^* \cong T^r$ (which exchanges the localization maps at $p$ and $\mathfrak{p}$) we see that the kernel of the map $h_{\infty}$ in $(3.18)$ is dual to the cokernel of the map $\text{loc}_p : S_p(E/K) \to E(K_p) \otimes \mathbb{Z}_p$, which is finite under our hypotheses. The result follows. \[\square\]

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

**Proposition 3.14.** Assume that $r = \text{rank}_\mathbb{Z}E(K) > 0$, $\text{III}(E/K)_{p^\infty}$ is finite, and $a_p(E) \not\equiv 1 \pmod{p}$. Then

$$\#(\mathcal{G}_{\mathfrak{p}}(K, E_{p^\infty})/\text{div}) = \#\text{III}(E/K)_{p^\infty} \cdot (\#\text{coker}(\text{loc}_p))^2,$$

where $\text{loc}_p : S_p(E/K) \to E(K_p) \otimes \mathbb{Z}_p$ is the restriction map.

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

$$E_{1,p}(K) := \ker\left\{ E(K) \otimes \mathbb{Z}_p \xrightarrow{\text{loc}_p} E(K_p) \otimes \mathbb{Z}_p \right\},$$

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

$$(3.19) \quad E(K) \otimes \mathbb{Z}_p = E_{1,p}(K) \oplus \mathbb{Z}_p y_p.$$ Then the finite module $U$ defined by the exactness of the sequence

$$(3.20) \quad 0 \to \mathbb{Z}_p y_p \to E(K_p) \otimes \mathbb{Z}_p \to U \to 0$$

satisfies

$$(3.21) \quad \#U = [E(K_p) \otimes \mathbb{Z}_p : \text{loc}_p(E(K) \otimes \mathbb{Z}_p)] = \#\text{coker}(\text{loc}_p),$$

using the assumption on $\text{III}(E/K)$ for the second equality. The hypothesis that $a_p(E) \not\equiv 1 \pmod{p}$ implies that $E(K_p)$ has no $p$-torsion, and so $E(K_p) \otimes \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of rank one. Tensoring $(3.21)$ with $\mathbb{Q}_p/\mathbb{Z}_p$, therefore yields

$$0 \to V \to (\mathbb{Q}_p/\mathbb{Z}_p) y_p \to E(K_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

with $\#V = \#U$, and from $(3.19)$ we deduce that

$$(3.22) \quad \ker\left\{ E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\lambda_p} E(K_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right\} = (E_{1,p}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \oplus V.$$

Now consider the $p$-relaxed Tate–Shafarevich group $\text{III}^{(p)}(E/K)$ defined by

$$\text{III}^{(p)}(E/K) := \ker\left\{ H^1(K, E) \to \prod_{w \not\mid p} H^1(K_w, E) \right\}.$$
It is immediately seen that its $p$-primary part fits in the exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}^{(p)}_E(K) \to \text{III}^{(p)}_E(K) = 0,$$

where $\text{Sel}^{(p)}_E(K)$ is the kernel of the map $H^1(K, E_p) \to \prod_{v|p} H^1(K_v, E_v)$. Consider also the commutative diagram

$$
\begin{array}{cccc}
0 & \to & E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & \text{Sel}^{(p)}_E(K) & \to & \text{III}^{(p)}_E(K) & \to & 0 \\
& & \downarrow \lambda_p & & \downarrow & & \downarrow & & \\
0 & \to & E(K_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & H^1(K, E_p) & \to & H^1(K_p, E_p) & \to & 0
\end{array}
$$

in which the unlabeled vertical maps are given by restriction. Since the map $\lambda_p$ is surjective by our assumptions, the snake lemma applied to this diagram yields the exact sequence

$$(3.24) \quad \# \text{coker}(\text{loc}_p) = \# \text{ker}(\lambda_p) = \# \text{Sel}_p(K, E_p) \to \# \text{III}_E^{(p)}(K) \to 0,$$

and hence from (3.23), (3.22) and (3.21) we conclude that

$$\#(\text{Sel}_p(K, E_p)_{/\div}) = \# \text{III}_E^{(p)}(K) \to \#V = \# \text{III}_E^{(p)}(K) \cdot \# \text{coker}(\text{loc}_p)$$

$$= \# \text{III}_E^{(p)}(K) \cdot \#(\text{coker}(\text{loc}_p))^2,$$

using Lemma 3.13 for the last equality.

As in the proof of Proposition 3.14 (assuming the hypotheses therein), let $y_1, \ldots, y_{r-1}$ be a $\mathbb{Z}_p$-basis of the kernel of

$$\text{loc}_p : E(K) \otimes \mathbb{Z}_p \to E(K_p) \otimes \mathbb{Z}_p,$$

and extend it to a $\mathbb{Z}_p$-basis $y_1, \ldots, y_p$ of $E(K) \otimes \mathbb{Z}_p$. In the following, we denote by $\log_{\omega_f} : E(K) \otimes \mathbb{Z}_p \to \mathbb{Z}_p$ is the composition of $\text{loc}_p$ with the formal group logarithm associated with $\mathbb{Z}_p$-basis $\omega_f \in \Omega_E^{1}/\mathbb{Z}_p$.

**Proposition 3.15.** Assume that $r = \text{rank}_E E(K) > 0$, $\text{III}_E^{(p)}(K) \to 0$, and $a_p(E) \not\equiv 1 \pmod p$. Then, up to a $p$-adic unit, we have

$$\# \text{coker}(\text{loc}_p) = p^{-1} \#(\mathbb{Z}_p/\log_{\omega_f}(y_p)).$$

**Proof.** Let $E_1(K_p)$ be the kernel of reduction modulo $p$, so there is an exact sequence

$$0 \to E_1(K_p) \to E(K_p) \to E(F_p) \to 0.$$

Set $Y := \mathbb{Z}_p y_p$, $Y_{p,1} := \text{loc}_p(Y) \cap (E_1(K_p) \otimes \mathbb{Z}_p)$ and $Z := Y/Y_{p,1}$ (a finite group), and consider the commutative diagram

$$
\begin{array}{cccc}
0 & \to & Y_{p,1} & \to & Y & \to & Z & \to & 0 \\
& & \downarrow \lambda_{p,1} & & \downarrow \text{loc}_p \cdot Y & & \downarrow & & \\
0 & \to & E_1(K_p) \otimes \mathbb{Z}_p & \to & E(K_p) \otimes \mathbb{Z}_p & \to & E(F_p) \otimes \mathbb{Z}_p & \to & 0
\end{array}
$$

Since the middle vertical is injective by our choice of $y_p$ and $E(F_p) \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p/(1-a_p(E)+p)$ is trivial by our assumption on $a_p(E)$, applying the snake lemma we deduce

$$(3.24) \quad \# \text{coker}(\text{loc}_p \cdot Y) \cdot \# Z = \# \text{coker}(\lambda_{p,1}).$$

On the other hand, noting that $\# Z \cdot y_p$ is a generator of $Y_{p,1}$ and the formal group logarithm induces an isomorphism $\log_{\omega_f} : E_1(K_p) \otimes \mathbb{Z}_p \simeq p \mathbb{Z}_p$, we find

$$(3.25) \quad \# \text{coker}(\lambda_{p,1}) = \frac{\# \mathbb{Z}_p/\log_{\omega_f}(Z \cdot y_p)}{\# \mathbb{Z}_p/\log_{\omega_f}(E_1(K_p) \otimes \mathbb{Z}_p)} = \# Z \cdot p^{-1} \#(\mathbb{Z}_p/\log_{\omega_f}(y_p)).$$
Since clearly \( \#\text{coker}(\text{loc}_p|_Y) = [E(K_p) \otimes \mathbb{Z}_p : \text{loc}_p(S_p(E/K))] \) by the definition of \( y_p \), combining (3.24) and (3.25) the result follows.

We can now conclude the proof of Theorem 3.2.

**Proof of Theorem 3.2.** By Proposition 3.8 we have \( \text{ord}_F(p(f) \geq 2p \) with \( p = \max\{r^+, r^-\} - 1 \), and the equality

\[
\hat{F}_p(f) = \#(\mathcal{Sel}_p(K, E_{p^\infty})/\text{div}) \cdot \det(A)^{-2} \cdot \prod_{k=1}^{p-1} \mathcal{R}_p^{(k)},
\]

in \((J^{2p}/J^{2p+1}) \otimes \mathbb{Q}\) up to a \( p \)-adic unit. On the other hand, combining Propositions 3.14 and 3.15 we obtain

\[
\#(\mathcal{Sel}_p(K, E_{p^\infty})/\text{div}) = \#(E/K)_{p^\infty} \cdot (\#\text{coker}(\text{loc}_p))^2 = \#(E/K)_{p^\infty} \cdot p^{-2} \cdot \log_{y(p)}^2
\]

with the last equality holding up to a \( p \)-adic unit. Recalling the Definition 2.20 of \( \text{Reg}_{p, \text{der}} \), the proof of Theorem 3.2 now follows from (3.26) and (3.27).  \( \square \)

**References**


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