On the Algebraic Functional Equation of the Eigenspaces of Mixed Signed Selmer Groups of Elliptic Curves with Good Reduction at Primes above $p$

Suman AHMED
School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, P. R. China
E-mail: npur.suman@gmail.com

Meng Fai LIM
School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan 430079, P. R. China
E-mail: limmf@mail.ccnu.edu.cn

Abstract Let $p$ be an odd prime number, and let $E$ be an elliptic curve defined over a number field which has good reduction at every prime above $p$. Under suitable assumptions, we prove that the $\eta$-eigenspace and the $\bar{\eta}$-eigenspace of mixed signed Selmer group of the elliptic curve are pseudo-isomorphic. As a corollary, we show that the $\eta$-eigenspace is trivial if and only if the $\bar{\eta}$-eigenspace is trivial. Our results can be thought as a reflection principle which relates an Iwasawa module in a given eigenspace with another Iwasawa module in a “reflected” eigenspace.

Keywords Algebraic functional equation, mixed signed Selmer groups

MR(2010) Subject Classification 11G10, 11R23

1 Introduction

The main conjecture of Iwasawa theory predicts a relation between a Selmer group and a conjectural $p$-adic $L$-function (see [2, 4, 8, 14, 18]). This $p$-adic $L$-function is expected to satisfy a conjectural functional equation in a certain sense. In view of the main conjecture and this conjectural functional equation, one would expect to have certain algebraic relationship between the corresponding Selmer groups. In this paper, we will examine this phenomenon for the eigenspaces of the mixed signed Selmer groups of elliptic curves with good reduction at primes above $p$. We shall describe our main result briefly in this introductory section.

Throughout the paper, $p$ will denote a fixed odd prime. Let $F'$ be a number field and $E$ an elliptic curve defined over $F'$. Let $F$ be a finite extension of $F'$. The following assumptions will be in full force throughout the paper.

(S1) The elliptic curve $E$ has good reduction at all primes of $F'$ above $p$, at least one of which is a supersingular reduction prime of $E$. 

Received December 23, 2019, accepted June 23, 2020
The second author is supported by National Natural Science Foundation of China (Grant Nos. 11550110172 and 11771164)
(S2) For each prime $u$ of $F'$ above $p$ at which the elliptic curve $E$ has supersingular reduction, we assume that the following statements are valid.

(a) $F'_u = \mathbb{Q}_p$.
(b) $a_u = 1 + p - |\bar{E}_u(\mathbb{F}_p)| = 0$, where $\bar{E}_u$ is the reduction of $E$ at $u$.
(c) $u$ is unramified in $F/F'$.

Denote by $\mathcal{F}_n = F(\mu_{p^{n+1}})$ and $\mathcal{F}_\infty = \bigcup_n \mathcal{F}_n$. We define a signed Selmer group $\text{Sel}_\sigma(E/F_\infty)$ (see the body of the paper for the precise definition) and write $X^\sigma(E/F_\infty)$ for its Pontryagin dual. We shall write $\Sigma^{ss}_p$ for the primes of $F$ above $p$ at which $E$ has good supersingular reduction. For a character $\eta$ of $\text{Gal}(F(\mu_p)/F)$, we write $\bar{\eta}$ for its contragradient. Denote by $e_\eta$ the idempotent $\frac{1}{p^v} \sum_{\sigma \in \text{Gal}(F(\mu_p)/F)} \eta(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\text{Gal}(F(\mu_p)/F)]$. The goal of the paper is to prove the following result.

**Theorem** (Theorem 4.1) Let $\eta$ be a character of $\text{Gal}(F(\mu_p)/F)$. For each $v \in \Sigma^{ss}$ with $s_v = +$, assume that $|F_v : \mathbb{Q}_p|$ is not divisible by 4. We then have that

$$\text{rank}_\Lambda(e_\eta X^\sigma(E/F_\infty)) = \text{rank}_\Lambda(e_\eta X^\sigma(E/F_\infty)'),$$

and that the torsion $\Lambda$-submodules of $e_\eta X^\sigma(E/F_\infty)$ and $e_\eta X^\sigma(E/F_\infty)'$ are pseudo-isomorphic.

Our result is in the spirit of prior results of Kim [10] (also see [4]). In fact, Kim proves a variant of our result for elliptic curves having good supersingular reduction at all primes above $p$. Our result thus is an improvement on his, namely, we allow the presence of primes of good ordinary reduction above $p$ and our signed Selmer groups can have mixed signs. As an application of our theorem, we prove the following.

**Corollary** (Corollary 4.2) Retain the setting of the above theorem. Then we have

$$e_\eta X^\sigma(E/F_\infty) = 0$$

if and only if $e_\eta X^\sigma(E/F_\infty)' = 0$.

The above theorem and corollary can be thought as a form of reflection principle reminiscent to that of class groups (for instance, see [21, §10.2]) which relates an Iwasawa module in a given eigenspace with another Iwasawa module in a “reflected” eigenspace. We also mention a viewpoint which may be interesting. Philosophically, one would expect that there should be a $p$-adic $L$-function on the analytic side which can be related to the signed Selmer groups via a main conjecture(s). Granted this, one will naturally hope for a result in the spirit of the Herbrand–Ribet Theorem which amounts to saying that the eigenspaces $e_\eta X^\sigma(E/F_\infty)$ and $e_\eta X^\sigma(E/F_\infty)'$ vanishes if and only if a certain twist of the conjectural $p$-adic $L$-function is a “unit” in an appropriate sense (see [1, Corollary 5.2.7] or [21]). For an elliptic curve $E$ defined over $\mathbb{Q}$, such a result is certainly true in view of recent progresses on the main conjecture (see [8, 14, 18, 20]). However, a construction of $p$-adic $L$-function for more general base fields is still absent. Despite this, it would still be interesting to look for Herbrand–Ribet Theorem type phenomenon in other Iwasawa-theoretical situations. We hope to pursue this line of study in a future work.

We now give an outline of our paper. In Section 2, we collect various results concerning $\Lambda$-modules and twist of $\Lambda[G]$-modules for a cyclic group $G$ whose order is coprime to $p$. In Section 3, we recall various facts on the arithmetic of an elliptic curve over a local field which
will be needed for the subsequent discussion of the paper. Section 4 is where we introduce the signed Selmer groups. We also need to work with the so-called strict signed Selmer group which coincides with the signed Selmer group on the infinite level. We do remark that the strict signed Selmer group and the signed Selmer group do not need to coincide on the intermediate subextensions. Despite this, they enjoy nice duality properties which will be crucial in proving our results. Once the machinery of the strict signed Selmer groups is set up, we can give the proof of Theorem 4.1 and Corollary 4.2.

2 Algebraic Preliminaries

2.1 Λ-modules

Throughout the paper, Λ will denote the ring \( \mathbb{Z}_p[[T]] \). By the Weierstrass preparation theorem (cf. [17, (5.3.4)] or [21, Theorem 7.3]), every \( f \in \Lambda \) can be written as a product \( u \cdot f_1 \), where \( u \) is a unit in \( \Lambda \) and \( f_1 \) is a Weierstrass polynomial in \( \mathbb{Z}_p[T] \). We shall then define the degree of \( f \) to be the degree of the associated Weierstrass polynomial \( f_1 \) (which is unique up to a unit) and denote it by \( \deg(f) \). For a finitely generated \( \Lambda \)-module \( M \), there exist irreducible Weierstrass polynomials \( f_j \), numbers \( r \), \( \alpha_i \), \( \beta_j \) and a homomorphism

\[
M \to \Lambda^r \oplus \left( \bigoplus_{i=1}^s \Lambda/p^{\alpha_i} \right) \oplus \left( \bigoplus_{j=1}^t \Lambda/f_j^{\beta_j} \right)
\]

with finite kernel and cokernel, where the numbers \( r \), \( \alpha_i \), \( \beta_j \) and the Weierstrass polynomials \( f_j \) are determined by \( M \) ([17, (5.3.8)] or [21, Theorem 13.12]). Then the rank of \( M \) is given by the number \( r \) which we denote by \( \text{rank}_\Lambda(M) \). The \( \mu \)-invariant \( \mu(M) \) (resp., \( \lambda \)-invariant \( \lambda(M) \)) of \( M \) is defined to be \( \sum_{i=1}^s \alpha_i \) (resp., \( \sum_{j=1}^t \beta_j \deg(f_j) \)). Finally, the characteristic ideal of \( M \) is defined to be the ideal generated by \( \prod_{i=1}^s p^{\alpha_i} \prod_{j=1}^t f_j^{\beta_j} \). We shall write \( \text{Char}(M) \) for this ideal. For a finitely generated \( \Lambda \)-module, we write \( M_{\Lambda\text{-tor}} \) for its torsion \( \Lambda \)-submodule. It is clear from the definition that one has \( \text{Char}(M) = \text{Char}(M_{\Lambda\text{-tor}}) \).

Lemma 2.1 Let \( M \) and \( N \) be two finitely generated \( \Lambda \)-modules. Suppose that for each \( m \), the quantity \( |(M/p^m)_{\Gamma_n}|/(N/p^m)_{\Gamma_n}| \) is bounded independent of \( n \). Then we have that \( \text{rank}_\Lambda(M) = \text{rank}_\Lambda(N) \), and that \( M[p^\infty] \) and \( N[p^\infty] \) are pseudo-isomorphic as \( \Lambda \)-modules.

Proof For each fixed \( m \), it follows from [15, Theorem 2.5.1] that

\[
|(M/p^m)_{\Gamma_n}| = p^{\mu(M/p^m)p^n+O(1)}
\]

as \( n \) varies. Therefore, it follows from this and the hypothesis of the lemma that \( \mu(M/p^m) = \mu(N/p^m) \) for every \( m \). The required conclusion now follows from an application of [15, Proposition 2.4.7].

For a finitely generated \( \Lambda \)-module \( M \), one can endow it with a natural compact topology (see [17, Proposition 5.2.17]). We then write \( M^c = \text{Hom}_{cts}(M, \mathbb{Q}_p/\mathbb{Z}_p) \) for the group of continuous group homomorphisms from \( M \) to \( \mathbb{Q}_p/\mathbb{Z}_p \), where \( \mathbb{Q}_p/\mathbb{Z}_p \) is given the discrete topology.

Lemma 2.2 Let \( M \) be a finitely generated \( \Lambda \)-module. Suppose that

\[
M \to \Lambda^r \oplus \left( \bigoplus_{i=1}^s \Lambda/p^{\alpha_i} \right) \oplus \left( \bigoplus_{j=1}^t \Lambda/f_j^{\beta_j} \right)
\]
with finite kernel and cokernel, where the numbers \( r, \alpha_i, \beta_j \) and the Weierstrass polynomials \( f_j \) is determined by \( M \). Then for every irreducible Weierstrass polynomial \( f \), we have

\[
\text{corank}_{\mathbb{Z}_p}((M^\vee \otimes \Lambda/f^n)^\Gamma) = \left( r + \sum_{j=1}^t \delta_{f_j} \min\{\beta_j, n\} \right) \deg(f),
\]

where \( \delta_{f_j} = 1 \) or \( 0 \) accordingly as \( f_j \Lambda = f \Lambda \) or \( f_j \Lambda \neq f \Lambda \).

**Proof** From the discussion in [4, p. 109], we have \((M^\vee \otimes \Lambda/f^n)^\Gamma = \text{Hom}_\Lambda(M, \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} \Lambda/f^n)\), where the \( \mathbb{Z}_p \)-corank of the latter is the \( \mathbb{Z}_p \)-rank of \( \text{Hom}_\Lambda(M, \Lambda/f^n) \). Since \( \text{Hom}_\Lambda(-, \Lambda/f^n) \) preserves finite direct sums and sends finite modules to finite modules, it suffices to prove the asserted equality in the lemma for an elementary \( \Lambda \)-module which is a straightforward verification.

We can now state the following proposition which is essentially taken from [4, Section 3].

**Proposition 2.3** Let \( M \) and \( N \) be two finitely generated \( \Lambda \)-modules. Suppose that the following two statements hold.

1. For each \( m \), the quantity \(|(M/p^m)_{\Gamma_n}|/(N/p^m)_{\Gamma_n}|\) is bounded independent of \( n \).
2. For each irreducible Weierstrass polynomial \( f \), we have

\[
\text{corank}_{\mathbb{Z}_p}((M^\vee \otimes \Lambda/f^n)^\Gamma) = \text{corank}_{\mathbb{Z}_p}((N^\vee \otimes \Lambda/f^n)^\Gamma)
\]

for \( n \geq 0 \).

Then we have \( \text{rank}_\Lambda(M) = \text{rank}_\Lambda(N) \), and \( M_{\Lambda\text{-tor}} \) is pseudo-isomorphic to \( N_{\Lambda\text{-tor}} \).

**Proof** Lemma 2.1 tells us that \( \text{rank}_\Lambda(M) = \text{rank}_\Lambda(N) \) and \( M[p^\infty] \) is pseudo-isomorphic to \( N[p^\infty] \). Hence, it remains to show that for each irreducible Weierstrass polynomial \( f \), the power of \( f \) occurring in \( M \) and \( N \) are the same, which is precisely a consequence of Lemma 2.2. \( \square \)

### 2.2 Twist of \( \Lambda \)-modules

Suppose that \( G \) is cyclic of order coprime to \( p \). (In most of our subsequent discussion, \( G \) is a subgroup of \( \mathbb{Z}/(p-1)\mathbb{Z} \).) Let \( \eta \) be a fixed character of \( G \). We write \( e_\eta \) for the idempotent \( \frac{1}{|G|} \sum_{\sigma \in G} \eta(\sigma)\sigma^{-1} \in \mathbb{Z}_p[G] \). As before, write \( \Lambda \) for the power series ring \( \mathbb{Z}_p[[T]] \) in one variable. We shall also view \( e_\eta \) as an element of \( \Lambda[G] \). For a \( \Lambda[G] \)-module \( M \), we write \( M^\eta = e_\eta M \). It is an easy exercise to check that \( \sigma \in G \) acts on \( M^\eta \) via multiplication by \( \eta(\sigma) \).

We shall write \( \mathbb{Z}_p(\eta) \) for the \( \mathbb{Z}_p[G] \)-module which is \( \mathbb{Z}_p \) as \( \mathbb{Z}_p \)-module with the action of \( G \) given by \( \sigma \cdot x = \eta(\sigma)x \) for \( \sigma \in G, x \in \mathbb{Z}_p \). If \( M \) is a \( \Lambda[G] \)-module, we write \( M(\eta) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\eta) \).

(Warning: \( M^\eta \neq M(\eta) \) in general; see Lemma 2.5 (4) below.) For a Weierstrass polynomial \( f \) of \( \Lambda \), we write \( M_f = M \otimes_{\mathbb{Z}_p} \Lambda/f \). We shall also denote by \( f^t \) the power series \( f(\frac{1}{1+T} - 1) \). For ease of discussion, we record a simple lemma.

**Lemma 2.4** Let \( I \) be a finite indexing set. Suppose that \( M_i \) and \( N_i \) are \( \mathbb{Z}_p \)-submodules of \( M \). Assume that \( N_i \subseteq M_i \) for every \( i \in I \) and that

\[
M = \bigoplus_i M_i = \bigoplus_i N_i.
\]

Then \( M_i = N_i \) for every \( i \).

**Proof** Let \( x \in M_j \). Then viewing \( x \) as an element of \( M = \bigoplus_i N_i \), we have \( x = \sum_i y_i \) for \( y_i \in N_i \). But since \( N_i \subseteq M_i \) for every \( i \in I \), the sum can be viewed as a direct sum.
decomposition in $M = \bigoplus_i M_i$. Hence we have $x = y_j$ which implies that $x \in N_j$. This proves the lemma.

We can now state the following lemma which tells us how the twists by $\eta$ and $f$ interact.

**Lemma 2.5** Let $M$ be a $\Lambda[G]$-module. Let $\eta$ be a character of $G$ and $f$ a power series of $\Lambda$ which is not divisible by $p$. Viewing $\Lambda/f$ as a $\Lambda[G]$-module with a trivial $G$-action, we have the following equalities of $\Lambda$-modules.

1. $e_\eta(M_f) = (e_\eta M)_f$.
2. $e_\eta(M^\vee f) = (e_\eta M_f)^\vee$.
3. $e_\eta M_{\text{div}} = (e_\eta M)_{\text{div}}$.
4. $e_\eta M = (M(\bar{\eta}))^G$.

**Proof** We begin by proving Statement (1). Note that

$$M_f = \bigoplus_\eta e_\eta(M_f),$$

where $\eta$ runs through all the character of $G$. On the other hand, we have

$$M_f = \left( \bigoplus_\eta e_\eta M \right)_f = \bigoplus_\eta (e_\eta M)_f.$$

It is easy to verify that $(e_\eta M)_f \subseteq e_\eta(M_f)$. Hence the equality now follows from Lemma 2.4. Statements (2) and (3) can be proven similarly. For Statement (4), one observes that $x \in e_\eta M \iff \sigma x = \eta(\sigma)x \iff \bar{\eta}(\sigma)x = x \iff x \in (M(\bar{\eta}))^G$. □

3 Local Considerations

3.1 Local Duality

Let $K$ be a local field of characteristic zero, and $L$ a finite cyclic Galois extension of $K$ with Galois group $G$. Suppose that the order of $G$ is coprime to $p$. (In most of our subsequent discussion, $G$ is a subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$.) Let $\eta$ be a character of $G$. Throughout this subsection, $M$ will denote a finite $\Lambda[\text{Gal}(\bar{K}/K)]$-module of order a power of $p$.

**Lemma 3.1** We have an isomorphism $e_\eta H^1(L, M) \cong H^1(K, M(\bar{\eta}))$.

**Proof** By Lemma 2.5(4), we have $e_\eta H^1(L, M) = (H^1(L, M(\bar{\eta}))^G$. Since $\text{Gal}(\bar{L}/L)$ acts trivially on $\mathbb{Z}_p(\bar{\eta})$, the latter is $H^1(L, M(\bar{\eta}))^G$. By the inflation-restriction sequence, we have

$$0 \rightarrow H^1(G, M(\bar{\eta})^{\text{Gal}(\bar{L}/L)}) \rightarrow H^1(K, M(\bar{\eta})) \rightarrow H^1(L, M(\bar{\eta}))^G \rightarrow H^2(G, M(\bar{\eta})^{\text{Gal}(\bar{L}/L)}).$$

Since $G$ is assumed to have order coprime to $p$, the $H^i(G, -)$ terms vanish, thus yielding the required isomorphism of the lemma. □

Recall that the local Tate duality gives us a perfect pairing

$$H^1(L, M) \times H^1(L, M^*) \rightarrow \mathbb{Q}/\mathbb{Z}_p,$$

where $M^* = \text{Hom}_{\mathbb{Z}_p}(M, \mu_{p\infty})$.

**Lemma 3.2** Let $C$ be a subgroup of $H^1(L, M)$, and let $D$ be its orthogonal complement with respect to the above perfect pairing. For a given character $\eta$ of $G$ and an element $f \in \Lambda$ which is coprime to $p$, $e_\eta C_f$ (resp., $e_\eta D_f$) can be viewed as subgroups of $H^1(K, M(\bar{\eta})_f)$ (resp.,
It follows from [3, Proposition 4.5] that (im \varepsilon) is the kernel of the following map
\[ H^1(K, M^*(\eta)) \to \mathbb{Q}_p/\mathbb{Z}_p. \]

**Proof** By the orthogonal relation between \( C \) and \( D \), we have short exact sequences
\[
0 \to C \to H^1(L, M) \to D^\vee \to 0,
0 \to D \to H^1(L, M^*) \to C^\vee \to 0.
\]
Taking idempotent and tensoring with \( \otimes_{\mathbb{Z}_p} \Lambda/f \) (or \( \otimes_{\mathbb{Z}_p} \Lambda/f^s \)), we obtain
\[
0 \to e_\eta C_f \to H^1(K, M(\bar{\eta})_f) \to (e_\eta D_f)_f^\vee \to 0,
0 \to e_\eta D_f \to H^1(K, M^*(\eta)f) \to (e_\eta C_f)_f^\vee \to 0,
\]
where the middle terms of the short exact sequences are obtained via Lemma 3.1. This proves the claims of the lemma. □

### 3.2 Ordinary Reduction at \( p \)

Let \( K \) be a finite extension of \( \mathbb{Q}_p \), and write \( L = K(\mu_p) \). Denote by \( G \) the Galois group Gal\((L/K)\) which has order dividing \( p - 1 \). Let \( K_\infty \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( K \). We write \( L_\infty = K_\infty L \) which is the cyclotomic \( \mathbb{Z}_p \)-extension of \( L \). We identify the completed group algebras \( \mathbb{Z}_p[[\text{Gal}(L_\infty/L)]] = \mathbb{Z}_p[[\text{Gal}(K_\infty/K)]] = \Lambda \) and identify the Galois groups Gal\((L_n/K_n)\) with \( G = \text{Gal}(L/K) \) for every \( n \).

Now let \( E \) denote an elliptic curve over \( K \) with good ordinary reduction. Write \( \tilde{E} \) (resp., \( \tilde{E} \)) for its formal group (resp., reduced curve) at \( K \). By [3, Corollary 3.2], we have that
\[
H^1(L_\infty, \tilde{E}[p^\infty]) = 0 \text{ which in turn yields}
\]
\[
0 \to \tilde{E}(L_\infty)[p^\infty] \to E(L_\infty)[p^\infty] \to \tilde{E}(L_\infty)[p^\infty] \to 0.
\]
The main theorem of Imai [7] says that \( E(L_\infty)[p^\infty] \) is finite. Consequently, so are \( \tilde{E}(L_\infty)[p^\infty] \) and \( \tilde{E}(L_\infty)[p^\infty] \). In fact, we have the following.

**Lemma 3.3** Let \( \eta \) be a character of Gal\((L_n/K_n)\) and \( f \in \Lambda \) which is coprime to \( p \). Then \( E(K_\infty)[p^\infty](\eta)_f \), \( E(K_\infty)[p^\infty]((\eta)f) \) and \( \tilde{E}(K_\infty)[p^\infty][\eta]_f \) are finite.

**Proof** Since \( E(K_\infty)[p^\infty][\eta]_f = E(K_\infty)[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\eta) \otimes_{\mathbb{Z}_p} \Lambda/f \Lambda \), the finiteness follows from the above observation that \( E(K_\infty)[p^\infty] \) is finite. The remaining cases can be proven similarly. □

Let \( \varepsilon_n \) denote the natural map
\[
H^1(L_n, \tilde{E}[p^\infty]) \to H^1(L_n, E[p^\infty]).
\]
It follows from [3, Proposition 4.5] that \((\text{im } \varepsilon_n)_{\text{div}} = E(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\). Now define \( C(E[p^m]/L_n) \) to be the kernel of the following map
\[
H^1(L_n, E[p^m]) \to \frac{H^1(L_n, E[p^\infty])}{(\text{im } \varepsilon_n)_{\text{div}}},
\]
It is easy to see that \( C(E[p^m]/L_n) \) identifies with \( E(L_n) \otimes \mathbb{Z}/p^m \). It then follows from this and a classical result of Tate [19] that \( C(E[p^m]/L_n) \) is orthogonal to itself under the perfect pairing
\[
H^1(L_n, E[p^m]) \times H^1(L_n, E[p^m]) \to \mathbb{Q}_p/\mathbb{Z}_p.
\]
Lemma 3.4 Fix a character $\eta$ of $\text{Gal}(L_n/K_n)$ and $f \in \Lambda$ which is coprime to $p$. Then $e_\eta C(E[p^m]/L_n)_f$ is orthogonal to $e_\eta C(E[p^m]/L_n)_f$ under the perfect pairing
\[ H^1(K_n, E[p^m]|(\bar{\eta})_f) \times H^1(K_n, E[p^m]|(\eta)_f) \to \mathbb{Q}_p/\mathbb{Z}_p. \]

Proof This follows immediately from combining Lemma 3.2 with the above discussion. $\square$

For later purposes, we require the following description of $e_\eta C(E[p^m]/L_n)_f$. Let $\theta_n$ denote the natural map
\[ H^1(K_n, E[p^\infty]|(\bar{\eta})_f) \to H^1(K_n, E[p^\infty]|(\eta)_f). \]
For each $m$, we define $C(E[p^m]|(\bar{\eta})_f/K_n)$ to be the kernel of the following map
\[ H^1(K_n, E[p^m]|(\bar{\eta})_f) \to H^1(K_n, E[p^\infty]|(\eta)_f). \]

Lemma 3.5 Let $\eta$ be a character of $\text{Gal}(L_n/K_n)$ and $f \in \Lambda$ which is coprime to $p$. Then we have
\[ e_\eta C(E[p^m]/L_n)_f \cong C(E[p^m]|(\bar{\eta})_f/K_n). \]

Proof This follows from a straightforward verification by making use of Lemmas 2.5 and 3.1. $\square$

The following lemma is the main calculation that will be needed in the eventual proof of our main theorem.

Lemma 3.6 For a character $\eta$ of $\text{Gal}(L_n/K_n)$ and $f \in \Lambda$ which is coprime to $p$, we have
\[ \frac{|C(E[p^m]|(\bar{\eta})_f/K_n)|}{|H^1(K_n, E[p^m]|(\eta)_f)|} = \frac{|H^2(K_n, E[p^m]|(\bar{\eta})_f)|}{|H^1(K_n, E[p^m]|(\eta)_f)|} = \frac{1}{|E(K_n)|^{p^m}|(\bar{\eta})_f|^{1/|K_n:Q_p|}}p^{-m|K_n:Q_p| \deg(f)}. \]

Proof By the local Euler characteristics formula (cf. [17, Theorem 7.3.1]), we have
\[ \frac{|H^2(K_n, E[p^m]|(\bar{\eta})_f)|}{|H^1(K_n, E[p^m]|(\eta)_f)|} = \frac{1}{|H^0(K_n, E[p^m]|(\bar{\eta})_f)|} \frac{|E(p^m)|(\bar{\eta})_f|^{-|K_n:Q_p|}}{p^{-2m|K_n:Q_p| \deg(f)}}. \]
On the other hand, by Lemma 3.5, we have a commutative diagram
\[
\begin{array}{c}
0 \to C(E[p^m]|(\bar{\eta})_f/K_n) \to H^1(K_n, E[p^m]|(\eta)_f) \\
\downarrow \quad \downarrow \\
H^1(K_n, E[p^m]|(\bar{\eta})_f) \to H^1(K_n, E[p^\infty]|(\eta)_f)|p^m| \to 0 \\
\end{array}
\]
with exact rows, where the surjectivity of the rightmost arrow on the top row follows from the fact that the rightmost arrow on the bottom row and the middle vertical map are surjective. By the snake lemma, we then have a short exact sequence
\[ 0 \to E(K_n)|p^\infty|(\bar{\eta})_f/p^m \to C(E[p^m]|(\bar{\eta})_f/K_n) \to (\im \theta_n)_{\div}[p^m] \to 0 \]
which in turn yields an equality
\[ |C(E[p^m]|(\bar{\eta})_f/K_n)| = |E(K_n)|^{p^\infty}|(\bar{\eta})_f/p^m||(\im \theta_n)_{\div}[p^m]|. \]
We now calculate $|\text{im} \theta_n|_{\text{div}}[p^m]$. To do this, we see that there is an exact sequence
\[ \tilde{E}(K_n)[p^\infty](\bar{\eta}) \rightarrow H^1(K_n, \tilde{E}[p^\infty](\bar{\eta}) \rightarrow H^1(K_n, E[p^\infty](\bar{\eta})]. \]
Since $\tilde{E}(K_n)[p^\infty](\bar{\eta})$ is finite, it follows that
\[ \text{corank}_{\mathbb{Z}_p}(\text{im} \theta_n)_{\text{div}} = \text{corank}_{\mathbb{Z}_p}(\text{im} \theta_n) = \text{corank}_{\mathbb{Z}_p} H^1(K_n, \tilde{E}[p^\infty](\bar{\eta})]. \]
By [4, p. 111, Formula (23)], the latter quantity is precisely $|K_n : \mathbb{Q}_p| \text{corank}_{\mathbb{Z}_p} \tilde{E}[p^\infty](\bar{\eta}) = |K_n : \mathbb{Q}_p| \deg f$. Hence we obtain $|\text{im} \theta_n|_{\text{div}}[p^m]| = p^m|K_n : \mathbb{Q}_p| \deg f$. Combining all the calculations, we obtain the desired formula of the lemma.

### 3.3 Supersingular Reduction at $p$

In this subsection, $K$ will denote a finite unramified extension of $\mathbb{Q}_p$. Let $E$ be an elliptic curve defined over $\mathbb{Q}_p$ which is assumed to have supersingular reduction with $a_p = 0$. Set $L_n = K(\mu_{p^n+1})$ and $L_\infty = \bigcup n L_n$. Write $\Gamma_n = \text{Gal}(L_\infty/L_n)$ for $n \geq 0$. We may identify $\text{Gal}(L/K)$ with a subgroup of $\text{Gal}(L_n/K)$ for every $n = 1, \ldots, \infty$. We then write $K_n$ for the fixed field of this subgroup.

**Lemma 3.7** Retain settings as above. Then $\tilde{E}(L_n)$ and $E(L_n)$ have no $p$-torsion for every $n \geq -1$.

**Proof** The first assertion follows from [13, Proposition 3.1]. The second follows from the first, the following short exact sequence
\[ 0 \rightarrow \tilde{E}(L_n) \rightarrow E(L_n) \rightarrow \tilde{E}(\mathbb{F}_p^\ell) \rightarrow 0 \]
and that $\tilde{E}(\mathbb{F}_p^\ell)$ has no $p$-torsion by the supersingular assumption.

**Lemma 3.8** Let $\eta$ be a character of $\text{Gal}(L_n/K_n)$ and $f$ a Weierstrass polynomial in $\Lambda$. Then $\tilde{E}(K_n)[p^\infty](\eta) = 0$ for every $n \geq 0$.

**Proof** This is immediate from Lemma 3.7.

Following [9–14], we define the following groups
\[ E^+(L_n) = \{ P \in \tilde{E}(L_n) : \text{tr}_{n/m+1}(P) \in \tilde{E}(L_m), \ 2 \mid m, \ 0 \leq m \leq n - 1 \}, \]
\[ E^-(L_n) = \{ P \in \tilde{E}(L_n) : \text{tr}_{n/m+1}(P) \in \tilde{E}(L_m), \ 2 \nmid m, \ -1 \leq m \leq n - 1 \}, \]
where $\text{tr}_{n/m+1} : E(L_n) \rightarrow E(L_{m+1})$ denotes the trace map and $L_{-1}$ is understood to be $K$.

We also write
\[ \delta = \begin{cases} 0, & \text{if } |K : \mathbb{Q}_p| \not\equiv 0 \text{ (mod 4)} \text{ or } \eta \neq 1, \\ 2, & \text{otherwise}. \end{cases} \]

**Proposition 3.9** Retain settings as above. The following statements are then valid.

(a) $(\tilde{E}^+(L_\infty)^n \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}$ are cofree $\mathbb{Z}_p$-modules for all $n$, and
\[ \text{corank}_{\mathbb{Z}_p}(\tilde{E}^+(L_\infty)^n \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}) = \begin{cases} |K : \mathbb{Q}_p|^0 + \delta, & \text{if } s = +, \\ |K : \mathbb{Q}_p|^0, & \text{if } s = - \end{cases} \]

(b) One has
\[ (\tilde{E}^+(L_\infty)^n \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \cong \begin{cases} \mathbb{Z}_p[[X]]^\oplus d \oplus \mathbb{Z}_p^\delta, & \text{if } s = +, \\ \mathbb{Z}_p[[X]]^\oplus d, & \text{if } s = - \end{cases} \]
Lemma 3.12

Writing our main theorem.

Corollary 3.11

In other words, we have short exact sequences

\[ H^1(L_n, E[p^\infty]) \cong H^1(L_\infty, E[p^\infty])^\Gamma_n. \]

Via this isomorphism, we may view \( \mathbb{H}_n^\pm \) as a subgroup of \( H^1(L_n, E(p)) \). Let \( M_n^\pm \) be the exact annihilator of \( \mathbb{H}_n^\pm \) with respect to the local Tate pairing

\[ H^1(L_n, E[p^\infty]) \times H^1(L_n, T_pE) \to \mathbb{Q}_p/\mathbb{Z}_p. \]

In other words, we have short exact sequences

\[ 0 \to \mathbb{H}_n^\pm[p^m] \to H^1(L_n, E[p^\infty])[p^m] \to (M_n^\pm[p^m])^\vee \to 0, \]

\[ 0 \to M_n^\pm[p^m] \to H^1(L_n, T_pE)[p^m] \to (\mathbb{H}_n^\pm[p^m])^\vee \to 0. \]

Since \( \mathbb{H}_n^\pm \) is divisible by Proposition 3.9 (a), it follows that there are two short exact sequences

\[ 0 \to \mathbb{H}_n^\pm[p^m] \to H^1(L_n, E[p^\infty])[p^m] \to (M_n^\pm[p^m])^\vee \to 0, \]

\[ 0 \to M_n^\pm[p^m] \to H^1(L_n, T_pE)[p^m] \to (\mathbb{H}_n^\pm[p^m])^\vee \to 0. \]

By appealing to Lemma 3.7 again, one has \( H^1(L_n, E[p^\infty])[p^m] \cong H^1(L_n, E[p^m]) \) and \( H^1(L_n, T_pE)[p^m] \cong H^1(L_n, E[p^m]) \). Combining this with the above short exact sequences, we see that \( M_n^\pm[p^m] \) is the exact annihilator of \( \mathbb{H}_n^\pm[p^m] \) with respect to the local Tate pairing

\[ H^1(L_n, E[p^m]) \times H^1(L_n, E[p^m]) \to \mathbb{Z}/p^m. \]

In fact, one even has the following.

Proposition 3.10 (Kim) One always has \( \mathbb{H}_n[p^m] = M_n^-/p^m \). In other words, \( \mathbb{H}_n[p^m] \) is the exact annihilator of itself with respect to the local Tate pairing

\[ H^1(L_n, E[p^m]) \times H^1(L_n, E[p^m]) \to \mathbb{Z}/p^m. \]

If \( |K : \mathbb{Q}_p| \) is not divisible by 4, we then have the same conclusion for \( \mathbb{H}_n^+[p^m] \).

Proof The first assertion is established by Kim in [9, Proposition 3.15]. One can check that the same proof carries over for the second assertion under the assumption that \( |K : \mathbb{Q}_p| \) is not divisible by 4 (also see [11, Proposition 3.4] or [12, Theorem 2.9]).

Corollary 3.11 Write \( K_n = L_n^G \). Then \( \mathbb{H}_n[p^m][\tilde{\eta}][\tilde{f}] \) is the orthogonal complement to \( \mathbb{H}_n[p^m][\tilde{\eta}][\tilde{f}] \), with respect to the perfect pairing

\[ H^1(K_n, E[p^m](\tilde{\eta})_f) \times H^1(K_n, E[p^m](\tilde{\eta})_f) \to \mathbb{Z}/p^m. \]

If \( |K : \mathbb{Q}_p| \) is not divisible by 4, we then have the same conclusion with \( \mathbb{H}_n^+[p^m][\tilde{\eta}][\tilde{f}] \) and \( \mathbb{H}_n^+[p^m][\tilde{\eta}][\tilde{f}] \).

Proof This follows from a combination of Lemma 3.2 and Proposition 3.10.

We end the subsection with a preliminary calculation which will be required in the proof of our main theorem.

Lemma 3.12 Writing \( K_n = L_n^G \), we have

\[ \frac{|\mathbb{H}_n[p^m][\tilde{\eta}]|}{|H^1(K_n, E[p^m](\tilde{\eta})_f)|} = p^{-m|K_n : \mathbb{Q}_p| \text{deg}(f)}. \]
If \(|K : \mathbb{Q}_p|\) is not divisible by 4, we have the same conclusion with \(\mathbb{H}^+_{\mu}[p^m]_{\eta}\).

**Proof** By the local Euler characteristics formula (cf. [17, Theorem 7.3.1]), we have

\[
\frac{|H^2(K_n, E[p^m](\bar{\eta})_f)|}{|H^1(K_n, E[p^m](\bar{\eta})_f)|} = \frac{1}{|H^0(K_n, E[p^m](\bar{\eta})_f)|} |E[p^m](\bar{\eta})_f|^{-|K_n : \mathbb{Q}_p|} = p^{-2m|K_n : \mathbb{Q}_p| \deg(f)},
\]

where the final equality follows from Lemma 3.8. Now observe that

\[
\mathbb{H}^+_{\mu}[p^m]_{\eta} = (e_\eta(\hat{E}(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n})_f = ((\hat{E}(L_\infty)^{\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n})_f
\]

By Proposition 3.9 (a) (and assuming that \(|K : \mathbb{Q}_p|\) is not divisible by 4 in the + case), the latter has size \(p^{m|K : \mathbb{Q}_p| \deg(f)}\). The conclusion of the lemma now follows from these calculations. □

### 3.4 Away from \(p\)

In this subsection, \(l\) is a prime \(\neq p\). Let \(K\) be a finite extension of \(\mathbb{Q}_l\), and write \(L = K(\mu_p)\). Denote by \(G\) the Galois group \(\text{Gal}(L/K)\) which has order dividing \(p-1\). Let \(K_\infty\) be the cyclotomic \(\mathbb{Z}_p\)-extension of \(K\). We write \(L_\infty = K_\infty L\) which is the cyclotomic \(\mathbb{Z}_p\)-extension of \(L\). Similarly as before, we identify the completed group algebras \(\mathbb{Z}_p[[\text{Gal}(L_\infty/L)]] = \mathbb{Z}_p[[\text{Gal}(K_\infty/K)]] = \Lambda\) and identify the Galois groups \(\text{Gal}(L_n/K_n)\) with \(\text{Gal}(L/K)\) for every \(n\).

For any discrete \(\text{Gal}(K/K)-\)module \(M\) and algebraic extension \(K\) of \(K\), we write \(H^1_{ur}(K, M)\) for the kernel of the map

\[
H^1(K, M) \to H^1(K^{ur}, M),
\]

where \(K^{ur}\) is the maximal unramified extension of \(K\). Via the inflation-restriction sequence, \(H^1_{ur}(K, M)\) identifies with \(H^1(\text{Gal}(K^{ur}/K), M(\mathcal{K}^{ur}))\).

Now let \(E\) denote an elliptic curve over \(K\). Let \(\eta\) be a character of \(\text{Gal}(L_n/K_n)\) and \(f\) a Weierstrass polynomial in \(\Lambda\).

**Lemma 3.13** We have \(e_\eta H^1_{ur}(L_n, E[p^m])_f = H^1_{ur}(K_n, E[p^m](\bar{\eta})_f)\) and

\[
\frac{|H^1_{ur}(K_n, E[p^m](\bar{\eta})_f)|}{|H^0(K_n, E[p^m](\bar{\eta})_f)|} \frac{|H^2(K_n, E[p^m](\bar{\eta})_f)|}{|H^1(K_n, E[p^m](\bar{\eta})_f)|} = 1.
\]

**Proof** The first equality follows from Lemmas 2.5 and 3.1. Local Euler characteristics formula (cf. [17, Theorem 7.3.1]) then tells us that

\[
\frac{|H^0(K_n, E[p^m](\bar{\eta})_f)|}{|H^1(K_n, E[p^m](\bar{\eta})_f)|} \frac{|H^2(K_n, E[p^m](\bar{\eta})_f)|}{|H^1(K_n, E[p^m](\bar{\eta})_f)|} = 1.
\]

Finally, one checks easily by definition that \(H^0(K_n, E[p^m](\bar{\eta})_f) = H^1_{ur}(K_n, E[p^m](\bar{\eta})_f)\). This proves the second equality. □

**Lemma 3.14** Fix a character \(\eta\) of \(\text{Gal}(L_n/K_n)\) and \(f \in \Lambda\) which is coprime to \(p\). Then \(H^1_{ur}(K_n, E[p^m](\bar{\eta})_f)\) is orthogonal to \(H^1_{ur}(K_n, E[p^m](\bar{\eta})_f)\) under the perfect pairing

\[
H^1(K_n, E[p^m](\bar{\eta})_f) \times H^1(K_n, E[p^m](\bar{\eta})_f) \to \mathbb{Q}_p/\mathbb{Z}_p.
\]

**Proof** It is well-known that \(H^1_{ur}(L_n, E[p^m])\) is orthogonal to itself under the perfect pairing

\[
H^1(L_n, E[p^m]) \times H^1(L_n, E[p^m]) \to \mathbb{Q}_p/\mathbb{Z}_p
\]

(for instance, see [4, p.113]). The conclusion of the lemma now follows from Lemmas 3.2 and 3.13. □
4 Mixed Signed Selmer Groups

4.1 Main Result

As a start, we recall the definition of the signed Selmer group [9–14]. Let \( F' \) be a number field and \( E \) an elliptic curve defined over \( F' \). Let \( F \) be a finite extension of \( F' \). Denote by \( \Sigma_p \) for the set of primes of \( F \) lying above \( p \). We shall also write \( \Sigma_p^{\text{ord}} \) (resp., \( \Sigma_p^{\text{ss}} \)) for the set of primes in \( \Sigma_p \) at which \( E \) has good ordinary reduction (resp., good supersingular reduction). The following assumptions will be in full force throughout the paper.

(S1) The elliptic curve \( E \) has good reduction at all primes of \( F' \) above \( p \), and at least one of which is a supersingular reduction prime of \( E \).

(S2) For each \( u \) of \( F' \) above \( p \) at which the elliptic curve \( E \) has supersingular reduction, assume that the following statements are valid.

(a) \( F'_u = \mathbb{Q}_p \).
(b) \( a_u = 1 + p - |\tilde{E}_u(F_p)| = 0 \), where \( \tilde{E}_u \) is the reduction of \( E \) at \( u \).
(c) \( u \) is unramified in \( F/F' \).

Denote by \( \mathcal{F}_n = F(p_{n+1}) \) and \( \mathcal{F}_\infty = \bigcup_n \mathcal{F}_n \). By (S1)–(S2), \( \text{Gal}(\mathcal{F}_0/F) \cong \mathbb{Z}_p/(p - 1) \) and every supersingular prime of \( E \) above \( p \) is totally ramified in \( \mathcal{F}_\infty/F \). Thus, we have \( \text{Gal}(\mathcal{F}_\infty/F) \cong \text{Gal}(\mathcal{F}_\infty/\mathcal{F}_0) \times \text{Gal}(\mathcal{F}_0/F) \cong \mathbb{Z}_p \times \mathbb{Z}/(p - 1) \mathbb{Z} \). We shall write \( \Gamma_n = \text{Gal}(\mathcal{F}_\infty/\mathcal{F}_n) \) and \( G = \text{Gal}(\mathcal{F}_0/F) \). We shall also write \( \Gamma = \Gamma_0 \). By fixing a topological generator of \( \Gamma \), we identify \( \mathbb{Z}_p[[\text{Gal}(\mathcal{F}_\infty/F)]] \) with \( \Lambda[G] \).

It follows from (S1) and (S2) that for each prime \( v \) of \( F \) above \( p \) at which \( E \) has supersingular reduction, there is a unique prime of \( \mathcal{F}_n \) lying above the said prime which, by abuse of notation, is still denoted by \( v \). For such a \( v \), we choose a sign \( s_v \) for it and write \( \overline{s} = (s_v)_{v \in \Sigma^{ss}} \in \{\pm\}^{\Sigma^{ss}} \). For each \( s_v \), define \( E^{s_v}(\mathcal{F}_{n,v}) \) as in Subsection 3.3. The mixed signed Selmer group is then given by

\[
\text{Sel}^{-\overline{s}}(E/\mathcal{F}_n) := \ker \left( H^1(\mathcal{F}_n, E[p^{\infty}]) \to \bigoplus_{w \in \Sigma^{ss}(\mathcal{F}_n)} H^1(\mathcal{F}_{n,w}, E[p^{\infty}]) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right) \times \bigoplus_{w \in \Sigma^{\text{ord}}(\mathcal{F}_n)} H^1(\mathcal{F}_{n,w}, E[p^{\infty}]) \otimes \mathbb{Q}_p/\mathbb{Z}_p \bigoplus_{w \in \Sigma} H^1(\mathcal{F}_{n,w}, E[p^{\infty}]) \big) \).
\]

Define \( \text{Sel}^{-\overline{s}}(E/\mathcal{F}_\infty) \) as \( \lim_n \text{Sel}^{-\overline{s}}(E/\mathcal{F}_n) \). Denote by \( \text{X}^{-\overline{s}}(E/\mathcal{F}_\infty) \) the Pontryagin dual of \( \text{Sel}^{-\overline{s}}(E/\mathcal{F}_\infty) \). It is not difficult to verify that this is finitely generated over \( \mathbb{Z}_p[[\Gamma]] \). In fact, one expects the following conjecture which is a natural extension of Mazur [16] and Kobayashi [14].

**Conjecture** \( X^{-\overline{s}}(E/\mathcal{F}_\infty) \) is a torsion \( \mathbb{Z}_p[[\Gamma]] \)-module.

When \( E \) has good ordinary reduction at all primes above \( p \), the above conjecture is precisely Mazur’s conjecture [16] which is known in the case when \( E \) is defined over \( \mathbb{Q} \) and \( F \) an abelian extension of \( \mathbb{Q} \) (see [8]). For an elliptic curve over \( \mathbb{Q} \) with good supersingular reduction at \( p \), this conjecture was established by Kobayashi (cf. [14]; also see [2] for some recent progress on this conjecture).

From now on, let \( \Sigma \) denote a fixed finite set of primes of \( F \) containing those above \( p \), the ramified primes of \( F/F' \) and all the bad reduction primes of \( E \). Write \( F_\Sigma \) for the maximal algebraic extension of \( F \) which is unramified outside \( \Sigma \). For any (possibly infinite) extension
Define Sel

Proof

\[ \text{Sel}^\infty(E/F_\infty) = \ker \left( H^1(G_\Sigma(F_\infty), E[p^\infty]) \to \bigoplus_{w \in \Sigma_{SS}(F_\infty)} H^1(F_{\infty,w}, E[p^\infty]) \right) \]

\[ \times \bigoplus_{w \in \Sigma_{ord}(F_\infty)} H^1(F_{\infty,w}, E[p^\infty]) \bigoplus_{w \in \Sigma_{ur}(F_\infty)} H^1(F_{\infty,w}, E[p^\infty]) \].

We can now state our main results.

**Theorem 4.1** Let \( \eta \) be a character of \( G = \text{Gal}(F(\mu_p)/F) \). For each \( v \in \Sigma_{SS} \) with \( s_v = + \), assume further that \( |F_v : Q_p| \) is not divisible by 4. We then have that

\[ \text{rank}_\Lambda(e_\eta X^{\infty}(E/F_\infty)) = \text{rank}_\Lambda(e_\eta X^{\infty}(E/F_\infty)^i), \]

and that the torsion \( \Lambda \)-submodules of \( e_\eta X^{\infty}(E/F_\infty) \) and \( e_\eta X^{\infty}(E/F_\infty)^i \) are pseudo-isomorphic.

**Corollary 4.2** Retain the setting of Theorem 4.1. Then the following statements are valid.

(a) \( e_\eta X^{\infty}(E/F_\infty) \) is torsion over \( \Lambda \) if and only if \( e_\eta X^{\infty}(E/F_\infty) \) is torsion over \( \Lambda \).

(b) \( e_\eta X^{\infty}(E/F_\infty) = 0 \) if and only if \( e_\eta X^{\infty}(E/F_\infty) = 0 \).

The proof of the theorem will be given in Subsection 4.3 and the proof of the corollary will be given in Subsection 4.4.

### 4.2 Strict Signed Selmer Groups

To prove our main result, we need to work with the so-called strict signed Selmer groups. The strict signed Selmer group of \( E \) over \( F_n \) is defined by

\[ \text{Sel}^\infty, \text{str}(E/F_n) := \ker \left( H^1(G_\Sigma(F_n), E[p^\infty]) \to \bigoplus_{w \in \Sigma_{SS}(F_n)} H^1(F_{n,w}, E[p^\infty]) \right), \]

where

\[ C_w(E[p^\infty]/F_n) = \begin{cases} 
(E^\ast_w(F_{\infty,w}) \otimes Q_p/Z_p)^{\Gamma_n}, & \text{if } w \in \Sigma_p(F_n), \\
(\text{im}(H^1(F_{n,w}, E[p^\infty]) \to H^1(F_{\infty,w}, E[p^\infty])))_{\text{div}}, & \text{if } w \in \Sigma_{\text{ord}}(F_n), \\
H^1(F_{n,w}, E[p^\infty]), & \text{if } w \nmid p.
\end{cases} \]

Define \( \text{Sel}^\infty, \text{str}(E/F_\infty) := \varprojlim_n \text{Sel}^\infty, \text{str}(E/F_n) \).

Note that in the case when \( \Sigma_{SS} = \emptyset \), this is the strict Selmer group as defined in the sense of Greenberg [4] (also see [6]). Our choice of naming the above as the strict signed Selmer group is inspired by this observation. In general, this strict Selmer group does not need to agree with the signed Selmer group on the intermediate level \( F_n \). But they do coincide upon taking limit which is the content of the next proposition.

**Proposition 4.3** We have an identification \( \text{Sel}^\infty, \text{str}(E/F_\infty) \cong \text{Sel}^\infty(E/F_\infty) \).

**Proof** By [3, Proposition 4.5], we have \( C_w(E[p^\infty]/F_n) = E(F_{n,w}) \otimes Q_p/Z_p \) for all \( w \in \Sigma_p(F_n) \) and so the local condition at \( \Sigma_p(F_n) \) for the strict signed Selmer group and the signed Selmer group at each \( F_n \) (and hence \( F_\infty \)) are the same. Similarly, one has the same conclusion for primes in \( S_p(F_{\text{cyc}}) \). Let \( w \) be a prime \( \Sigma_p^{\infty} \). Recall that we also write \( w \) for the prime of \( F_\infty \) above \( w \). In general, \( (E^\ast_w(F_{\infty,w}) \otimes Q_p/Z_p)^{\Gamma_n} \) and \( E^\ast_w(F_{n,w}) \otimes Q_p/Z_p \) do not
need to agree (one can see this by comparing their \( \mathbb{Z}_p \)-coranks). But upon taking limit, they are both equal to \( E^{sw}(\mathcal{F}_{\infty, w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \). In conclusion, we have established our assertion. \( \square \)

We now show that this strict signed Selmer group enjoys a control theorem parallel to that in the ordinary situation (see [5, 16]; also see [12, 14]).

**Proposition 4.4** There is an injection

\[
\text{Sel}^{\natural, \text{str}}(E/\mathcal{F}_n) \to \text{Sel}^{\natural}(E/\mathcal{F}_\infty)^{\Gamma_n}
\]

with finite cokernel which is bounded independent of \( n \).

**Proof** Consider the following diagram

\[
\begin{array}{cccccc}
0 & \longrightarrow & \text{Sel}^{\natural, \text{str}}(E/\mathcal{F}_n) & \longrightarrow & H^1(G_\Sigma(\mathcal{F}_n), E[p^\infty]) & \longrightarrow \bigoplus_{w \in \Sigma(\mathcal{F}_n)} H^1(\mathcal{F}_{n, w}, E[p^\infty]) \\
 & & \downarrow & & \downarrow & \\
0 & \longrightarrow & \text{Sel}^{\natural, \text{str}}(E/\mathcal{F}_\infty)^{\Gamma_n} & \longrightarrow & H^1(G_\Sigma(\mathcal{F}_\infty), E[p^\infty])^{\Gamma_n} & \longrightarrow \bigoplus_{w \in \Sigma(\mathcal{F}_\infty)} H^1(\mathcal{F}_{\infty, w}, E[p^\infty])^{\Gamma_n}
\end{array}
\]

with exact rows. Now the middle vertical map is surjective with kernel \( H^1(\Gamma_n, E(\mathcal{F}_\infty)[p^\infty]) \). By Lemma 3.7 and (S1), this kernel is trivial. Hence it remains to show that the rightmost vertical map has finite kernel which is bounded independent of \( n \). For primes in \( \Sigma_p^{\text{ord}} \) and primes not dividing \( p \), this is established in the mist of proving the control theorem in the ordinary case (for instance, see [5, Theorem 1.2 and Section 3]). It therefore remains to consider the primes in \( \Sigma_p^{\text{ss}} \). By our definition of \( C_w(E[p^\infty]/\mathcal{F}_n) \), we have

\[
C_w(E[p^\infty]/\mathcal{F}_n) = (E^{sw}(\mathcal{F}_{\infty, w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n} = C_w(E[p^\infty]/\mathcal{F}_\infty)^{\Gamma_n}
\]

and hence the map is injective for these primes. \( \square \)

We now define mod-\( p^m \) strict signed Selmer group on the level of \( F_n \). This is given by

\[
\text{Sel}^{\natural, \text{str}}(E[p^m]/\mathcal{F}_n) := \ker \left( H^1(G_\Sigma(\mathcal{F}_n), E[p^m]) \to \bigoplus_{w \in \Sigma^{\text{ss}}(\mathcal{F}_n)} H^1(\mathcal{F}_{n, w}, E[p^m]) \right),
\]

where

\[
C_w(E[p^m]/\mathcal{F}_n) = \begin{cases} 
(E^{sw}(\mathcal{F}_{\infty, w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}[p^m], & \text{if } w \in \Sigma_p^{\text{ss}}(\mathcal{F}_n), \\
\ker \left( H^1(\mathcal{F}_{n, w}, E[p^m]) \to H^1(\mathcal{F}_{n, w}, E[p^{\infty}]) \right), & \text{if } w \in \Sigma_p^{\text{ord}}(\mathcal{F}_n), \\
H^1_{\text{ur}}(\mathcal{F}_{n, w}, E[p^m]), & \text{if } w \nmid p.
\end{cases}
\]

**Proposition 4.5** The kernel and cokernel of the map

\[
\text{Sel}^{\natural, \text{str}}(E[p^m]/\mathcal{F}_n) \to \text{Sel}^{\natural, \text{str}}(E/\mathcal{F}_n)[p^m]
\]

are finite and bounded independent of \( m \) and \( n \).
Proof. Consider the following diagram

\[
\begin{array}{ccccccc}
0 & \rightarrow & \text{Sel}^{\overline{\eta}, \mathrm{str}}(E[p^m]/\mathcal{F}_n) & \rightarrow & H^1(G_{\Sigma}(\mathcal{F}_n), E[p^m]) & \rightarrow & \bigoplus_{w \in \Sigma(\mathcal{F}_n)} \frac{H^1(F_{n,w}, E[p^m])}{C_w(E[p^m]/\mathcal{F}_n)} \\
0 & \rightarrow & \text{Sel}^{\overline{\eta}, \mathrm{str}}(E/\mathcal{F}_n)[p^m] & \rightarrow & H^1(G_{\Sigma}(\mathcal{F}_n), E[p^\infty])[p^m] & \rightarrow & \bigoplus_{w \in \Sigma(\mathcal{F}_n)} \frac{H^1(F_{n,w}, E[p^\infty])}{C_w(E[p^\infty]/\mathcal{F}_n)} [p^m]
\end{array}
\]

with exact rows. By appealing to Lemma 3.7, one can show that the middle map is an isomorphism. It remains to show that the rightmost map is finite and bounded independent of \(n\) and \(\eta\). By a similar argument to that in Lemma 3.1, we have

\[
\begin{align*}
&H^1(G_{\Sigma}(\mathcal{F}_n), E[p^\infty]) \\
&\cong \bigoplus_{w \in \Sigma(\mathcal{F}_n)} \frac{H^1(F_{n,w}, E[p^\infty])}{C_w(E[p^\infty]/\mathcal{F}_n)} [p^m]
\end{align*}
\]

4.3 Proof of Theorem 4.1

This subsection is devoted to proving Theorem 4.1. As a start, we determine \(e_\eta \text{Sel}^{\overline{\eta}, \mathrm{str}}(E/\mathcal{F}_\infty)_f\) for a character \(\eta\) of \(G = \text{Gal}(F(\mu_p)/F)\) and a power series \(f \in \Lambda\) which is not divisible by \(p\).

For the remainder of the paper, we write \(F_n = \mathcal{F}_n^G\) and \(F_\infty = \bigcup_n F_n\). Note that \(F_\infty\) is precisely the cyclotomic \(\mathbb{Z}_p\)-extension of \(F\).

Lemma 4.6 For a character \(\eta\) of \(G = \text{Gal}(F(\mu_p)/F)\) and a power series \(f \in \Lambda\) which is not divisible by \(p\), we have

\[
e_\eta \text{Sel}^{\overline{\eta}, \mathrm{str}}(E/\mathcal{F}_\infty)_f \cong \ker \left( H^1(G_{\Sigma}(\mathcal{F}_n), E[p^\infty]|(\overline{\eta})_f) \rightarrow \bigoplus_{w \in \Sigma(\mathcal{F}_\infty)} \frac{H^1(F_{n,w}, E[p^\infty]|(\overline{\eta})_f)}{C_w(E[p^\infty]|(\overline{\eta})_f/F_n)} \right),
\]

where

\[
C_w(E[p^\infty]|(\overline{\eta})_f/F_n) = \begin{cases} (E^{ss}(\mathcal{F}_\infty)_w)^{\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n} & \text{if } w \in \Sigma^p(F_\infty), \\
(\text{im} \left( H^1(F_{n,w}, E[p^\infty]|(\overline{\eta})_f) \rightarrow H^1(F_{n,w}, E[p^\infty]|(\overline{\eta})_f) \right))_{\text{div}} & \text{if } w \in \Sigma^\text{ord}(F_\infty), \\
H^1_{\text{ur}}(F_{n,w}, E[p^\infty]|(\overline{\eta})_f) & \text{if } w \nmid p,
\end{cases}
\]

and

\[
e_\eta \text{Sel}^{\overline{\eta}, \mathrm{str}}(E[p^m]/\mathcal{F}_n)_f \cong \ker \left( H^1(G_{\Sigma}(\mathcal{F}_n), E[p^m]|(\overline{\eta})_f) \rightarrow \bigoplus_{w \in \Sigma(\mathcal{F}_\infty)} \frac{H^1(F_{n,w}, E[p^m]|(\overline{\eta})_f)}{C_w(E[p^m]|(\overline{\eta})_f/F_n)} \right),
\]

where

\[
C_w(E[p^m]|(\overline{\eta})_f/F_n) = \begin{cases} (E^{ss}(\mathcal{F}_n)_w)^{\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n} [p^m] & \text{if } w \in \Sigma^p(F_n), \\
\ker \left( H^1(F_{n,w}, E[p^m]|(\overline{\eta})_f) \rightarrow H^1(F_{n,w}, E[p^\infty]|(\overline{\eta})_f)/C_w(E[p^\infty]|(\overline{\eta})_f/F_n) \right) & \text{if } w \in \Sigma^\text{ord}(F_n), \\
H^1_{\text{ur}}(F_{n,w}, E[p^m]|(\overline{\eta})_f) & \text{if } w \nmid p.
\end{cases}
\]

Proof. By a similar argument to that in Lemma 3.1, we have \(e_\eta H^1(G_{\Sigma}(\mathcal{F}_n), E[p^\infty])_f \cong H^1(G_{\Sigma}(\mathcal{F}_n), E[p^\infty]|(\overline{\eta})_f)\). It therefore remains to show that the \(e_\eta\)-component of the local
condition in the definition of the signed Selmer group \( \text{Sel}^\pi, \text{str}(E/F) \) coincides with \( C_w(E[p^\infty](\bar{\eta})_f / F_\infty) \). This follows from a direct verification noting Lemmas 2.5, 3.5 and 3.14. □

**Remark 4.7** We have set up our notation in a way so that for each \( w \in \Sigma(F_n) \), one has

\[
e_\eta \left( \bigoplus_{u \in \Sigma(F_n), u | w} C_u(E[p^\infty]/F_n) \right) = C_w(E[p^\infty](\bar{\eta})_f / F_n)
\]

and

\[
e_\eta \left( \bigoplus_{u \in \Sigma(F_n), u | w} C_u(E[p^m]/F_n) \right) = C_w(E[p^m](\bar{\eta})_f / F_n).
\]

**Proposition 4.8** For a character \( \eta \) of \( G = \text{Gal}(F(\mu_p)/F) \) and a power series \( f \in \Lambda \) which is not divisible by \( p \), we have

\[
\frac{|e_\eta \text{Sel}^\pi, \text{str}(E/F_n)f|}{|e_\eta \text{Sel}^\pi, \text{str}(E/F_n)f'|} = \prod_{w \in \Sigma_p^{ord}(F_n)} \frac{|E(F_{n,w})|_{p^\infty}(\bar{\eta})_f / p^m|}{|E(F_{n,w})|_{p^m}(\bar{\eta})_f / p^m|}.
\]

Furthermore, the expression on the right is bounded independent of \( m \) and \( n \) (for a fixed \( f \)).

**Proof** Each term on the right is bounded independent of \( m \) and \( n \) (for a fixed \( f \)) by Lemma 3.3. But since \( F_\infty/F \) is the cyclotomic \( \mathbb{Z}_p \)-extension, there are only finite number of primes in \( \Sigma_p^{ord}(F_\infty) \). Hence the expression on the right is bounded independent of \( m \) and \( n \) (for a fixed \( f \)). It therefore remains to prove the equality as asserted in the proposition. In view of Corollary 3.11, Lemmas 3.4 and 3.14, the local conditions \( C_w(E[p^m](\bar{\eta})_f / F_n) \) and \( C_w(E[p^m](\bar{\eta})_f / F_n) \) are orthogonal complement to each other. Thus, by a Poitou–Tate duality argument (for instance, see [4, p. 125] or [10, p. 89]), we have

\[
\frac{|e_\eta \text{Sel}^\pi, \text{str}(E/F_n)f|}{|e_\eta \text{Sel}^\pi, \text{str}(E/F_n)f'|} = \prod_{w \in \Sigma_p^{ord}(F_n)} \frac{|H^1(G_\Sigma(F_n), E[p^m](\bar{\eta})_f)|}{|H^2(G_\Sigma(F_n), E[p^m](\bar{\eta})_f)|} \frac{|C(E[p^m](\bar{\eta})_f / F_n)|}{|H^1(F_n, E[p^m](\bar{\eta})_f)|},
\]

where in the calculation, we have made use of the fact that \( H^0(G_\Sigma(F_n), E[p^m](\bar{\eta})_f) = 0 \) (which is a consequence of Lemma 3.8). Again, taking Lemma 3.8 into account, the global Euler characteristic formula tells us that

\[
\frac{|H^1(G_\Sigma(F_n), E[p^m](\bar{\eta})_f)|}{|H^2(G_\Sigma(F_n), E[p^m](\bar{\eta})_f)|} = p^{r_1(F_n)+2r_2(F_n)m \text{ deg}(f)} = p^{[F_n: \mathbb{Q}]m \text{ deg}(f)},
\]

where \( r_1(F_n) \) (resp., \( r_2(F_n) \)) is the number of real places of \( F_n \) (resp., number of pairs of complex places of \( F_n \)). The required formula now follows from combining this calculation with Lemmas 3.6, 3.12 and 3.13. □

We can now prove the main theorem of the paper.

**Proof of Theorem 4.1** We shall verify that the hypotheses of Proposition 2.3 are satisfied. By virtue of Proposition 4.3, we are reduced to showing that for a fixed \( f \), the quantity

\[
\frac{|(e_\eta \text{Sel}^\pi, \text{str}(E/F_\infty)f)_{\Gamma_n[p^m]|}}{|(e_\eta \text{Sel}^\pi, \text{str}(E/F_\infty)f')_{\Gamma_n[p^m]|}}
\]
is bounded independent of $m$ and $n$. Since $e_\eta(-)_f$ is exact on sequence of $\Lambda[G]$-modules, it follows from Propositions 4.4 and 4.5 that the kernel and cokernel of the maps
\[
e\eta \text{ Sel}^\sim,\text{str}(E/F_n)_{/F_n}[p^m] \to e\eta \text{ Sel}^\sim,\text{str}(E/F_\infty)_{/F_\infty}[p^m],
\]
\[
e\eta \text{ Sel}^\sim,\text{str}(E/p^m)_{/F_n} \to e\eta \text{ Sel}^\sim,\text{str}(E/F_n)_{/F_n}[p^m]
\]
are finite and bounded independent of $m$ and $n$. It follows from this that we are reduced to showing that the quantity
\[
\frac{|e\eta \text{ Sel}^\sim,\text{str}(E/p^m)_{/F_n}|}{|e\eta \text{ Sel}^\sim,\text{str}(E/F_n)_{/F_n}|}
\]
is bounded independent of $m$ and $n$. But this is precisely the assertion of Proposition 4.8. Hence we have completed the proof of our theorem. \(\square\)

4.4 Proof of Corollary 4.2

We retain the setting of the previous subsections. Recall that by Lemmas 4.3 and 4.6, one has
\[
e\eta \text{ Sel}^\sim(E/F_\infty) \cong \ker \left( H^1(G\Sigma(F_\infty), E[p^\infty](\bar{\eta})) \to \bigoplus_{w \in \Sigma(F_\infty)} H^1(F_{\infty,w}, E[p^\infty](\bar{\eta})) C_w(E[p^\infty](\bar{\eta}))/F_\infty \right),
\]
where
\[
C_w(E[p^\infty](\bar{\eta}))/F_\infty = \begin{cases} 
E^\wedge = (F_\infty,\wedge)^\vee \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } w \in \Sigma_p^\text{ss}(F_\infty), \\
\text{im} (H^1(F_\infty,w, E[p^\infty](\bar{\eta})) \to H^1(F_{\infty,w}, E[p^\infty](\bar{\eta}))), & \text{if } w \in \Sigma_p^\text{ord}(F_\infty), \\
0, & \text{if } w \nmid p.
\end{cases}
\]

To continue, we require the following result which is a slight refinement of [11, Theorem 3.14] and [13, Theorem 1.3] (also see [5, Proposition 4.14]).

**Proposition 4.9** If $e\eta \text{ Sel}^\sim(E/F_\infty)$ is cotorsion over $\Lambda$, then $(e\eta \text{ Sel}^\sim(E/F_\infty))^\vee$ has no nontrivial finite $\Lambda$-submodules.

**Proof** Observe that it follows from Lemma 3.8 that one has $E(F_\infty)[p^\infty](\bar{\eta}) = 0$. The conclusion of the proposition will now follow from a similar argument to that in [5, Proposition 4.14] or [11, Theorem 3.14]. \(\square\)

We can now give the proof of Corollary 4.2.

**Proof of Corollary 4.2** The first assertion is immediate from the rank equality of Theorem 4.1. We now proceed proving the second assertion. Suppose that $e\eta X^\sim(E/F_\infty) = 0$. Then by Theorem 4.1, $e\eta X^\sim(E/F_\infty)^\vee$ is a finite $\Lambda$-module, and in particular, a torsion $\Lambda$-module. Thus, we may apply Proposition 4.9 to conclude that $e\eta X^\sim(E/F_\infty)$ has no nontrivial finite $\Lambda$-submodule. It then follows from these observations that $e\eta X^\sim(E/F_\infty) = 0$. \(\square\)

**Acknowledgements** The authors thank the referee for the comments on a previous draft of the paper. The research of this article took place when S. Ahmed was a postdoctoral fellow at Central China Normal University, and he would like to acknowledge the hospitality and conducive working conditions provided by the said institute.
References

[1] Bleher, F., Chinburg, T., Greenberg, R., et al.: Higher Chern classes in Iwasawa theory. Amer. J. Math., 142(2), 627–682 (2020)

[2] Büyükboduk, K., Lei, A.: Integral Iwasawa theory of Galois representations for non-ordinary primes. Math. Z., 286, 361–398 (2017)

[3] Coates, J., Greenberg, R.: Kummer theory for abelian varieties over local fields. Invent. Math., 124, 129–174 (1996)

[4] Greenberg, R.: Iwasawa theory for p-adic representations, In: Algebraic Number Theory–in honor of K. Iwasawa (J. Coates, R. Greenberg, B. Mazur and I. Satake eds.), Adv. Std. in Pure Math. 17, 1989, 97–137

[5] Greenberg, R.: Iwasawa theory for elliptic curves, In: Arithmetic Theory of Elliptic Curves (Cetraro, 1997) (C. Viola ed.), Lecture Notes in Math., Vol. 1716, Springer, Berlin, 1999, 51–144

[6] Guo, L.: On a generalization of Tate dualities with application to Iwasawa theory. Compos. Math., 85(2), 125–161 (1993)

[7] Imai, H.: A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions. Proc. Japan Acad., 51, 12–16 (1975)

[8] Kato, K.: p-adic Hodge theory and values of zeta functions of modular forms, In: Cohomologies p-adiques et applications arithmétiques. III., Astérisque 295, 2004, 117–290

[9] Kim, B. D.: The parity conjecture for elliptic curves at supersingular reduction primes. Compo. Math., 143, 47–72 (2007)

[10] Kim, B. D.: The algebraic functional equation of an elliptic curve at supersingular primes. Math. Res. Lett., 14(1), 83–94 (2007)

[11] Kim, B. D.: The plus/minus Selmer groups for supersingular primes. J. Aust. Math. Soc., 95(2), 189–200 (2013)

[12] Kim, B. D.: Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field. Canad. J. Math., 66(4), 826–843 (2014)

[13] Kitajima, T., Otsuki, R.: On the plus and the minus Selmer groups for elliptic curves at supersingular primes. Tokyo J. Math., 41(1), 273–303 (2018)

[14] Kobayashi, S.: Iwasawa theory for elliptic curves at supersingular primes. Invent. Math., 152(1), 1–36 (2003)

[15] Lim, M. F.: Comparing the $\pi$-primary submodules of the dual Selmer groups. Asian J. Math., 21(6), 1153–1182 (2017)

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

[17] Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, 2nd Ed., Grundlehren Math. Wiss. 323, Springer-Verlag, Berlin, 2008

[18] Skinner, C., Urban, E.: The Iwasawa main conjectures for $GL_2$. Invent. Math., 195(1), 1–277 (2014)

[19] Tate, J.: Duality theorems in Galois cohomology over number fields, In: 1963 Proc. Internat. Congr. Mathematicians, Stockholm, 1962, 288–295

[20] Wan, X.: Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture, arXiv:1411.6352v7 [math.NT]

[21] Washington, L. C.: Introduction to Cyclotomic Fields, 2nd Ed., Grad. Texts in Math. Vol. 83, Springer-Verlag, Berlin, New York, 1996