On the algebraic functional equation for the mixed signed Selmer group over multiple $\mathbb{Z}_p$-extensions

Suman Ahmed∗  Meng Fai Lim†

Abstract
Let $E$ be an elliptic curve defined over a number field with good reduction at all primes above a fixed odd prime $p$, where at least one of which is a supersingular prime of $E$. In this paper, we will establish the algebraic functional equation for the mixed signed Selmer groups of an elliptic curve with good reduction at every prime above $p$ over a multiple $\mathbb{Z}_p$-extension.

Keywords and Phrases: Algebraic functional equation, signed Selmer groups.
Mathematics Subject Classification 2010: 11G05, 11R23, 11S25.

1 Introduction
Throughout this article, $p$ will always denote an odd prime number. Let $E$ be an elliptic curve defined over a number field $F$. If $E$ has good ordinary reduction at every prime of $F$ above $p$, a well-known conjecture of Mazur [22] asserts that the $p$-primary Selmer group of $E$ over the cyclotomic $\mathbb{Z}_p$-extension is cotorsion over $\mathbb{Z}_p[[\text{Gal}(F^{\text{cy}}/F)]]$. Following Iwasawa [8], Mazur went on further predicting that the characteristic ideal of this cotorsion Selmer group has a precise description in terms of an appropriate $p$-adic $L$-function which nowadays is coined the Iwasawa main conjecture (also see [6, 9, 27]). In view of the above correspondence, one would expect that there should be an algebraic relation of the characteristic ideals of the Selmer groups mirroring the functional equation of the $p$-adic $L$-function. Indeed, this has been extensively studied by Greenberg [6], where he even established such a relation (which he coined as “the algebraic functional equation”) unconditionally without assuming the main conjecture nor the existence of the $p$-adic $L$-function. Subsequently, this direction of study has been generalized to more general $p$-adic Lie extensions (for instance, see [16, 29, 30]).

However, if the elliptic curve $E$ has supersingular reduction at one prime above $p$, then the $p$-primary Selmer group of $E$ over $F^{\text{cy}}$ is not expected to be cotorsion over $\mathbb{Z}_p[[\text{Gal}(F^{\text{cy}}/F)]]$ (see [26]). It was due to the remarkable insight of Kobayashi [15] that one has to replace the consideration of the $p$-primary Selmer group by some smaller subgroups. More precisely, Kobayashi constructed the plus and minus Selmer groups of an elliptic curve over $\mathbb{Q}^{\text{cy}}$ which are contained in the $p$-primary Selmer groups. He was able to show that these signed Selmer groups are cotorsion over $\mathbb{Z}_p[[\text{Gal}(\mathbb{Q}^{\text{cy}}/\mathbb{Q})]]$, and formulate a main conjecture (and even prove one-side divisibility) relating the characteristic ideals of these signed Selmer groups to the signed

∗School of Mathematics and Statistics, Central China Normal University, Wuhan, 430079, P.R.China. E-mail: npur.suman@gmail.com
†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
p-adic L-functions of Pollack [25]. Motivated by this main conjecture, Kim [11] first established an algebraic functional equation for the signed Selmer group over a cyclotomic $\mathbb{Z}_p$-extension (also see [11] [19] [28]). In [12], Kim developed a theory of mixed signed Selmer groups of an elliptic curve over $\mathbb{Z}_p^2$-extension of an imaginary quadratic field, where he chose either the plus or minus condition for each supersingular prime, and so in this situation, one has four signed Selmer groups to work with. He then proposed a main conjecture relating these Selmer groups to the mixed signed $p$-adic L-functions of Loeffler [21]. Recently, Büyükboduk-Lei [4] has established an analytic functional equation for (some of) the $p$-adic L-functions of Loeffler. In view of this and the main conjecture, one would expect that the signed Selmer groups would satisfy an algebraic functional equation.

The goal of this paper is to prove such an algebraic functional equation. In fact, we shall put ourselves in a slightly more general framework following that of Kitajima-Otsuki [14]. Namely, our elliptic curve has good reduction at all primes of $F$ above $p$, where at least one of which is a supersingular prime of the said elliptic curve. Let $F_\infty$ be a $\mathbb{Z}_p^d$-extension of $F$ which contains the cyclotomic $\mathbb{Z}_p$-extension $F^{\text{cyc}}$ and satisfies the property that every prime of $F^{\text{cyc}}$ above $p$ at which $E$ has good supersingular reduction is unramified in $F_\infty/F^{\text{cyc}}$. The latter ramification condition on $F_\infty$ is necessary for us to be able to apply the work of Kim [12] in defining the plus/minus norm groups which in turn is required for the definition of the mixed signed Selmer groups over the $\mathbb{Z}_p^d$-extension $F_\infty$. We should mention that the mixed signed Selmer group defined here is a blend of those considered in [12] and [14], which was also studied in [17]. In [16], Lai-Longhi-Tan-Trihan developed a theory of $\Gamma$-system (where $\Gamma \cong \mathbb{Z}_p^d$) which they utilized to prove an algebraic functional equation for abelian varieties with good ordinary reduction at all primes above $p$ over a $\mathbb{Z}_p^d$-extension of a global field. We shall adopt their approach in proving our algebraic functional equation for the mixed signed Selmer group over the $\mathbb{Z}_p^d$-extension $F_\infty$. To the best knowledge of the authors, the (appropriate) $p$-adic $L$-functions have not been constructed in this mixed reduction setting. Therefore, besides providing evidence to the main conjecture in the scenario considered by Kim and Loeffler, our result also provides some positive belief for the conjectural functional equation of the (conjectural) $p$-adic $L$-functions in this mixed reduction setting.

It would definitely be interesting to study whether the techniques in this article can be applied to the setting of the multi-signed Selmer groups for a non-ordinary motive with Hodge-Tate weights being 0 and 1 as considered by Büyükboduk-Lei [2, 3]. Over the cyclotomic $\mathbb{Z}_p$-extension, such an algebraic functional equation for these multi-signed Selmer groups has been established in [19]. However, unlike the elliptic curve situation, where a local theory of plus/minus norm groups over the $\mathbb{Z}_p^2$-extension of $\mathbb{Q}_p$ is available thanks to the work of Kim [12], it is not clear to the authors how to extend the local theory of Büyükboduk-Lei to the $\mathbb{Z}_p^2$-extension of $\mathbb{Q}_p$ at this point of writing.

We now give an outline of the paper. In Section 2 we review the plus/minus conditions of Kobayashi as extended by Kim to a $\mathbb{Z}_p^2$-extension of $\mathbb{Q}_p$. We also discuss a result of Kim on the orthogonality properties of these plus/minus conditions under the local Tate pairing. Section 3 is where we define the signed Selmer groups. We also introduce the strict signed Selmer groups. These latter Selmer groups coincide with the signed Selmer group on the level of $F_\infty$ (but may differ on the intermediate finite subextensions). However, the local conditions in defining these strict signed Selmer group satisfy certain orthogonality conditions, which is an important aspect for our proof, as it allows us to invoke a theorem of Flach [5]. Our main theorem (Theorem 3.3) is stated in this section, and its proof will be given in Section 4. In this last section, we will show that the strict signed Selmer groups, via a combination of the results of Kim and Flach, give
rise to a $\Gamma$-system in the sense of Lai-Longhi-Tan-Trihan \cite{16}. From there, we apply the machinery developed by Lai et al to establish our theorem.

Acknowledgement

We thank Byoung Du Kim and Antonio Lei for their interests and comments. We also like to thank Antonio Lei for making us aware of the paper \cite{4}. 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. M. F. Lim is supported by the National Natural Science Foundation of China under Grant No. 11550110172 and Grant No. 11771164.

2 Supersingular elliptic curves over local fields

In this section, we record certain results on supersingular elliptic curves over a $p$-adic local field. Let $E$ be an elliptic curve defined over $\mathbb{Q}_p$ with good supersingular reduction and $a_p = 1 + p - |\overline{E}(\mathbb{F}_p)| = 0$, where $\overline{E}$ is the reduction of $E$. Denote by $\hat{E}$ the formal group of $E$. For convenience, if $L$ is an extension of $\mathbb{Q}_p$, we shall write $\hat{E}(L)$ for $\hat{E}(\mathfrak{m}_L)$, where $\mathfrak{m}_L$ is the maximal ideal of the ring of integers of $L$. Fix a finite unramified extension $K$ of $\mathbb{Q}_p$. Denote by $K^{\text{cyc}}$ (resp., $K^{\text{nr}}$) the cyclotomic (resp, the unramified) $\mathbb{Z}_p$-extension of $K$.

If $n \geq 0$ is an integer, we write $K_n$ (resp. $K^{(n)}$) for the unique subextension of $K^{\text{cyc}}/K$ (resp. $K^{\text{nr}}/K$), whose degree over $K$ is equal to $p^n$.

Lemma 2.1. The formal groups $\hat{E}(K^{(m)}K_n)$ has no $p$-torsion for all integers $m,n \geq 0$. In particular, $E(K^{(m)}K_n)$ has no $p$-torsion for every $m,n$.

Proof. The first assertion is \cite{14} Proposition 3.1 or \cite{15} Proposition 8.7. For the second assertion, consider the following short exact sequence

$$0 \rightarrow \hat{E}(K^{(m)}K_n) \rightarrow E(K^{(m)}K_n) \rightarrow \hat{E}(k_{m,n}) \rightarrow 0,$$

where $k_{m,n}$ is the residue field of $K^{(m)}K_n$. Since $\hat{E}(k_{m,n})$ has no $p$-torsion by our assumption that $E$ has good supersingular reduction, the second assertion follows from the first assertion.

Following \cite{10} \cite{11} \cite{12} \cite{14} \cite{15} \cite{17}, we define the following plus/minus norm groups.

Definition 2.2.

$$\hat{E}^+(K^{(m)}K_n) = \left\{ P \in \hat{E}(K^{(m)}K_n) : \operatorname{tr}_{n/\ell+1}(P) \in E(K^{(m)}K_{\ell}), 2 \mid \ell, 0 \leq \ell \leq n-1 \right\},$$

$$\hat{E}^-(K^{(m)}K_n) = \left\{ P \in \hat{E}(K^{(m)}K_n) : \operatorname{tr}_{n/\ell+1}(P) \in E(K^{(m)}K_{\ell}), 2 \mid \ell, 0 \leq \ell \leq n-1 \right\},$$

where $\operatorname{tr}_{n/\ell+1} : \hat{E}(K^{(m)}K_{\ell+1}) \rightarrow \hat{E}(K^{(m)}K_{\ell})$ denotes the trace map with respect to the formal group law of $\hat{E}$.

For the rest of this subsection, we write $L_\infty = \cup_{m,n \geq 0} K^{(m)}K_n$. Note that $G := \text{Gal}(L_\infty/K) \cong \mathbb{Z}_p^2$. Denote by $G_n$ the subgroup $G^{p^n}$ of $G$ and set $L_n$ to be the fixed field of $G_n$. In particular, one has $\text{Gal}(L_n/K) \cong \mathbb{Z}/p^n \times \mathbb{Z}/p^n$. 

3
Write $H_\pm^+ = \hat{E}(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $H_n^+ = (H_\infty^+)^G_n$. By [13, Lemma 8.17], the group $H_\infty^+$ injects into $H^1(L_\infty, E[p^\infty])$ via the Kummer map. In view of Lemma 2.1 it follows from the Hochshild-Serre spectral sequence that there is an isomorphism

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

Thus, $H_\infty^+$ can be viewed as a subgroup of $H^1(L_n, E[p^\infty])$ via this isomorphism. By Lemma 2.1 again, we have an identification

$$H^1(L_n, E[p^m]) \cong H^1(L_n, E[p^\infty])|_{p^m}$$

which further enables us to view $H_\infty[p^m]$ as a subgroup of $H^1(L_n, E[p^m])$. Under these observations, we may now state the following result of Kim.

**Proposition 2.3 (Kim).** The group $H^-_n[p^m]$ is the exact annihilator of itself with respect to the local Tate pairing

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

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

**Proof.** See [10, Proposition 3.15] and [12, Theorem 2.9].

### 3 Signed Selmer groups

For the remainder of the paper, $E$ will denote an elliptic curve defined over a number field $F'$. Let $F$ be a finite extension of $F'$. We introduce the following axiomatic conditions which will be in force throughout the paper.

**S(1)** 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 $E$.

**S(2)** For each prime $u$ of $F'$ above $p$ at which $E$ has good supersingular reduction, we always have

(a) $F'_u \cong \mathbb{Q}_p$ and $u$ is unramified in $F/F'$;

(b) $a_u = 1 + p - |\tilde{E}_u(F_p)| = 0$, where $\tilde{E}_u$ is the reduction of $E$ at $u$.

From now on, we fix a finite set $\Sigma$ of primes of $F$ which contains all the primes above $p$, all the ramified primes of $F/F'$, the bad reduction primes of $E$ and the archimedean primes. Let $F_\Sigma$ denote the maximal algebraic extension of $F$ which is unramified outside $\Sigma$. For every extension $L$ of $F$ contained in $F_\Sigma$, we write $G_\Sigma(L) = \text{Gal}(F_\Sigma/L)$. Denote by $\Sigma^{ss}$ the set of primes of $F$ above $p$ at which $E$ has good supersingular reduction. By (S1), the set $\Sigma^{ss}$ is nonempty. For any subset $S$ of $\Sigma$ and any extension $L$ of $F$, we shall write $S(L)$ for the set of primes of $L$ above $S$.

Let $F_\infty$ be a $\mathbb{Z}_p$-extension of $F$ which always satisfies the following hypothesis.

**S(3)** The field $F_\infty$ contains the cyclotomic $\mathbb{Z}_p$-extension $F^{cyc}$, and has the property that every $w \in \Sigma^{ss}(F^{cyc})$ is unramified in $F_\infty/F^{cyc}$.
Note that $F_\infty \subseteq F_\Sigma$ (cf. [8, Theorem 1]). Write $\Gamma = \text{Gal}(F_\infty/F) \cong \mathbb{Z}_p^d$. Let $F_n$ be the unique subextension of $F_\infty/F$ such that $\text{Gal}(F_n/F) \cong (\mathbb{Z}/p^n)^d$. Let $\vec{s} = (s_v)_{v \in \Sigma^{ss}} \in \{+,-\}^{\Sigma^{ss}}$ be a fixed choice of signs. For each $w \in \Sigma^{ss}(F_n)$, we set $s_w = s_v$, where $v$ is the prime of $F$ below $w$. By (S3), $F_{n,w}$ is the compositum of a subextension of the cyclotomic $\mathbb{Z}_p$-extension of $F_v$ and a subextension of the unramified $\mathbb{Z}_p$-extension of $F_v$. Hence we can define $\overline{E}^{ss}(F_{n,w})$ as in Definition [22].

**Definition 3.1.** For $\vec{s} = (s_v)_{v \in \Sigma^{ss}} \in \{+,-\}^{\Sigma^{ss}}$, the signed Selmer group $\text{Sel}^{\vec{s}}(E/F_n)$ is then defined by

$$\ker \left( H^1(G_\Sigma(F_n), E[p^\infty]) \rightarrow \bigoplus_{w \in \Sigma^{ss}(F_n)} \frac{H^1(F_{n,w}, E[p^\infty])}{E^{ss}(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w \in \Sigma^{ss}(F_n) \setminus \Sigma^{ss}(F_n)} \frac{H^1(F_{n,w}, E[p^\infty])}{E(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right).$$

We set $\text{Sel}^{\vec{s}}(E/F_\infty) = \lim_{n \to \infty} \text{Sel}^{\vec{s}}(E/F_n)$ and write $X^{\vec{s}}(E/F_\infty)$ for its Pontryagin dual.

The module $X^{\vec{s}}(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[[\Gamma]]$. One generally expects a stronger assertion on the structure of this module.

**Conjecture 3.2.** For all choices of $\vec{s} \in \{+,-\}^{\Sigma^{ss}}$, the Selmer group $X^{\vec{s}}(E/F_\infty)$ is torsion over $\mathbb{Z}_p[[\Gamma]]$.

Over the cyclotomic $\mathbb{Z}_p$-extension, when $E$ has good ordinary reduction at all primes above $p$, the above conjecture is precisely Mazur’s conjecture in [22], which is known to hold in the case when $E$ is defined over $\mathbb{Q}$ and $F$ an abelian extension of $\mathbb{Q}$ (see [9]). For an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at $p$, this conjecture has been proven to be true by Kobayashi [13]; see also [2] for a generalization of this conjecture for abelian varieties. Over a multiple $\mathbb{Z}_p$-extension, the above conjecture is a natural extension of Mazur’s conjecture (for instance, see [24]). When $E$ has supersingular reduction, this was studied in [13, 17, 18, 20].

We introduce one last hypothesis.

**(S4)** For our fixed choice of $\vec{s}$, we have $4 \nmid |F_v : \mathbb{Q}_p|$ whenever $s_v = +$.

For a $\mathbb{Z}_p[[\Gamma]]$-module $M$, we write $M^\vee$ for the $\Lambda$-module which is $M$ as $\mathbb{Z}_p$-module with a $\Gamma$-action given by $\gamma \cdot x = \gamma^{-1}x$ for $\gamma \in \Gamma$ and $x \in M$. If $M$ and $N$ are two torsion $\mathbb{Z}_p[[\Gamma]]$-modules which are pseudo-isomorphic to each other, we write $M \sim N$.

We can now state our main result.

**Theorem 3.3.** Suppose that (S1) – (S4) are valid. Assume that $X^{\vec{s}}(E/F_\infty)$ is torsion over $\mathbb{Z}_p[[\Gamma]]$ for our fixed choice of $\vec{s}$. Then we have a pseudo-isomorphism

$$X^{\vec{s}}(E/F_\infty) \sim X^{\vec{s}}(E/F_\infty)^{\vee}.$$ 

In particular, the characteristic ideal of $X^{\vec{s}}(E/F_\infty)$ coincides with the characteristic ideal of $X^{\vec{s}}(E/F_\infty)^{\vee}$.

The proof of the theorem will be given in Section [4]. As mentioned in the introduction, in proving our main result, we need to work with the so-called strict signed Selmer groups which we shall recall here. The strict signed Selmer group of $E$ over $F_n$ is given by

$$\text{Sel}^{\vec{s},\text{str}}(E/F_n) := \ker \left( H^1(G_\Sigma(F_n), E[p^\infty]) \rightarrow \bigoplus_{w \in \Sigma(F_n)} C_w \left( E[p^\infty]/F_n \right) \right),$$

where $C_w \left( E[p^\infty]/F_n \right)$ is defined as follows.
(1) Suppose that \( w \) divides \( p \) and is a good supersingular prime of \( E \). We take

\[
C_w \left( E[p^\infty]/F_n \right) := \left( \bigoplus_{x|w} E^{ss}(F_{\infty,x}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\Gamma_n},
\]

where \( x \) runs through all the primes of \( F_\infty \) above \( w \).

(2) If \( w \) divides \( p \) and is a good ordinary reduction prime of \( E \), we set \( C_w \left( E[p^\infty]/F_n \right) \) to be

\[
\text{im} \left( H^1(F_{n,w}, \hat{E}[p^\infty]) \to H^1(F_{n,w}, E[p^\infty]) \right)_{\text{div}}.
\]

(3) If \( w \) does not divide \( p \), then \( C_w \left( E[p^\infty]/F_n \right) \) is simply defined to be the kernel of the map

\[
H^1(F_{n,w}, E[p^\infty]) \to H^1(F_{n,w}^{ur}, E[p^\infty]),
\]

where \( F_{n,w}^{ur} \) is the maximal unramified extension of \( F_{n,w} \).

Define \( \text{Sel}^\top,\text{str}(E/F_\infty) := \lim_{\rightarrow n} \text{Sel}^\top,\text{str}(E/F_n) \). Note that in the case when \( \Sigma^{ss} = \emptyset \), this is the strict Selmer group as defined in the sense of Greenberg [6]. Our choice of naming the above as the strict signed Selmer group is inspired by this observation. In general, the strict signed Selmer group needs not agree with the signed Selmer group on the intermediate level \( F_n \). But they do coincide upon taking limit and we record this fact here.

**Proposition 3.4.** We have an identification \( \text{Sel}^\top,\text{str}(E/F_\infty) \cong \text{Sel}^\top(E/F_\infty) \).

**Proof.** This has a similar proof to that in [1, Proposition 4.3]. \( \square \)

Here, and subsequently, we shall write \( S_{\text{div}}(E/F_n) \) for the \( p \)-divisible part of \( \text{Sel}^\top,\text{str}(E/F_n) \). In other words, \( S_{\text{div}}(E/F_n) \) is the maximal \( p \)-divisible subgroup of \( \text{Sel}^\top,\text{str}(E/F_n) \). The main reason for working with the strict signed Selmer groups lies in the following proposition which will play a crucial role in the proof of Theorem 3.3.

**Proposition 3.5.** Suppose that \((S1) - (S4)\) are valid. There is a perfect pairing

\[
\text{Sel}^\top,\text{str}(E/F_n)/S_{\text{div}}(E/F_n) \times \text{Sel}^\top,\text{str}(E/F_n)/S_{\text{div}}(E/F_n) \to \mathbb{Q}_p/\mathbb{Z}_p.
\]

**Proof.** By virtue of our assumption \((S4)\), we may apply Proposition 2.3 to conclude that the local condition at each supersingular prime is its own annihilator under the Tate pairing. For the local conditions at the remaining primes, such properties are well-known (for instance, see [7] or [1]). Hence we may apply the main result of Flach [5] to obtain the perfect pairing in the proposition. \( \square \)

We end the section with one more useful observation.

**Lemma 3.6.** Suppose that \((S1) - (S3)\) are valid. For every \( n \), the restriction map

\[
\text{Sel}^\top,\text{str}(E/F_n) \to \text{Sel}^\top(E/F_\infty)^{\Gamma_n}
\]

is an injection, where \( \Gamma_n = \text{Gal}(F_\infty/F_n) \).

6
Proof. A standard diagram chasing argument shows that the kernel of the restriction map is contained in the kernel of the following restriction map

\[ H^1(G_{\Sigma}(F_n), E[p^\infty]) \to H^1(G_{\Sigma}(F_\infty), E[p^\infty])^{\Gamma_n} \]

on cohomology, which is precisely given by \( H^1(\Gamma_n, E(F_\infty)[p^\infty]) \). On the other hand, by Lemma 2.1, we have \( E(F_\infty,w)[p^\infty] = 0 \) for each \( w \in \Sigma^{ss}(F_\infty) \). It follows from this that \( E(F_\infty)[p^\infty] = 0 \) and so the kernel is trivial which is what we want to show. \( \square \)

4 Proof of the main theorem

As before, \( \Gamma = \text{Gal}(F_\infty/F) \cong \mathbb{Z}_d^d \) for some \( d \geq 2 \). We shall write \( \Lambda \) for the Iwasawa algebra \( \mathbb{Z}_p[[\Gamma]] \). For a finitely generated torsion \( \Lambda \)-module \( M \), we have a pseudo-isomorphism

\[ \bigoplus_i \Lambda/\xi_i \to M, \]

where \( \xi_i \) are irreducible elements in \( \Lambda \) (cf. [23, §5]). We shall write

\[ [M] = \bigoplus_i \Lambda/\xi_i. \]

Note that the module \([M]\) is uniquely determined by \( M \) (up to isomorphism).

Recall that for a \( \mathbb{Z}_p[[\Gamma]] \)-module \( M \), we write \( M' \) for the \( \Lambda \)-module which is \( M \) as \( \mathbb{Z}_p \)-module with a \( \Gamma \)-action given by \( \gamma \cdot x = \gamma^{-1} x \) for \( \gamma \in \Gamma \) and \( x \in M \). Then one easily sees that

\[ [M'] = [M]' \]

In view of this, Theorem 3.3 is equivalent to saying that

\[ [X^{\overline{\theta}}(E/F_\infty)]' = [X^{\overline{\theta}}(E/F_\infty)]. \]

4.1 First reduction

Write \( \mu_{p^n} \) for the group of all \( p \)-power roots of unity. Following [16], we say that \( f \in \Lambda \) is a simple element if there exist \( \gamma \in \Gamma - \Gamma^p \) and \( \zeta \in \mu_{p^n} \) such that \( f = f_{\gamma,\zeta} \), where

\[ f_{\gamma,\zeta} := \prod_{\sigma \in \text{Gal}({\mathbb{Q}_p}((\mu_p))/\mathbb{Q}_p)} (\gamma - \sigma(\zeta)). \]

Let \( M \) be a finitely generated \( \Lambda \)-torsion module. We define \([M]_{si}\) to be the the sum over those \( \xi_i \) in \([M]\) which are simple and \([M]_{ns}\) as its complement. In particular, we have \([M] = [M]_{si} \oplus [M]_{ns}\). The simple component enjoys the following property.

Lemma 4.1. Let \( M \) be a finitely generated torsion \( \Lambda \)-module. Then we have

\[ [M]_{si} = [M]_{si}. \]

Proof. See [16] pp 1930, Formula (9)]. \( \square \)
In view of the preceding lemma and the remark before Subsection 4.1, the proof of Theorem 3.3 is reduced to showing that the non-simple component of $X^\infty(E/F_\infty)$ is invariant under $\iota$, or in other words,

$$[X^\infty(E/F_\infty)]^\iota = [X^\infty(E/F_\infty)]_{ns}.$$ 

To verify this latter relation, we make use of the theory of $\Gamma$-system as developed by Lai-Longhi-Tan-Trihan in [16] which we now recall.

### 4.2 $\Gamma$-system

Here, we will only collect the properties of a $\Gamma$-system required for the proof of our theorem. For a more in-depth discussion, we refer readers to the paper [16]; see especially Section 3 of the said paper.

**Definition 4.2.** Consider a collection

$$\mathfrak{A} = \{a_n, b_n, \langle , \rangle_n, r^n_m, c^n_m \mid n \geq m \geq 0\},$$

which satisfies all of the following properties.

1. (Γ-1) For every $n$, $a_n$ and $b_n$ are finite $\mathbb{Z}_p$-modules with an action of $\Gamma$ factoring through $\mathbb{Z}_p[\Gamma/\Gamma^p]$.
2. (Γ-2) For every $n \geq m$, the maps

   $$r^n_m : a_m \times b_m \rightarrow a_n \times b_n,$$

   $$c^n_m : a_n \times b_n \rightarrow a_m \times b_m$$

   are $\Lambda$-morphisms such that $r^n_m(a_m) \subseteq a_n$, $r^n_m(b_m) \subseteq b_n$, $c^n_m(a_n) \subseteq a_m$ and $c^n_m(b_n) \subseteq b_m$ with $r^n_n = c^n_n = id$. Also, $\{a_n \times b_n, r^n_m\}_n$ forms an inductive system and $\{a_n \times b_n, c^n_m\}_n$ forms a projective system.
3. (Γ-3) The composition $r^n_m \circ c^n_m$ coincides with the norm map associated with $Gal(F_n/F_m)$ and the composition $c^n_m \circ r^n_m$ coincides with multiplication by $p^{n-m}$.
4. (Γ-4) For each $n$, $\langle , \rangle_n : a_n \times b_n \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ is a perfect pairing which is compatible with the $\Gamma$-action and the maps $r^n_m$ and $c^n_m$. More precisely, we have

   $$\langle \gamma a, \gamma b \rangle_n = \langle a, b \rangle_n$$

   for every $\gamma \in \Gamma$,

   $$\langle a_n, r^n_m(b_m) \rangle_n = \langle c^n_m(a_n), b_m \rangle_m$$

   for every $a_n \in a_n, b_m \in b_m$,

   and

   $$\langle r^n_m(a_m), b_n \rangle_n = \langle a_m, c^n_m(b_n) \rangle_m$$

   for every $a_m \in a_m, b_n \in b_n$.

Write $a = \varprojlim a_n$ and $b = \varprojlim b_n$, where the transition maps are given by $c^n_m$. We then say that $\mathfrak{A}$ is a $\Gamma$-system if both $a$ and $b$ are finitely generated torsion $\Lambda$-modules.

**Remark 4.3.** We say a little on comparing our notation with that in [16]. Our $r^n_m$ here is $r^n_m$ there and $c^n_m$ here is $c^n_m$ there. The reason behind our choice of notation here is because for our application, our maps $r^n_m$ (resp. $c^n_m$) are induced by restriction maps on cohomology (resp., corestriction maps on cohomology).
Let $\mathfrak{A}$ be a $\Gamma$-system. By (Γ-2), we can define the inductive limit $\lim_{\overset{\longrightarrow}{m}} a_m$, whose transition maps are given by $r_{m,n}^a$. Note that by (Γ-4), the Pontryagin dual of this inductive limit coincides with $b$.

Now, denote by $r_n$ the natural morphism $a_n \longrightarrow \lim_{\overset{\longrightarrow}{m}} a_m$, whose kernel is in turn denoted by $a_0^n$. The module $b_0^n$ is defined similarly. Write $a_1^n$ (resp., $b_1^n$) for the annihilator of $b_0^n$ (resp., $a_0^n$) with respect to the perfect pairing $\langle \ , \rangle_n$. Define $a'_n$ to be the image of $a_1^n$ under the natural quotient map $a_n \longrightarrow a_n/a_0^n$. The module $b'_n$ is defined similarly. One then sets $a_i^n = \lim_{\overset{\longleftarrow}{n}} a_i^n$, $b_i^n = \lim_{\overset{\longleftarrow}{n}} b_i^n$ ($i = 0, 1$), $a'_n = \lim_{\overset{\longleftarrow}{n}} a'_n$ and $b'_n = \lim_{\overset{\longleftarrow}{n}} b'_n$, where the transition maps are induced by $c_{n,m}$. The connections between these modules are recorded in the following lemma.

**Lemma 4.4.** The following statements are valid.

(a) We have isomorphisms $\lim_{\overset{\longrightarrow}{n}} b_n/b_0^n \cong (a^1)^\vee$ and $\lim_{\overset{\longrightarrow}{n}} a_n/a_0^n \cong (b^1)^\vee$. Here $(\ )^\vee$ is the Pontryagin dual.

(b) There are short exact sequence of $\Lambda$-modules

$$0 \longrightarrow a^0 \longrightarrow a \longrightarrow a' \longrightarrow 0,$$

$$0 \longrightarrow b^0 \longrightarrow b \longrightarrow b' \longrightarrow 0.$$

**Proof.** (a) Since $a_1^n$ is the annihilator of $b_0^n$ with respect to the perfect pairing $\langle \ , \rangle_n$, we have $b_n/b_0^n \cong (a_1^n)^\vee$. Taking direct limit and noting (Γ-4), we obtain the first isomorphism. The second isomorphism can be proved similarly.

(b) It suffices to establish the first short exact sequence, the second being similar. Firstly, note that we have the following short exact sequences

$$0 \longrightarrow a_0^n \longrightarrow a_1^n + a_0^n \longrightarrow a'_n \longrightarrow 0,$$

$$0 \longrightarrow b_0^n \longrightarrow b_n \longrightarrow b_n/b_0^n \longrightarrow 0$$

of $\Lambda$-modules. Since, one clearly has $\lim_{\overset{\longrightarrow}{n}} b_0^n = 0$, it follows from the second exact sequence that $\lim_{\overset{\longrightarrow}{n}} b_n \cong \lim_{\overset{\longrightarrow}{n}} b_n/b_0^n$. Upon taking dual and noting (a), we obtain the identification $a \cong a^1$. It follows from this that upon taking the inverse limit of the first exact sequence, we have

$$0 \longrightarrow a^0 \longrightarrow a \longrightarrow a' \longrightarrow 0,$$

and this completes the proof of the lemma.

The significance of the modules $a'$ and $b'$ lies in the following result which will be used in the proof of our main theorem.

**Proposition 4.5 (Lai-Longhi-Tan-Trihan).** Let $\mathfrak{A}$ be a $\Gamma$-system. Then we have

$$[a']^i_{ns} = [b']^i_{ns}.$$

**Proof.** See [16, Corollary 3.3.4].

9
4.3 Finishing the proof

We return to the setting in Section 3. In particular, we retain the notation from there. Recall that $S_{\text{div}}(E/F_n)$ denotes the $p$-divisible part of $\text{Sel}^\ast(E/F_n)$. We set $a_n(E) = b_n(E) = \text{Sel}^\ast,\text{str}(E/F_n)/S_{\text{div}}(E/F_n)$. Write $S_{\text{div}}(E/F_\infty) = \lim_n \text{Sel}_{\text{div}}(E/F_n)$. The limit of these groups sit in the following short exact sequence

$$0 \rightarrow S_{\text{div}}(E/F_\infty) \rightarrow \text{Sel}^\ast(E/F_\infty) \rightarrow \lim_n a_n(E) \rightarrow 0,$$

where we have identified $\text{Sel}^\ast,\text{str}(E/F_n) \cong \text{Sel}^\ast(E/F_\infty)$ (cf. Lemma 3.4).

The morphisms $r_m^n(E)$ are induced by the restriction maps on the signed Selmer groups which in turn are induced by those from cohomology groups. On the other hand, the morphisms $c_m^n(E)$ are induced by the corestriction maps on the signed Selmer groups which in turn are induced by those from cohomology groups. As seen in Proposition 3.5 there is a perfect pairing

$$\text{Sel}^\ast,\text{str}(E/F_n)/S_{\text{div}}(E/F_n) \times \text{Sel}^\ast,\text{str}(E/F_n)/S_{\text{div}}(E/F_n) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

which we shall denote by $\langle , \rangle_{E,n}$.

Lemma 4.6. Suppose that $X^\ast(E/F_\infty)$ is torsion over $\mathbb{Z}_p[[\Gamma]]$. Then

$$\mathfrak{A} = \{a_n(E), b_n(E), \langle , \rangle_{E,n}, r_m^n(E), c_m^n(E) \mid n \geq m \geq 0\}$$

is a $\Gamma$-system.

Proof. The verification of $(\Gamma-1)-(\Gamma-4)$ is a straightforward (but maybe tedious) exercise. Finally, by definition, we have that $\alpha(E) = \beta(E)$ is a $\Lambda$-submodule of $X^\ast(E/F_\infty)$. Since $X^\ast(E/F_\infty)$ is assumed to be torsion over $\mathbb{Z}_p[[\Gamma]]$, so is $\alpha(E)$. Thus, we have the lemma.

The next lemma is concerned with the structure of $Y(E/F_\infty) := \text{Sel}_{\text{div}}(E/F_\infty)\uparrow^\Gamma$.

Lemma 4.7. Suppose that $X^\ast(E/F_\infty)$ is torsion over $\mathbb{Z}_p[[\Gamma]]$. Then we have $[Y(E/F_\infty)] = [Y(E/F_\infty)]_{\text{st}}$.

Proof. By [10] Theorem 4.1.3, we see that $(\text{Sel}^\ast(E/F_\infty)^{\Gamma_n})_{\text{div}}$ is annihilated by a product $f$ of simple elements for every $n$. Now by Lemma 3.6 $S_{\text{div}}(E/F_n)$ can be viewed as a submodule of $(\text{Sel}^\ast(E/F_\infty)^{\Gamma_n})_{\text{div}}$. Thus, it is also annihilated by $f$ for every $n$. Consequently, the module $Y(E/F_\infty)$ is annihilated by $f$, and in particular, one has $[Y(E/F_\infty)] = [Y(E/F_\infty)]_{\text{st}}$.

We can now give the proof of the main result of the paper.

Proof of Theorem As seen in Subsection 4.1 it remains to show that

$$[X^\ast(E/F_\infty)]_{\text{st}}^t = [X^\ast(E/F_\infty)]_{\text{ns}}.$$

On the other hand, by a combination of Proposition 3.5 and Lemma 4.6 we obtain $[\alpha'(E)]_{\text{ns}} = [\beta'(E)]_{\text{ns}}$. Since $\alpha'(E) = \beta'(E)$, the conclusion of the theorem will follow from this once we show that $[\alpha'(E)]_{\text{ns}} = [X^\ast(E/F_\infty)]_{\text{ns}}$. As a start, consider the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \rightarrow & S_{\text{div}}(E/F_n) & \rightarrow & \text{Sel}^\ast,\text{str}(E/F_n) & \rightarrow & a_n(E) & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & S_{\text{div}}(E/F_\infty)^{\Gamma_n} & \rightarrow & \text{Sel}^\ast(E/F_\infty)^{\Gamma_n} & \rightarrow & \left(\lim_m a_m(E)\right)^{\Gamma_n} & \\
\end{array}$$
with exact rows, where we write $\Gamma_n = \Gamma^p_n$. By definition, the kernel of the rightmost map is $a_0^n(E)$. Since the middle map is injective by Lemma 3.6, it follows from the snake lemma that $a_0^0(E)$ injects into $S_{\text{div}}(E/F_\infty)^{\Gamma_n}/S_{\text{div}}(E/F_n)$. Since $S_{\text{div}}(E/F_\infty)^{\Gamma_n}$ is annihilated by a product $f$ of simple elements for every $n$ by Lemma 4.7, so is $a_0^0(E)$. Hence we have $[a^0(E)] = [a^0(E)]_{ns}$. It then follows from this and Lemma 4.4 that $[a(E)]_{ns} = [a'(E)]_{ns}$.

On the other hand, we also have the following short exact sequence

$$0 \rightarrow a(E) \rightarrow X^s(E/F_\infty) \rightarrow Y(E/F_\infty) \rightarrow 0.$$ 

It then follows from this and Lemma 1.4 that $[a(E)]_{ns} = [X^s(E/F_\infty)]_{ns}$. Combining this with the conclusion obtained in the previous paragraph, we have $[a'(E)]_{ns} = [X^s(E/F_\infty)]_{ns}$ as required.

References

[1] S. Ahmed and M. F. Lim, On the algebraic functional equation of the eigenspaces of mixed signed Selmer groups of elliptic curves with good reduction at primes above $p$, [arXiv:1912.09023] [math.NT].

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

[3] K. Büyükboduk and A. Lei, Coleman-adapted Rubin-Stark Kolyvagin systems and supersingular Iwasawa theory of CM abelian varieties. Proc. London Math. Soc. (3) 111 (2015), no. 6, 1338-1378.

[4] K. Büyükboduk and A. Lei, Functional equation for $p$-adic Rankin-Selberg $L$-functions. Ann. Math. Qué. 44 (2020), no. 1, 9-25.

[5] M. Flach, A generalisation of the Cassels-Tate pairing. J. Reine Angew. Math. 412 (1990), 113-127.

[6] R. Greenberg, Iwasawa theory for $p$-adic representations, in Algebraic Number Theory-in honor of K. Iwasawa, ed. J. Coates, R. Greenberg, B. Mazur and I. Satake, Adv. Std. in Pure Math. 17, 1989, pp. 97-137.

[7] L. Guo. On a generalization of Tate dualities with application to Iwasawa theory. Compos. Math. 85 (1993), no. 2, 125-161.

[8] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann. of Math. (2) 98 (1973), 246-326.

[9] K. Kato, $p$-adic Hodge theory and values of zeta functions of modular forms, in: Cohomologies $p$-adiques et applications arithmétiques. III., Astérisque 295, 2004, ix, pp. 117-290.

[10] B. D. Kim, The parity conjecture for elliptic curves at supersingular reduction primes. Compos. Math. 143 (2007), no. 1, 47-72.

[11] B. D. Kim, The algebraic functional equation of an elliptic curve at supersingular primes. Math. Res. Lett. 15 (2008), no. 1, 83-94.

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

[13] B. D. Kim and J. Park, The main conjecture of Iwasawa theory for elliptic curves with complex multiplication over abelian extensions at supersingular primes. Acta Arith. 181 (2017), no. 3, 209-238.

[14] T. Kitajima and R. Otsuki, On the plus and the minus Selmer groups for elliptic curves at supersingular primes. Tokyo J. Math. Vol. 41 No. 1 (2018) 273-303.

[15] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes. Invent. Math. 152 (2003), no. 1, 1-36.

[16] K. F. Lai, I. Longhi, K-S Tan and F. Trihan, Pontryagin duality for Iwasawa modules and abelian varieties. Trans. Amer. Math. Soc. 370 (2018), no. 3, 1925-1958.

[17] A. Lei and M. F. Lim, Akashi series of signed Selmer groups of elliptic curves with semistable reduction at primes above $p$, [arXiv:2001.09204] [math.NT].

[18] A. Lei and B. Palvannan, Codimension two cycles in Iwasawa theory and elliptic curves with supersingular reduction, Forum Math., Sigma (2019), Vol. 7, e25, 81 pages.
[19] A. Lei and G. Ponsinet, Functional equations for multi-signed Selmer groups. Ann. Math. Qué. 41 (2017), no. 1, 155-167.

[20] A. Lei and F. Sprung, Ranks of elliptic curves over $\mathbb{Z}_p^2$-extensions, to appear in Israel J. Math.

[21] D. Loeffler, $p$-adic integration on ray class groups and non-ordinary $p$-adic $L$-functions. Iwasawa theory 2012, 357–378, Contrib. Math. Comput. Sci., 7, Springer, Heidelberg, 2014.

[22] B. Mazur, Rational points of abelian varieties with values in towers of number fields. Invent. Math. 18 (1972), 183-260.

[23] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, 2nd edn., Grundlehren Math. Wiss. 323 (Springer-Verlag, Berlin, 2008).

[24] Y. Ochi and O. Venjakob, On the ranks of Iwasawa modules over $p$-adic Lie extensions. Math. Proc. Cambridge Philos. Soc. 135 (2003), no. 1, 25-43.

[25] R. Pollack, On the $p$-adic $L$-function of a modular form at a supersingular prime. Duke Math. J. 118 (2003), no. 3, 523-558.

[26] P. Schneider, $p$-adic height pairings II. Invent. Math. 79 (1985), no. 2, 329-374.

[27] C. Skinner and E. Urban, The Iwasawa main conjectures for $GL_2$. Invent. Math. 195 (2014), no. 1, 1-277.

[28] F. Sprung, On pairs of $p$-adic $L$-functions for weight-two modular forms. Algebra Number Theory 11 (2017), no. 4, 885-928.

[29] G. Zábrádi, Characteristic elements, pairings and functional equations over the false Tate curve extension. Math. Proc. Cambridge Philos. Soc. 144 (2008), no. 3, 535–574.

[30] G. Zábrádi, Pairings and functional equations over the $GL_2$-extension. Proc. Lond. Math. Soc. (3) 101 (2010), no. 3, 893-930.