*Math. Res. Lett.* **14** (2008), *no.* 1, 83–94 

# THE ALGEBRAIC FUNCTIONAL EQUATION OF AN ELLIPTIC CURVE AT SUPERSINGULAR PRIMES

Byoung Du (B.D.) Kim

Abstract. Since the analytic functional equation holds for the $\pm$-$p$-adic $L$-functions constructed in [7], the algebraic functional equation for the $\pm$-Selmer groups is expected to hold as well. In this paper, we show it following the ideas of [1] and [4].

## 1. Introduction

We let $E$ be an elliptic curve defined over $\mathbb{Q}$ and let $p > 3$ be a prime at which $E$ has good supersingular reduction. We let $K$ be an abelian extension of $\mathbb{Q}$ such that $[K : \mathbb{Q}]$ is prime to $p$ and $p$ is unramified over $K/\mathbb{Q}$.

Let $K_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $K$. We define $Sel_p^-(E/K_\infty)$ following [5], [2], and [4]. We will explain this construction in the following sections.

Throughout this paper we use the following notation: Let $g = [K : \mathbb{Q}]$, $O = \mathbb{Z}_p[\mu_g]$, and $F = \mathbb{Q}_p(\mu_g)$. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$, $\Lambda = \mathbb{Z}_p[[\Gamma]]$, and $\Lambda_O = \Lambda \otimes O$ (the reason for tensoring with $O$ will be explained later in this introduction). We identify $\Lambda_O$ with the integral power series ring $O[[X]]$ by identifying a topological generator $\gamma$ of $\Gamma$ with $1 + X$. When $M$ is a $O$-module, we let $M^\vee$ denote the $O$-Pontryagin dual $\mathrm{Hom}_O(M, F/O)$ where $\mathrm{Hom}_O$ is the set of continuous $O$-homomorphisms.

Using Kato's and Rohrlich's work we will show $Sel_p^-(E/K_\infty)$ is $\Lambda$-cotorsion, and following Greenberg's idea we will show

$$\left(Sel_p^-(E/K_\infty) \otimes O\right)^\vee \sim \left(Sel_p^-(E/K_\infty)^\iota \otimes O\right)^\vee \tag{1}$$

where $\sim$ is a $O[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$-pseudo-isomorphism (a homomorphism with finite kernel and cokernel) and $\iota$ is the standard involution given by $g \to g^{-1}$ for any $g \in \mathrm{Gal}(K_\infty/\mathbb{Q})$.

This implies that the characteristic ideal $(a) \subset \Lambda$ of the Pontryagin dual of $Sel_p^-(E/K_\infty)$ is nonzero and satisfies the algebraic functional equation $(a) = (a^\iota)$. Pollack showed the analytic counterpart of this result, the analytic functional equation of minus-$p$-adic $L$-functions. (See [7] Theorem 5.13. He also proved that of plus-$p$-adic $L$-functions.) The main conjecture of Iwasawa theory of $\pm$-Selmer groups (see [5]) implies the analytic functional equation is equivalent to the algebraic functional equation.

Furthermore it is possible to formulate and prove one divisibility of the main conjecture of Iwasawa theory for $Sel_p^-(E/K_\infty)$ similar to [5], in which one divisibility of that conjecture for $Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty}))$ was proven. (The proof is very similar to [5], and we will omit it.)

Received by the editors September 28, 2006. Revision received March 27, 2007.

Applying our technique to the plus Selmer groups might be a little difficult. The construction of plus norm subgroups in [4] does not seem to always work unlike minus norm subgroups. However, when $K = \mathbb{Q}(\mu_p)$ or $p$ splits completely over $K/\mathbb{Q}$, we have the plus norm subgroups as constructed in [5] and [2], and we can prove the algebraic functional equation for the plus Selmer groups without modifying our technique.

This paper uses the idea of [1] which we now recall.

We let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $\mathbb{Q}_\infty = K_\infty^\Delta$. We let $\mathbb{Q}_n$ denote the subfield of $\mathbb{Q}_\infty$ with $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ (similarly $K_n$ denotes the subfield of $K_\infty$ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$), and $\Gamma_n$ denote $\mathrm{Gal}(K_\infty/K_n)$.

We let $A$ denote $E[p^\infty] \otimes O$. For a character $\eta$ of $\Delta$ we let $\epsilon_\eta = \sum_{\sigma \in \Delta} \eta(\sigma^{-1})\sigma$ and $A_\eta$ be $A$ with action twisted by $\eta$. (As you might have noticed, to twist the action of $\Delta$ by $\eta$, we need to tensor $E[p^\infty]$ with $O$.)

The group $\Delta$ acts naturally on $Sel_p^-(E/K_\infty)$. Since $[K : \mathbb{Q}]$ is prime to $p$, we have the decomposition $Sel_p^-(E/K_\infty) \otimes O \cong \oplus_\eta \epsilon_\eta (Sel_p^-(E/K_\infty) \otimes O)$ where $\eta$ runs over all characters of $\Delta$. Thus to show

$$Sel_p^-(E/K_\infty) \otimes O \sim Sel_p^-(E/K_\infty)^\iota \otimes O$$

as $O[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$-modules, it is enough to show

$$\epsilon_\eta(Sel_p^-(E/K_\infty) \otimes O) \sim \epsilon_{\bar{\eta}}(Sel_p^-(E/K_\infty)^\iota \otimes O)$$

as $\Lambda_O$-modules for each character $\eta$ of $\Delta$.

To do so, we will define a local condition $H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,v}, A_\eta)$ for every place $v$ of $\mathbb{Q}_\infty$ such that the group $S_\eta = H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)$ associated to this local condition is isomorphic to $(Sel_p^-(E/K_\infty) \otimes O)^{\bar{\eta}}$. By Iwasawa theory (see proposition 3.6), to show $S_\eta \sim S_{\bar{\eta}}^\iota$, it is sufficient to show that $\mathrm{corank}_O(S_\eta \otimes \Lambda_O/(f))^\Gamma = \mathrm{corank}_O(S_{\bar{\eta}} \otimes \Lambda_O/(f^\iota))^\Gamma$ for every monic polynomial $f \in \Lambda_O$ and that $|S_\eta^{\Gamma_m}[p^n]|/|S_{\bar{\eta}}^{\Gamma_m}[p^n]|$ is bounded as $m$ and $n$ vary. The critical part in establishing this is to show the local conditions satisfy duality with respect to the local pairings (proposition 2.5).

**Remark 1.1.** *For an $O$-module $M$ with $\Delta$-action and a character $\eta$ of $\Delta$, we let $M^\eta$ denote the submodule of $M$ where every $\sigma \in \Delta$ acts as multiplication by $\eta(\sigma)$. In fact, we can identify $M^\eta = \epsilon_\eta M$ and will use them interchangeably.*

## 2. The minus decomposition of a formal group

As we mentioned earlier, let $K_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $K$. In other words $K_\infty$ is $K(\mu_{p^\infty})^{\Delta'}$ where $\mathrm{Gal}(K(\mu_{p^\infty})/K) \cong \Gamma \times \Delta'$ with $\Gamma \cong \mathbb{Z}_p$ and a torsion subgroup $\Delta'$. We let $K_n$ denote the subfield of $K_\infty$ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Suppose $P$ is a prime of $K$ lying above $p$. Let $k$ be $K_P$, $k_n$ be $K_{n,q}$ where $q$ denotes the unique prime of $K_n$ lying above $P$, and $k_\infty$ be $\cup_{n=0}^\infty k_n$ (also let $k_{-1} = k$).

For an extension $L$ of $\mathbb{Q}_p$ we let $O_L$ denote the ring of integers of $L$, and $m_L$ denote the unique maximal ideal of $O_L$. Let $\hat{E}$ be the formal group over $\mathbb{Z}_p$ associated to $E$. We let $\hat{E}(L)$ denote $\hat{E}(m_L)$.

**Definition 2.1.** *We define*

$$\hat{E}^-(k_n) := \{x \in \hat{E}(k_n) | Tr_{n/m+1} x \in \hat{E}(k_m) \text{ for all } -1 \leq m < n,\ m \text{ odd}\},$$

$$\mathbb{H} = \cup_{n=0}^{\infty} \hat{E}^-(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p,$$

$$\mathbb{H}_n = \mathbb{H}^{\Gamma_n}.$$

From [4] we have the following.

**Proposition 2.2.** (1) *Let $\Lambda_P$ denote $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$. We have*

$$\mathrm{Hom}(\mathbb{H}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \Lambda_P^{[K_P:\mathbb{Q}_p]}.$$

(2) *For any integer $m$, $\mathbb{H}_n[p^m]$ is the exact annihilator of itself with respect to the Tate local pairing*

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

*Proof.* This is precisely [4] propositions 3.13 and 3.15 since $k_\infty/k$ is a totally ramified extension. You can also see [4] propositions 3.17 and 3.18. □

Let $f(X)$ be a monic distinguished polynomial of $\Lambda_O$ (*i.e.* $f(X) = X^k + a_1 X^{k-1} + \cdots + a_k$ where $p|a_i$ for every $i$).

Let $Y_f$ denote $\Lambda_O/(f(X))$ and $\Lambda_O$ act on $\mathrm{Hom}_O(Y_f, O)$ as follows: for $\sigma \in \Gamma$ and $\phi \in \mathrm{Hom}_O(Y_f, O)$, $(\sigma \circ \phi)(x) = \phi(\sigma^{-1}x)$. Then $\mathrm{Hom}_O(Y_f, O)$ is isomorphic to $Y_{f^\iota} = \Lambda_O/f^\iota(X)$ as a $\Lambda_O$-module.

We recall $A = E[p^\infty] \otimes O$ and for a character $\eta$ of $\Delta$, $A_\eta$ is $A$ with action twisted by $\eta$. We let $A_f$ denote $A \otimes_O Y_f$ and $A_{f,\eta}$ denote $A_\eta \otimes_O Y_f$. The following is essentially from [5] proposition 8.7.

**Lemma 2.3.** *We have $A^{G_{k_\infty}} = 0$.*

*Proof.* Let $F$ be the unramified quadratic extension of $\mathbb{Q}_p$ and $x$ be any nontrivial $p$-torsion of $\hat{E}$. [5] proposition 8.6 shows $\hat{E}$ is isomorphic over $O_F$ to a Lubin-Tate group of height 2, thus $F(x)$ is a totally ramified extension of $F$ of degree $p^2 - 1$. Since we assume $k$ is an unramified extension of $\mathbb{Q}_p$, $kF$ is also unramified over $\mathbb{Q}_p$. Therefore $\hat{E}(kF)$ does not contain $x$. In other words, $\hat{E}(kF)[p] = 0$.

On the other hand, $\hat{E}(k_n)[p]$ can be written as a union of disjoint orbits $\cup_i [x_i]$ where $[x_i]$ denotes an orbit $\{x_i^\sigma | \sigma \in \mathrm{Gal}(k_n/k)\}$. If $\mathrm{Gal}(k_n/k)$ does not act trivially on $x_i$, the order of $[x_i]$ is divisible by $p$. Since $\hat{E}(k)[p] = 0$, the only point on which $\mathrm{Gal}(k_n/k)$ acts trivially is 0. Therefore the order of $\hat{E}(k_n)[p]$ is not divisible by $p$. Hence $\hat{E}(k_n)[p] = 0$.

Since $E$ has good supersingular reduction at $p$, we have $E[p] = \hat{E}[p]$; therefore we have $E(k_n)[p] = 0$. Since $G_{k_\infty}$ acts trivially on $O$ of $A = E[p^\infty] \otimes O$, we have $A^{G_{k_\infty}} = 0$. □

Since $G_{k_\infty}$ acts trivially on $Y_f$, we have $A_f^{G_{k_\infty}} = 0$ and $A_{f,\eta}^{G_{k_\infty}} = 0$. Thus from the Serre-Hochschild spectral sequence we have

$$H^1(k_n, A_f) \xrightarrow{\sim} H^1(k_\infty, A_f)^{\Gamma_n}.$$

For any integer $m$, we have a short exact sequence

$$0 \to A_f[p^m] \to A_f \xrightarrow{p^m} A_f \to 0.$$

This sequence induces a long exact sequence of cohomology groups. Combined with $A_f^{G_{k_n}} = 0$, this long exact sequence induces

$$H^1(k_n, A_f[p^m]) \xrightarrow{\sim} H^1(k_n, A_f)[p^m].$$

We identify $H^1(k_n, A_f)$ with $H^1(k_\infty, A_f)^{\Gamma_n}$ and $H^1(k_n, A_f[p^m])$ with $H^1(k_n, A_f)[p^m]$. We define the following.

**Definition 2.4.** *We define*

$$\mathbb{H}_f := \mathbb{H} \otimes Y_f \subset H^1(k_\infty, E[p^\infty]) \otimes Y_f = H^1(k_\infty, A_f),$$

$$\mathbb{H}_f^n[p^m] := \mathbb{H}_f[p^m]^{\Gamma_n} \subset H^1(k_n, A_f[p^m]).$$

Since $Y_{f^\iota}$ is isomorphic to $\mathrm{Hom}_O(Y_f, O)$, there is a natural pairing $Y_f \times Y_{f^\iota} \to O$. When we let $G_K$ act on $Y_f$ through the canonical map $G_K \to \Gamma \to \Lambda$ and act on $O$ trivially, we can check that this pairing is an $O$-linear $G_K$-equivariant perfect pairing. Combined with the Weil pairing $E[p^m] \times E[p^m] \to \mathbb{Z}/p^m\mathbb{Z}(1)$, we have an $O$-linear $G_K$-equivariant perfect pairing $A_f[p^m] \times A_{f^\iota}[p^m] \to O/p^mO(1)$. By the cup product this induces a local pairing

$$(\ ,\ )_n : H^1(k_n, A_f[p^m]) \times H^1(k_n, A_{f^\iota}[p^m]) \to H^2(k_n, O/p^mO(1)) \xrightarrow{inv} O/p^mO.$$

We will prove the following proposition.

**Proposition 2.5.** *For any integer $n \geq 0$, $\mathbb{H}_f^n[p^m]$ is the exact annihilator of $\mathbb{H}_{f^\iota}^n[p^m]$ with respect to the pairing above.*

*Proof.* We let $M_n$ be the exact annihilator of $\mathbb{H}_f^n[p^m]$ with respect to $(\ ,\ )_n$ for every integer $n \geq 0$. We consider the maps $\mathrm{Res}_n^{n+1} : H^1(k_n, A_f[p^m]) \to H^1(k_{n+1}, A_f[p^m])$ and $\mathrm{Cor}_n^{n+1} : H^1(k_{n+1}, A_f[p^m]) \to H^1(k_n, A_f[p^m])$. Similar to the discussion before definition 2.4 we can identify $H^1(k_n, A_f[p^m])$ with its image under $\mathrm{Res}_n^{n+1}$ because $\mathrm{Res}_n^{n+1}$ is injective. From [4] proposition 2.1 we have $\mathrm{Res}_n^{n+1} \circ \mathrm{Cor}_n^{n+1} = N_{n+1/n}$. Thus we have

$$\mathrm{Res}_n^{n+1} \circ \mathrm{Cor}_n^{n+1}(\mathbb{H}_f^{n+1}[p^m]) \subset \mathbb{H}_f^{n+1}[p^m]^{\mathrm{Gal}(k_{n+1}/k_n)} = \mathbb{H}_f^n[p^m].$$

Inductively we have $\mathrm{Cor}_n^{n'} \mathbb{H}_f^{n'}[p^m] \subset \mathbb{H}_f^n[p^m]$ for any integer $n' > n$.

Let $j > n$ be an integer large enough so that $G_{k_j}$ acts trivially on $Y_f/p^mY_f$. Combined with proposition 2.2.(2), it implies $M_j = \mathbb{H}_{f^\iota}^j[p^m]$. For $i \leq j$, by the property of cup product we have $(\mathrm{Cor}_i^j\, x, y)_i = (x, \mathrm{Res}_i^j\, y)_j$ for any $x \in H^1(k_j, A_f[p^m])$ and $y \in H^1(k_i, A_{f^\iota}[p^m])$. Assume $(\mathbb{H}_f^n[p^m], y)_n = 0$ (equivalently $y \in M_n$). Then we have $(\mathbb{H}_f^j[p^m], \mathrm{Res}_n^j\, y)_j = 0$ because $\mathrm{Cor}_n^j\, \mathbb{H}_f^j[p^m] \subset \mathbb{H}_f^n[p^m]$. Thus $\mathrm{Res}_n^j\, y \in M_j$, *i.e.*, $M_n \subset M_j$ when we consider $H^1(k_n, A_{f^\iota}[p^m])$ as a subgroup of $H^1(k_j, A_{f^\iota}[p^m])$. More precisely we have $M_n \subset M_j^{\mathrm{Gal}(k_j/k_n)}$. Since we have $M_j = \mathbb{H}_{f^\iota}^j[p^m]$, we have $M_n \subset \mathbb{H}_{f^\iota}^n[p^m]$.

We can check

$$\begin{aligned} |M_n| &= \left|H^1(k_n, A_f[p^m])\right| / \left|\mathbb{H}_f^n[p^m]\right| \\ &= \left|\mathbb{H}_{f^\iota}^n[p^m]\right|. \end{aligned}$$

Thus we have $M_n = \mathbb{H}_{f^\iota}^n[p^m]$. □

## 3. The algebraic functional equation

We fix a finite set $\Sigma$ of places of $\mathbb{Q}$ which includes $p$, all primes of bad reduction of $E$, all primes ramified over $K/\mathbb{Q}$, and infinite places. For a number field $L$ and a set $\Omega$ of places of $\mathbb{Q}$ we let $L_\Omega$ denote the maximal extension of $L$ unramified outside the primes lying above $\Omega$. For any prime $P$ of $K_n$ ($n \le \infty$) lying above $p$, by the Serre-Hochschild sequence we have

$$\begin{aligned} &H^1(K_{n,P}/\mathbb{Q}_{n,p}, A_{f,\eta}^{G_{K_{n,P}}}) \to H^1(\mathbb{Q}_{n,p}, A_{f,\eta}) \\ &\qquad \to H^1(K_{n,P}, A_{f,\eta})^{\mathrm{Gal}(K_{n,P}/\mathbb{Q}_{n,p})} \to H^2(K_{n,P}/\mathbb{Q}_{n,p}, A_{f,\eta}^{G_{K_{n,P}}}). \end{aligned}$$

In the previous section we saw $A_f^{G_{K_{\infty,P}}} = 0$, thus the first and last groups are trivial. Thus we can deduce

$$H^1(\mathbb{Q}_{n,p}, A_{f,\eta}) \xrightarrow{\sim} \left(\prod_{P|p} H^1(K_{n,P}, A_{f,\eta})\right)^{\Delta} = \epsilon_{\bar{\eta}} \prod_{P|p} H^1(K_{n,P}, A_f).$$

**Proposition 3.1.** *Let $\mathbb{H}_P$ denote the group $\mathbb{H}$ in definition 2.1 for each $P|p$. We have an isomorphism of $\Lambda_O$-modules*

$$(\epsilon_\eta \cdot \prod_{P|p} \mathbb{H}_P \otimes O)^\vee \cong \Lambda_O.$$

*Proof.* Since $\mathbb{H}_P^\Gamma \cong \hat{E}(K_P) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong K_P/O_{K_P}$, we have $\epsilon_\eta \prod_{P|p} (\mathbb{H}_P \otimes O)^\Gamma \cong \epsilon_\eta \prod_{P|p} K_P/O_{K_P} \otimes O \cong F/O$. Therefore by Nakayama's lemma the $O$-Pontryagin dual of $\epsilon_\eta \cdot \prod_{P|p} \mathbb{H}_P \otimes O$ is a $\Lambda_O$-module generated by one element, and our claim follows. □

**Definition 3.2.** *We let $\mathbb{H}_{P,f}$ denote $\mathbb{H}_P \otimes Y_f$. For every $m, n \leq \infty$ we let $H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m])$ be the inverse image of $\epsilon_{\bar{\eta}} \prod_{P|p} \mathbb{H}_{P,f}[p^m]^{\Gamma_n}$ under the isomorphism*

$$H^1(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m]) \to \epsilon_{\bar{\eta}} \prod_{P|p} H^1(K_{n,P}, A_f[p^m]).$$

*For a local field $L$ and a $G_L$-module $B$, we let $H^1_{ur}(L, B)$ denote $H^1(L^{ur}/L, B^{L^{ur}})$ where $L^{ur}$ is the maximal unramified extension of $L$. For a prime $w$ not lying above $p$ we let $H^1_{\mathcal{F}}(\mathbb{Q}_{n,w}, A_{f,\eta}[p^m]) = H^1_{ur}(\mathbb{Q}_{n,w}, A_{f,\eta}[p^m])$.*

*We define*

$$H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}[p^m]) = \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, A_{f,\eta}[p^m]) \to \prod \frac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}\right)$$

*where $v$ runs over all the primes of $\mathbb{Q}_n$ lying above $\Sigma$.*

When $f = (X)$, we let $H^1_{\mathcal{F}}(\mathbb{Q}_n, A_\eta[p^m])$ denote $H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}[p^m])$. We note that when $w$ is not lying above $p$, we have $H^1_{ur}(\mathbb{Q}_{\infty,w}, A_\eta) = 0$ because $\mathbb{Q}_{\infty,w}/\mathbb{Q}_v$ is a $\mathbb{Z}_p$-extension.

Since $A_{f,\eta}^{G_{K_{\infty,P}}} = 0$ for any prime $P$ of $K$ with $P|p$, we have $H^1(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m]) = H^1(\mathbb{Q}_{n,p}, A_{f,\eta})[p^m]$, and we can check that under this identification we have

$$H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m]) = H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta})[p^m].$$

The following commutative diagram is given by the property of cup product.

$$\begin{array}{ccccc} H^1(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m]) & \times & H^1(\mathbb{Q}_{n,p}, A_{f^\iota,\bar{\eta}}[p^m]) & \to & O/p^mO \\ \downarrow \mathrm{Res} & & \uparrow \mathrm{Cor} & & \downarrow \\ \epsilon_{\bar{\eta}} \prod_{P|p} H^1(K_{n,P}, A_f[p^m]) & \times & \epsilon_\eta \prod_{P|p} H^1(K_{n,P}, A_{f^\iota}[p^m]) & \to & O/p^mO. \end{array}$$

(Commutativity means we have $(\mathrm{Res}\, x, y) = (x, \mathrm{Cor}\, y)$.) Here Res is an isomorphism as discussed before proposition 3.1. Since $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $[K : \mathbb{Q}]$ and $[K : \mathbb{Q}]$ is prime to $p$, we have

$$\mathrm{Cor}(\epsilon_\eta \prod_{P|p} \mathbb{H}_{P,f^\iota}[p^m]^{\Gamma_n}) = \mathrm{Cor} \circ \mathrm{Res}\left(H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f^\iota,\bar{\eta}}[p^m])\right) = H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f^\iota,\bar{\eta}}[p^m]).$$

Thus $H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m])$ is the exact annihilator of $H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f^\iota,\bar{\eta}}[p^m])$. From [1] chapter 8 we have the following.

**Lemma 3.3.** *For $m, n < \infty$ we have $\left|H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}[p^m])\right| = \left|H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f^\iota,\bar{\eta}}[p^m])\right|$.*

*Proof.* For a totally real field $F$ and a finite $G_F$-module $M$ let $\chi_F(M)$ denote the Euler characteristic $|H^0(F, M)| \cdot |H^2(F, M)|/|H^1(F, M)|$. Assume that the order of $M$ is prime to 2. Then it is known that $\chi_F(M) = 1/|M^-|^{[F:\mathbb{Q}]}$ where $M^-$ is the maximal subgroup of $M$ where the complex conjugation acts by multiplication by -1.

Let $F = \mathbb{Q}_n$, $M = A_{f,\eta}[p^m]$, and $M^* = A_{f^\iota,\bar{\eta}}[p^m]$. We can easily check $M^* = \mathrm{Hom}_O(M, O/p^mO(1))$.

Following Greenberg ([1]) we use the following notation: we let

$$S := H^1_{\mathcal{F}}(F, M), \qquad S^* := H^1_{\mathcal{F}}(F, M^*),$$
$$P^i_\Sigma := \prod H^i(F_v, M), \qquad P^{i,*}_\Sigma := \prod H^i(F_v, M^*),$$

(every product in this proof runs over all places $v$ of $F$ lying above $\Sigma$ unless mentioned otherwise),

$$L_v := H^1_{\mathcal{F}}(F_v, M), \qquad L^*_v := H^1_{\mathcal{F}}(F_v, M^*),$$
$$L := \prod L_v, \qquad L^* := \prod L^*_v,$$
$$\lambda^i : H^i(F_\Sigma/F, M) \to P^i_\Sigma,$$
$$G^i := \operatorname{im}\lambda^i, \quad K^i = \ker\lambda^i,$$

(and define $\lambda^{i,*}$, $G^{i,*}$, and $K^{i,*}$ similarly).

Then we have

$$|S| = |K^1| \cdot |G^1 \cap L| = |K^1| \cdot |G^1| \cdot |L| \cdot |G^1 \cdot L|^{-1}.$$

We have $|K^1| \cdot |G^1| = |H^1(F_\Sigma/F, M)|$. By global duality $G^1$ is the exact annihilator of $G^{1,*}$ with respect to the local pairing between $P^1_\Sigma$ and $P^{1,*}_\Sigma$ (for a statement of global duality or Poitou-Tate duality see [6] Theorem I.4.10 or [10] Theorem 3.1).

If $v|p$, $L_v$ is the exact annihilator of $L^*_v$ by our previous discussion. If $v \nmid p$, it follows from the definition that $L_v$ is the exact annihilator of $L^*_v$. Hence we have $|G^1 \cdot L| = |P^1_\Sigma|/|G^{1,*} \cap L^*|$. Therefore we have

$$|S| = |H^1(F_\Sigma/F, M)| \cdot |L| \cdot \frac{|G^{1,*} \cap L^*|}{|P^1_\Sigma|}.$$

From the definition of the global Euler characteristic we have

$$\begin{aligned} |H^1(F_\Sigma/F, M)| &= \chi_F(M)^{-1}|H^0(F_\Sigma/F, M)| \cdot |H^2(F_\Sigma/F, M)| \\ &= \chi_F(M)^{-1}|H^2(F_\Sigma/F, M)|. \end{aligned}$$

By global duality we have $|K^{1,*}| = |K^2|$, and thus we have

$$|G^{1,*} \cap L^*| = |S^*|/|K^{1,*}| = |S^*|/|K^2|.$$

On the other hand, by global duality we have $|\operatorname{coker}\lambda^2| = |H^0(F_\Sigma/F, M^*)|$; thus we have

$$\frac{|H^2(F_\Sigma/F, M)|}{|K^2|} = |G^2| = \frac{|P^2_\Sigma|}{|\operatorname{coker}\lambda^2|} = \frac{|P^2_\Sigma|}{|H^0(F_\Sigma/F, M^*)|} = |P^2_\Sigma|.$$

Then we check

$$\begin{aligned} \frac{|L|}{|P^1_\Sigma|} &= \frac{\prod_{v\nmid p} |H^1(F^{ur}_v/F_v, M^{I_v})|}{\prod_{v\nmid p} |H^1(F_v, M)|} \prod_{P|p} \frac{|L_P|}{|H^1(F_P, M)|} \\ &= \prod_{v\nmid p} \frac{|H^0(F_v, M)|}{|H^1(F_v, M)|} \cdot \frac{1}{|M|^{p^n[K:\mathbb{Q}]}}. \end{aligned}$$

Since we have $\chi_F(M)^{-1} = |M|^{p^n[K:\mathbb{Q}]}$ and $|H^1(F_v, M)| = |H^0(F_v, M)| \cdot |H^2(F_v, M)|$ when $v \nmid p$, we obtain $|S| = |S^*|$. $\square$

**Lemma 3.4.** *The kernel and cokernel of*

$$H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}[p^m]) \to H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta})[p^m]$$

*are finite and bounded as* $m, n$ *vary.*

*Proof.* We consider the following diagram.

$$\begin{array}{ccccc} 0 \to & H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}[p^m]) & \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, A_{f,\eta}[p^m]) \to & \displaystyle\prod_v \frac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])} \\ & \downarrow & \downarrow & \downarrow \\ 0 \to & H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta})[p^m] & \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, A_{f,\eta})[p^m] \to & \displaystyle\prod_v \frac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta})}. \end{array}$$

(every product in this proof runs over all primes lying above $\Sigma$ unless mentioned otherwise). The center vertical map is naturally surjective, and its kernel is $A_{f,\eta}^{G_{\mathbb{Q}_n}}/p^m A_{f,\eta}^{G_{\mathbb{Q}_n}} = 0$.

We let $f_{v,m}$ denote the map $\dfrac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])} \to \dfrac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta})}$ for each $v$. As mentioned after definition 3.2 we have $H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta}[p^m]) = H^1_{\mathcal{F}}(\mathbb{Q}_{n,p}, A_{f,\eta})[p^m]$, thus $f_{p,m}$ is injective. Let $v$ be a prime not lying above $p$. From the Serre-Hochschild spectral sequence we can see that $\dfrac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta}[p^m])}$ and $\dfrac{H^1(\mathbb{Q}_{n,v}, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_{n,v}, A_{f,\eta})}$ are subgroups of $H^1(\mathbb{Q}_{n,v}^{ur}, A_{f,\eta}[p^m])$ and $H^1(\mathbb{Q}_{n,v}^{ur}, A_{f,\eta})$ respectively. From the long exact sequence induced from $A_{f,\eta}[p^m] \to A_{f,\eta} \xrightarrow{p^m} A_{f,\eta}$ we have

$$A_{f,\eta}^{I_v}/p^m A_{f,\eta}^{I_v} = \ker\left(H^1(\mathbb{Q}_{n,v}^{ur}, A_{f,\eta}[p^m]) \to H^1(\mathbb{Q}_{n,v}^{ur}, A_{f,\eta})\right).$$

Let $l$ be the residue characteristic of $v$ and fix an embedding $\overline{\mathbb{Q}} \to \mathbb{C}_l$ such that $v$ is the prime of $\mathbb{Q}_n$ corresponding to this embedding. Let $n'$ be any integer bigger than $n$ and $w$ be the prime of $\mathbb{Q}_{n'}$ corresponding to the embedding. Since $I_v = I_w$, we have $A_{f,\eta}^{I_v}/p^m A_{f,\eta}^{I_v} = A_{f,\eta}^{I_w}/p^m A_{f,\eta}^{I_w}$. In other words, $A_{f,\eta}^{I_v}/p^m A_{f,\eta}^{I_v}$ does not depend on $n$.

Furthermore, the size of $A_{f,\eta}^{I_v}/p^m A_{f,\eta}^{I_v}$ is bounded by the size of $A_{f,\eta}^{I_v}/(A_{f,\eta}^{I_v})_{div}$. Since no prime splits completely over $\mathbb{Q}_\infty/\mathbb{Q}$, the kernel of $\prod_v f_{v,m}$ is bounded as $m, n$ vary. By the Snake Lemma our claim follows. $\square$

From lemmas 3.3 and 3.4 we have the following corollary.

**Corollary 3.5.** *We have* $\operatorname{corank}_O H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f,\eta}) = \operatorname{corank}_O H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{f^\iota,\bar{\eta}})$ *for every* $n$. *Also* $\left|H^1_{\mathcal{F}}(\mathbb{Q}_n, A_\eta)[p^m]\right| / \left|H^1_{\mathcal{F}}(\mathbb{Q}_n, A_{\bar{\eta}})[p^m]\right|$ *is bounded as* $m, n$ *vary.*

We note the following proposition.

**Proposition 3.6** ([1] chapter 3)**.** *Let $X$ and $Y$ be co-finitely generated $\Lambda_O$-modules. Assume that $X, Y$ satisfy*

*1.* $\mathrm{corank}_O(X \otimes_O \Lambda_O/(f^e))^\Gamma = \mathrm{corank}_O(Y \otimes_O \Lambda_O/(f^e))^\Gamma$ *for every monic irreducible distinguished polynomial $f(X) \in \Lambda_O$ and every $e < \infty$,*

*2. for every $e < \infty$, $|X^{\Gamma_n}[p^e]|/|Y^{\Gamma_n}[p^e]|$ is bounded as $n$ varies.*

*Then $X^\vee$ is pseudo-isomorphic to $Y^\vee$.*

Using proposition 3.6 we prove the following.

**Proposition 3.7.** *Let $X_\eta$ be $H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)^\vee$. Then we have $X_\eta \sim X^\iota_{\bar{\eta}}$ as $\Lambda_O$-modules.*

*Proof.* Since $G_{\mathbb{Q}_\infty}$ acts trivially on $Y_f$ and $Y_f$ is a free $O$-module, we have

$$\begin{aligned} H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta) \otimes Y_f &= \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A_\eta) \otimes Y_f \to \prod_w \frac{H^1(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}\right) \\ &= \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A_{f,\eta}) \to \prod_w \frac{H^1(\mathbb{Q}_{\infty,w}, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}\right) \end{aligned}$$

where $w$ runs over all the primes lying above $\Sigma$.

Using the Serre-Hochschild spectral sequence one can easily check

$$H^1(\mathbb{Q}, A_{f,\eta}) \xrightarrow{\sim} H^1(\mathbb{Q}_\infty, A_{f,\eta})^\Gamma. \tag{2}$$

From the definition we have

$$(H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,p}, A_\eta) \otimes Y_f)^\Gamma = (\epsilon_{\bar{\eta}} \cdot \prod_{P|p} \mathbb{H}_P \otimes Y_f)^\Gamma = H^1_{\mathcal{F}}(\mathbb{Q}_p, A_{f,\eta}),$$

thus we have an injection

$$0 \to \frac{H^1(\mathbb{Q}_p, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_p, A_{f,\eta})} \to \frac{H^1(\mathbb{Q}_{\infty,p}, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,p}, A_\eta) \otimes Y_f}. \tag{3}$$

For any prime $w$ of $\mathbb{Q}_\infty$ lying above a prime $v \neq p$ of $\mathbb{Q}$, we have $H^1(\mathbb{Q}_v^{ur}, A_{f,\eta}) = H^1(\mathbb{Q}_{\infty,w}, A_{f,\eta})$ because $\mathbb{Q}_{\infty,w}/\mathbb{Q}_v$ is a $\mathbb{Z}_p$-extension (in fact, the only $\mathbb{Z}_p$-extension and the only unramified $\mathbb{Z}_p$-extension). For the same reason we have

$$H^1(\mathbb{Q}^{ur}_{\infty,w}/\mathbb{Q}_{\infty,w}, A_\eta^{G_{\mathbb{Q}^{ur}_{\infty,w}}}) = H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,w}, A_\eta) = 0.$$

Thus we have

$$\frac{H^1(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f} = \frac{H^1(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}{H^1_{ur}(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f} = H^1(\mathbb{Q}_{\infty,w}, A_{f,\eta}) = H^1(\mathbb{Q}_v^{ur}, A_{f,\eta}).$$

Since $\dfrac{H^1(\mathbb{Q}_v, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_v, A_{f,\eta})} \to H^1(\mathbb{Q}_v^{ur}, A_{f,\eta})$ is an injection by the definition of $H^1_{\mathcal{F}}$, we have an injection

$$0 \to \frac{H^1(\mathbb{Q}_v, A_{f,\eta})}{H^1_{\mathcal{F}}(\mathbb{Q}_v, A_{f,\eta})} \to \frac{H^1(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,w}, A_\eta) \otimes Y_f}. \tag{4}$$

From (2), (3), (4), and the snake lemma we can see $H^1_{\mathcal{F}}(\mathbb{Q}, A_{f,\eta}) = (H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta) \otimes Y_f)^\Gamma$.

Combined with corollary 3.5 we have

$$\mathrm{corank}_O (H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta) \otimes Y_f)^\Gamma = \mathrm{corank}_O (H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_{\bar{\eta}}) \otimes Y_{f^\iota})^\Gamma.$$

Similarly we can check $H^1_{\mathcal{F}}(\mathbb{Q}_n, A_\eta) = H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)^{\Gamma_n}$. By corollary 3.5 we can see $|H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)^{\Gamma_n}[p^m]|/|H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_{\bar{\eta}})^{\Gamma_n}[p^m]|$ is bounded as $m$ and $n$ vary.

By proposition 3.6 our claim follows. □

We let $H^1_{\mathcal{F}}(K_{\infty,P}, A) := \mathbb{H}_P \otimes O$ and $H^1_{\mathcal{F}}(K_{\infty,P}, E[p^\infty]) := \mathbb{H}_P$ for $P|p$, and let $H^1_{\mathcal{F}}(K_{\infty,w}, A) := H^1_{ur}(K_{\infty,w}, A)$ and $H^1_{\mathcal{F}}(K_{\infty,w}, E[p^\infty]) := H^1_{ur}(K_{\infty,w}, E[p^\infty])$ for primes $w$ not lying above $p$. We define a group

$$S_p^-(A/K_\infty) := \ker\left( H^1(K_\Sigma/K_\infty, A) \to \prod_w \frac{H^1(K_{\infty,w}, A)}{H^1_{\mathcal{F}}(K_{\infty,w}, A)} \right),$$

and the minus Selmer group

$$Sel_p^-(E/K_\infty) := \ker\left( H^1(K_\Sigma/K_\infty, E[p^\infty]) \to \prod_w \frac{H^1(K_{\infty,w}, E[p^\infty])}{H^1_{\mathcal{F}}(K_{\infty,w}, E[p^\infty])} \right)$$

where $w$ runs over all the places lying above $\Sigma$. We can easily check $S_p^-(A/K_\infty) = Sel_p^-(E/K_\infty) \otimes O$ (compare this definition with that of [5], [2], and [4]).

We note that the definitions of $H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)$ and $S_p^-(A/K_\infty)$ do not depend on the choice of $\Sigma$. Indeed when we take all places of $\mathbb{Q}$ for $\Sigma$, we still have the same $H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta)$ and $S_p^-(A/K_\infty)$. We consider the following diagram:

$$\begin{array}{ccccccc}
0 \to & H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta) \to & H^1(\mathbb{Q}_\infty, A_\eta) \to & \displaystyle\prod_v \frac{H^1(\mathbb{Q}_{\infty,v}, A_\eta)}{H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,v}, A_\eta)} \\
 & \downarrow & \downarrow & \downarrow \prod f_v \\
0 \to & S_p^-(A/K_\infty)^{\bar{\eta}} \to & H^1(K_\infty, A)^{\bar{\eta}} \to & \displaystyle\prod_w \frac{H^1(K_{\infty,w}, A)}{H^1_{\mathcal{F}}(K_{\infty,w}, A)}
\end{array}$$

where $v$ and $w$ run over all places of $\mathbb{Q}_\infty$ and $K_\infty$ respectively.

Since $A^{G_{K_{\infty,P}}} = 0$ for any prime $P$ lying above $p$, we have $A^{G_{K_\infty}} = 0$. Using that, we have $H^1(K_\infty, A)^{\bar{\eta}} = H^1(K_\infty, A_\eta)^{\mathrm{Gal}(K/\mathbb{Q})} = H^1(\mathbb{Q}_\infty, A_\eta)$ by the Serre-Hochschild spectral sequence. From the definition of $H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,p}, A_\eta)$ we can see $f_p$ is an injection. Recall that when $v$ and $w$ are not lying above $p$, we have $H^1_{\mathcal{F}}(\mathbb{Q}_{\infty,v}, A_\eta) = H^1_{\mathcal{F}}(K_{\infty,w}, A) = 0$. Since the order of $\mathrm{Gal}(K_{\infty,w}/\mathbb{Q}_{\infty,v})$ is prime to $p$, we have

$$\ker\left(H^1(\mathbb{Q}_{\infty,v}, A_\eta) \to H^1(K_{\infty,w}, A_\eta)\right) = H^1(K_{\infty,w}/\mathbb{Q}_{\infty,v}, A_\eta^{G_{K_{\infty,w}}}) = 0.$$

Thus we have the following.

**Proposition 3.8.** *We have* $H^1_{\mathcal{F}}(\mathbb{Q}_\infty, A_\eta) \cong S_p^-(A/K_\infty)^{\bar{\eta}}$.

The next proposition is a simple consequence of Rohrlich and Kato's work.

**Proposition 3.9.** *$Sel_p^-(E/K_\infty)$ is $\Lambda$-cotorsion.*

*Proof.* For a finite group $G$, a character $\chi$ of $G$, and a $\mathbb{Z}_p[G]$-module $M$ we let $M^\chi$ be the $\chi$-part of $M \otimes \mathbb{Z}_p[\chi]$. By [4] lemma 4.20 there is an integer $N$ such that for any $n > N$ with odd $n - N$ and a primitive character $\chi$ of $\mathrm{Gal}(K_n/K_N)$ we have

$$\mathrm{corank}_{\mathbb{Z}_p[\chi]}\, Sel_p(E/K_n)^\chi = \mathrm{rank}_{\mathbb{Z}_p[\chi]} \left(Sel_p^-(E/K_\infty)^{\Gamma_n}\right)^\chi .$$

By Rohrlich ([8], [9]) $L(E/\mathbb{Q}, \chi, 1) \neq 0$ for all but finitely many Dirichlet characters $\chi$ of $\mathrm{Gal}(K_n/\mathbb{Q})$ as $n$ varies. By Kato ([3]), if $L(E/\mathbb{Q}, \chi, 1) \neq 0$, we have $\mathrm{corank}_{\mathbb{Z}_p[\chi]}\, Sel_p(E/K_n)^\chi = 0$. Therefore there are infinitely many integers $n$ such that $\mathrm{corank}_{\mathbb{Z}_p[\chi]} \left(Sel_p^-(E/K_\infty)^{\Gamma_n}\right)^\chi = 0$ for any primitive character $\chi$ of $\mathrm{Gal}(K_n/K_N)$. Thus $Sel_p^-(E/K_\infty)$ is $\Lambda$-cotorsion. $\square$

Combined with propositions 3.7 and 3.8 we have the following.

**Theorem 3.10.** *Let $X = (Sel_p^-(E/K_\infty) \otimes O)^\vee$. For each character $\eta$ of $\Delta$ we have $X^\eta \sim X^{\iota,\bar{\eta}}$ as $\Lambda_O$-modules, or equivalently $X \sim X^\iota$ as $O[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$-modules. Consequently we have the following: let $(a) \subset \Lambda$ be the characteristic ideal of $Sel_p^-(E/K_\infty)^\vee$. We have $(a) = (a^\iota)$.*

It is more tricky to deal with $Sel_p^+(E/K_\infty)$. Although it is not explained in [4], it is not clear that the plus norm subgroup in [4] always has the property the minus norm subgroup has. More specifically (using the notation of [4] propositions 3.12 and 3.13) it is not clear that the set $\{c_{0,i}\}_{0,1,\cdots,d-1}$ linearly generates $\hat{E}(m)$. Consequently it is not clear that we have $(\cup_{n=1}^\infty \hat{E}^+(m_{k_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \Lambda^d$. However, Kobayashi's plus/minus norm subgroups for $\mathbb{Q}(\mu_{p^\infty})$ have this property. We can apply our technique to both $\pm$-Selmer groups with little difficulty to obtain the following.

**Theorem 3.11.** *We have*

$$Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty}))^\vee \sim Sel_p^\pm(E/\mathbb{Q}(\mu_{p^\infty}))^{\vee,\iota}$$

*where $\sim$ is a pseudoisomorphism for $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$-modules.*

Iovita and Pollack's plus/minus norm subgroups also work well under the following condition: The prime $p$ splits completely over $K/\mathbb{Q}$. Note that any prime of $K$ lying above $p$ is totally ramified in the cyclotomic $\mathbb{Z}_p$-extension $K_\infty$. Assuming this condition we can prove a similar result.

**Theorem 3.12.** *We have*

$$\left(Sel_p^\pm(E/K_\infty) \otimes O\right)^\vee \sim \left(Sel_p^\pm(E/K_\infty)^\iota \otimes O\right)^\vee .$$


## Acknowledgements

The author is grateful to Karl Rubin, Ralph Greenberg, and Robert Pollack for many insightful conversations. He is also grateful to the anonymous referee for many good suggestions.

## References


[1] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure Math. (1989), no. 17, 97–137.

[2] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over* $\mathbb{Z}_p$*-extensions of number fields*, to appear in Crelle.

[3] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms* (2004), no. 295, 117–290.

[4] B. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compositio Math. (2007), no. 143, 47–72.

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

[6] J. Milne, *Arithmetic duality theorems*, Perspectives in Math, 1 (1986)

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

[8] D. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. (1984), no. 75, 404–423.

[9] ———, *L-functions and division towers*, Math. Ann. (1988), no. 281, 611–632.

[10] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Cong. Math. (1962)



Department of Mathematics, Northwestern University, 2033 Sheridan Road, Evanston, IL, 60208 U.S.A.

*E-mail address*: bdkim@math.northwestern.edu