ON THE REFINED CONJECTURES ON FITTING IDEALS OF SELMER GROUPS OF ELLIPTIC CURVES WITH SUPERSINGULAR REDUCTION

CHAN-HO KIM AND MASATO KURIHARA

Abstract. In this paper, we study the Fitting ideals of Selmer groups over finite subextensions in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ of an elliptic curve over $\mathbb{Q}$. Especially, we present a proof of the “weak main conjecture” à la Mazur and Tate for elliptic curves with good (supersingular) reduction at an odd prime $p$. We also prove the “strong main conjecture” suggested by the second named author under certain assumptions. The key idea is the explicit comparison among “finite layer objects”, “±-objects”, and “fine objects” in Iwasawa theory. The case of good ordinary reduction and their non-primitive variants are also treated.

Contents

1. Introduction .............................. 1
2. Review of the case for elliptic curves with good ordinary reduction .... 8
3. Tools from ±-Iwasawa theory .......... 9
4. Comparison of local conditions at $p$ ... 12
5. The non-CM case ......................... 14
6. Vanishing of coker $g_n$ .................. 19
7. Allowing the Tamagawa defect ........ 22
Acknowledgement ............................ 24
Appendix A. Lemmas on Fitting ideals ... 25
References ................................ 27

1. Introduction

1.1. Overview. The aim of this paper is to understand Selmer groups of an elliptic curve with supersingular reduction at $p$ over finite subextensions in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ by using ±-Iwasawa theory à la Kobayashi-Pollack. Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at an odd prime $p$. We assume that $a_p(E) \not\equiv 1 \pmod{p}$ throughout this article.

The ±-Iwasawa theory is developed to understand Iwasawa theory for elliptic curves at supersingular primes (with assumption $a_p(E) = 0$). In the supersingular setting, the usual Selmer groups over $\mathbb{Z}_p$-extensions and $p$-adic $L$-functions do not behave well in the classical framework of Iwasawa theory. Introducing ±-Selmer groups and ±-$p$-adic $L$-functions, Kobayashi [Kob03] and Pollack [Pol03] could apply the standard techniques of Iwasawa theory of elliptic curves with ordinary reduction to the supersingular setting.

On the other hand, Mazur-Tate conjectures [MT87] and the refined Iwasawa theory à la the second named author ( [Kur02], [Kur03], and [Kur14]) focus on understanding Iwasawa theory over finite abelian extensions over $\mathbb{Q}$.

In general, the refined Iwasawa theory (at finite layers) is regarded as a more delicate subject than the usual Iwasawa theory (at the infinite layer) since neither we can apply the theory...
of Iwasawa modules to finite layer objects nor we can ignore “finite errors”. It is well-known that the structure of group rings at finite layers is much more complicated than that of the Iwasawa algebra.

In this article, we consider the following conjectures for subextensions in the cyclotomic $\mathbb{Z}_p$-extension. This case is the simplest because the Galois group is cyclic of $p$-power order, and only one prime ramifies. Their precise formulations are given in §1.2.

**Conjecture 1.1** (Mazur-Tate’s weak main conjecture, Conjecture 1.4). Assume that $E$ has no rational $p$-torsion. Then the Mazur-Tate element of $E$ at a finite layer is contained in the Fitting ideal of the dual Selmer group of $E$ over the finite extension.

**Conjecture 1.2** (The strong main conjecture, Conjecture 1.6). Assume that $E$ has no rational $p$-torsion and $p$ does not divide the Tamagawa number of $E$. Then the Mazur-Tate element of $E$ at a finite layer and the traces of the Mazur-Tate elements of $E$ at all the lower layers generate the Fitting ideal of the dual Selmer group of $E$ over the finite extension.

In the case of good ordinary reduction with non-anomalous prime $p$ ($a_p(E) \not\equiv 1 (\mod p)$), both conjectures follow from several standard ingredients in Iwasawa theory, including (the Euler system divisibility of) the main conjecture, the non-existence of proper $\Lambda$-submodules of finite index in the Selmer groups over the Iwasawa algebra $\Lambda$, and the exact control theorem. Although this case is more or less well-known to experts, the argument is not explicitly written in the literature. Thus, we give a proof for the case of good ordinary reduction in §2. We note that in this case the Fitting ideal of the Selmer group is principal.

In the case of good supersingular reduction, the situation becomes much more complicated. Actually, the Fitting ideal of the Selmer group is never principal in this case. Very fortunately, we are able to strengthen the argument of the good ordinary reduction case by making an explicit comparison between Selmer groups and $\pm$-Selmer groups in finite layers. This approach allows us to obtain the weak main conjecture (Conjecture 1.4). The proof is given in §4. We obtain Theorem 1.14 (Main Theorem I) in this way.

Concerning the strong main conjecture, we prove it under certain assumptions in Theorem 1.20 (Main Theorem III). Since there are many examples which satisfy these assumptions (Example 1.21), we provide many examples for which the strong main conjecture (Conjecture 1.6) holds. More generally, even without assuming the assumptions in Theorem 1.20, we are able to prove Theorem 1.18 (Main Theorem II), which is slightly weaker than the strong main conjecture, since the statement involves an error term.

In the proof of Theorem 1.18, we make an explicit comparison between Selmer groups and fine Selmer groups in finite layers. This comparison can be regarded as the finite layer version of the construction of algebraic $p$-adic $L$-functions à la Perrin-Riou. See [PR00, 2.4.3 Proposition], [PR03, §3.1], for example. The error term in Theorem 1.18 occurs in this finite layer comparison. Indeed, the assumptions in Theorem 1.20 are strong enough to force the error term to vanish. As a result, we deduce a “lower bound” of Selmer groups over finite extensions from the Iwasawa main conjecture and some Fitting ideal techniques (in Appendix A). The proof of Theorem 1.18 is given in §5 and the proof of Theorem 1.20 is given in §6.

It seems that our approach does not work directly for a more general non-ordinary setting (possibly non-zero $a_p(E)$) since the $\mathbb{Z}/b$-Iwasawa theory à la Sprung [Spr12] does not behave well in finite layers. See [Spr12, Open Problem 7.22] for detail.

In the rest of this section, we introduce various conjectures we concern and state our main results and their applications. In §2, we review the case for elliptic curves with good ordinary reduction and give a proof of Theorem 1.14 (Main Theorem I) for this case. In §3, we review relevant $\pm$-Iwasawa theory for elliptic curves. In §4, we prove Theorem 1.14 (Main Theorem I) for elliptic curves with supersingular reduction. In §5, we prove Theorem 1.18 (Main Theorem II). In §6, we prove Theorem 1.20 (Main Theorem III). In §7, we consider a non-primitive
generalization of Main Theorem I (Theorem 1.22) removing the restriction on Tamagawa numbers. In Appendix A, we study refined techniques on Fitting ideals.

1.2. Conjectures. We recall various conjectures on the arithmetic of elliptic curves.

1.2.1. Birch and Swinnerton-Dyer conjecture. One of the leading problems of modern number theory is the following conjecture.

Conjecture 1.3 (Birch and Swinnerton-Dyer). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then

\[
\text{rk}_\mathbb{Z}E(\mathbb{Q}) = \text{ord}_{s=1}L(E, s).
\]

We recall the formulation of the refinements and variants of Conjecture 1.3.

1.2.2. Setting the stage. Let \( p \) be an odd prime. Fix embeddings \( \iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \) and \( \iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C} \).

Let \( E \) be an elliptic curve over \( \mathbb{Q} \) of conductor \( N \) with \( (N, p) = 1 \). Let \( n \geq 1 \) be an integer. Let \( Q_n \) be the subextension of \( \mathbb{Q} \) in \( \mathbb{Q}(\mu_{p^n+1}) \) with \( \text{Gal}(Q_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z} \).

Let \( Q_\infty = \bigcup_{n \geq 1} Q_n \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \). Let \( \Gamma_n := \text{Gal}(Q_\infty/Q_n) \) and \( \Gamma := \text{Gal}(Q_\infty/\mathbb{Q}) \).

Let \( \Lambda := \mathbb{Z}_p[\text{Gal}(Q_n/Q)] = \mathbb{Z}_p[\Gamma/\Gamma_n] \) and \( \Lambda := \lim_{\leftarrow n} \Lambda_n = \mathbb{Z}_p[\text{Gal}(Q_\infty/Q)] = \mathbb{Z}_p[\Gamma] \). Let \( \omega_n = \omega_n(X) := (1 + X)^{pn} - 1 \) Fixing a generator of \( \text{Gal}(Q_n/\mathbb{Q}) \) and \( \text{Gal}(Q_\infty/\mathbb{Q}) \), respectively, we have isomorphisms

\[
\Lambda_n \simeq \mathbb{Z}_p[X]/(\omega_n(X)) \quad \Lambda \simeq \mathbb{Z}_p[X]
\]

by sending the generators to \( 1 + X \). Via the latter isomorphism, we also regard \( \omega_n \in \Lambda \).

Let \( \Phi_n(1 + X) = \omega_n/\omega_{n-1} \) where \( \Phi_n \) is the \( p^n \)-th cyclotomic polynomial. Let \( \omega_0^\pm(X) := X \) and \( \omega_0^\pm(X) := 1 \) and

\[
\omega_n^+ = \omega_n^+(X) := X \cdot \prod_{0 < m \leq n, m: \text{odd}} \Phi_m(1 + X) \quad \omega_n^- = \omega_n^-(X) := X \cdot \prod_{0 < m \leq n, m: \text{even}} \Phi_m(1 + X)
\]

Then we have \( \omega_n(X) = \omega_n^+(X) \cdot \omega_n^-(X) \), respectively. We also regard \( \omega_n^\pm, \omega_n^\pm \) as elements in \( \Lambda_n \) or \( \Lambda \) via fixed isomorphisms. Also, we identify \( \Lambda_n = \mathbb{Z}_p[\text{Gal}(Q_n/Q)] \simeq \mathbb{Z}_p[\text{Gal}(Q_n/pQ)] \) if necessary. Here, \( Q_{n,p} \) is the completion of \( Q_n \) at \( p \).

Let \( f \in S_2(\Gamma_0(N)) \) be the newform attached to \( E \) by [BCDT01, Theorem A]. Let \( G'_{n+1} := \text{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q})/\{\pm 1\} \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \times \{\pm 1\} \) and denote by \( \sigma_a \) the element corresponding to \( a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times /\{\pm 1\} \). We define

\[
\theta'_{n+1}(f) := \sum_{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times /\{\pm 1\}} \left[ \frac{a}{p^{n+1}} \right]^+ \cdot \sigma_a \in \mathbb{Z}_p[G'_{n+1}].
\]

Here, \( \left[ \frac{a}{b} \right]^+ \) is defined by

\[
2\pi \int_0^\infty f \left( \frac{a}{b} + iy \right) dy = \left[ \frac{a}{b} \right]^+ \cdot \Omega_E^+ + \left[ \frac{a}{b} \right]^- \cdot \Omega_E^-
\]

where \( \Omega_E^\pm \) are the Néron periods of \( E \). We write \( \Omega_E = \Omega_E^+ \). The Mazur-Tate element \( \theta_n(f) \) of \( f \) at \( Q_n \) is defined by the image of \( \theta'_{n+1}(f) \) in \( \Lambda_n \). For simplicity, we assume that \( E[p] \) is irreducible, and then we do not have to care about the integrality of Mazur-Tate elements and the Manin constant issue. See [Kur02, page 200–201].
We also define
\[ \delta_n := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left( \frac{a}{n} \right)^+ \cdot \prod_{\ell | n} \log_{\ell}(a) \in \mathbb{F}_p \]
where \( n \) is the square-free product of Kolyvagin primes, \( \left( \frac{a}{n} \right)^+ \) is the mod \( p \) reduction of \( \left( \frac{a}{n} \right) \), and \( \log_{\ell}(a) \) is the mod \( p \) reduction of the discrete logarithm of \( a \) modulo \( \ell \) (with a fixed primitive root modulo \( \ell \), indeed). Here, a prime \( \ell \) is a Kolyvagin prime if \( (\ell, Np) = 1 \), \( \ell \equiv 1 \pmod{p} \), and \( a_\ell(E) \equiv \ell + 1 \pmod{p} \). This number is used to check the equality of the main conjecture for elliptic curves with any good reduction.

Let \( \Sigma \) be a finite set of places of \( \mathbb{Q} \) including \( p, \infty \), and the bad reduction primes of \( E \), and \( \mathbb{Q}_\Sigma \) be the maximal extension of \( \mathbb{Q} \) unramified outside \( \Sigma \). We define the \textbf{Selmer group of \( E \) over \( \mathbb{Q}_n \)} by
\[
\text{Sel}(\mathbb{Q}_n, E[p^\infty]) := \ker \left( H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) \to \prod_v \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)
\]
where \( H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) := H^1(\text{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_n), E[p^\infty]) \) is the Galois cohomology group, \( v \) runs over all the (finite) places of \( \mathbb{Q}_n \) dividing the places in \( \Sigma \), and \( \mathbb{Q}_{n,v} \) is the completion of \( \mathbb{Q}_n \) at \( v \). We also define the \textbf{Selmer group of \( E \) over \( \mathbb{Q}_\infty \)} by
\[
\text{Sel}(\mathbb{Q}_\infty, E[p^\infty]) := \lim_{n \to \infty} \text{Sel}(\mathbb{Q}_n, E[p^\infty]).
\]
For a \( \mathbb{Z}_p \)-module \( M \), let \( M^\vee := \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) \). For a ring \( R \) and a finitely presented \( R \)-module \( M \), we denote its Fitting ideal by \( \text{Fitt}_R(M) \).

1.2.3. Mazur-Tate’s refined conjecture. In [MT87], Mazur and Tate gave the following conjecture, which implies Conjecture 1.15. Conjecture 1.15 is a refinement of the Birch and Swinnerton-Dyer conjecture (Conjecture 1.3) in some sense. As we said in §1.1, \( a_p(E) \equiv 1 \pmod{p} \) is always assumed.

\textbf{Conjecture 1.4} ([MT87, Conjecture 3, “weak main conjecture”]).
\[
\theta_n(f) \in \text{Fitt}_{\Lambda_n} \left( \text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \right).
\]

\textbf{Remark 1.5.} Note that the original statement covers general abelian extensions of \( \mathbb{Q} \) as we mentioned in §1.1. There are other approaches towards Conjecture 1.4 due to Bley-Macias Castillo [BMC17, Theorem 2.12] assuming the \( p \)-part of the relevant equivariant Tamagawa number conjecture, Emerton-Pollack-Weston [EPW] using the \( p \)-adic local Langlands correspondence as well as Kato’s zeta elements, and C. Popescu using the theory of 1-motives. If \( a_p(E) \equiv 1 \pmod{p} \), then the formulation would not seem to work for certain cases.

1.2.4. The (refined)\(^2\) conjecture. Comparing with Conjecture 1.4, the second named author proposed the following more refined conjecture, which we call the “strong main conjecture”. (cf. [MT87, Remark after Conjecture 3].) This conjecture can be regarded as a refinement of the Iwasawa main conjecture. As we said in §1.1, \( a_p(E) \equiv 1 \pmod{p} \) is always assumed.

\textbf{Conjecture 1.6} ([Kur02, Conjecture 0.3, “strong main conjecture”]). \textit{Let} \( E \) \textit{be an elliptic curve over} \( \mathbb{Q} \) \textit{with good reduction at an odd prime} \( p \). \textit{Assume the following conditions:}
\begin{enumerate}
\item \( E(\mathbb{Q})[p] \) \textit{is trivial.}
\item \( p \) \textit{does not divide Tamagawa number} \( \text{Tam}(E) \).
\end{enumerate}
\textit{Then}
\[
(\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))) = \text{Fitt}_{\Lambda_n} \left( \text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \right).
\]
\textit{Here,} \( \nu_{n-1,n} \) \textit{is the trace map} \( \Lambda_{n-1} \to \Lambda_n \) \textit{defined by} \( \sigma \mapsto \sum_{\tau \mapsto \sigma} \tau \) \textit{for} \( \sigma \in \text{Gal}(\mathbb{Q}_{n-1}/\mathbb{Q}) \) \textit{where} \( \tau \) \textit{runs over all elements of} \( \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \) \textit{projecting to} \( \sigma \).

\textbf{Remark 1.7.} This conjecture explains the growth of \( \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \) as \( n \) goes to infinity.
The second named author proved Conjecture 1.6 for the “most basic” case (cf. [IP06, §5]) using Kato’s zeta elements.

**Theorem 1.8** ([Kur02, Theorem 0.1.(4)]). If we further assume

1. $E$ has good supersingular reduction at $p$,
2. $p$ does not divide $\frac{L(E,1)}{\Omega_E}$, and
3. $E[p]$ is surjective

as well as the assumptions of Conjecture 1.6, then Conjecture 1.6 is true.

**Remark 1.9.** Note that $a_p(E) = 0$ is not assumed in Theorem 1.8. In [Pol05, Theorem 1.1.(3)], Pollack proved an algebraic analogue of Theorem 1.8 using a formal group argument assuming $a_p(E) = 0$. His work does not require the surjectivity of $E[p]$.

**Remark 1.10.** For the case of $p = 2$, Conjecture 1.6 may not hold. See [Pol05, Remark 1.2] and [KO06] for detail.

Pollack reformulates Conjecture 1.6 in terms of his signed $p$-adic $L$-functions under the assumption $a_p(E) = 0$. See §3.1 for the characterization of the $\pm p$-adic $L$-functions $L^\pm_p(Q_\infty, f)$. We recall a proposition of Pollack, which shows us the connection between Mazur-Tate elements and $\pm p$-adic $L$-functions.

**Proposition 1.11** ([Pol03, Proposition 6.18]).

$$\theta_n(f) \equiv \tilde{\omega}_n^+ \cdot L^+_p(Q_\infty, f) \pmod{\omega_n}$$

in $\Lambda$, if $n$ is even/odd, respectively.

Then, as ideals of $\Lambda$, the following equality holds

$$(\omega_n, \theta_n(f), \nu_{n-1,n} (\theta_{n-1}(f))) = (\omega_n, \tilde{\omega}_n^+ \cdot L^+_p(Q_\infty, f), \tilde{\omega}_n^- \cdot L^-_p(Q_\infty, f)).$$

Thus, assuming $a_p(E) = 0$, Conjecture 1.6 is equivalent to the following conjecture.

**Conjecture 1.12** ([Pol03, Conjecture 6.19]). We assume $a_p(E) = 0$ as well as the conditions in Conjecture 1.6. Then

$$(\tilde{\omega}_n^+ \cdot L^+_p(Q_\infty, f) \pmod{\omega_n}, \tilde{\omega}_n^- \cdot L^-_p(Q_\infty, f) \pmod{\omega_n}) = \text{Fitt}_{\Lambda}(\text{Sel}(Q_\infty, E[p\infty])^\vee).$$

**Remark 1.13.** In the non-CM case, both Mazur-Tate elements and $\pm p$-adic $L$-functions come from Kato’s zeta elements. See [Kur02, Lemma 7.2] for Mazur-Tate elements using the $P_n$-pairing made by the second named author and [Kob03, Theorem 6.3] for $\pm p$-adic $L$-functions using $\pm$-Coleman maps. Thus, Proposition 1.11 can be interpreted as a comparison between the $P_n$-pairing and $\pm$-Coleman maps (modulo $\omega_n$). Both methods extend the dual exponential map but in different ways. See [KP07, §1] for detail.

1.3. **Main theorems.** We state three main theorems (mainly for elliptic curves with good supersingular reduction).

**Theorem 1.14** (Main Theorem I). Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at an odd prime $p$. Assume that

- $E[p]$ is surjective if $E$ is non-CM, and
- $p$ does not divide Tamagawa number $\text{Tam}(E)$.

Assume one of the followings:

1. $p \nmid a_p(E)$ and $a_p(E) \neq 1 \pmod{p}$, or
2. $a_p(E) = 0$. 


Then
\[(\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))) \subseteq \text{Fitt}_{\Lambda_n} \left( \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \right)^\vee.\]

Thus, Mazur-Tate’s weak main conjecture (Conjecture 1.4) for $E$ over $\mathbb{Q}_n$ holds. Furthermore, in Case (ord), if the equality of the Iwasawa main conjecture (Theorem 2.2) holds, then the inclusion becomes equality. In other words, the strong main conjecture (Conjecture 1.6) holds.

See §2 for proof of Case (ord) and §4 for proof of Case (ss).

Let $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \overline{\mathbb{Q}}_p^\times$ be a character and $\mathbb{Z}_p[\chi]$ be the ring generated by the image of $\chi$ over $\mathbb{Z}_p$. The map $\chi$ naturally extends to an algebra homomorphism $\mathbb{Z}_p[\text{Gal}(\mathbb{Q}_n/\mathbb{Q})] \rightarrow \mathbb{Z}_p[\chi]$ defined by $\gamma \mapsto \chi(\gamma)$ where $\gamma \in \text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ and also denote it by $\chi$. Then we also define the augmentation ideal at $\chi$ by

\[I_{\chi} := \ker (\chi : \Lambda_n \rightarrow \mathbb{Z}_p[\chi]).\]

Let $L \subseteq \Lambda_n$. We say $L$ vanishes to infinite order at $\chi$ if $L$ is contained in all powers of $I_{\chi}$. We say $L$ vanishes to order $r$ at $\chi$ if $L \subseteq I_{\chi}^{r+1} \setminus I_{\chi}^r$. See [MT87, (1.5)] for detail.

**Conjecture 1.15** ([MT87, Conjecture 1, “weak vanishing conjecture”]). The order of vanishing of $\theta_n(f)$ at $\chi$ is greater than or equal to the dimension of the $\chi$-part of the Mordell-Weil group of $E(\mathbb{Q}_n)$.

**Corollary 1.16.** Under the same assumptions of Theorem 1.14, Conjecture 1.15 holds.

**Proof.** [MT87, Proposition 3]. \(\square\)

**Remark 1.17.**

1. In both conditions (ord) and (ss) in Theorem 1.14, $a_p(E) \not\equiv 1 \pmod{p}$ or $a_p(E) = 0$ ensures that $E(\mathbb{Q})[p]$ is trivial.

2. An anticyclotomic analogue of Theorem 1.14 is being investigated in [Kim].

3. See [Ota18] for the development towards Conjecture 1.15.

In the case of non-CM elliptic curves with good supersingular reduction, we can also obtain a lower bound of the Selmer groups as follows. Let $T = \varprojlim E[p^n]$ be the $p$-adic Tate module of $E$, $\mathbb{H}^1_{\text{glob}}(T)$ be the global Iwasawa cohomology (defined in §5.1), and

\[\text{coker } g_n := \text{coker} \left( \mathbb{H}^1(\mathbb{Q}_n/\mathbb{Q}, T) \rightarrow \mathbb{H}^1(\mathbb{Q}_n,p,T) / \text{im} \mathbb{H}^1_{\text{glob}}(T) \right) \]

where $\text{im } B$ is the image of $B$ in $A$ in the notation $\frac{A}{\text{im } B}$. Note that the notation “coker $g_n$” coincides with that of [Kob03, (10.36) and Proposition 10.6]. See §5.2 for detail.

**Theorem 1.18** (Main Theorem II). Let $E$ be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at an odd prime $p$. Assume that

- $a_p(E) = 0$,
- $E[p]$ is surjective,
- $p$ does not divide Tamagawa number $\text{Tam}(E)$, and
- the equalities of the $\pm$-main conjectures (Theorem 3.5) hold.

Then

\[\text{Fitt}_{\Lambda_n} (\text{coker } g_n) \subseteq \text{Fitt}_{\Lambda_n} (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee) \subseteq (\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))) \subseteq \text{Fitt}_{\Lambda_n} (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee) .\]

See §5 for proof. Although coker $g_n$ might not be zero in general, if coker $g_n = 0$, then Conjecture 1.6 holds.

**Remark 1.19.** As a $\mathbb{Z}_p$-module, coker $g_n$ is finitely generated. Also, coker $g_n$ stabilizes as $n \gg 0$. See [Kob03, (Proof of) Proposition 10.6].

\[\text{Proof.}\]
We define the **fine Selmer groups of** $E$ **over** $\mathbb{Q}_n$ by
\[ \text{Sel}_0(\mathbb{Q}_n, E[p^\infty]) := \ker (\text{Sel}(\mathbb{Q}_n, E[p^\infty]) \to H^1(\mathbb{Q}_{n,p}, E[p^\infty])) \]
and $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]) := \varprojlim_n \text{Sel}_0(\mathbb{Q}_n, E[p^\infty])$ as in [KP07, §0.3].

**Theorem 1.20** (Main Theorem III). **Under the assumptions of** Theorem 1.18, **we further assume**

1. $(\text{fineNF}) \text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee}$ **has no nontrivial finite $\Lambda$-submodule, and**
2. **if** $\Phi_n(1 + X)$ **divides a generator of** $\text{char}_E(\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]))$, **then** $\text{rk}_\mathbb{Z} E(\mathbb{Q}_n) > \text{rk}_\mathbb{Z} E(\mathbb{Q}_{n-1})$ **(if** $n = 0$, **then** $\Phi_0(1 + X) = X$ **and this inequality means** $\text{rk}_\mathbb{Z} E(\mathbb{Q}) > 0$). Then $coker g_n = 0$. Therefore, the strong main conjecture (Conjecture 1.6)
\[ (\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))) = \text{Fitt}_\mathbb{A}_n (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^{\vee}) \]
holds.

See §6 for proof.

**Example 1.21.** There are many examples satisfying Assumptions (fineNF) and (III) in Theorem 1.20.

1. **We note that** Assumption (III) **is satisfied if at least one of the following conditions is satisfied:**
   - (a) **The characteristic ideal of** $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee}$ **is prime to** $\omega_n$ **for all** $n$.
   - (b) **If** $\Phi_n(1 + X)$ **divides a generator of the characteristic ideal of** $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee}$, **then** $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ **is finite for all** $n$.

In fact, the implication of Assumption (III) from (a) is trivial, and that from (b) can be proved by the control theorem for fine Selmer groups. (cf. [Kur02, Lemma 4.2, Remark 4.4])

2. **If one of them below occurs, then both Assumptions (fineNF) and (III) follow:**
   - $\text{Sel}_0(\mathbb{Q}, E[p^\infty])$ **is trivial. (See [Kur02, Lemma 4.3] and [Pol05],.)}
   - $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])_{\Gamma_n}$ **is trivial. (It is a weaker condition than the above.)
   - $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]) = \ker (E(\mathbb{Q}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E(\mathbb{Q}_\infty, p) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$.

Note that the first two cases never occur if $\text{rk}_\mathbb{Z} E(\mathbb{Q}) > 1$. The fine Selmer group is said to be **all Mordell-Weil** if the fine Selmer group lie in the last case. In the all Mordell-Weil case, $\text{Sel}_0(\mathbb{Q}_n, E[p^\infty])^{\vee}$ **is free over** $\mathbb{Z}_p$, **so Assumptions (fineNF) and (III) follow.**

3. **It is conjectured by Greenberg that the roots of a generator of** $\text{char}_E(\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee})$ **are all of the form** $\zeta - 1$ **where** $\zeta$ **is a** $p$-power root of unity. **See [KP07, Problem 0.7] for detail. Under the assumptions of** Theorem 1.18, **Assumption (fineNF),** **the above Greenberg’s conjecture, and several “standard” conjectures including the** $p$-adic Birch and Swinnerton-Dyer conjecture [KP07, (2.3), §2.6], **we can show that** $\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])$ **is all Mordell-Weil. Therefore, the essential condition is only Assumption (fineNF).**

Even if we remove the Tamagawa number assumption, we still have a non-primitive variant of Theorem 1.14. Its proof is given in §7.

**Theorem 1.22** (A non-primitive variant, Corollary 7.4). **Let** $E$ **be an elliptic curve over** $\mathbb{Q}$ **with good reduction at an odd prime** $p$. **Let** $\Sigma_0$ **be the set of primes** $\ell$ **such that the local Tamagawa number of** $E$ **at** $\ell$ **is divisible by** $p$. **Assume that** $E[p]$ **is surjective if** $E$ **is non-CM. One of Assumption (ord) and Assumption (ss) in** Theorem 1.14 **holds. Then**
\[ (\theta_{n}^{\Sigma_0}(f), \nu_{n-1,n}(\theta_{n-1}^{\Sigma_0}(f))) \subseteq \text{Fitt}_\mathbb{A}_n (\text{Sel}^{\Sigma_0}(\mathbb{Q}_n, E[p^\infty])^{\vee}) \]
where $\theta_{n}^{\Sigma_0}(f)$ **is the** $\Sigma_0$-non-primitive Mazur-Tate element defined in §7 and $\text{Sel}^{\Sigma_0}(\mathbb{Q}_n, E[p^\infty])$ **is the** $\Sigma_0$-non-primitive Selmer group defined in §7. Furthermore, in Case (ord), **if the equality
of the Iwasawa main conjecture (Theorem 2.2) holds, then the inclusion becomes equality. In other words, a \(\Sigma_0\)-non-primitive version of the strong main conjecture holds.

2. Review of the case for elliptic curves with good ordinary reduction

In this section, we prove Theorem 1.14 for elliptic curves with good ordinary reduction.

2.1. Tools from Iwasawa theory. Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with good ordinary reduction at \(p\). We first recall the \(\Lambda\)-cotorsion property of Selmer groups.

**Theorem 2.1** ([Rub88, Theorem 4.4], [Gre99, Theorem 1.5], [Kat04, Theorem 17.4.(1)]). The Selmer group \(\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])\) is \(\Lambda\)-cotorsion.

The following theorem is due to Rubin (for the CM case), Kato, Skinner-Urban, X. Wan, and Kim-Kim-Sun (for the non-CM case).

**Theorem 2.2** (Iwasawa main conjecture, [Kat04, Theorem 17.4.(3)]). Let \(p\) be an odd prime. Let \(E\) be an elliptic curve over \(\mathbb{Q}\). Assume that

1. \(p \nmid a_p(E)\),
2. if \(E\) has no CM, then \(E[p]\) is surjective, and

Then

\[ (L_p(\mathbb{Q}_\infty, f_\alpha)) \subseteq \text{char}_\Lambda (\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee) \]

where \(L_p(\mathbb{Q}_\infty, f_\alpha)\) is the \(p\)-adic \(L\)-function of the \(p\)-stabilized form \(f_\alpha\) with the unit root \(\alpha\).

Furthermore, the inclusion becomes equality provided that one of the following statements holds:

- \(E\) has CM ([Rub91, Theorem 12.3]),
- there exists a prime \(q\|N\) such that \(\overline{\rho}\) is ramified at \(q\) ([SU14, Theorem 3.29]),
- there exists a real quadratic field \(F/\mathbb{Q}\) such that
  - \(p\) is unramified in \(F\),
  - any prime \(q\) dividing \(N\) such that \(q \equiv -1 \pmod{p}\) is inert in \(F/\mathbb{Q}\), and any other prime dividing \(N\) splits in \(F/\mathbb{Q}\),
  - the canonical period of \(f\) over \(F\) is the square of its canonical period over \(\mathbb{Q}\) up to a \(p\)-adic unit,
- \(\tilde{\delta}_n \neq 0\) for some \(n\) and \(p \nmid \prod_{q|N_{sp}} (q - 1) \cdot \prod_{q|N_{ns}} (q + 1)\) where \(N_{sp}\) is the product of split multiplicative reduction primes of \(E\) and \(N_{ns}\) is the product of non-split multiplicative reduction primes of \(E\) ([Wan15, Theorem 4]), or

**Theorem 2.3** ([Gre99, Proposition 4.14], [HM00, Corollary]). The Selmer group \(\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])\) has no proper \(\Lambda\)-submodule of finite index.

**Theorem 2.4** ([Gre99, Proposition 3.7, Proposition 3.8 and Proposition 3.9]). If \(a_p(E) \not\equiv 1 \pmod{p}\) and \(p \nmid \text{Tam}(E)\), then the restriction map

\[ \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \to \text{Sel}(\mathbb{Q}_\infty, E[p^\infty])[\omega_n] \]

is an isomorphism.

2.2. Proof of Theorem 1.14 for the case of good ordinary reduction. This is basically obtained in [Kur03, Corollary 10.3]. From Theorem 2.2, we have

\[ (L_p(\mathbb{Q}_\infty, f_\alpha)) \subseteq \text{char}_\Lambda (\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee) . \]

By Theorem 2.1 and Theorem 2.3, characteristic ideals are equal to Fitting ideals via Lemma A.7; thus, we have

\[ (L_p(\mathbb{Q}_\infty, f_\alpha)) \subseteq \text{Fitt}_\Lambda (\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee) . \]
Taking quotient by $\omega_n$, we have

$$(\vartheta_n(f_\alpha) \subseteq \text{Fitt}_\Lambda_n ((\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])[\omega_n])^\vee)$$

where

$$\vartheta_n(f_\alpha) = \frac{1}{\alpha^n} \cdot \left( \theta_n(f) - \frac{1}{\alpha} \cdot \nu_{n-1,n}(\theta_{n-1}(f)) \right)$$

is the $p$-stabilized Mazur-Tate element with the unit root $\alpha$. Using Theorem 2.4, we have

$$(\vartheta_n(f_\alpha) \subseteq \text{Fitt}_\Lambda_n (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee).$$

Also, since $a_p(E) \not\equiv 1 \pmod{p}$, it is not difficult to observe

$$\vartheta_n(f_\alpha) = u \cdot \theta_n(f)$$

for some $u \in \Lambda_n^\times$. It shows that

$$(\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f)) \subseteq \text{Fitt}_\Lambda_n (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee).$$

We also note that $\nu_{n-1,n}(\theta_{n-1}(f))$ is a multiple of $\vartheta_n(f)$, so the ideal $(\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))$ is a principal ideal generated by $\vartheta_n(f)$, equivalently by $\theta_n(f)$.

Furthermore, if we start with the equality of the main conjecture, then the last inclusion also becomes equality. In other words, we have

$$(\theta_n(f)) = \text{Fitt}_\Lambda_n (\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee).$$

3. **Tools from $\pm$-Iwasawa theory**

3.1. **Basic objects of $\pm$-Iwasawa theory.** We quickly recall the basic objects of $\pm$-Iwasawa theory. For a more detailed description, we refer [Kob03] for the algebraic side and [Pol03] for the analytic side.

**Remark 3.1** (Sign convention). We fix the sign convention of $\pm$-Iwasawa theory as follows:

1. Selmer groups: [Kob03]
2. $p$-adic $L$-functions: [Pol03] = $- [Kob03]
3. Coleman maps: [KP07] = $- [Kob03]

3.1.1. **Local conditions at $p$.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$. Then we define

$$E^+(\mathbb{Q}_{n,p}) := \{ P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1}(P) \in E(\mathbb{Q}_{m,p}) \text{ for even } m \ (0 \leq m < n) \}$$

$$E^- (\mathbb{Q}_{n,p}) := \{ P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1}(P) \in E(\mathbb{Q}_{m,p}) \text{ for odd } m \ (0 \leq m < n) \}$$

where $\mathbb{Q}_{n,p}$ is the completion of $\mathbb{Q}_n$ at $p$ and $\text{Tr}_{n/m+1} : E(\mathbb{Q}_{n,p}) \to E(\mathbb{Q}_{m+1,p})$ is the trace map.

3.1.2. **The norm subgroups.** Let $\widehat{E}$ be the formal group associated to $E$ and $m_n$ be the maximal ideal of $\mathbb{Q}_{n,p}$. We define

$$\widehat{E}^+(m_n) := \{ P \in \widehat{E}(m_n) : \text{Tr}_{n/m+1}(P) \in \widehat{E}(m_m) \text{ for even } m \ (0 \leq m < n) \}$$

$$\widehat{E}^-(m_n) := \{ P \in \widehat{E}(m_n) : \text{Tr}_{n/m+1}(P) \in \widehat{E}(m_m) \text{ for odd } m \ (0 \leq m < n) \}$$

where $\text{Tr}_{n/m+1} : \widehat{E}(m_n) \to \widehat{E}(m_{m+1})$ is the trace map.
3.1.3. ±-Selmer groups. Following [Kob03, Definition 1.1] and [Kim13, Definition 3.1], we define the ±-Selmer groups of \( E \) over \( \mathbb{Q}_n \) by

\[
\text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty]) := \ker \left( \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \to \frac{H^1(\mathbb{Q}_n, E[p^\infty])}{E^\pm(\mathbb{Q}_n/p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)
\]

and the ±-Selmer groups of \( E \) over \( \mathbb{Q}_\infty \) by

\[
\text{Sel}^\pm(\mathbb{Q}_\infty, E[p^\infty]) := \lim_{\mathbb{n} \to \infty} \text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty]),
\]

respectively. Note that it is easy to see

\[
\text{Sel}_0(\mathbb{Q}_n, E[p^\infty]) \subseteq \text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty]) \subseteq \text{Sel}(\mathbb{Q}_n, E[p^\infty]),
\]

respectively.

3.1.4. ±-p-adic L-functions and ±-Coleman maps. We recall the characterization of ±-p-adic L-functions \( L_p^\pm(\mathbb{Q}_\infty, f) \in \Lambda \) by their interpolation property [PR04, (10), (11), and (12)]:

\[
\chi \left( L_p^+(\mathbb{Q}_\infty, f) \right) = (-1)^{(n+1)/2} \cdot \frac{\tau(\chi)}{\chi(\omega_n^\pm)} \cdot \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{if } \chi \text{ has order } p^n \text{ with } n \text{ odd}
\]

\[
\chi \left( L_p^-(\mathbb{Q}_\infty, f) \right) = (-1)^{(n/2)+1} \cdot \frac{\tau(\chi)}{\chi(\omega_n^\pm)} \cdot \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{if } \chi \text{ has order } p^n > 1 \text{ with } n \text{ even}
\]

\[
\mathbb{1} \left( L_p^+(\mathbb{Q}_\infty, f) \right) = (p-1) \cdot \frac{L(E, 1)}{\Omega_E}
\]

\[
\mathbb{1} \left( L_p^-(\mathbb{Q}_\infty, f) \right) = 2 \cdot \frac{L(E, 1)}{\Omega_E}
\]

where \( \mathbb{1} \) is the trivial character and \( \tau(\chi) \) is the Gauss sum of \( \chi \).

We also recall ±-Coleman maps. Our sign convention follows that of [KP07].

**Theorem 3.2** ([Kob03, Theorem 6.2, Theorem 6.3, and §8], [KP07, §1.1]). There exist maps

\[
\text{Col}_n^\pm : H^1(\mathbb{Q}_n, p, T) \to \Lambda_n/\omega_n^\pm
\]

such that

1. \( \text{Col}_n^+ : H^1(\mathbb{Q}_n, p, T)/\ker \text{Col}_n^\pm \cong \Lambda_n/\omega_n^\pm \) and
2. \( \text{Col}_n^\pm(\text{loc } z_{\text{Kato}, n}) = L_p^\pm(\mathbb{Q}_n, f) \)

where \( z_{\text{Kato}, n} \in H^1(\mathbb{Q}_n, T) \) is Kato’s zeta element at \( \mathbb{Q}_n \) and \( L_p^\pm(\mathbb{Q}_n, f) := L_p^\pm(\mathbb{Q}_\infty, f) \pmod{\omega_n^\pm} \).

By taking the inverse limit with respect to \( n \), we have maps

\[
\text{Col}^\pm : H^1_{\text{loc}}(T) \to \Lambda
\]

such that

1. \( \text{Col}^\pm \) are surjective and
2. \( \text{Col}^\pm(\text{loc } z_{\text{Kato}}) = L_p^\pm(\mathbb{Q}_\infty, f) \)

where

\[
H^1_{\text{loc}}(T) := \lim_{\mathbb{n} \to \infty} H^1(\mathbb{Q}_n, p, T)
\]

and \( z_{\text{Kato}} \in H^1(\mathbb{Q}_\infty, T) \) is Kato’s zeta element at \( \mathbb{Q}_\infty \).

**Remark 3.3.** The construction of \( \text{Col}_n^\pm \) in [Kob03] uses certain local points of formal groups of elliptic curves via Honda theory, and that in [KP07] uses the \( P_n \)-paring defined by the second named author in [Kur02] and Proposition 1.11.
3.2. \(\pm\)-main conjectures. We recall the \(\Lambda\)-cotorsion property of \(\pm\)-Selmer groups.

**Theorem 3.4** ([Kob03, Theorem 7.3.ii]), [PR04, Theorem 6.3]). Let \(p\) be an odd prime. Let \(E\) be an elliptic curve over \(\mathbb{Q}\). Assume that \(a_p(E) = 0\). Then \(\text{Sel}^\pm(Q_\infty, E[p^\infty])\) is \(\Lambda\)-cotorsion, respectively.

**Theorem 3.5** (\(\pm\)-main conjectures, [Kob03, Theorem 4.1], [PR04, Theorem in Introduction]). Let \(p\) be an odd prime. Let \(E\) be an elliptic curve over \(\mathbb{Q}\). Assume that

1. \(a_p(E) = 0\), and
2. if \(E\) has no CM, then \(E[p]\) is surjective.

Then

\[
(L_p^\mp(Q_\infty, f)) \subseteq \text{char}_A(\text{Sel}^\pm(Q_\infty, E[p^\infty])^\vee) .
\]

Furthermore, the inclusion becomes equality provided that one of the following statements hold:

- \(E\) has CM ([PR04, Theorem in Introduction]),
- there exists a prime \(q\parallel N\) such that \(\overline{p}\) is ramified at \(q\) ([Wan18a, Theorem 1.4]),
- \(N\) is square-free and there exists two primes \(q\parallel N\) such that \(\overline{p}\) is ramified at \(q\) ([Wan18a, Remark 1.5]),
- \(N\) is square-free ([Wan18b, Theorem 1.4]), [Spr16, Theorem 1.1]), or
- \(\delta_n \neq 0\) for some \(n\) and \(p \nmid \prod_{q \parallel N_{sp}} (q - 1) \cdot \prod_{q \parallel N_{ns}} (q + 1)\) where \(N_{sp}\) is the product of split multiplicative reduction primes of \(E\) and \(N_{ns}\) is the product of non-split multiplicative reduction primes of \(E\) ([KKS, Theorem 1.1]).

Note that Sprung’s work [Spr16] also applies to the \(a_p(E) \neq 0\) case.

3.3. Nonexistence of proper \(\Lambda\)-submodules of finite index. We recall B.D. Kim’s result on the analogue of Theorem 2.3 for the supersingular setting. For the further development along this direction, see [KO18].

**Theorem 3.6** ([Kim13, Theorem 1.1]). The Selmer group \(\text{Sel}^\pm(Q_\infty, E[p^\infty])\) has no proper \(\Lambda\)-submodule of finite index, respectively.

3.4. \(\pm\)-exact control theorems.

**Theorem 3.7** (\(\pm\)-exact control theorems, [Kob03, Theorem 9.3], [IP06, Theorem 6.8]). If \(p \nmid \text{Tam}(E)\), then the restriction map

\[
\text{Sel}^\pm(Q_n, E[p^\infty])[\omega_n^\pm] \rightarrow \text{Sel}^\pm(Q_\infty, E[p^\infty])[\omega_n^\pm]
\]

is an isomorphism.

**Proof.** The \(a_p(E) = 0\) condition ensures that \(E(Q)[p]\) is trivial, and it implies that the restriction map is injective as in [Kob03, Lemma 9.1]. The failure of the surjectivity comes only from prime-to-\(p\) local conditions; thus, the situation coincides with the ordinary case. The \(p \nmid \text{Tam}(E)\) condition ensures that the failure vanishes. See [Kob03, Theorem 9.3] and [Gre99, Proposition 3.8] for detail.

3.5. The consequence.

**Corollary 3.8.** Let \(p\) be an odd prime. Let \(E\) be an elliptic curve over \(\mathbb{Q}\). Assume that

1. \(a_p(E) = 0\),
2. if \(E\) has no CM, then \(E[p]\) is surjective, and
3. \(p \nmid \text{Tam}(E)\).

Then we have

\[
(\widetilde{\omega}_n^\mp \cdot L_p^\mp(Q_\infty, f) \mod \omega_n) \subseteq \widetilde{\omega}_n^\mp \cdot \text{Fitt}_A (\text{Sel}^\pm(Q_n, E[p^\infty])^\vee)
\]

in \(\Lambda_n\), respectively.
Proof. By Theorem 3.4, Theorem 3.5, Theorem 3.6, and Lemma A.7, we have
\[(L_p^\mp(Q_\infty, f)) \subseteq \text{Fitt}_\Lambda (\text{Sel}^{\pm}(Q_\infty, E[p^\infty])^\vee)\]
under the conditions of Theorem 3.5. Taking quotient by \(\omega_n^\pm\), we obtain
\[(L_p^\mp(Q_\infty, f) \pmod{\omega_n^\pm}) \subseteq \text{Fitt}_{\Lambda_n/\omega_n^\pm} \left( (\text{Sel}^{\pm}(Q_\infty, E[p^\infty])[\omega_n^\pm])^\vee \right)\]
in \(\Lambda_n/\omega_n^\pm\), respectively. By Theorem 3.7 with the \(p \nmid \text{Tam}(E)\) condition, we obtain
\[(L_p^\mp(Q_\infty, f) \pmod{\omega_n^\pm}) \subseteq \text{Fitt}_{\Lambda_n/\omega_n^\pm} \left( (\text{Sel}^{\pm}(Q_n, E[p^\infty])[\omega_n^\pm])^\vee \right)\]
in \(\Lambda_n/\omega_n^\pm\), respectively. Since
\[
\text{Fitt}_{\Lambda_n/\omega_n^\pm} \left( (\text{Sel}^{\pm}(Q_n, E[p^\infty])[\omega_n^\pm])^\vee \right) = \frac{\text{Fitt}_{\Lambda_n} (\text{Sel}^{\pm}(Q_n, E[p^\infty])^\vee) + (\omega_n^\pm)}{(\omega_n^\pm)} \quad \text{Lemma A.6}
\]
in \(\Lambda_n/\omega_n^\pm\), we have inclusions
\[(L_p^\mp(Q_\infty, f) \pmod{\omega_n}) + (\omega_n^\pm) \subseteq \text{Fitt}_{\Lambda_n} (\text{Sel}^{\pm}(Q_n, E[p^\infty])^\vee) + (\omega_n^\pm)\]
in \(\Lambda_n\), respectively. Multiplying \(\omega_n^\pm\), the conclusion immediately follows. \( \square \)

Remark 3.9. If we assume the equality of \(\pm\)-main conjectures, then the inclusion in Corollary 3.8 becomes equality.

4. Comparison of local conditions at \(p\)

Consider the exact sequence of \(\Lambda_n\)-modules (cf. [KO18, (4.2)])
\[
\left( \frac{E(Q_n,p) \otimes Q_p/\mathbb{Z}_p}{E^\pm(Q_n,p) \otimes Q_p/\mathbb{Z}_p} \right)^\vee \xleftarrow{t^\pm} \text{Sel}(Q_n, E[p^\infty])^\vee \xrightarrow{\text{Sel}(Q_n, E[p^\infty])^\vee} 0.
\]
Then we have
\[
\text{Fitt}_{\Lambda_n} \left( \left( \frac{E(Q_n,p) \otimes Q_p/\mathbb{Z}_p}{E^\pm(Q_n,p) \otimes Q_p/\mathbb{Z}_p} \right)^\vee / \ker(t^\pm) \right) \cdot \text{Fitt}_{\Lambda_n} \left( \text{Sel}^{\pm}(Q_n, E[p^\infty])^\vee \right) \subseteq \text{Fitt}_{\Lambda_n} \left( \text{Sel}(Q_n, E[p^\infty])^\vee \right)
\]
by Lemma A.2. By Lemma A.1, we also have
\[
\text{Fitt}_{\Lambda_n} \left( \left( \frac{E(Q_n,p) \otimes Q_p/\mathbb{Z}_p}{E^\pm(Q_n,p) \otimes Q_p/\mathbb{Z}_p} \right)^\vee \right) \subseteq \text{Fitt}_{\Lambda_n} \left( \left( \frac{E(Q_n,p) \otimes Q_p/\mathbb{Z}_p}{E^\pm(Q_n,p) \otimes Q_p/\mathbb{Z}_p} \right)^\vee / \ker(t^\pm) \right) .
\]
We observe that
\[
\left( \frac{E(Q_n,p) \otimes Q_p/\mathbb{Z}_p}{E^\pm(Q_n,p) \otimes Q_p/\mathbb{Z}_p} \right)^\vee \cong \left( \frac{\hat{E}(m_n) \otimes Q_p/\mathbb{Z}_p}{E^\pm(m_n) \otimes Q_p/\mathbb{Z}_p} \right)^\vee \quad \text{[KO18, Lemma 3.14]}
\]
\[
\cong \left( \frac{\hat{E}(m_n)}{E^\pm(m_n) \otimes Q_p/\mathbb{Z}_p} \right)^\vee .
\]
Due to [IP06, Proposition 4.11], we have the following exact sequence
\[
0 \longrightarrow \hat{E}(p\mathbb{Z}_p) \xrightarrow{f} \hat{E}^+(m_n) \oplus \hat{E}^-(m_n) \xrightarrow{g} \hat{E}(m_n) \longrightarrow 0
\]
\[
\xrightarrow{\cong} \quad \xrightarrow{\cong} \quad \xrightarrow{\cong} \quad \text{[IP06, Proposition 5.8]}
\]
\[
0 \longrightarrow \omega_n^+ \Lambda_n \longrightarrow \omega_n^- \Lambda_n \oplus \omega_n^+ \Lambda_n \longrightarrow \omega_n^- \Lambda_n \longrightarrow 0
\]
where \(f\) is the diagonal embedding and \(g: (a, b) \mapsto a - b\). Note that \(\omega_n^+ \omega_n^- \Lambda_n \cong \Lambda_n / \Lambda_n \cong \mathbb{Z}_p\).
This implies that
\[
\hat{E}(m_n)/\hat{E}^\pm(m_n) \cong (\omega_n^+, \omega_n^-) \Lambda_n/\omega_n^+ \Lambda_n.
\]
Then
\[
\text{Fitt}_{\Lambda_n}\left(\left(\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n} \otimes \mathbb{Q}_p / \mathbb{Z}_p\right)\right)^\vee = \text{Fitt}_{\Lambda_n}\left(\left(\frac{\tilde{E}(m_n)/\tilde{E}(m_n)}{\mathbb{Q}_p / \mathbb{Z}_p}\right)\right)^\vee.
\]

The following proposition is due to Robert Pollack.

**Proposition 4.1.**

\[
\text{Fitt}_{\Lambda_n}\left(\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n} \otimes \mathbb{Q}_p / \mathbb{Z}_p\right)^\vee = \tilde{\omega}_n^+ \Lambda_n,
\]

respectively.

**Proof.** Since the multiplication by \(\omega_n^\pm\) induces an isomorphism \(\Lambda_n / \tilde{\omega}_n^+ \Lambda_n \simeq \omega_n^\pm \Lambda_n\), we have
\[
\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n} \simeq \omega_n^\pm \Lambda_n
\]
\[
\simeq \Lambda_n / \tilde{\omega}_n^+ \Lambda_n.
\]

We compute
\[
\left(\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n} \otimes \mathbb{Q}_p / \mathbb{Z}_p\right)^\vee \simeq \text{Hom}_{\mathbb{Z}_p}\left(\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n} \otimes \mathbb{Q}_p / \mathbb{Z}_p, \mathbb{Q}_p / \mathbb{Z}_p\right)
\]
\[
\simeq \text{Hom}_{\mathbb{Z}_p}\left(\frac{\tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-}{\tilde{\omega}_n^+ \Lambda_n}, \text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p / \mathbb{Z}_p, \mathbb{Q}_p / \mathbb{Z}_p)\right)
\]
\[
\simeq \text{Hom}_{\mathbb{Z}_p}\left(\tilde{\omega}_n^+ \Lambda_n, \mathbb{Z}_p\right).
\]

A direct calculation shows the following identities:
\[
\tilde{\omega}_n^{+, t} := \prod_{2 \leq m \leq n, m: \text{even}} \Phi_m\left(\frac{1}{1 + X}\right)
\]
\[
= \prod_{2 \leq m \leq n, m: \text{even}} \Phi_m(1 + X) \cdot (1 + X)^{-p^{m-1}(p-1)}
\]
\[
= \left(\prod_{2 \leq m \leq n, m: \text{even}} (1 + X)^{-p^{m-1}(p-1)}\right) \cdot \tilde{\omega}_n^+ .
\]

and
\[
\tilde{\omega}_n^{-, t} := \prod_{1 \leq m \leq n, m: \text{odd}} \Phi_m\left(\frac{1}{1 + X}\right)
\]
\[
= \prod_{1 \leq m \leq n, m: \text{odd}} \Phi_m(1 + X) \cdot (1 + X)^{-p^{m-1}(p-1)}
\]
\[
= \left(\prod_{1 \leq m \leq n, m: \text{odd}} (1 + X)^{-p^{m-1}(p-1)}\right) \cdot \tilde{\omega}_n^- .
\]

We write
\[
c^+ = \left(\prod_{2 \leq m \leq n, m: \text{even}} (1 + X)^{-p^{m-1}(p-1)}\right), \quad c^- = \left(\prod_{1 \leq m \leq n, m: \text{odd}} (1 + X)^{-p^{m-1}(p-1)}\right).
\]
and note that they are invertible in $\Lambda_n$.

We consider a perfect pairing $\Lambda_n \times \Lambda_n \to \mathbb{Z}_p$ defined by $(\sigma, \tau) = 1$ if $\tau = \sigma^{-1}$ and $(\sigma, \tau) = 0$ otherwise. Then the pairing induces an isomorphism

$$\text{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p) \cong \Lambda_n$$

with the reversed $\Lambda_n$-action. Then we have

$$\text{Hom}_{\mathbb{Z}_p}(\Lambda_n/\omega_n^+, \mathbb{Z}_p) \cong \text{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p)[\omega_n^+]$$

$$\cong \Lambda_n[\omega_n^+]$$

$$\cong \Lambda_n^\wedge.$$ (\omega_n^+ \in \Lambda_n^\wedge)

To sum up, we have

$$\omega_n^+ \cdot \text{Fitt}_{\Lambda_n}(\text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty])^\vee) = \text{Fitt}_{\Lambda_n} \left( \left( \frac{(\omega_n^+, \omega_n^-) \Lambda_n \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\omega_n^+ \Lambda_n} \right)^\vee \right) \cdot \text{Fitt}_{\Lambda_n}(\text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty])^\vee)$$

$$= \text{Fitt}_{\Lambda_n} \left( \left( \hat{E}(m_n)/\hat{E}^\pm(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\vee \right) \cdot \text{Fitt}_{\Lambda_n}(\text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty])^\vee)$$

$$\subseteq \text{Fitt}_{\Lambda_n} \left( \left( \frac{E(\mathbb{Q}_n, p) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\mathbb{Z}_p} \right)^\vee \right) \cdot \text{Fitt}_{\Lambda_n}(\text{Sel}^\pm(\mathbb{Q}_n, E[p^\infty])^\vee)$$

By Corollary 3.8, we have

$$(\omega_n^+ \cdot L_p^1(\mathbb{Q}_\infty, f) \mod \omega_n) \subseteq \text{Fitt}_{\Lambda_n}(\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee).$$

It proves one inclusion of Conjecture 1.12 (Pollack’s reformulation). Thus, Theorem 1.14 is proved.

**Remark 4.2.** If we can do a similar computation with Wach modules, then it seems possible to generalize the result to modular forms of higher weight (still in the Fontaine-Laffaille range). See [Lei11] for the formulation of $\pm$-Iwasawa theory for modular forms of higher weight.

5. **The non-CM case**

The goal of this section is to prove the inclusion

$$\text{Fitt}_{\Lambda_n}(\ker g_n) \cdot \text{Fitt}_{\Lambda_n}(\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee) \subseteq (\theta_n(f), \nu_{n-1}(\theta_{n-1}(f)))$$

in Theorem 1.18. Note that the inclusion gives us a lower bound of Selmer groups (up to some error). Throughout this section, we assume

1. $E$ is non-CM ($\Rightarrow E[p]$ is surjective);
2. $p$ does not divide $\text{Tam}(E)$;
3. The equality of the $\pm$-main conjecture (Conjecture 3.5).

5.1. **Kato’s main conjecture and fine Selmer groups.** Let $j : \text{Spec}(\mathbb{Q}_n) \to \text{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p])$ be the natural map. Let

$$H^1_{\text{glob}}(T) := \varprojlim_n H^1_{\text{et}}(\text{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_*T)$$

where $H^1_{\text{et}}(\text{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_*T)$ is the étale cohomology group. Then $H^1_{\text{glob}}(T) \simeq H^1(\mathbb{Q}_\infty, T) \simeq H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T) \simeq \lim_{\leftarrow n} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T)$ by [MR04, Lemma 5.3.1] and [Kob03, Proposition 7.1.(i)]. Let

$$H^1_{\text{glob}}(V) := H^1_{\text{glob}}(T) \otimes \mathbb{Q}_p.$$
Theorem 5.1 ([Kat04, Theorem 12.4.(1) and (3)]). The following statements hold:
(1) \( \mathbb{H}^2_{\text{glob}}(T) \) is a finitely generated torsion module over \( \Lambda \).
(2) \( \mathbb{H}^1_{\text{glob}}(T) \) is free of rank one over \( \Lambda \).

We recall the Iwasawa main conjecture without \( p \)-adic zeta functions à la Kato and Perrin-Riou.

Conjecture 5.2 ([Kat04, Conjecture 12.10]).

\[
\text{char}_\Lambda \left( \left( \mathbb{H}^1_{\text{glob}}(T) / \Lambda \mathfrak{z}_{\text{Kato}} \right)_{\text{tors}} \right) = \text{char}_\Lambda (\mathbb{H}^2_{\text{glob}}(T))
\]

where \( M_{\text{tors}} \) is the \( \Lambda \)-torsion submodule of \( M \).

Theorem 5.3 ([Kob03, Theorem 7.4]). Conjecture 5.2 and the equalities of the \( \pm \)-main conjectures (Theorem 3.5) are equivalent.

Note that we crucially use Conjecture 5.2 in the argument.

Theorem 5.4 ([Kur02, §6], [Kob03, Theorem 7.1.ii]). As \( \Lambda \)-modules, \( \text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee \) and \( \mathbb{H}^2_{\text{glob}}(T) \) are pseudo-isomorphic.

5.2. Selmer groups and fine Selmer groups in finite layers. Let

\[
\mathcal{Y}'_n := \text{coker} \left( \mathbb{H}^1_{\text{glob}}(T)_{\Gamma_n} \to \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \right),
\]

\[
\mathcal{Y}_n := \text{coker} \left( \mathbb{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \to \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \right),
\]

and

\[
\mathcal{Z}_n := \text{im} \left( \mathbb{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \to \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \right).
\]

Consider the following commutative diagram

\[
\begin{array}{ccccccccc}
\text{ker } g_n & \to & 0 & \to & \text{ker } f_n \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{H}^1_{\text{glob}}(T)_{\Gamma_n} & \to & \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} & \to & \mathcal{Y}'_n & \to & 0 \\
\downarrow g_n & & \downarrow \simeq & & \downarrow f_n \\
0 & \to & \mathcal{Z}_n & \to & \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} & \to & \mathcal{Y}_n & \to & 0 \\
\downarrow \text{coker } g_n & & \downarrow & & \downarrow & & \downarrow \text{coker } f_n \\
& & & & & & & & \\
\end{array}
\]

with \( \text{ker } f_n \simeq \text{coker } g_n \) by snake lemma. Let \( \mathcal{Y}'_n / \text{coker } g_n := \mathcal{Y}'_n / \text{ker } f_n \subseteq \mathcal{Y}_n \). Then we have

\[
\text{Fitt}_\Lambda (\mathcal{Y}_n) \subseteq \text{Fitt}_\Lambda (\mathcal{Y}'_n / \text{coker } g_n)
\]

by Lemma A.10. Using the Poitou-Tate sequence ([PR00, A.3.2.Proposition], [Kob03, (7.18)]), we have the following exact sequence with splitting

\[
\begin{array}{ccccccccc}
\mathbb{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) & \to & \frac{\mathbb{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} & \to & \text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee & \to & \text{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee & \to & 0 \\
\downarrow & & & & \downarrow \mathcal{Y}_n & & \downarrow 0 \\
0 & & & & & & & & 0.
\end{array}
\]
5.3. A presentation of the difference between Selmer groups and fine Selmer groups. It is ideal to compute a presentation matrix of \( \mathcal{Y}_n \) from the following exact sequence

\[
\begin{array}{c}
H^1(Q_{\Sigma}/Q_n, T) \\ E(Q_{n,p}) \otimes \mathbb{Z}_p
\end{array} \longrightarrow \mathcal{Y}_n \longrightarrow 0.
\]

However, it seems out of reach with current techniques; instead, we compute a slightly easier version, a presentation matrix of \( \mathcal{Y}_n' \) from the following exact sequence

\[
\begin{array}{c}
\mathbb{H}^1_{\text{glob}}(T)_{\Gamma_n} \\ E(Q_{n,p}) \otimes \mathbb{Z}_p
\end{array} \longrightarrow \mathcal{Y}_n' \longrightarrow 0.
\]

We regard \( \mathcal{Y}_n' \) as the quotient of \( H^1(Q_{n,p}, T) \) by local constraint \( E(Q_{n,p}) \otimes \mathbb{Z}_p \) and global constraint \( \mathbb{H}^1_{\text{glob}}(T)_{\Gamma_n} \).

5.3.1. The generators. Let \( \mathbb{H}^1_{\text{loc}}(T) \) be the local Iwasawa cohomology group. Since \( E \) is supersingular at \( p \), \( E[p] \) is irreducible as a \( G_{\mathbb{Q}_p} \) module. Then \( \mathbb{H}^1_{\text{loc}}(T) \) is free of rank 2 over \( \Lambda \) since \( H^1(Q_{p}, T) \) is free of rank 2 over \( \mathbb{Z}_p \).

**Proposition 5.5** ([KP07, Proposition 1.2]). Let \( \text{Col} := \text{Col}^+ \oplus \text{Col}^- \). The following sequence

\[
0 \longrightarrow \mathbb{H}^1_{\text{loc}}(T) \xrightarrow{\text{Col}} \Lambda \oplus \Lambda \xrightarrow{r} \mathbb{Z}_p \longrightarrow 0
\]

is exact where \( r(h(X), k(X)) := h(0) - \frac{p^2 - 1}{2} \cdot k(0) \).

We pick a \( \Lambda \)-basis \( (e_1, e_2) \) of \( \mathbb{H}^1_{\text{loc}}(T) = \ker(r) \) by

\[
\text{Col}(e_1) = \left( \frac{p - 1}{2}, 1 \right)
\]

\[
\text{Col}(e_2) = (X, 0).
\]

Then

\[
\mathbb{H}^1_{\text{loc}}(T) = \Lambda e_1 \oplus \Lambda e_2
\]

\[
\simeq \Lambda \text{Col}(e_1) \oplus \Lambda \text{Col}(e_2)
\]

\[
\subset \Lambda \oplus \Lambda.
\]

By the irreducibility of \( E[p] \) as a \( G_{\mathbb{Q}_p} \) module, we have

\[
\mathbb{H}^1_{\text{loc}}(T)_{\Gamma_n} = H^1(Q_{n,p}, T)
\]

\[
= \Lambda_n e_1 \oplus \Lambda_n e_2.
\]

5.3.2. The local constraint. Consider the exact sequence

\[
0 \longrightarrow \xrightarrow{\text{Col}} \xrightarrow{\ker(\text{Col}_n^+)} \xrightarrow{\ker(\text{Col}_n^-)} \xrightarrow{\Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+} \xrightarrow{0}
\]

We investigate the image of \( e_1 \) and \( e_2 \) in \( \Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+ \) under \( \text{Col}_n \). Then we naturally obtain the following relations of \( \mathbb{H}^1(Q_{n,p}, T)_{E(Q_{n,p}) \otimes \mathbb{Z}_p} \):

\[
\tilde{\omega}_n^- \cdot e_2 = (\tilde{\omega}_n^-, X, 0)
\]

\[
= (\omega_n^-, 0)
\]

\[
= (0, 0) \in \Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+
\]
\[ \omega_n^+ \cdot e_1 - \frac{p-1}{2} \cdot \omega_n^+ \cdot e_2 = (\omega_n^+ \cdot \frac{p-1}{2}, \omega_n^+ - \frac{p-1}{2} \cdot \omega_n^+ - X, 0) = (0, \omega_n^+) = (0, 0) \in \Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+. \]

Also, since \( E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \) is generated by two elements over \( \Lambda_n \) via a formal group argument as in [IP06, Proposition 4.11], we know that \( H^1(\mathbb{Q}_{n,p}, T)/E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \) is the module with two generators \( e_1, e_2 \) and the above two relations (these relations are all).

5.3.3. The global constraint. Due to Theorem 5.1.(2), we have
\[ \mathbb{H}^1_{\text{glob}}(T) \cong \Lambda \]
and let \( b \) be a \( \Lambda \)-generator of \( \mathbb{H}^1_{\text{glob}}(T) \). Then \( b \) is also a \( \Lambda_n \)-generator of \( \mathbb{H}^1_{\text{glob}}(T) \Gamma_n \cong \Lambda_n \). We write the image of \( b \) by \((b_1, b_2)\) under the map
\[ \mathbb{H}^1_{\text{glob}}(T) \xrightarrow{\text{loc}} \mathbb{H}^1_{\text{loc}}(T) \xrightarrow{\text{Col}^+ \oplus \text{Col}^-} \Lambda \oplus \Lambda \]

Since
\[ H^1(\mathbb{Q}_{n,p}, T)/E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \hookrightarrow \Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+, \]
we have
\[ \mathcal{Y}_n' = \frac{H^1(\mathbb{Q}_{n,p}, T)/E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p + \text{im } \mathbb{H}^1_{\text{glob}}(T)}{(b_1, b_2)}. \]

where \( \text{im } \mathbb{H}^1_{\text{glob}}(T) \) is the image of \( \mathbb{H}^1_{\text{glob}}(T) \) in \( H^1(\mathbb{Q}_{n,p}, T) \) and it is a quotient of \( \mathbb{H}^1_{\text{glob}}(T) \Gamma_n \). Then
\[ b_2 e_1 - \frac{b_1 - \frac{p-1}{2} b_2}{X} e_2 = b_2 \left( \frac{p-1}{2}, 1 \right) - \frac{b_1 - \frac{p-1}{2} b_2}{X} (X, 0) = (b_1, b_2) = (0, 0) \in \mathcal{Y}_n' \]

5.3.4. A presentation matrix. Using all the above discussion on generators and relations arising from
\[ \mathbb{H}^1_{\text{glob}}(T) \Gamma_n \xrightarrow{H^1(\mathbb{Q}_{n,p}, T)/E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \mathcal{Y}_n' \xrightarrow{0}, \]
we know there are 2 generators and 3 relations. Now we describe a presentation matrix \( A \) of \( \mathcal{Y}_n' \) over \( \Lambda_n \)
\[ (\Lambda_n)^{\oplus 3} \xrightarrow{A} \Lambda \text{Col}(e_1) \oplus \Lambda \text{Col}(e_2) \xrightarrow{\mathcal{Y}_n'} 0 \]
by
\[ A = \begin{pmatrix} 0 & \omega_n^+ & b_2 \\ \omega_n^- & -\frac{p-1}{2} \omega_n^+ & b_1 - \frac{p-1}{2} b_2 \\ -\frac{p-1}{2} \omega_n^+ & b_1 - \frac{p-1}{2} b_2 & X \end{pmatrix}. \]

A direct computation of minors of the above matrix \( A \) yields the following statement.

Proposition 5.6.
\[ \text{Fitt}_{\Lambda_n}(\mathcal{Y}_n') = (\omega_n^+ b_1, \omega_n^- b_2). \]
5.4. **Putting it all together.** Consider the exact sequence

\[
0 \longrightarrow (\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee})_{\text{mft}} \longrightarrow \text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee} \longrightarrow \mathcal{S} \longrightarrow 0
\]

where \(M_{\text{mft}}\) is the maximal finite torsion \(\Lambda\)-submodule of \(M\). Then we have

\[
\text{char}_{\Lambda} ((\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee})_{\text{mft}}) \cdot \text{char}_{\Lambda} (\mathcal{S}) = \text{char}_{\Lambda} (\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee}).
\]

Since \(\text{char}_{\Lambda} ((\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee})_{\text{mft}})\) is trivial and the projective dimension of \(\mathcal{S}\) over \(\Lambda\) is \(\leq 1\) \(\text{pd}_{\Lambda} \mathcal{S} \leq 1\), we have

\[
\text{Fitt}_{\Lambda} (\mathcal{S}) = (c) \subseteq \Lambda
\]

where \(\mathbf{z}_{\text{Kato}} = c \cdot b\) in \(\mathbb{H}_{\text{glob}}^{1}(T)\) with \(b\) the chosen \(\Lambda\)-generator of \(\mathbb{H}_{\text{glob}}^{1}(T)\) in §5.3.3.

By the control theorem for fine Selmer groups ([Kur02, Lemma 4.2 and Remark 4.4]), we have

\[
\text{Sel}_{0}(\mathbb{Q}_{n}, E[p^\infty])^{\vee} \simeq (\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee})_{\Gamma_{n}}.
\]

Consider two exact sequences with compatibility

\[
0 \longrightarrow \mathcal{Y}_{n} \longrightarrow \text{Sel}(\mathbb{Q}_{n}, E[p^\infty])^{\vee} \longrightarrow (\text{Sel}_{0}(\mathbb{Q}_{\infty}, E[p^\infty])^{\vee})_{\Gamma_{n}} \longrightarrow 0
\]

\[
0 \longrightarrow \mathcal{A}_{n} \longrightarrow \text{Sel}(\mathbb{Q}_{n}, E[p^\infty])^{\vee} \longrightarrow \mathcal{S}_{\Gamma_{n}} \longrightarrow 0
\]

where \(\mathcal{A}_{n}\) is defined to be the kernel of the map \(\text{Sel}(\mathbb{Q}_{n}, E[p^\infty])^{\vee} \rightarrow \mathcal{S}_{\Gamma_{n}}\).

Since \(\text{pd}_{\Lambda} \mathcal{S} \leq 1\), we have \(\mathcal{S}\) admits a presentation by a square matrix over \(\Lambda\). Thus, \(\mathcal{S}_{\Gamma_{n}}\) also admits a presentation by a square matrix over \(\Lambda_{n}\). Then we have

\[
\text{Fitt}_{\Lambda_{n}} (\text{Sel}(\mathbb{Q}_{n}, E[p^\infty])^{\vee}) = \text{Fitt}_{\Lambda_{n}} (\mathcal{A}_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\mathcal{S}_{\Gamma_{n}}) \subseteq \text{Fitt}_{\Lambda_{n}} (\mathcal{Y}_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\mathcal{S}_{\Gamma_{n}})
\]

where Lemma A.4 and Lemma A.10 are used to obtain the first equality and the second inclusion, respectively. Multiplying \(\text{Fitt}_{\Lambda_{n}} (\text{coker } g_{n})\), we have

\[
\text{Fitt}_{\Lambda_{n}} (\text{coker } g_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\text{Sel}(\mathbb{Q}_{n}, E[p^\infty])^{\vee}) \subseteq \text{Fitt}_{\Lambda_{n}} (\text{coker } g_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\mathcal{Y}_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\mathcal{S}_{\Gamma_{n}}) \subseteq \text{Fitt}_{\Lambda_{n}} (\mathcal{Y}_{n}) \cdot \text{Fitt}_{\Lambda_{n}} (\mathcal{S}_{\Gamma_{n}})
\]

\[
= (\tilde{\omega}_{n}^{+} b_{1}, \tilde{\omega}_{n}^{-} b_{2}) \cdot (c)
\]

\[
= (\tilde{\omega}_{n}^{+} \text{Col}^{+} (\text{loc } b), \tilde{\omega}_{n}^{-} \text{Col}^{-} (\text{loc } b)) \cdot (c)
\]

\[
= (\tilde{\omega}_{n}^{+} \text{Col}^{+} (c \cdot \text{loc } b), \tilde{\omega}_{n}^{-} \text{Col}^{-} (c \cdot \text{loc } b))
\]

\[
= (\tilde{\omega}_{n}^{+} \text{Col}^{+} (\text{loc } \mathbf{z}_{\text{Kato}}), \tilde{\omega}_{n}^{-} \text{Col}^{-} (\text{loc } \mathbf{z}_{\text{Kato}}))
\]

\[
= (\tilde{\omega}_{n}^{+} L_{p}^{+} (\mathbb{Q}_{\infty}, f), \tilde{\omega}_{n}^{-} L_{p}^{-} (\mathbb{Q}_{\infty}, f)).
\]
This section is entirely devoted to prove the following proposition in order to obtain Theorem 1.20. We keep all the assumptions in §5 in this section.

### Proposition 6.1.

If (fineNF) $\text{Sel}_0(Q_\infty, E[p^\infty])^\vee$ has no nontrivial finite $\Lambda$-submodule, and

1. if $\text{char} \Lambda(\text{Sel}_0(Q_\infty, E[p^\infty])^\vee) \subseteq (\Phi_n(1 + X))$, then $\text{rk}_Z(E(Q_n) > \text{rk}_Z(E(Q_{n-1})$ (if $n = 0$, then $\Phi_0(1 + X) = X$ and this inequality means $\text{rk}_Z(E(Q) > 0)$),

then $\text{coker } g_n = 0$.

#### 6.1. Reduction.

We recall the following exact sequence ([BP07, (Proof of) Proposition 3.4])

\[ 0 \rightarrow \frac{H^1_{\text{loc}}(T)}{\text{im } H^1_{\text{glob}}(T)} \rightarrow \text{Sel}(Q_\infty, E[p^\infty])^\vee \rightarrow \text{Sel}_0(Q_\infty, E[p^\infty])^\vee \rightarrow 0 \]

and take $\Gamma_n$-coinvariant. Then we have

\[ 0 \rightarrow C_n \rightarrow \frac{H^1(Q_{n,p}, T)}{\text{im } H^1_{\text{glob}}(T)} \rightarrow (\text{Sel}(Q_\infty, E[p^\infty])^\vee)_{\Gamma_n} \rightarrow \text{Sel}_0(Q_n, E[p^\infty])^\vee \rightarrow 0 \]

where

\[ C_n := \text{coker } (\text{Sel}(Q_\infty, E[p^\infty])^\vee, \Gamma_n \rightarrow \text{Sel}_0(Q_\infty, E[p^\infty])^\vee, \Gamma_n) \]

and $\text{im } H^1_{\text{glob}}(T) := \text{im } \left( H^1_{\text{glob}}(T) \rightarrow H^1(Q_{n,p}, T) \right)$. We also have an exact sequence

\[ 0 \rightarrow Z_n \rightarrow \frac{H^1(Q_{n,p}, T)}{E(Q_{n,p}) \otimes Z_p} \rightarrow \text{Sel}(Q_n, E[p^\infty])^\vee \rightarrow \text{Sel}_0(Q_n, E[p^\infty])^\vee \rightarrow 0 \]

as in §5.2.

Let $\pi_{\text{glob,n}} : H^1(Q_{n,p}, T) \rightarrow \frac{H^1(Q_{n,p}, T)}{\text{im } H^1_{\text{glob}}(T)}$ be the natural projection and

\[ \tilde{C}_n := \pi_{\text{glob,n}}^{-1}(C_n) \subseteq H^1(Q_{n,p}, T) \]

be the inverse image of $C_n$ with respect to $\pi_{\text{glob,n}}$, and it obviously contains $\text{im } H^1_{\text{glob}}(T)$.

Considering the following commutative diagram

\[ \begin{array}{ccc}
0 & \rightarrow & \tilde{C}_n \\
\downarrow & & \downarrow \\
0 & \rightarrow & C_n \\
\downarrow & & \downarrow \\
0 & \rightarrow & Z_n \\
\end{array} \]

\[ \begin{array}{ccc}
0 & \rightarrow & H^1(Q_{n,p}, T) \\
\downarrow & & \downarrow \\
0 & \rightarrow & \frac{H^1(Q_{n,p}, T)}{\text{im } H^1_{\text{glob}}(T)} \\
\downarrow & & \downarrow \\
0 & \rightarrow & \frac{H^1(Q_{n,p}, T)}{E(Q_{n,p}) \otimes Z_p} \\
\end{array} \]

\[ \begin{array}{ccc}
0 & \rightarrow & E(Q_{n,p}) \otimes Z_p \\
\downarrow & & \downarrow \\
0 & \rightarrow & (\text{Sel}(Q_\infty, E[p^\infty])^\vee)_{\Gamma_n} \\
\downarrow & & \downarrow \\
0 & \rightarrow & \text{Sel}(Q_n, E[p^\infty])^\vee \\
\end{array} \]

\[ \begin{array}{ccc}
0 & \rightarrow & \text{Sel}_0(Q_n, E[p^\infty])^\vee \\
\downarrow & & \downarrow \\
0 & \rightarrow & \text{Sel}_0(Q_n, E[p^\infty])^\vee \\
\end{array} \]

\[ 0 \rightarrow \text{Sel}_0(Q_n, E[p^\infty])^\vee \rightarrow 0 \]

it is observed that $\tilde{C}_n$ surjects $Z_n$ under the natural quotient map

\[ H^1(Q_{n,p}, T) \rightarrow \frac{H^1(Q_{n,p}, T)}{E(Q_{n,p}) \otimes Z_p} \]

since

\[ \left( \frac{H^1(Q_{n,p}, T)}{\tilde{C}_n} \right) / (E(Q_{n,p}) \otimes Z_p) = \left( \frac{H^1(Q_{n,p}, T)}{E(Q_{n,p}) \otimes Z_p} \right) / Z_n \]
as a subgroup of $\text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee$.

Consider the composition of surjective maps

$$\tilde{C}_n \longrightarrow \mathbb{Z}_n \longrightarrow \text{coker } g_n$$

and then it factors through $C_n$ by definition. Let

$$C'_n := C_n \cap \text{im} \left( E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \to H^1(\mathbb{Q}_{n,p}, T) \right) \subseteq H^1(\mathbb{Q}_{n,p}, T) \text{ im } H^1_{\text{glob}}(T).$$

Then Sequence (6.2) and the following exact sequence

$$0 \longrightarrow \text{coker } g_n \longrightarrow H^1(\mathbb{Q}_{n,p}, T) \text{ im } H^1_{\text{glob}}(T) \longrightarrow \text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow \text{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow 0$$

show that $C'_n = \ker (C_n \to \text{coker } g_n)$. Thus, we have the exact sequence

$$0 \longrightarrow C'_n \xrightarrow{\varphi_n} C_n \longrightarrow \text{coker } g_n \longrightarrow 0.$$ 

We can easily observe the following statement.

**Proposition 6.2.** The following statements are equivalent:

1. $\text{coker } g_n = 0$.
2. $\varphi_n : C'_n \to C_n$ is an isomorphism.
3. All the classes in $C_n$ lie in $E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p := \text{im} \left( E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \to H^1(\mathbb{Q}_{n,p}, T) \right)$.

In particular, if $C_n = 0$, then $\text{coker } g_n = 0$.

From now on, we prove Proposition 6.1 using induction on $n$.

6.2. When the rank does not grow. In this subsection, we assume that

**Assumption 6.3.** $\Phi_n$ does not divide a generator of $\text{char}_\Lambda(\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee)$.

If $n = 0$, then

$$\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee, \Gamma = 0.$$ 

Now we suppose $n > 0$.

**Lemma 6.4.** Let $M$ be a finitely generated torsion $\Lambda$-module with no non-trivial finite $\Lambda$-submodule. Suppose that $\Phi_n$ does not divide a generator of $\text{char}_\Lambda(M)$. Then $M^{\Gamma_n} = M^{\Gamma_n}$. 

**Proof.** We may assume $M = M^{\Gamma_n}$, i.e. $\omega_n M = 0$. Using the structure theorem of finitely generated $\Lambda$-modules, $M$ is a submodule of $M'$ of finite index with

$$M' \simeq \bigoplus_{i=1}^m \Lambda/f_i \Lambda.$$ 

Since $\omega_n M = 0$, we also have $\omega_n M' = 0$. It shows that each $f_i$ divides $\omega_n$. Since $\Phi_n$ does not divide $\text{char}_\Lambda(M') = (\prod_{i=1}^m f_i)$, each $f_i$ is prime to $\Phi_n$. Thus, each $f_i$ divides $\omega_{n-1} = \omega_n/\Phi_n$ and then $\omega_{n-1} M' = 0$. Hence, $\omega_{n-1} M = 0$. 

By Lemma 6.4, we have

$$\text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee, \Gamma_{n-1} \simeq \text{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee, \Gamma_n.$$
Note that Assumption (fineNF) is used here. Thus, the natural map $C_{n-1} \to C_n$ is surjective. Then we have the following commutative diagram

$$
\begin{array}{ccc}
C_n & \longrightarrow & \text{coker } g_n \\
\uparrow & & \uparrow \\
C_{n-1} & \longrightarrow & \text{coker } g_{n-1}
\end{array}
$$

and $\text{coker } g_{n-1} = 0$ by the induction hypothesis. Thus, the lower horizontal map $C_{n-1} \to \text{coker } g_{n-1}$ becomes the zero map and then $\text{coker } g_n = 0$.

6.3. When the rank grows.

In this subsection, we assume that

**Assumption 6.5.** $\Phi_n$ divides a generator of $\text{char}_\Lambda (\text{Sel}_0(Q_\infty, E[p^\infty])^\vee)$.

If $n = 0$, then Assumption (III) implies $\text{rk}_Z E(Q) > 0$, so the natural map

$$
E(Q) \otimes \mathbb{Z}_p \to E(Q_p) \otimes \mathbb{Z}_p
$$

is surjective.

For a faithful character $\psi_n$ of $\text{Gal}(Q_n/\mathbb{Q})$, let

$$
M_{\psi_n} := M/\psi_n M
$$

where $M$ is a $\Lambda_n$-module.

Now we suppose $n > 0$. By Assumption (III), we have

$$
\text{rk}_Z E(Q_n) > \text{rk}_Z E(Q_{n-1}).
$$

Then

$$
(E(Q_n) \otimes \mathbb{Z}_p)_{\psi_n} \to (E(Q_{n-1}) \otimes \mathbb{Z}_p)_{\psi_{n-1}}
$$

is surjective.

First, we explicitly write down the connecting map

$$
C_n \to \frac{H^1(Q_{n,p}, T)}{\text{im } H^1_{\text{glob}}(T)}
$$

in Sequence (6.2). Let

$$
[f] \in C_n = \text{coker } (\text{Sel}(Q_\infty, E[p^\infty])^\vee) \cap \text{Sel}_0(Q_\infty, E[p^\infty])^\vee,
$$

with a representative $f \in \text{Sel}_0(Q_\infty, E[p^\infty])^\vee [\omega_n] \subseteq \text{Sel}_0(Q_\infty, E[p^\infty])^\vee$. Via Sequence (6.1), we lift $f$ to $\tilde{f} \in \text{Sel}(Q_\infty, E[p^\infty])^\vee$. Due to the definition of $C_n$, $\omega_n \tilde{f}$ depends only on $[f]$. Also, since $\omega_n f$ maps to $\omega_n f = 0$ in Sequence (6.1), we have

$$
\omega_n \tilde{f} \in \frac{H^1_{\text{loc}}(T)}{H^1_{\text{glob}}(T)} \subseteq \text{Sel}(Q_\infty, E[p^\infty])^\vee.
$$

This means that there exists an element $P \in H^1_{\text{loc}}(T)$ such that

$$
\omega_n \tilde{f}(x) = \langle P, j(x) \rangle
$$

for any $x \in \text{Sel}(Q_\infty, E[p^\infty])$ where $j : \text{Sel}(Q_\infty, E[p^\infty]) \to H^1(Q_{\infty,p}, E[p^\infty])$ is the natural localization map and $\langle -, - \rangle$ is the local Tate pairing between $H^1_{\text{loc}}(T)$ and $H^1(Q_{\infty,p}, E[p^\infty])$.

Putting $P_n := P \mod \omega_n \in H^1(Q_{n,p}, T)$, we have the following diagram

$$
\begin{array}{ccc}
H^1_{\text{loc}}(T) & \longrightarrow & H^1(Q_{n,p}, T) \\
\downarrow & & \downarrow \\
H^1_{\text{loc}}(T) & \longrightarrow & H^1(Q_{n,p}, T)
\end{array}
$$

and

$$
\begin{array}{ccc}
H^1_{\text{loc}}(T) & \longrightarrow & H^1(Q_{n,p}, T) \\
\downarrow & & \downarrow \\
H^1_{\text{glob}}(T) & \longrightarrow & H^1(Q_{n,p}, T)
\end{array}
$$

with

$$
\omega_n \tilde{f} \longrightarrow P_n := \omega_n \tilde{f} \mod \omega_n.
$$

21
Note that \( P_n = \omega_n \tilde{f} (\mod \omega_n) \) \( \in \frac{H^1(Q_{n,p}, T)}{\im \mathbb{H}^1_{\text{glob}}(T)} \) is not necessarily zero since \( \tilde{f} \) may not be contained in \( \frac{H^1_{\text{loc}}(T)}{\mathbb{H}^1_{\text{glob}}(T)} \). To sum up, the map

\[
C_n \rightarrow \frac{H^1(Q_{n,p}, T)}{\im \mathbb{H}^1_{\text{glob}}(T)}
\]

is defined by

\[
[f] \mapsto \overline{P}_n.
\]

Now we prove that \( P_n \in E(Q_{n,p}) \otimes \mathbb{Z}_p \) in \( H^1(Q_{n,p}, T) \). By the local Tate duality, it suffices to check

\[
\langle P_n, E(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rangle = 0.
\]

Consider the exact sequence

\[
0 \rightarrow E(Q_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow E(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow (E(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{\psi_n} \rightarrow 0.
\]

By the induction hypothesis, we have \( coker g_{n-1} = 0 \). Thus, the map in Sequence (6.3)

\[
\varphi_{n-1} : C_{n-1} \rightarrow C_{n-1}
\]

is an isomorphism and also \( P_{n-1} := P_n (\mod \omega_{n-1}) \) is contained in \( E(Q_{n-1,p}) \otimes \mathbb{Z}_p \). Therefore,

\[
\langle P_n, E(Q_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rangle = 0.
\]

By Sequence (6.5), we only need to show that

\[
\langle P_n, E(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rangle \psi_n = 0
\]

in order to prove (6.4). By Assumption (III), the localization map

\[
E(Q_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \psi_n \rightarrow (E(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \psi_n
\]

is surjective. Furthermore, \( \omega_n \tilde{f} \) vanishes on \( E(Q_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \) since

\[
E(Q_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \text{Sel}(Q_n, E[p^\infty]) \subseteq \text{Sel}(Q_n, E[p^\infty])[\omega_n].
\]

This shows that Equation (6.7) holds. Sequence (6.5), Equation (6.6), and Equation (6.7) complete the proof of Equation (6.4).

### 7. Allowing the Tamagawa Defect

The goal of this section is to prove a non-primitive variant (Theorem 1.22 = Corollary 7.4) of Theorem 1.14 removing the \( p \nmid \text{Tam}(E) \) condition. It is well-known that the \( p \nmid \text{Tam}(E) \) implies the corresponding modular form is not of minimal level (via [Lun16, Proposition 4.2 and Theorem 4.3]). As a payoff, we only obtain a weaker generalization of Theorem 1.14, which is a non-primitive version (cf. [GV00]). The fundamental obstruction of this case is the finite error term appeared in the control theorem. In order to remove the error term, we replace all the objects we considered by their non-primitive versions. Also, we only focus on the case of supersingular reduction in this section since the case of ordinary reduction is easier.

Let \( E \) be an elliptic curve over \( \mathbb{Q} \) of conductor \( N \) with supersingular reduction at \( p \). Assume that \( a_p(E) = 0 \). Let \( f \in S_2(\Gamma_0(N)) \) be the newform corresponding to \( E \) as before. Let \( \overline{\gamma} : G_{\mathbb{Q}} \rightarrow \text{Aut}_{E_p}(E[p^\infty]) \simeq \text{GL}_2(F_p) \) be the mod \( p \) representation arising from the \( p \)-torsion points on \( E \). Let \( N(\overline{\gamma}) \) be the prime-to-\( p \) conductor of \( \overline{\gamma} \). Let \( \Sigma_0 \subseteq \Sigma \) be the set of primes dividing \( N/N(\overline{\gamma}) \). Note that \( p, \infty \notin \Sigma_0 \).

We define the \( \Sigma_0 \)-non-primitive Selmer group of \( E \) over \( \mathbb{Q}_n \) by

\[
\text{Sel}^\Sigma_0(Q_n, E[p^\infty]) := \ker \left( H^1(Q_{\Sigma}/Q_n, E[p^\infty]) \rightarrow \prod_{w,w'\mid \ell_0} \frac{H^1(Q_{n,w} \otimes E[p^\infty])}{E(Q_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right).
\]
As in [Kim09, §2], we also define the \(\Sigma_0\)-non-primitive \(\pm\)-Selmer groups of \(E\) over \(Q_n\) by

\[
\text{Sel}^{\pm, \Sigma_0}(Q_n, E[p^\infty]) := \ker\left( \frac{H^1(Q_{\Sigma}/Q_n, E[p^\infty])}{E^+(Q_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \prod_{w | \ell, \ell \in \Sigma_0, \ell \neq p} \frac{H^1(Q_{n,w}, E[p^\infty])}{E(Q_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right).
\]

We also define \(\Sigma_0\)-non-primitive \(\pm\)-Selmer groups of \(E\) over \(Q_\infty\) by

\[
\text{Sel}^{\pm, \Sigma_0}(Q_\infty, E[p^\infty]) := \lim_{n \to \infty} \text{Sel}^{\pm, \Sigma_0}(Q_n, E[p^\infty]).
\]

Then the difference between \(\pm\)-Selmer groups and their \(\Sigma_0\)-non-primitive variants is given as follows.

**Lemma 7.1** ([Kim09, Corollary 2.5]).

\[
\text{Sel}^{\pm, \Sigma_0}(Q_\infty, E[p^\infty]) / \text{Sel}^{\pm, \Sigma_0}(Q_\infty, E[p^\infty]) \simeq \prod_{w | \ell, \ell \in \Sigma_0, \ell \neq p} H^1(Q_{\infty,w}, E[p^\infty]).
\]

Let \(\ell \in \Sigma_0\) and \(\gamma_\ell\) be the arithmetic Frobenius map at \(\ell\) in the decomposition subgroup \(\Gamma_\ell := \text{Gal}(Q_{\infty, \eta}/Q_\ell)\) of \(\text{Gal}(Q_{\infty}/Q)\) at a prime \(\eta\) of \(Q_\infty\) dividing \(\ell\). Following [GV00, (15)], consider

\[
P_\ell^* := \begin{cases} 
1 - a_\ell(f)\ell^{-1}\gamma_\ell + \ell^{-1}\gamma_\ell^2 & \text{if } \ell \nmid N \\
1 - a_\ell(f)\ell^{-1}\gamma_\ell & \text{if } \ell | N \\
1 & \text{if } \ell^2 | N
\end{cases}
\]

in \(\mathbb{Z}_p[\Gamma_\ell]\). We define the **Iwasawa theoretic Euler factor** \(P_\ell\) of \(f\) at \(\ell\) by the natural image of \(P_\ell^*\) in \(\Lambda\) and it satisfies the following equality of ideals in \(\Lambda\).

**Lemma 7.2** ([GV00, Proposition 2.4]).

\[
(P_\ell) = \text{char}_\Lambda \left( \left( \prod_{w | \ell} H^1(Q_{\infty,w}, E[p^\infty]) \right)^\vee \right).
\]

We define the \(\Sigma_0\)-non-primitive \(\pm\)-\(p\)-adic \(L\)-functions of \(f\) by

\[
L_p^{\pm, \Sigma_0}(Q_\infty, f) := L_p^{\pm}(Q_\infty, f) \cdot \prod_{\ell \in \Sigma_0} P_\ell
\]

and the \(\Sigma_0\)-non-primitive Mazur-Tate elements of \(f\) at \(Q_n\) by

\[
\theta_{n, \Sigma_0}^*(f) := \theta_n(f) \cdot \prod_{\ell \in \Sigma_0} P_{\ell, n}
\]

where \(P_{\ell, n} := P_\ell \pmod{\omega_n} \in \Lambda_n\). If one wants to define \(\theta_{n, \Sigma_0}^*(f)\) by \(\theta_n(f^{\Sigma_0})\) with the same period of \(f\) where \(f^{\Sigma_0}\) is the oldform of level \(N(\mathfrak{p}) \cdot \prod_{\ell \in \Sigma_0} \ell^2\) arising from \(f\), then Ihara’s lemma is required to compare two definitions.

We recall \(\Sigma_0\)-non-primitive versions of the main ingredients:

**Proposition 7.3** (\(\Sigma_0\)-non-primitive variants of Theorem 3.5, Theorem 3.6, and Theorem 3.7).

1. Assume that \(\mathfrak{p}\) is surjective if \(E\) is non-CM. Then

\[
(L_p^{\pm, \Sigma_0}(Q_\infty, f)) \subset \text{char}_\Lambda \left( \text{Sel}^{\pm, \Sigma_0}(Q_\infty, E[p^\infty])^\vee \right).
\]

Furthermore, the inclusion becomes equality provided that \(E\) has CM.

2. \(\text{Sel}^{\pm, \Sigma_0}(Q_\infty, E[p^\infty])\) has no proper \(\Lambda\)-submodule of finite index.

23
(3) The restriction map
\[ \text{Sel}^{\pm, \Sigma_0}(\mathbb{Q}_n, E[p\infty])[\omega_n^\pm] \rightarrow \text{Sel}^{\pm, \Sigma_0}(\mathbb{Q}_\infty, E[p\infty])[\omega_n^\pm] \]
is an isomorphism.

Proof.

(1) It follows from Theorem 3.5, Lemma 7.1, and Lemma 7.2. (cf. [GV00, Theorem 1.5.3].)

(2) It is [Kim09, Proposition 2.11].

(3) It is a direct consequence of Theorem 3.7 because we remove the local conditions at all \( \ell \in \Sigma_0 \), which contain all the error term.

□

From this proposition, we obtain the following corollary, the main theorem of this section.

Corollary 7.4. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) of conductor \( N \) with good reduction at an odd prime \( p \). Let \( N(\overline{p}) \) be the prime-to-\( p \) conductor of the mod \( p \) representation \( E[p] \). Let \( \Sigma_0 \) be the set of primes dividing \( N/N(\overline{p}) \). Assume that \( E[p] \) is surjective if \( E \) is non-CM. Also, assume one of the followings:

(\text{ord}) \( p \nmid a_p(f) \) and \( a_p(f) \neq 1 \pmod{p} \), or
(\text{ss}) \( a_p(f) = 0 \).

Then
\[ \left( \theta_n^{\Sigma_0}(f), \nu_{n-1,n}(\theta_n^{\Sigma_0}(f)) \right) \subseteq \text{Fitt}_{\Lambda_n} \left( \text{Sel}^{\Sigma_0}(\mathbb{Q}_n, E[p\infty])^\vee \right). \]

In Case (ord), if the equality of the Iwasawa main conjecture holds, then the inclusion becomes equality.

Proof. For Case (ord), apply the argument in §2 to the \( \Sigma_0 \)-non-primitive setting with the ordinary analogue of Proposition 7.3 (Theorem 2.2 with [GV00, Theorem 1.5.3], [GV00, Proposition 2.5], and the \( \Sigma_0 \)-non-primitive variant of Theorem 2.4). For Case (ss), apply the argument in §4 to the \( \Sigma_0 \)-non-primitive setting with Proposition 7.3. □

Remark 7.5. Although we have Lemma 7.2, we cannot recover the original conjecture
\[ \left( \theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f)) \right) \subseteq \text{Fitt}_{\Lambda_n} \left( \text{Sel}(\mathbb{Q}_n, E[p\infty])^\vee \right) \]
from Corollary 7.4 in an obvious way because \( \Lambda_n \) is not a domain.

Acknowledgement

C.K. thanks M.K. for introducing this subject; Robert Pollack for sharing his ideas, helpful discussion, and support; Shinichi Kobayashi for answering questions on \( \pm \)-Selmer groups; Jaehoon Lee for careful reading of an earlier version; GilYoung Cheong, B.D. Kim, Myoungil Kim, Takahiro Kitajima, and Kazuto Ota for helpful discussions. C.K. is partially supported by “Overseas Research Program for Young Scientists” through Korea Institute for Advanced Study (KIAS) and by Basic Science Research Program through the National Research Foundation of Korea (NRF-2018R1C1B6007009).

M.K. thanks Ralph Greenberg and Robert Pollack for the discussion with them on the subject of this paper (held more than 10 years ago). He also thanks C.K. heartily for letting him come back to this interesting subject through many discussions and questions. M.K. is partially supported by JSPS Core-to-core program, “Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry”.

24
Appendix A. Lemmas on Fitting Ideals

All the modules in this section are finitely presented over their base rings. Let $R$ be a commutative ring with unity.

Lemma A.1 ([MW84, 1, Appendix]). Let $M \to N$ be a surjective map of $R$-modules. Then
\[ \text{Fitt}_R(M) \subseteq \text{Fitt}_R(N). \]

Lemma A.2 ([MW84, 9, Appendix]). Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Then
\[ \text{Fitt}_R(M_1) \cdot \text{Fitt}_R(M_3) \subseteq \text{Fitt}_R(M_2). \]

Lemma A.3 ([Nor76, Theorem 22, Page 80]). Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Assume that $M_3$ has presentation by a square matrix. Then
\[ \text{Fitt}_R(M_1) \cdot \text{Fitt}_R(M_3) = \text{Fitt}_R(M_2). \]

Proof. Denote a presentation matrix of $M_i$ by $A_i$ for $i = 1, 2, 3$. In other words,
\[
\begin{array}{ccc}
R^{\oplus s} & \xrightarrow{A_1} & R^{\oplus r} \\
R^{\oplus (s+m)} & \xrightarrow{A_2} & M_1 \\
R^{\oplus m} & \xrightarrow{A_3} & R^{\oplus m} \\
\end{array}
\]
with $r \leq s$. Then we have
\[ A_2 = \begin{pmatrix} A_1 \\ 0 \\ A_3 \end{pmatrix} \in M_{(r+m) \times (s+m)}(R). \]
Considering $(r + m) \times (r + m)$ minors of $A_2$, it is easy to see that the upper-triangular part $(\ast)$ of $A_2$ does not affect the determinants of the minors. Thus, the conclusion follows. \(\square\)

Remark A.5. If $R = \mathbb{Z}[G]$ with a finite abelian group $G$, for example, and $M$ is torsion with $\text{pd}_R M \leq 1$, then $\text{Fitt}_R(M)$ is a principal ideal generated by a non-zero divisor. Thus, Lemma A.3 is slightly stronger than Lemma A.4 for this case.

Lemma A.6 ([MW84, 4, Appendix]). Let $M$ be a finitely presented $R$-module. If $I \subseteq R$ is an ideal, then
\[ \text{Fitt}_{R/I}(M/IM) = \pi(\text{Fitt}_R(M)) \]
where $\pi : A \to A/I$ is the natural quotient map.

The following lemma is the key to replace characteristic ideals by Fitting ideals. Though several proofs of this lemma are known, we want to give here a new proof.

Lemma A.7. Let $M$ be a finitely generated torsion $\Lambda$-module. Assume that $M$ has no non-trivial finite $\Lambda$-submodule. Then
\[ \text{char}_\Lambda(M) = \text{Fitt}_\Lambda(M). \]

Proof. If $M$ has no nontrivial finite $\Lambda$-submodule, then $\text{depth}(M) = 1$, i.e. there exists an element $x \in \Lambda$ such that the multiplication by $x$ map on $M$ is injective. By Auslander-Buchsbaum formula, we have
\[ \text{pd}_\Lambda(M) + \text{depth}(M) = \text{depth}(\Lambda) \]
with $\text{depth}(M) = 1$, and $\text{depth}(\Lambda) = 2$. Thus, $\text{pd}_\Lambda(M) = 1$. This shows that $M$ is the cokernel of a $\Lambda$-homomorphism $f : \Lambda^n \to \Lambda^n$. Then both the characteristic ideal and the Fitting ideal...
of $M$ are generated by $\det(f)$, and we get the conclusion. See also [Win85, Proposition 2.1] and [Tal12, Lemma 1.3.3 and Proposition 1.3.4]. □

**Remark A.8.** This lemma is an enhanced version of [MW84, page 327–328, Appendix] removing the $\mu = 0$ assumption. (cf. [Kur03, §1.1].)

**Lemma A.9.** Let $M$ and $N$ be $\Lambda_n$-modules. We assume that $M$ and $N$ have no finite $\Lambda$-torsion submodule provided that we regard $M$ and $N$ as $\Lambda$-modules. If $N \subseteq M$, then

$$\text{Fitt}_{\Lambda_n}(M) \subseteq \text{Fitt}_{\Lambda_n}(N).$$

**Proof.** We regard $M$ and $N$ as $\Lambda$-modules. Then we have

$$\text{Fitt}_{\Lambda}(M) = \text{char}_{\Lambda}(M) \quad \text{Fitt}_{\Lambda}(N) = \text{char}_{\Lambda}(N)$$

by Lemma A.7. Consider the exact sequence of $\Lambda$-modules

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$$

Then we have

$$\text{Fitt}_{\Lambda}(M) = \text{char}_{\Lambda}(M) \quad = \text{char}_{\Lambda}(N) \cdot \text{char}_{\Lambda}(M/N) \quad = \text{Fitt}_{\Lambda}(N) \cdot \text{char}_{\Lambda}(M/N) \quad \subseteq \text{Fitt}_{\Lambda}(N)$$

By taking quotient by $\omega_n$ with Lemma A.6, we have

$$\text{Fitt}_{\Lambda_n}(M) \subseteq \text{Fitt}_{\Lambda_n}(N).$$

□

**Lemma A.10.** If $A \subset B$ as finitely generated $\Lambda_n$-modules, then

$$\text{Fitt}_{\Lambda_n}(B) \subseteq \text{Fitt}_{\Lambda_n}(A).$$

**Proof.** We regard $A$ and $B$ as $\Lambda$-modules. Consider the exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow B/A \rightarrow 0.$$}

Then we have

$$\text{char}_{\Lambda}(A) \cdot \text{char}_{\Lambda}(B/A) = \text{char}_{\Lambda}(B).$$

Hence, we have

$$\text{char}_{\Lambda}(B) \subseteq \text{char}_{\Lambda}(A).$$

Consider the following two exact sequences as $\Lambda$ or $\Lambda_n$-modules with compatibility

$$0 \rightarrow B_{\text{mft}} \rightarrow B \rightarrow B' \rightarrow 0$$

$$0 \rightarrow A_{\text{mft}} \rightarrow A \rightarrow A' \rightarrow 0$$

where $A_{\text{mft}}$ and $B_{\text{mft}}$ are the maximal finite torsion $\Lambda$-submodules of $A$ and $B$, respectively. Thus, $A'$ and $B'$ have no finite $\Lambda$-submodule and indeed have no finite $\Lambda_n$-submodule. Then we have

$$\text{Fitt}_{\Lambda_n}(B') \subseteq \text{Fitt}_{\Lambda_n}(A')$$

by Lemma A.9. Also, by Mazur-Wiles [MW84, Corollary to Proposition 3, Appendix., Page 328], we have

$$\text{Fitt}_{\Lambda_n}(B_{\text{mft}}) \subseteq \text{Fitt}_{\Lambda_n}(A_{\text{mft}}).$$
Then Lemma A.3 and Lemma A.6 show us that

\[
Fitt_{\Lambda_n}(A) = Fitt_{\Lambda_n}(A_{\text{infl}}) \cdot Fitt_{\Lambda_n}(A')
\]

\[
Fitt_{\Lambda_n}(B) = Fitt_{\Lambda_n}(B_{\text{infl}}) \cdot Fitt_{\Lambda_n}(B').
\]

Thus, the conclusion follows. \(\square\)

REFERENCES

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over \(\mathbb{Q}\): wild 3-adic exercises*, Journal of the American Mathematical Society 14 (2001), no. 4, 843–939.

[BMC17] Werner Bley and Daniel Macias Castillo, *Congruences for critical values of higher derivatives of twisted Hasse-Weil \(L\)-functions*, Journal für die reine und angewandte Mathematik 722 (2017), 105–135.

[EPW] Matthew Emerton, Robert Pollack, and Tom Weston, *Explicit reciprocity laws and Iwasawa theory for modular forms*, in preparation.

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997) (Berlin) (C. Viola, ed.), Lecture Notes in Mathematics, vol. 1716, Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, Springer-Verlag, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12-19, 1997, pp. 51–144.

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Inventiones Mathematicae 142 (2000), no. 1, 17–63.

[HM00] Yoshitaka Hachimori and Kazuo Matsuno, *On finite \(\Lambda\)-submodules of Selmer groups of elliptic curves*, Proceedings of the American Mathematical Society 128 (2000), no. 9, 2539–2541.

[IP06] Adrian Iovita and Robert Pollack, *Iwasawa theory of elliptic curves at supersingular primes over \(\mathbb{Z}_p\)-extensions of number fields*, Journal für die reine und angewandte Mathematik 598 (2006), 71–103.

[Kat04] Kazuya Kato, *\(p\)-adic Hodge theory and values of zeta functions of modular forms*, Astérisque 295 (2004), 117–290.

[Kim] Chan-Ho Kim, *An anticyclotomic Mazur-Tate conjecture for modular forms*, submitted, arXiv:1612.03743.

[Kim09] Byoung Du Kim, *The Iwasawa invariants of the plus/minus Selmer groups*, The Asian Journal of Mathematics 13 (2009), no. 2, 181–190.

[Kim13] ______, *The plus/minus Selmer groups for supersingular primes*, The Journal of the Australian Mathematical Society 95 (2013), no. 2, 189–200.

[KKS] Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun, *On the indivisibility of derived Kato’s Euler systems and the main conjecture for modular forms*, submitted, arXiv:1709.05780.

[KO06] Masato Kurihara and Rei Otsuki, *On the growth of Selmer groups of an elliptic curve with supersingular reduction in the \(Z_p\)-extensions of \(\mathbb{Q}\)*, Pure and Applied Mathematics Quarterly 2 (2006), no. 2, 557–568. (Special Issue: In honor of John H. Coates, Part 2 of 2).

[KO18] Takahiro Kitajima and Rei Otsuki, *On the plus and the minus Selmer groups for elliptic curves at supersingular primes*, Tokyo Journal of Mathematics (2018), to appear.

[Kob03] Shinichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Inventiones Mathematicae 152 (2003), no. 1, 1–36.

[KP07] Masato Kurihara and Robert Pollack, *Two \(p\)-adic \(L\)-functions and rational points on elliptic curves with supersingular reduction*, London Mathematical Society Lecture Note Series, vol. 320, Cambridge University Press, 2007, pp. 300–332.

[Kur02] Masato Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Inventiones Mathematicae 149 (2002), 195–224.

[Kur03] ______, *Iwasawa theory and Fitting ideals*, Journal für die reine und angewandte Mathematik 561 (2003), 39–86.

[Kur14] ______, *Refined Iwasawa theory for \(p\)-adic representations and the structure of Selmer groups*, Münster Journal of Mathematics 7 (2014), no. 1, 149–223.

[Lei11] Antonio Lei, *Iwasawa theory for modular forms at supersingular primes*, Compositio Mathematica 147 (2011), no. 3, 803–838.

[Lun16] Benjamin Lundell, *Quantitative level lowering*, American Journal of Mathematics 138 (2016), no. 2, 419–448.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin Systems*, Memoirs of the American Mathematical Society, vol. 168, American Mathematical Society, March 2004.
Barry Mazur and John Tate, *Refined conjectures of the “Birch and Swinnerton-Dyer type”*, Duke Mathematical Journal **54** (1987), no. 2, 711–750.

Barry Mazur and Andrew Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Inventiones Mathematicae **76** (1984), no. 2, 179–330.

Douglas Geoffrey Northcott, *Finite Free Resolutions*, Cambridge Tracts in Mathematics, vol. 71, Cambridge University Press, 1976.

Kazuto Ota, *Kato's Euler system and the Mazur-Tate refined conjecture of BSD type*, American Journal of Mathematics (2018), to appear.

Robert Pollack, *On the $p$-adic $L$-function of a modular form at a supersingular prime*, Duke Mathematical Journal **118** (2003), no. 3, 523–558.

Robert Pollack, *An algebraic version of a theorem of Kurihara*, Journal of Number Theory (special issue in honor of Arnold Ross) **110/1** (2005), 164–177.

Bernadette Perrin-Riou, *$p$-adic $L$-Functions and $p$-adic Representations*, SMF/AMS Texts and Monographs, vol. 3, American Mathematical Society, 2000, Translated by Leila Schneps.

Arithmétique des courbes elliptiques à réduction supersingulière en $p$, Experimental Mathematics **12** (2003), no. 2, 155–186.

Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Annals of Mathematics **159** (2004), no. 1, 447–464.

Karl Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Inventiones Mathematicae **93** (1988), no. 3, 701–714.

The “main conjectures” of Iwasawa theory for imaginary quadratic fields, Inventiones Mathematicae **103** (1991), no. 1, 25–68.

Florian Sprung, *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*, Journal of Number Theory **132** (2012), no. 7, 1483–1506.

The Iwasawa main conjecture for elliptic curves at odd supersingular primes, preprint, arXiv:1610.10017, 2016.

Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for $GL_2$*, Inventiones Mathematicae **195** (2014), no. 1, 1–277.

Reza Taleb, *An equivariant main conjecture in Iwasawa theory and the Coates-Sinnot conjecture*, Ph.D. thesis, McMaster University, October 2012, Open Access Dissertations and Theses. Paper 7563, under the supervision of Manfred Kolster.

Xin Wan, *The Iwasawa main conjecture for Hilbert modular forms*, Forum of Mathematics, Sigma **3** (2015), e18 (95 pages).

Xin Wan, *Iwasawa main conjecture for non-ordinary modular forms*, preprint, arXiv:1607.07729, January 2018.

Xin Wan, *Iwasawa main conjecture for supersingular elliptic curves*, preprint, arXiv:1411.6352, February 2018.

Kay Wingberg, *Duality theorems for $\Gamma$-extensions of algebraic number fields*, Compositio Mathematica **55** (1985), no. 3, 333–381.

*School of Mathematics, Korea Institute for Advanced Study (KIAS), 85 Hoe-giro, Dongdaemun-gu, Seoul 02455, Republic of Korea*

*E-mail address: chanho.math@gmail.com*

*Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan*

*E-mail address: kurihara@math.keio.ac.jp*