Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Toshiro HIRANOUCHI et Tatsuya OHSHITA

Asymptotic behavior of class groups and cyclotomic Iwasawa theory of elliptic curves

Tome 35, nº 2 (2023), p. 591-657.

https://doi.org/10.5802/jtnb.1258

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **35** (2023), 591–657

Asymptotic behavior of class groups and cyclotomic Iwasawa theory of elliptic curves

par Toshiro HIRANOUCHI et Tatsuya OHSHITA

Résumé. Dans cet article, nous étudions une relation entre certains quotients de groupes des classes d'idéaux et le module d'Iwasawa cyclotomique X_∞ du dual de Pontrjagin du groupe de Selmer fin d'une courbe elliptique E sur $\mathbb{Q}$. Nous considérons l'extension galoisienne K_n^E de $\mathbb{Q}$ engendrée par les coordonnées des points de p^n-torsion de E et introduisons le quotient A_n^E du p-Sylow du groupe des classes d'idéaux de K_n^E découpé par la représentation galoisienne modulo p^n sur le groupe $E[p^n]$. Nous décrivons le comportement asymptotique des A_n^E en utilisant le module d'Iwasawa X_∞. En particulier, sous certaines conditions, nous obtenons une formule asymptotique à la Iwasawa pour l'ordre de A_n^E en utilisant les invariants d'Iwasawa de X_∞.

Abstract. In this article, we study a relation between certain quotients of ideal class groups and the cyclotomic Iwasawa module X_∞ of the Pontrjagin dual of the fine Selmer group of an elliptic curve E defined over $\mathbb{Q}$. We consider the Galois extension field K_n^E of $\mathbb{Q}$ generated by coordinates of all p^n-torsion points of E, and introduce a quotient A_n^E of the p-Sylow subgroup of the ideal class group of K_n^E cut out by the modulo p^n Galois representation $E[p^n]$. We describe the asymptotic behavior of A_n^E by using the Iwasawa module X_∞. In particular, under certain conditions, we obtain an asymptotic formula as Iwasawa's class number formula on the order of A_n^E by using Iwasawa's invariants of X_∞.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. For each $N \in \mathbb{Z}_{>0}$, we denote by $E[N]$ the subgroup of $E(\overline{\mathbb{Q}})$ consisting of elements annihilated by N. Fix an odd prime number p at which E has good reduction. For each $n \in \mathbb{Z}_{>0}$, we put $K_n^E := \mathbb{Q}(E[p^n])$, and $h_n := \mathrm{ord}_p \#(\mathrm{Cl}(\mathcal{O}_{K_n^E}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, where ord_p denotes the additive p-adic valuation normalized by $\mathrm{ord}_p(p) = 1$ and $\mathrm{Cl}(\mathcal{O}_{K_n^E})$ is the ideal class group of the ring of integers $\mathcal{O}_{K_n^E}$. In recent papers [6, 18, 19], there has been renewal of interest in an asymptotic behavior of the class numbers $\{h_n\}_{n\geq 0}$ along the tower of number fields K_n^E. It has been shown

Manuscrit reçu le 13 mai 2022, révisé le 20 octobre 2022, accepté le 14 novembre 2022.
2020 *Mathematics Subject Classification.* 11R29, 11G05, 11R23.
Mots-clefs. class number; elliptic curve; Iwasawa theory.
The work of the first author is supported by JSPS KAKENHI 20K03536. The work of the second author is supported by JSPS KAKENHI 18H05233, 20K14295 and 21K18577.

that an asymptotic inequality which gives a *lower bound* of $\{h_n\}_{n\geq 0}$ in terms of the Mordell–Weil rank $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ of E (cf. Remark 1.12). For some generalizations of these results including abelian varieties over a number field, see [5] and [14]. In these works, the divisible part of *the fine Selmer group* $\mathrm{Sel}_p(\mathbb{Q}, E[p^\infty])$ (cf. Definition 5.3) plays important roles.

We define a quotient A_n^E of $\mathrm{Cl}(\mathcal{O}_{K_n^E})\otimes_{\mathbb{Z}}\mathbb{Z}_p$, which is cut out by the Galois representation $E[p^n]$ (see (1.2) below). In this paper, we shall describe the asymptotic behavior of A_n^E by using the fine Selmer group $\mathrm{Sel}_p(K_n, E[p^n])$, where we put $K_n := \mathbb{Q}(\mu_{p^n})$. As an application of our result, we shall show an asymptotic formula on the order of A_n^E using Iwasawa's μ and λ-invariants of the cyclotomic Iwasawa module associated with the fine Selmer group of the elliptic curve E, as "Iwasawa's class number formula" ([8]).

1.1. The statements of the main results. In order to state our main results, let us introduce some notation. For each $N \in \mathbb{Z}_{>0}$, we denote by $\mu_N := \boldsymbol{\mu}_N(\overline{\mathbb{Q}})$ the group of N-th roots of unity. For each $m \in \mathbb{Z}_{\geq 0}$, we define $K_m := \mathbb{Q}(\mu_{p^m})$ (in particular, we put $K_0 := \mathbb{Q}$), and set $K_\infty := \bigcup_{m\geq 0} K_m$. For each $m_1, m_2 \in \mathbb{Z}_{\geq 0}\cup\{\infty\}$ with $m_2 > m_1$, we set $\mathcal{G}_{m_2,m_1} := \mathrm{Gal}(K_{m_2}/K_{m_1})$, and put $\Delta := \mathcal{G}_{1,0} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. For any $m \geq 1$, we have $\mathcal{G}_{m,0} = \Delta \times \mathcal{G}_{m,1}$. We can regard $\mathbb{Z}_p[\Delta]$ as a subring of $\mathbb{Z}_p[\mathcal{G}_{m,0}]$. We put $\widehat{\Delta} := \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$. For each $\chi \in \widehat{\Delta}$, we define $\mathbb{Z}_p(\chi) := \mathbb{Z}_p$ to be the $\mathbb{Z}_p[\Delta]$-algebra where Δ acts via χ, and for a $\mathbb{Z}_p[\Delta]$-module M, we set $M_\chi := M\otimes_{\mathbb{Z}_p[\Delta]}\mathbb{Z}_p(\chi)$. We have $M = \bigoplus_{\chi\in\widehat{\Delta}} M_\chi$ because p is odd. For each $m, n \in \mathbb{Z}_{\geq 0}$, we define

$$R_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,0}] = \mathbb{Z}_p/p^n\mathbb{Z}_p[\mathrm{Gal}(K_m/\mathbb{Q})],$$

and put $R_n := R_{n,n}$. For each number field L, that is, a finite extension of $\mathbb{Q}$, and each $n \in \mathbb{Z}_{\geq 0}\cup\{\infty\}$, let $\mathrm{Sel}(L, E[p^n])$ be the Selmer group in the classical sense, and $\mathrm{Sel}_p(L, E[p^n])$ the kernel of the localization map

$$\mathrm{Sel}(L, E[p^n]) \longrightarrow \prod_{v|p} H^1(L_v, E[p^n])$$

which is called *the fine Selmer group* (for details, see Definition 5.3 and Remark 5.6 later). For each $m, n \in \mathbb{Z}_{\geq 0}$, the group $\mathrm{Sel}_p(K_m, E[p^n])$ becomes an $R_{m,n}$-module. For any $n \in \mathbb{Z}_{\geq 0}$, the field $K_n^E = \mathbb{Q}(E[p^n])$ contains μ_{p^n} and hence $K_n^E \supseteq K_n = \mathbb{Q}(\mu_{p^n})$ because of the Weil pairing $E[p^n]\times E[p^n] \to \mu_{p^n}$ ([24, Chapter III, Corollary 8.1.1]).

Let

$$\rho_n^E\colon \mathrm{Gal}(K_n^E/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

be the natural left action of $\mathrm{Gal}(K_n^E/\mathbb{Q})$ on $E[p^n]$, and

$$(\rho_n^E)^\vee\colon \mathrm{Gal}(K_n^E/\mathbb{Q})^{\mathrm{op}} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]^\vee) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \tag{1.1}$$

be the right action of $\mathrm{Gal}(K_n^E/\mathbb{Q})$ on the Pontrjagin dual

$$E[p^n]^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(E[p^n], \mathbb{Z}/p^n\mathbb{Z})$$

of $E[p^n]$. We define an R_n-module A_n^E by

$$A_n^E := (M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee) \otimes_{\mathbb{Z}[\mathrm{Gal}(K_n^E/K_n)]} \mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]), \tag{1.2}$$

where $(M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee)$ denotes the matrix algebra $M_2(\mathbb{Z}/p^n\mathbb{Z})$ of degree two over $\mathbb{Z}/p^n\mathbb{Z}$ equipped with the right action of $\mathrm{Gal}(K_n^E/\mathbb{Q})$ (for the precise definition, see (6.28) in Section 6). We denote by

$$(A_n^E)^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(A_n^E, \mathbb{Z}/p^n\mathbb{Z})$$

the Pontrjagin dual of A_n^E. The following theorem is the main result of our paper.

Theorem 1.1 (Theorem 6.16)**.** *Let E be an elliptic curve over $\mathbb{Q}$, and p an odd prime number where E has good reduction. Suppose that E satisfies the following conditions* (C1)*,* (C2) *and* (C3)*.*

(C1) *The Galois representation*

$$\rho_1^E \colon G_{K_\infty} := \mathrm{Gal}(\overline{\mathbb{Q}}/K_\infty) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

is absolutely irreducible over $\mathbb{F}_p$.

(C2) *For any $n \in \mathbb{Z}_{\geq 1}$ and any place v of K_n where the base change $E_{K_{n,v}}$ of E has potentially multiplicative reduction, we have $E(K_{n,v})[p] = 0$.*

(C3) *If E has complex multiplication, the ring* $\mathrm{End}(E)$ *of endomorphisms of E defined over $\overline{\mathbb{Q}}$ is the* maximal *order of an imaginary quadratic field.*

Then, there exists a family of R_n-homomorphisms

$$r_n : \mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \longrightarrow (A_n^E)^\vee$$

such that the kernel $\mathrm{Ker}(r_n)$ *and the cokernel* $\mathrm{Coker}(r_n)$ *are finite with order bounded independently of n.*

Remark 1.2. As we see Proposition 4.1 below, the condition (C1) is satisfied if the following condition $(\mathrm{C1})_{\mathrm{str}}$ holds:

$(\mathrm{C1})_{\mathrm{str}}$ The Galois representation

$$\rho^E = \rho^{E,p} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

is surjective.

Note that if E does not have complex multiplication, then the map ρ^E is surjective for all but finitely many prime number p by Serre's open image theorem ([22, 4.4, Théorème 3], [23, p. IV-11]).

Remark 1.3. In Section 4, we show that for any elliptic curve E over $\mathbb{Q}$, there exists a quadratic twist $E'/\mathbb{Q}$ of E which satisfies the condition (C2) (Proposition 4.2).

Remark 1.4. If the condition (C1) for E is satisfied, then the ring homomorphism $\mathbb{Z}_p[G_{K_\infty}] \to M_2(\mathbb{F}_p)$ induced by $\rho_1^E = (\rho^E \bmod p)$ is surjective, where $M_2(\mathbb{F}_p)$ is the matrix algebra of degree two over $\mathbb{F}_p$. Hence, with the aid of Nakayama's lemma for finitely generated $\mathbb{Z}_p$-modules, the condition (C1) for E implies that the homomorphism

$$(\rho_n^E)^\vee \colon \mathbb{Z}_p[G_{K_n}^{\mathrm{op}}] \longrightarrow M_2(\mathbb{Z}/p^n\mathbb{Z})$$

of $\mathbb{Z}_p$-algebras induced by (1.1) is surjective. Under the assumption of (C1), we can regard A_n^E as a quotient of $\mathrm{Cl}(\mathcal{O}_{K_n^E})$.

Remark 1.5. For each $n \in \mathbb{Z}_{\geq 1}$, we define an R_n-module

$$S_n := \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_n^E/K_n)]}(\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) \otimes_{\mathbb{Z}} \mathbb{Z}_p, E[p^n]).$$

In Section 6, we prove Theorem 1.1 by constructing $\mathrm{Gal}(K_n/\mathbb{Q})$-homomorphisms

$$\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \longrightarrow S_n^{\oplus 2} \xleftarrow{\simeq} (A_n^E)^\vee,$$

where the orders of the kernel and the cokernel of the former map are bounded and the latter is an isomorphism.

Remark 1.6. In [16], under certain assumptions on (E,p), Prasad and Shekhar studied a relation between $\mathrm{Sel}_p(\mathbb{Q}, E[p])$ and

$$\widetilde{S} := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Cl}(\mathcal{O}_{K_1^E}) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p]).$$

Here, we give a remark on a relation between $\widetilde{S}$ and our A_1^E. Let $\mathbf{1} \in \widehat{\Delta}$ be the trivial character. Note that $S_{1,\mathbf{1}}$ in the sense of Remark 1.5 is an $\mathbb{F}_p$-subspace of $\widetilde{S}$. Moreover, if $E(\mathbb{Q}_p)[p] = \{0\}$, then the natural injection $S_{1,\mathbf{1}} \hookrightarrow \widetilde{S}$ becomes an isomorphism. Indeed, in such case, for any $f \in \widetilde{S}$ and any prime ideal $\mathfrak{p}$ of K_1^E, it follows from the comparison of the action of the decomposition group at $\mathfrak{p}$ in $\mathrm{Gal}(K_1^E/\mathbb{Q})$ that we have $f([\mathfrak{p}] \otimes 1) = 0$. Hence by Remark 1.5, we deduce that if $E(\mathbb{Q}_p)[p] = \{0\}$, then we have $A_{1,\mathbf{1}}^E \simeq \widetilde{S}^{\oplus 2}$.

Here, we shall note that Theorem 1.1 gives a description of the asymptotic behavior of the higher Fitting ideals of the $\mathbb{Z}_p$-modules A_n^E. Let M be a finitely generated $\mathbb{Z}_p$-module. For each $i \in \mathbb{Z}_{\geq 0}$, we denote by $\mathrm{Fitt}_{\mathbb{Z}_p,i}(M)$ the i-th Fitting ideal of M (cf. Definition 2.1), and put

$$\Phi_i(M) := \mathrm{ord}_p(\mathrm{Fitt}_{\mathbb{Z}_p,i}(M)) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

The sequence $\{\Phi_i(M)\}_{i\geq 0}$ determines the isomorphism class of the $\mathbb{Z}_p$-module M (see Remark 2.4). There is an equality $\Phi_i(A^E_{n,\chi}) = \Phi_i((A^E_{n,\chi^{-1}})^\vee)$ for any $\chi \in \widehat{\Delta}$ because $A^E_{n,\chi}$ is non-canonically isomorphic to

$$(A^E_{n,\chi^{-1}})^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(A^E_{n,\chi^{-1}}, \mathbb{Z}/p^n\mathbb{Z})$$

as a $\mathbb{Z}_p$-module. Similarly, we have $\Phi_i(A^E_n) = \Phi_i((A^E_n)^\vee)$.

Let $\{a_n\}_n$ and $\{b_n\}_n$ be sequences of real numbers. we write $a_n \succ b_n$ if it holds that $\liminf_{n\to\infty}(a_n - b_n) > -\infty$, namely, if the sequence $\{a_n - b_n\}_n$ is bounded below. If $a_n \succ b_n$ and $b_n \succ a_n$, then we write $a_n \sim b_n$. For a family of homomorphisms $f_n \colon M_n \to M'_n$ of finitely generated torsion $\mathbb{Z}_p$-modules if the order of $\mathrm{Ker}(f_n)$ and that of $\mathrm{Coker}(f_n)$ are bounded independently of n, then we have $\Phi_i(M_n) \sim \Phi_i(M'_n)$ for any $i \in \mathbb{Z}_{\geq 0}$ (Lemma 2.8). Theorem 1.1 implies the following corollary:

Corollary 1.7. *Let E be an elliptic curve over $\mathbb{Q}$, and p an odd prime number where E has good reduction. Suppose that E satisfies the conditions* (C1)*,* (C2) *and* (C3)*. Then, for any $i \in \mathbb{Z}_{\geq 0}$ and $\chi \in \widehat{\Delta}$, it holds*

$$\Phi_i(A^E_{n,\chi}) = \Phi_i((A^E_{n,\chi^{-1}})^\vee) \sim \Phi_i\left(\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2}_{\chi^{-1}}\right),$$

and moreover, we have $\Phi_i(A^E_n) = \Phi_i((A^E_n)^\vee) \sim \Phi_i\left(\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2}\right)$.

1.2. Asymptotic formulas as Iwasawa's class number formula. For each $\chi \in \widehat{\Delta}$, we put $h^E_{n,\chi} := \mathrm{ord}_p(\# A^E_{n,\chi})$, and $h^E_n := \mathrm{ord}_p(\# A^E_n) = \sum_{\chi\in\widehat{\Delta}} h^E_{n,\chi}$. Since A^E_n is a quotient of $\mathrm{Cl}(\mathcal{O}_{K^E_n})$ as noted in Remark 1.4, we have

$$h_n := \mathrm{ord}_p(\#\,\mathrm{Cl}(\mathcal{O}_{K^E_n}) \otimes \mathbb{Z}_p) \geq h^E_n.$$

As we shall see below, Corollary 1.7 for $i = 0$ gives a description of asymptotic behavior of h^E_n like "Iwasawa's class number formula". Let us introduce Iwasawa theoretic notation. We put $\Gamma := \mathcal{G}_{\infty,1} = \mathrm{Gal}(K_\infty/K_1)$. There is a non-canonical isomorphism $\Gamma \simeq \mathbb{Z}_p$ and fix a topological generator $\gamma \in \Gamma$. We set $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$. There exists an isomorphism $\Lambda \xrightarrow{\simeq} \mathbb{Z}_p[\![T]\!]$ of $\mathbb{Z}_p$-algebras sending γ to $1+T$. For each $m, n \in \mathbb{Z}_{>0}$, we define

$$\Lambda_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,1}] \simeq \Lambda/(p^n, \gamma^{p^{m-1}} - 1),$$

and put $\Lambda_n := \Lambda_{n,n}$. Since we have $\mathcal{G}_{m,0} = \Delta \times \mathcal{G}_{m,1}$, the equality $R_{m,n} = \Lambda_{m,n}[\Delta]$ holds. In the following, we introduce the Iwasawa module of the Pontrjagin dual of the fine Selmer groups. Write

$$\mathrm{Sel}_p(K_\infty, E[p^\infty]) := \varinjlim_m \mathrm{Sel}_p(K_m, E[p^\infty]).$$

For any $m, n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, define

$$X_{m,n} := \mathrm{Sel}_p(K_m, E[p^n])^\vee := \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathrm{Sel}_p(K_m, E[p^n]), \mathbb{Q}_p/\mathbb{Z}_p\right),$$

and put $X_n := X_{n,n}$. It is known that the Λ-module X_∞ is finitely generated and torsion ([9]). Take any $\chi \in \widehat{\Delta}$. The control theorem of the fine Selmer groups (Corollary 5.10) implies that

$$\Phi_0(X_{\infty,\chi} \otimes_\Lambda \Lambda_n) \sim \Phi_0(X_{n,\chi}) \sim \Phi_0\left(\mathrm{Sel}_p(K_n, E[p^n])_{\chi^{-1}}\right). \tag{1.3}$$

Since $X_{\infty,\chi}$ is a finitely generated torsion Λ-module, we can define Iwasawa's μ and λ-invariants $\mu(X_{\infty,\chi})$ and $\lambda(X_{\infty,\chi})$ of the Λ-module $X_{\infty,\chi}$ (for the definitions see Section 3). By Proposition 3.2 proved later, we have

$$\Phi_0(X_{\infty,\chi} \otimes_\Lambda \Lambda_n) \sim \mu(X_{\infty,\chi})p^{n-1} + \lambda(X_{\infty,\chi})n. \tag{1.4}$$

The invariants Φ_0, μ and λ satisfy the additivity property (cf. (2.4) in Section 2). Corollary 1.7 for $i = 0$ and the equations (1.3), (1.4) imply the following.

Corollary 1.8. *Let E be an elliptic curve over $\mathbb{Q}$, and p an odd prime number where E has good reduction. Suppose that E satisfies the conditions* (C1)*,* (C2) *and* (C3)*. Then, for any $\chi \in \widehat{\Delta}$, we have*

$$h^E_{n,\chi} \sim 2\left(\mu(X_{\infty,\chi})p^{n-1} + \lambda(X_{\infty,\chi})n\right),$$

and moreover, $h^E_n \sim 2\left(\mu(X_\infty)p^{n-1} + \lambda(X_\infty)n\right)$.

As we note below, by assuming the Iwasawa main conjecture for elliptic curves, the constants $\mu(X_\infty)$ and $\lambda(X_\infty)$ are described in terms of Kato's Euler systems. Let us recall the Iwasawa main conjecture (in the formulation using Kato's Euler systems). By using Euler systems of Beilinson–Kato elements, Kato constructed a Λ-submodule Z of $\mathbf{H}^1$, where we set

$$\mathbf{H}^q = \mathbf{H}^q(T_p(E)) := \varprojlim_m H^q(K_m, T_p(E))$$

for each $q \in \mathbb{Z}_{\geq 0}$ (or the construction of Z, see [9, Theorem 12.6] for the Galois representation $T = T_p(E) \subseteq V_{\mathbb{Q}_p}(f_E)$, where f_E is the cuspform attached to E). The Iwasawa main conjecture for (f_E, p, χ) with $\chi \in \widehat{\Delta}$ in the sense of [9, Conjecture 12.10] (combined with [9, Theorem 12.6]) predicts the equality

$$\mathrm{char}_\Lambda(\mathbf{H}^2_\chi) = \mathrm{char}_\Lambda(\mathbf{H}^1_\chi/Z_\chi). \tag{1.5}$$

Since E has good reduction at p, for the left hand side of (1.5), we have $\mathrm{char}_\Lambda(X_{\infty,\chi}) = \mathrm{char}_\Lambda(\mathbf{H}^2_\chi)$ because of the following:

- By the limit of the Poitou–Tate exact sequence, our X_∞ coincides with

$$\mathbf{H}^2(T_p(E))_0 := \mathrm{Ker}\left(\mathbf{H}^2 \longrightarrow \mathbf{H}^2_{\mathrm{loc}} := \varprojlim_m H^2(\mathbb{Q}_p(\mu_{p^m}), T_p(E))\right)$$

  (see, for instance, the proof of [15, Proposition 3.17]).

- When E has good reduction at p, the local duality of the Galois cohomology and Imai's result [7] imply that the order of $\mathbf{H}^2_{\mathrm{loc}}$ is finite, and hence the index of $\mathbf{H}^2(T_p(E))_0$ in $\mathbf{H}^2(T_p(E))$ is finite.

By using the Euler systems, Kato proved that the half side of (1.5), that is, the inclusion

$$\mathrm{char}_\Lambda(\mathbf{H}^2_{0,\chi}) \supseteq \mathrm{char}_\Lambda(\mathbf{H}^1_\chi/Z_\chi)$$

holds for any $\chi \in \widehat{\Delta}$ under the following condition which is satisfied when $(\mathrm{C1})_{\mathrm{str}}$ holds:

The image of the Galois representation

$$\rho^E|_{G_{K_\infty}} : G_{K_\infty} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

contains $SL_2(\mathbb{Z}_p)$

(See [9, Theorem 13.4]. Note that $(\mathrm{C1})_{\mathrm{str}}$ implies the assumption (3) in [9, Theorem 13.4]). By summarizing all χ-parts, the following corollary follows from Corollary 1.8.

Corollary 1.9. *Let E be an elliptic curve over $\mathbb{Q}$, and p an odd prime number where E has good reduction.*

(1) *Suppose that E satisfies the conditions* $(\mathrm{C1})_{\mathrm{str}}$ *and* (C2)*. Then, we have*

$$h_n^E \prec 2\left(\mu(\mathbf{H}^1/Z)p^{n-1} + \lambda(\mathbf{H}^1/Z)n\right).$$

(2) *Suppose that E satisfies the conditions* (C1), (C2) *and* (C3)*. Let $\chi_0 \in \widehat{\Delta}$. Then, if the Iwasawa main conjecture for (f_E, p, χ_0) holds, we have*

$$h_{n,\chi_0}^E \sim 2\left(\mu(\mathbf{H}^1_{\chi_0}/Z_{\chi_0})p^{n-1} + \lambda(\mathbf{H}^1_{\chi_0}/Z_{\chi_0})n\right).$$

In particular, if the Iwasawa main conjecture for (f_E, p, χ) holds for every $\chi \in \widehat{\Delta}$, then we have

$$h_n^E \sim 2\left(\mu(\mathbf{H}^1/Z)p^{n-1} + \lambda(\mathbf{H}^1/Z)n\right).$$

Let $\mathbf{1} \in \widehat{\Delta}$ be the trivial character. In [26], Skinner and Urban proved the Iwasawa main conjecture for $(f_E, p, \mathbf{1})$ with the following conditions (see [26, Theorem 3.33]):

- The pair (E, p) satisfies $(\mathrm{C1})_{\mathrm{str}}$.
- The elliptic curve E has good ordinary reduction at p.
- There exists a prime number ℓ_0 where E has multiplicative reduction.

These conditions are satisfied when E is semistable, and p is a prime number of good ordinary reduction satisfying $p \geq 11$ (see [26, Theorem 3.34]). We obtain the following corollary.

Corollary 1.10. *Suppose that E is semistable, and let p be a prime number with $p \geq 11$ where E has good ordinary reduction. If E satisfies the condition* (C2)*, then we have*

$$h^E_{n,\mathbf{1}} \sim 2\left(\mu(\mathbf{H}^1_{\mathbf{1}}/Z_{\mathbf{1}})p^{n-1} + \lambda(\mathbf{H}^1_{\mathbf{1}}/Z_{\mathbf{1}})n\right).$$

Let us see the relation between our results and previous works on the asymptotic behavior of h_n. By the arguments in [14, Section 4.1], for any number field L, we have

$$\operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_p(L, E[p^\infty]) \geq \operatorname{rank}_{\mathbb{Z}} E(L) - [L : \mathbb{Q}].$$

(Indeed, the fine Selmer group $\operatorname{Sel}_p(L, E[p^\infty])$ contains the kernel of

$$E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(L \otimes_{\mathbb{Q}} \mathbb{Q}_p) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = \prod_{v|p} E(L_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,$$

and we have $\operatorname{corank}_{\mathbb{Z}_p}\left(\prod_{v|p} E(L_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\right) = \sum_{v|p}[L_v : \mathbb{Q}_p] = [L : \mathbb{Q}]$.) By the control theorem of fine Selmer groups (Corollary 5.10 and Remark 5.11), we deduce that

$$\lambda(X_\infty) \geq \operatorname{rank}_{\mathbb{Z}} E(K_m) - \varphi(p^m)$$

for any $m \in \mathbb{Z}_{\geq 0}$, where φ denotes Euler's totient function. Thus, Corollary 1.8 implies the following.

Corollary 1.11. *Let E be an elliptic curve over $\mathbb{Q}$ which has good reduction at an odd prime p. Suppose that E satisfies the conditions* (C1)*,* (C2) *and* (C3)*. Then, for any fixed $m \in \mathbb{Z}_{\geq 0}$, we have*

$$h_n \geq h^E_n \succ 2(r_m - \varphi(p^m))n$$

as $n \to \infty$, where we put $r_m := \operatorname{rank}_{\mathbb{Z}} E(K_m)$.

Remark 1.12. The assertion of Corollary 1.11 for $m = 0$ implies the "asymptotic parts" of the results by [6, 18, 19], and that for general $m \geq 0$ implies [14] for the p-adic representation $T_p(E) = \varprojlim_n E[p^n]$ of G_{K_m}. (Here, the "asymptotic parts" means the assertions without description of constant error factors.) Our results, in particular Theorem 1.1 and Corollary 1.8, can be regarded as a refinement of them in the following senses.

- Corollary 1.8 determines the quotient A^E_n of the ideal class group $\mathrm{Cl}(\mathcal{O}_{K^E_n})$, whose growth is described by the fine Selmer groups.
- Theorem 1.1 describes not only the asymptotic behavior of the order of A^E_n but also asymptotic behavior of the R_n-module (and in particular, $\mathbb{Z}_p$-module) structure.

Example 1.13. Let E be the elliptic curve over $\mathbb{Q}$ of the LMFDB label 5077.a1 (the Cremona label 5077a1), which is defined by the equation

$$y^2 + y = x^3 - 7x + 6,$$

and set $p := 7$. It is known the following ([11]):

(i) The elliptic curve E does not have CM, and (E, p) satisfies $(\mathrm{C1})_{\mathrm{str}}$.
(ii) The conductor of E is 5077, which is a prime number, and E has non-split multiplicative reduction at 5077.
(iii) The rank of $E(\mathbb{Q})$ is 3.
(iv) Let $\widetilde{X} := \mathrm{Sel}(\mathbb{Q}_\infty, E[7^\infty])^\vee$ be the Iwasawa module of the Pontrjagin dual of the classical Selmer group of E over the cyclotomic $\mathbb{Z}_7$-extension field $\mathbb{Q}_\infty$ of $\mathbb{Q}$. We have $\mu(\widetilde{X}) = 0$, and $\lambda(\widetilde{X}) = 3$.

The properties (iii) and (iv) imply that we have $\mathrm{char}_\Lambda(\widetilde{X}) = (\gamma - 1)^3\Lambda$. We further obtain $\mathrm{char}_\Lambda(X_{\infty,\mathbf{1}}) = (\gamma-1)^2\Lambda$ (see, for instance, [30, Proposition VI.10]). This implies that $\mu(X_{\infty,\mathbf{1}}) = 0$ and $\lambda(X_{\infty,\mathbf{1}}) = 2$. Moreover, we can show that the pair (E, p) satisfies the condition (C2) (see Example 4.7 in Section 4.3). Therefore, we obtain

$$h^E_{n,\mathbf{1}} \sim 2n.$$

Notation. Let L/F be a Galois extension with $G = \mathrm{Gal}(L/F)$, and M a topological abelian group equipped with a $\mathbb{Z}$-linear action of G. For each $i \in \mathbb{Z}_{\geq 0}$, we denote by $H^i(L/F, M) = H^i_{\mathrm{cont}}(G, M)$ the i-th continuous Galois cohomology group. If L is a separable closure of F, then we write $H^i(F, M) = H^i(L/F, M)$. When F is a non-archmedean local field, we denote by F^{ur} the maximal unramified extension of F. We define $H^1_{\mathrm{ur}}(F, M) = \mathrm{Ker}(H^1(F, M) \to H^1(F^{\mathrm{ur}}, M))$ (cf. [17, Definition 1.3.1]).

For a $\mathbb{Z}_p$-module A, let A_{div} denote its maximal divisible subgroup. For an abelian group M and an endomorphism f of M, we put $M[f] := \mathrm{Ker}(f)$. In particular, if M is a module over a ring R, then, for each $a \in R$, we set $M[a] := \{x \in M | ax = 0\}$. For an elliptic curve E over a field K and a field extension L/K, we will denote by $E_L := E \otimes_K L$ the base change to L.

Acknowledgments. The authors thank to the referee for careful reading, and many valuable suggestions to improve our manuscript.

2. The higher Fitting ideals

Definition 2.1 (cf. [4, Section 20.2])**.** Let R be a commutative ring, and M a finitely presented R-module given by a presentation

$$R^m \xrightarrow{A} R^n \longrightarrow M \longrightarrow 0 \tag{2.1}$$

with $m \geq n$. We define *the i-th Fitting ideal* $\mathrm{Fitt}_{R,i}(M)$ of the R-module M to be the ideal of R generated by $(n-i) \times (n-i)$ minors (that is, the determinants of the submatrices) of the matrix A. When $i \geq n$, we define $\mathrm{Fitt}_{R,i}(M) := R$.

Remark 2.2. The ideal $\mathrm{Fitt}_{R,i}(M)$ in Definition 2.1 does not depend on the choice of the presentation (2.1) ([4, Corollary-Definition 20.4]).

Remark 2.3. The higher Fitting ideals are compatible with base change in the following sense: Let R be a commutative ring, and M a finitely presented R-module. Then, for any R-algebra S and any $i \in \mathbb{Z}_{\geq 0}$, we have $\mathrm{Fitt}_{S,i}(S \otimes_R M) = \mathrm{Fitt}_{R,i}(M)S$ ([4, Corollary 20.5]).

Remark 2.4. Let R be a PID, and suppose that M is a finitely generated R-module. By the structure theorem of finitely generated modules over a PID, the R-module M is isomorphic to an elementary R-module $R^{\oplus r} \oplus \bigoplus_{j=1}^{s} R/d_jR$ with a sequence $\{d_j\}_j \subseteq R \smallsetminus R^{\times}$ satisfying $d_j \mid d_{j-1}$ for every j. We have

$$\mathrm{Fitt}_{R,i}(M) = \begin{cases} \{0\} & \text{if } i < r, \\ \left(\prod_{j=i-r+1}^{s} d_j\right) R & \text{if } r \leq i < s + r, \\ R & \text{if } i \geq s + r. \end{cases} \tag{2.2}$$

In particular, the higher Fitting ideals $\{\mathrm{Fitt}_{R,i}(M)\}_i$ determine the isomorphism class of the R-module M.

Remark 2.5. Let R be a commutative ring, and M an R-module with the presentation (2.1). Let N be an R-submodule of M.

(1) For any $i \in \mathbb{Z}_{\geq 0}$, we have $\mathrm{Fitt}_{R,i}(M) \subseteq \mathrm{Fitt}_{R,i}(M/N)$. Indeed, we have a presentation of M/N of the form $R^{m+k} \xrightarrow{(A|B)} R^n \to M/N \to 0$ whose relation matrix is the augmented matrix $(A \mid B)$ of A and some $n \times k$ matrix B with some k. Every $(n-i) \times (n-i)$ minor of A becomes an $(n-i) \times (n-i)$ minor of $(A \mid B)$.

(2) Suppose that $R = \mathbb{Z}_p$, and M is a torsion $\mathbb{Z}_p$-module. For any finitely generated torsion $\mathbb{Z}_p$-module L, we denote by $L^{\vee} = \mathrm{Hom}_{\mathbb{Z}_p}(L, \mathbb{Q}_p/\mathbb{Z}_p)$ the Pontrjagin dual of L. The dual $N^{\vee}$ is a quotient of $M^{\vee}$, and there are non-canonical isomorphisms $M \simeq M^{\vee}$ and $N \simeq N^{\vee}$. By (1), we have
$$\mathrm{Fitt}_{R,i}(M) = \mathrm{Fitt}_{R,i}(M^{\vee}) \subseteq \mathrm{Fitt}_{R,i}(N^{\vee}) = \mathrm{Fitt}_{R,i}(N)$$
for any $i \in \mathbb{Z}_{\geq 0}$.

As in Section 1, we introduce the following notation:

Definition 2.6. Let M be a finitely generated torsion $\mathbb{Z}_p$-module. For each $i \in \mathbb{Z}_{\geq 0}$, we define

$$\Phi_i(M) = \mathrm{ord}_p(\mathrm{Fitt}_{\mathbb{Z}_p,i}(M)) := \min\{m \in \mathbb{Z}_{\geq 0} \mid p^m \in \mathrm{Fitt}_{\mathbb{Z}_p,i}(M)\}.$$

If M is a torsion $\mathbb{Z}_p$-module isomorphic to $\bigoplus_{j=1}^{s} \mathbb{Z}_p/p^{e_j}\mathbb{Z}_p$ with a decreasing sequence $\{e_j\}_j \subseteq \mathbb{Z}_{>0}$, then

$$\Phi_i(M) = \begin{cases} \sum_{j=i+1}^{s} e_j & \text{if } 0 \leq i < s, \\ 0 & \text{if } i \geq s, \end{cases} \tag{2.3}$$

immediately follows from (2.2). In particular, we have $\Phi_0(M) = \mathrm{ord}_p(\#M)$. The additivity of Φ_0 holds:

$$\Phi_0(M \oplus N) = \Phi_0(M) + \Phi_0(N) \tag{2.4}$$

for finitely generated torsion $\mathbb{Z}_p$-modules M and N. As noted in Section 1, the isomorphism class of a finitely generated torsion $\mathbb{Z}_p$-module M is determined by $\{\Phi_i(M)\}_i$ by (2.3).

Lemma 2.7. *Let M be a finitely generated torsion $\mathbb{Z}_p$-module. Then, for any $i \in \mathbb{Z}_{\geq 0}$, we have*

$$\Phi_i(M) = \min_{(a_1,\dots,a_i)\in M^i} \mathrm{ord}_p \left(\# \left(M \Big/ \sum_{j=1}^{i} \mathbb{Z}_p a_j \right) \right).$$

Proof. By the structure theorem, we have $M = \bigoplus_{j=1}^{s} (\mathbb{Z}/p^{e_j}\mathbb{Z}) m_j$, where the sequence $\{e_j\} \subseteq \mathbb{Z}_{>0}$ is decreasing. For any $j \in \mathbb{Z}$ with $1 \leq j \leq s$, the annihilator of $m_j \in M$ is $p^{e_j}\mathbb{Z}_p$. Fix any $i \in \mathbb{Z}_{\geq 0}$. If $i = 0$ or $i \geq s$, then the assertion of Lemma 2.7 is clear. Now, we assume $1 \leq i \leq s-1$. Put $N_0 := \sum_{j=1}^{i} \mathbb{Z}_p m_j$. We have

$$\mathrm{ord}_p(\#(M/N_0)) = \mathrm{ord}_p \left(\# \left(\bigoplus_{j=i+1}^{s} (\mathbb{Z}/p^{e_j}\mathbb{Z}) m_j \right) \right) = \sum_{j=i+1}^{s} e_j \overset{(2.3)}{=} \Phi_i(M).$$

Take any $a_1, \dots, a_i \in M$, and put $N := \sum_{j=1}^{i} \mathbb{Z}_p a_j$. In order to prove Lemma 2.7, it suffices to show the following inequality

$$\Phi_i(M) \leq \mathrm{ord}_p(\#(M/N)).$$

Let $\pi_N \colon \mathbb{Z}_p^i \twoheadrightarrow N$ be the surjection given by the generators $a_1, \dots, a_i \in N$, and take a presentation

$$\mathbb{Z}_p^k \xrightarrow{A} \mathbb{Z}_p^i \xrightarrow{\pi_N} N \longrightarrow 0$$

for some $k \geq 1$. By definition, the $\mathbb{Z}_p$-module M is torsion, so is N. We can choose $k = i$. Since M/N is a torsion $\mathbb{Z}_p$-module, there is a square presentation

$$0 \longrightarrow \mathbb{Z}_p^t \xrightarrow{B} \mathbb{Z}_p^t \longrightarrow M/N \longrightarrow 0$$

by the structure theorem. This gives a presentation

$$\mathbb{Z}_p^{i+t} \xrightarrow{C} \mathbb{Z}_p^{i+t} \longrightarrow M \longrightarrow 0$$

with $C = \left(\begin{smallmatrix} A & * \\ O & B \end{smallmatrix}\right)$. We obtain $\#(M/N) = \det B \in \mathrm{Fitt}_{\mathbb{Z}_p,i}(M/N)$. This implies $\#(M/N) \geq \Phi_i(M)$. $\square$

Let $\{a_n\}_n$ and $\{b_n\}_n$ be sequences of real numbers. We write $a_n \succ b_n$ if it holds that $\liminf_{n\to\infty}(a_n - b_n) > -\infty$, namely, if the sequence $\{a_n - b_n\}_n$ is bounded below. If $a_n \succ b_n$ and $b_n \succ a_n$, then we write $a_n \sim b_n$.

Lemma 2.8. *Let $\{M_n\}_{n\geq 0}$ be a sequence of finitely generated torsion $\mathbb{Z}_p$-modules, and suppose that for each $n \in \mathbb{Z}_{\geq 0}$, a $\mathbb{Z}_p$-submodule N_n of M_n is given. Then, the following hold.*

(1) *If $\{(M_n : N_n)\}_{n\geq 0}$ is bounded, then we have $\Phi_i(M_n) \sim \Phi_i(N_n)$ for any $i \in \mathbb{Z}_{\geq 0}$.*

(2) *If $\{\# N_n\}_{n\geq 0}$ is bounded, then we have $\Phi_i(M_n) \sim \Phi_i(M_n/N_n)$ for any $i \in \mathbb{Z}_{\geq 0}$.*

Proof. Let us show the assertion (1). Suppose that there exists some $B \in \mathbb{Z}_{>0}$ such that $(M_n : N_n) \leq p^B$ for any $n \in \mathbb{Z}_{\geq 0}$. Since N_n is a submodule of M_n, by Remark 2.5 (2), we have $\Phi_i(M_n) \geq \Phi_i(N_n)$. In order to prove the assertion (1), it suffices to show that $\Phi_i(M_n) \leq \Phi_i(N_n) + B$. By Lemma 2.7, there exist $a_1, \ldots, a_i \in N_n$ such that

$$\mathrm{ord}_p\left(\#\left(N_n \Big/ \sum_{j=1}^{i} \mathbb{Z}_p a_j\right)\right) = \Phi_i(N_n).$$

Since $(M_n : N_n) \leq p^B$, Lemma 2.7 implies that

$$\Phi_i(M_n) \leq \mathrm{ord}_p\left(\#\left(M_n \Big/ \sum_{j=1}^{i} \mathbb{Z}_p a_j\right)\right) \leq \Phi_i(N_n) + B.$$

Accordingly, we obtain $\Phi_i(M_n) \sim \Phi_i(N_n)$, and the assertion (1) is verified. By taking the Pontrjagin dual, the assertion (2) immediately follows from (1). $\square$

3. Iwasawa's invariants and asymptotic behavior

As in Section 1, for each $n \in \mathbb{Z}_{\geq 0}$, we define $K_n = \mathbb{Q}(\mu_{p^n})$ and $K_\infty = \bigcup_{n\geq 0} K_n$. We put $\Gamma := \mathcal{G}_{\infty,1} = \mathrm{Gal}(K_\infty/K_1)$. There is a non-canonical isomorphism $\Gamma \simeq \mathbb{Z}_p$ and fix a topological generator $\gamma \in \Gamma$. We set $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$. There exists an isomorphism $\Lambda \xrightarrow{\simeq} \mathbb{Z}_p[\![T]\!]$ of $\mathbb{Z}_p$-algebras sending γ to $1 + T$. By this isomorphism, we identify Λ with $\mathbb{Z}_p[\![T]\!]$. For each $m, n \in \mathbb{Z}_{>0}$, we define

$$\Lambda_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,1}] \simeq \Lambda/(p^n, \gamma^{p^{m-1}} - 1),$$

where $\mathcal{G}_{m,1} = \mathrm{Gal}(K_m/K_1)$. Finally, we put $\Lambda_n := \Lambda_{n,n}$. In this section, let us study the asymptotic behavior of $\Phi_0(M \otimes \Lambda_n)$ for any finitely generated Λ-module M from the view point of the structure theorem of finitely generated Λ-module (for instance, see [29, Theorem 13.12]).

First, let us recall the notion of pseudo-isomorphism. Let M and N be finitely generated Λ-modules. We say that a homomorphism $f \colon M \to N$ of Λ-modules is a *pseudo-isomorphism* if both the kernel and the cokernel of f have finite order.

Lemma 3.1. *Let M and N be finitely generated torsion Λ-modules, and $\iota\colon M \to N$ a pseudo-isomorphism of Λ-modules. Then, we have*

$$\Phi_0(M \otimes_\Lambda \Lambda_n) \sim \Phi_0(N \otimes_\Lambda \Lambda_n).$$

Proof. Let $\iota\colon M \to N$ be a pseudo-isomorphism of Λ-modules. Since the map $\iota\colon M \to N$ is the composite of the surjection $\iota\colon M \twoheadrightarrow \operatorname{Im}\iota$ and the inclusion $\operatorname{Im}\iota \hookrightarrow N$, we may consider the cases when ι is surjective, or when ι is injective.

First, suppose that ι is surjective. For any $n \in \mathbb{Z}_{>0}$, we have an exact sequence

$$(\operatorname{Ker}\iota) \otimes_\Lambda \Lambda_n \longrightarrow M \otimes_\Lambda \Lambda_n \xrightarrow{\iota\otimes\Lambda_n} N \otimes_\Lambda \Lambda_n \longrightarrow 0.$$

Since $\iota \otimes \Lambda_n$ is a surjection, and since we have $\#((\operatorname{Ker}\iota) \otimes_\Lambda \Lambda_n) \leq \#(\operatorname{Ker}\iota)$, by Lemma 2.8, we obtain $\Phi_0(M \otimes_\Lambda \Lambda_n) \sim \Phi_0(N \otimes_\Lambda \Lambda_n)$.

Next, suppose that ι is injective. Take any $n \in \mathbb{Z}_{>0}$. We have an exact sequence

$$\operatorname{Tor}_1^\Lambda(\operatorname{Coker}\iota, \Lambda_n) \longrightarrow M \otimes_\Lambda \Lambda_n \xrightarrow{\iota\otimes\Lambda_n} N \otimes_\Lambda \Lambda_n \longrightarrow (\operatorname{Coker}\iota) \otimes_\Lambda \Lambda_n \longrightarrow 0.$$

Clearly, we have $\#\operatorname{Coker}(\iota \otimes \Lambda_n) = \#((\operatorname{Coker}\iota) \otimes_\Lambda \Lambda_n) \leq \#(\operatorname{Coker}\iota)$. Note that $\operatorname{Tor}_1^\Lambda(\operatorname{Coker}\iota, \Lambda_n)$ is a subquotient of $(\operatorname{Coker}\iota)^{\oplus 2}$ because we have a projective resolution

$$0 \longrightarrow \Lambda \xrightarrow{\begin{pmatrix} \gamma^{p^{n-1}}-1 \\ -p^n \end{pmatrix}} \Lambda^{\oplus 2} \xrightarrow{\begin{pmatrix} p^n & \gamma^{p^{n-1}}-1 \end{pmatrix}} \Lambda \longrightarrow \Lambda_n = \Lambda/(p^n, \gamma^{p^{n-1}} - 1)$$

of the Λ-module Λ_n. Consequently, we obtain $\#\operatorname{Ker}(\iota \otimes \Lambda_n) \leq \#(\operatorname{Coker}\iota)^2$. By Lemma 2.8, we deduce that $\Phi_0(M \otimes_\Lambda \Lambda_n) \sim \Phi_0(N \otimes_\Lambda \Lambda_n)$. $\square$

Let M be a finitely generated torsion Λ-module. By the structure theorem (cf. [29, Theorem 13.12]), there exists a pseudo-isomorphism

$$M \longrightarrow \left(\bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda\right) \tag{3.1}$$

of Λ-modules for some $s, t \in \mathbb{Z}_{\geq 0}$, some $n_1, \dots, n_s, m_1, \dots, m_t \in \mathbb{Z}_{>0}$ and some distinguished polynomials $f_1(T), \dots, f_t(T) \in \mathbb{Z}_p[T]$ which are irreducible over $\mathbb{Q}_p$. (Recall that a non-constant polynomial $f(T) \in \mathbb{Z}_p[T]$ is said to be *distinguished* if $f(T)$ is a monic polynomial satisfying $f(T) \equiv T^{\deg f(T)} \bmod p\mathbb{Z}_p[T]$.) The *characteristic ideal* $\operatorname{char}_\Lambda(M)$ of the Λ-module M is the principal ideal of Λ generated by

$$p^{\sum_{i=1}^{s} n_i} \prod_{j=1}^{t} f_j(T)^{m_j}.$$

We define the *Iwasawa μ-invariant* $\mu(M)$ by $\mu(M) := \sum_{i=1}^{s} n_i$, and the *Iwasawa λ-invariant* $\lambda(M)$ by $\lambda(M) := \sum_{j=1}^{t} m_j \deg f_j(T)$. Note that

$\mathrm{char}_\Lambda(M)$, $\mu(M)$ and $\lambda(M)$ are independent of the choice of the pseudo-isomorphism (3.1).

Proposition 3.2. *For any finitely generated torsion Λ-module M, we have*

$$\Phi_0(M \otimes_\Lambda \Lambda_n) \sim \mu(M)p^{n-1} + \lambda(M)n. \tag{3.2}$$

Proof. By the structure theorem, Lemma 3.1 and the additivity of Φ_0 (cf. (2.4)), we reduce the proof into the following three cases:

(i) the case when $M = \Lambda/p^m\Lambda$ for some $m \in \mathbb{Z}_{>0}$,

(ii) the case when $M = \Lambda/g_d(1+T)^m\Lambda$ for some $d, m \in \mathbb{Z}_{>0}$, where $g_d(T) \in \mathbb{Z}_p[T]$ denotes the p^d-th cyclotomic polynomial, or

(iii) the case when $M = \Lambda/f(T)^m\Lambda$ for some $m \in \mathbb{Z}_{>0}$ and for some distinguished polynomial $f(T) \in \mathbb{Z}_p[T]$ irreducible over $\mathbb{Q}_p$ whose roots in $\overline{\mathbb{Q}}_p$ are not of the form $\zeta - 1$ for p-power roots ζ of unity.

Case (i). $M = \Lambda/p^m\Lambda$ for some $m \in \mathbb{Z}_{>0}$. Take any $n \in \mathbb{Z}_{\geq m}$. Then, we have

$$M \otimes_\Lambda \Lambda_n \simeq \Lambda/(p^m, \gamma^{p^{n-1}} - 1) \simeq \mathbb{Z}/p^m\mathbb{Z}[\mathrm{Gal}(K_n/K_1)] = \Lambda_{n,m}.$$

This implies that

$$\Phi_0(M \otimes \Lambda_n) = \Phi_0(\Lambda_{n,m}) = \Phi_0\left((\mathbb{Z}/p^m\mathbb{Z})^{\oplus p^{n-1}}\right) = \mathrm{ord}_p(p^{mp^{n-1}}) = mp^{n-1}.$$

The sequence $\{\Phi_0(M \otimes \Lambda_n) - mp^{n-1}\}_n$ is bounded so that

$$\Phi_0(M) \sim mp^{n-1}.$$

Since we have $\mu(M) = m$ and $\lambda(M) = 0$ in this case, we obtain (3.2).

Case (ii). $M = \Lambda/g_d(1+T)^m\Lambda$ for some $d, m \in \mathbb{Z}_{>0}$, where $g_d(T) \in \mathbb{Z}_p[T]$ denotes the p^d-th cyclotomic polynomial. The cyclotomic polynomial $g_d(T)$ has degree $(p-1)p^{d-1}$. We have $\mu(M) = 0$ and $\lambda(M) = m(p-1)p^{d-1}$. We put $\mathcal{O}_d := \mathbb{Z}_p[\mu_{p^d}]$. Set $\widetilde{\Lambda} := \mathcal{O}_d \otimes_{\mathbb{Z}_p} \Lambda = \mathcal{O}_d[\![T]\!]$, and $\widetilde{\Lambda}_n := \mathcal{O}_d \otimes_{\mathbb{Z}_p} \Lambda_n$. The cyclotomic polynomial $g_d(T)$ is decomposed into $g_d(T) = \prod_{\zeta \in \mu_{p^d}^\times}(T - \zeta)$ in $\widetilde{\Lambda}$, where $\mu_{p^d}^\times$ denotes the set of primitive p^d-th roots of unity in $\overline{\mathbb{Q}}_p$. We have an injective homomorphism

$$\iota\colon \mathcal{O}_d \otimes_{\mathbb{Z}_p} M \simeq \widetilde{\Lambda} \Big/ \left(\prod_{\zeta \in \mu_{p^d}^\times} (T - \zeta + 1)^m\right)\widetilde{\Lambda} \hookrightarrow \prod_{\zeta \in \mu_{p^d}^\times} \widetilde{\Lambda}/(T - \zeta + 1)^m\widetilde{\Lambda}$$

of $\widetilde{\Lambda}$-modules, where the last homomorphism is given by the diagonal mapping. The cokernel of ι has finite order. In particular, the map ι is a pseudo-isomorphism of Λ-modules. Hence, we obtain

$$\Phi_0(M \otimes_{\mathbb{Z}_p} \widetilde{\Lambda}_n) \sim \sum_{\zeta \in \mu_{p^d}^\times} \Phi_0\left(\left(\widetilde{\Lambda}/(T - \zeta + 1)^m\widetilde{\Lambda}\right) \otimes_{\widetilde{\Lambda}} \widetilde{\Lambda}_n\right).$$

Since $\mathcal{O}_d$ is a free $\mathbb{Z}_p$-module of rank $\#\mu_{p^d}^\times = (p-1)p^{d-1}$, we have

$$\Phi_0(\mathcal{O}_d \otimes_{\mathbb{Z}_p} M) = (p-1)p^{d-1}\Phi_0(M).$$

For each $\zeta \in \mu_{p^d}^\times$, put $\widetilde{M}_{n,\zeta} := \big(\widetilde{\Lambda}/(T-\zeta+1)^m\widetilde{\Lambda}\big) \otimes_{\widetilde{\Lambda}} \widetilde{\Lambda}_n$. In order to prove (3.2) for our case, it suffices to show that

$$\Phi_0\big(\widetilde{M}_{n,\zeta}\big) \sim \lambda(M)n = m(p-1)p^{d-1}n. \tag{3.3}$$

Fix any $\zeta \in \mu_{p^d}^\times$. We set $\varpi_d := \zeta - 1$, and $\widetilde{T} := T - \varpi_d = T - \zeta + 1$. Note that we have $\widetilde{\Lambda} = \mathcal{O}_d[\![\widetilde{T}]\!]$. For each $k \in \mathbb{Z}_{\geq 0}$, we define the ideal I_k of $\widetilde{\Lambda}$ by

$$I_k := \Big(\widetilde{T}^{p^k}, \varpi_d^{p^k}, p\widetilde{T}^{p^{k-1}}, p\varpi_d^{p^{k-1}}, p^2\widetilde{T}^{p^{k-2}}, p^2\varpi_d^{p^{k-2}}, \dots, p^k\widetilde{T}, p^k\varpi_d\Big)_{\widetilde{\Lambda}}.$$

By definition, we have $I_k = \widetilde{T}^{p^k}\widetilde{\Lambda} + \varpi_d^{p^k}\widetilde{\Lambda} + pI_{k-1}$.

Claim 1. *For any $k \in \mathbb{Z}_{\geq 0}$, we have*

$$(1+T)^{p^k} - 1 \in I_k. \tag{3.4}$$

Proof of Claim 1. For any $k \in \mathbb{Z}_{>0}$ and any $h(\widetilde{T}) \in I_{k-1}$, we have $ph(\widetilde{T}) \in I_k$. For any $f_1(\widetilde{T}), f_2(\widetilde{T}) \in \widetilde{\Lambda}$, it holds that

$$\begin{aligned}
&\Big(1 + f_1(\widetilde{T})\widetilde{T}^{p^k} + f_2(\widetilde{T})\varpi_d^{p^k} + ph(\widetilde{T})\Big)^p \\
&\qquad\qquad \equiv 1 + f_1(\widetilde{T})^p\widetilde{T}^{p^{k+1}} + f_2(\widetilde{T})^p\varpi_d^{p^{k+1}} \bmod pI_k.
\end{aligned}$$

We show the claim by induction on k. For the case $k = 0$, we have $(1+T)-1 = T = \widetilde{T} + \varpi_d$ and this is in $I_0 = (\widetilde{T}, \varpi_d)_{\widetilde{\Lambda}}$. We assume the assertion for $k \geq 0$: $(1+T)^{p^k} - 1 \in I_k$. Thus, there exist $f_1(\widetilde{T}), f_2(\widetilde{T}) \in \widetilde{\Lambda}$ and $h(\widetilde{T}) \in I_{k-1}$ such that $(1+T)^{p^k} - 1 = f_1(\widetilde{T})\widetilde{T}^{p^k} + f_2(\widetilde{T})\varpi_d^{p^k} + ph(\widetilde{T})$. We have

$$\begin{aligned}
(1+T)^{p^{k+1}} - 1 &= \Big(1 + (1+T)^{p^k} - 1\Big)^p - 1 \\
&= \Big(1 + f_1(\widetilde{T})\widetilde{T}^{p^k} + f_2(\widetilde{T})\varpi_d^{p^k} + ph(\widetilde{T})\Big)^p - 1 \\
&\equiv f_1(\widetilde{T})^p\widetilde{T}^{p^{k+1}} + f_2(\widetilde{T})^p\varpi_d^{p^{k+1}} \bmod pI_k.
\end{aligned}$$

This implies the assertion $(1+T)^{p^{k+1}} - 1 \in I_k$. □

Let $N \in \mathbb{Z}_{>0}$ be an integer satisfying that $p^N > \max\{m, (p-1)p^{d-1}\}$. Take any $n \in \mathbb{Z}_{>N}$. Note that as we see below, for $\nu \in \mathbb{Z}$ with $0 \leq \nu \leq n-1$, we have $p^\nu\widetilde{T}^{p^{n-1-\nu}}, p^\nu\varpi_d^{p^{n-1-\nu}} \in \big(\widetilde{T}^m, p^{n-1-N}\big)_{\widetilde{\Lambda}}$:

- When $0 \leq \nu < n-1-N$, we have $\widetilde{T}^{p^{n-1-\nu}} \in \widetilde{T}^{p^N}\widetilde{\Lambda} \subseteq \widetilde{T}^m\widetilde{\Lambda}$, and
  $$p^\nu\varpi^{p^{n-1-\nu}} = p^\nu(\varpi^{p^N})^{p^{n-1-N-\nu}} \in p^{\nu+p^{n-1-N-\nu}}\widetilde{\Lambda} \subseteq p^{n-1-N}\widetilde{\Lambda}.$$

- When $n-1-N \leq \nu \leq n-1$, we clearly have

$$p^{\nu}\widetilde{T}^{p^{n-1-\nu}}, p^{\nu}\varpi_d^{p^{n-1-\nu}} \in p^{n-1-N}\widetilde{\Lambda}.$$

Consequently, it holds that $I_{n-1} \subseteq (\widetilde{T}^m, p^{n-1-N})_{\widetilde{\Lambda}}$. By (3.4) for $k = n-1$, we obtain

$$\left(\widetilde{T}^m, (1+T)^{p^{n-1}} - 1, p^n\right)_{\widetilde{\Lambda}} \subseteq \left(\widetilde{T}^m, p^{n-N-1}\right)_{\widetilde{\Lambda}}. \tag{3.5}$$

Obviously, we also have

$$\left(\widetilde{T}^m, p^{n-1}\right)_{\widetilde{\Lambda}} \subseteq \left(\widetilde{T}^m, (1+T)^{p^{n-1}} - 1, p^n\right)_{\widetilde{\Lambda}}. \tag{3.6}$$

Since we have

$$\widetilde{M}_{n,\zeta} = \left(\widetilde{\Lambda}/(T-\zeta+1)^m\widetilde{\Lambda}\right) \otimes_{\widetilde{\Lambda}} \widetilde{\Lambda}_n \simeq \widetilde{\Lambda}/\left(\widetilde{T}^m, (1+T)^{p^{n-1}} - 1, p^n\right)_{\widetilde{\Lambda}},$$

by (3.5) and (3.6), we obtain

$$\Phi_0\left(\widetilde{\Lambda}/(\widetilde{T}^m, p^{n-1-N})_{\widetilde{\Lambda}}\right) \leq \Phi_0\left(\widetilde{M}_{n,\zeta}\right) \leq \Phi_0\left(\widetilde{\Lambda}/(\widetilde{T}^m, p^{n-1})_{\widetilde{\Lambda}}\right).$$

For any $\nu \in \mathbb{Z}_{>0}$, it holds that

$$\Phi_0\left(\widetilde{\Lambda}/(\widetilde{T}^m, p^{\nu})_{\widetilde{\Lambda}}\right) = \Phi_0\left(\bigoplus_{j=0}^{m-1}(\mathcal{O}_d/p^{\nu}\mathcal{O}_d)T^j\right) = m(p-1)p^{d-1}\nu.$$

So, we obtain

$$m(p-1)p^{d-1}(n-1-N) \leq \Phi_0\left(\widetilde{M}_{n,\zeta}\right) \leq m(p-1)p^{d-1}(n-1).$$

Hence, the sequence $\{\Phi_0(\widetilde{M}_{n,\zeta}) - \lambda(M)n\}_n$ is bounded, and hence (3.3) holds. This completes the proof of (3.2) for the case (ii).

Case (iii). $M = \Lambda/f(T)^m\Lambda$ for some $m \in \mathbb{Z}_{>0}$ and for some distinguished polynomial $f(T) \in \mathbb{Z}_p[T]$ irreducible over $\mathbb{Q}_p$ whose roots in $\overline{\mathbb{Q}}_p$ are not of the form $\zeta - 1$ for p-power roots ζ of unity. Put $d := \deg(f(T))$. Note that in this case, we have $\mu(M) = 0$, and $\lambda(M) = md$. Let $N_1 \in \mathbb{Z}_{\geq 2}$ be an integer satisfying

$$(p-1)p^{N_1-2} > d = \deg(f(T)) \tag{3.7}$$

Take any $n \in \mathbb{Z}_{\geq N_1}$. For each $\nu \in \mathbb{Z}_{>0}$, we put $\mathcal{O}_{\nu} := \mathbb{Z}_p[\mu_{p^{\nu}}]$, and fix $\zeta_{p^{\nu}} \in \mu_{p^{\nu}}$ a primitive p^{ν}-th root of unity. Then, we have an injective homomorphism

$$e_n\colon\ \Lambda/((1+T)^{p^{n-1}} - 1)\Lambda \hookrightarrow \Lambda/((1+T)^{p^{n-2}} - 1)\Lambda \times \mathcal{O}_{n-1}$$

of $\mathbb{Z}_p$-modules which sends $\gamma = 1+T$ to $(\gamma, \zeta_{p^{n-1}})$. We set $Q_n := \mathrm{Coker}(e_n)$. Note that the order of Q_n is finite. We denote $g_{n-1}(T) \in \mathbb{Z}_p[T]$ by the p^{n-1}-th cyclotomic polynomial. Putting $\varpi_{n-1} := \zeta_{p^{n-1}} - 1$, we have

$$\begin{aligned}
Q_n &\simeq \Lambda\Big/\Big((1+T)^{p^{n-2}} - 1\ , g_{n-1}(1+T)\Big) \\
&\simeq \Big(\Lambda/(g_{n-1}(1+T))\Big)\Big/\Big((1+T)^{p^{n-2}} - 1\Big) \\
&\simeq \mathcal{O}_{n-1}\Big/\Big(\zeta_{p^{n-1}}^{p^{n-2}} - 1\Big) \\
&= \mathcal{O}_{n-1}\Bigg/\Bigg(\prod_{\zeta \in \mu_{p^{n-2}}} (\zeta_{p^{n-1}} - \zeta)\Bigg) \\
&\overset{(\star)}{=} \mathcal{O}_{n-1}/(\varpi_{n-1}^{p^{n-2}}).
\end{aligned} \tag{3.8}$$

Here, the last equality $(\star)$ follows from the equalities $(\zeta_{p^{n-1}} - \zeta)\mathcal{O}_{n-1} = (\varpi_{n-1} - (\zeta - 1))\mathcal{O}_{n-1} = \varpi_{n-1}\mathcal{O}_{n-1}$ for each $\zeta \in \mu_{p^{n-2}}$. Let us consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{\Lambda}{((1+T)^{p^{n-1}} - 1)} \arrow[r, "e_n"] \arrow[d, "\times f(T)^m"] & \dfrac{\Lambda}{((1+T)^{p^{n-2}} - 1)} \times \mathcal{O}_{n-1} \arrow[r] \arrow[d, "\times f(T)^m"] & Q_n \arrow[r] \arrow[d, "\times f(T)^m"] & 0 \\
0 \arrow[r] & \dfrac{\Lambda}{((1+T)^{p^{n-1}} - 1)} \arrow[r, "e_n"] & \dfrac{\Lambda}{((1+T)^{p^{n-2}} - 1)} \times \mathcal{O}_{n-1} \arrow[r] & Q_n \arrow[r] & 0.
\end{tikzcd} \tag{3.9}$$

Since $\Lambda = \mathbb{Z}_p[\![T]\!]$ is a UFD, and since $f(T)$ is prime to $(1+T)^{p^{n-1}} - 1$, we have

$$\left(\frac{\Lambda}{((1+T)^{p^{n-1}}-1)}\right)[f(T)^m] = \left(\frac{\Lambda}{((1+T)^{p^{n-2}}-1)} \times \mathcal{O}_{n-1}\right)[f(T)^m] = 0.$$

By applying the snake lemma to the diagram (3.9), we obtain the exact sequence

$$\begin{aligned}
0 \longrightarrow Q_n[f(T)^m] &\overset{\delta}{\longrightarrow} \frac{\Lambda}{((1+T)^{p^{n-1}} - 1, f(T)^m)} \\
&\longrightarrow \frac{\Lambda}{((1+T)^{p^{n-2}} - 1, f(T)^m)} \times \frac{\mathcal{O}_{n-1}}{(f(\varpi_{n-1})^m)} \longrightarrow \frac{Q_n}{f(T)^m Q_n} \longrightarrow 0.
\end{aligned} \tag{3.10}$$

Since the order of Q_n is finite, it holds that

$$\Phi_0(Q_n[f(T)^m]) = \Phi_0(Q_n/f(T)^m Q_n).$$

We put $M_k := \Lambda\big/\left((1+T)^{p^k}-1, f(T)^m\right)$ for each $k \in \mathbb{Z}_{>0}$. By (3.10), we obtain a recurrence formula:

$$\Phi_0\left(M_{n-1}\right) = \Phi_0\left(M_{n-2}\right) + \Phi_0\left(\mathcal{O}_{n-1}/(f(\varpi_{n-1})^m)\right).$$

The distinguished polynomial

$$f(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_0$$

satisfies $p \mid a_i$ and hence $a_i \in p\mathcal{O}_{n-1} = \varpi_{n-1}^{(p-1)p^{n-2}}\mathcal{O}_{n-1}$ for $0 \le i \le d-1$. By (3.7) combined with $n \ge N_1$, we have $\varpi_{n-1}^{(p-1)p^{n-2}}\mathcal{O}_{n-1} \subsetneq \varpi_{n-1}^{d}\mathcal{O}_{n-1}$. It holds that $f(\varpi_{n-1})\mathcal{O}_{n-1} = \varpi_{n-1}^{d}\mathcal{O}_{n-1}$, and hence

$$\Phi_0\left(\mathcal{O}_{n-1}/(f(\varpi_{n-1})^m)\right) = md = \lambda(M).$$

Therefore, we obtain

$$\Phi_0\left(M_{n-1}\right) = \Phi_0\left(M_{n-2}\right) + \lambda(M) \tag{3.11}$$

for any $n \ge N_1$. For each $n \in \mathbb{Z}_{>0}$, we have $M \otimes_\Lambda \Lambda_n \simeq M_{n-1}/p^n M_{n-1}$. Let us show the following claim.

Claim 2. *Let $N_2 \in \mathbb{Z}_{>N_1}$ be an integer satisfying $p^{N_2-2} > md$, and $k_{N_2} \in \mathbb{Z}_{\ge 0}$ be the integer satisfying that*

$$\mathrm{Ann}_{\mathcal{O}_1}(M_{N_2} \otimes_{\mathbb{Z}_p} \mathcal{O}_1) = \varpi_1^{k_{N_2}}\mathcal{O}_1,$$

where we put $\varpi_1 := \zeta_p - 1 \in \mathcal{O}_1 = \mathbb{Z}_p[\mu_p]$. Then, for any $n \in \mathbb{Z}_{>2N_2}$, we have

$$\mathrm{Ann}_{\mathcal{O}_1}(M_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1) \supseteq \varpi_1^{k_{N_2}+n-1-N_2}\mathcal{O}_1.$$

Proof of Claim 2. Since $\mathcal{O}_1$ is flat over $\mathbb{Z}_p$, by taking $(\,\cdot\,) \otimes_{\mathbb{Z}_p} \mathcal{O}_1$, the exact sequence (3.10) induces an exact sequence

$$0 \longrightarrow Q_n[f(T)^m] \otimes_{\mathbb{Z}_p} \mathcal{O}_1 \longrightarrow M_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1 \longrightarrow M_{n-2} \otimes_{\mathbb{Z}_p} \mathcal{O}_1 \times \frac{\mathcal{O}_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1}{(\varpi_{n-1}^{md} \otimes 1)}.$$

By (3.8), we have $Q_n \simeq \mathcal{O}_{n-1}/\left(\varpi_{n-1}^{p^{n-2}}\right)$ and thus

$$\begin{aligned} Q_n[f(T)^m] \otimes_{\mathbb{Z}_p} \mathcal{O}_1 &\simeq \left(\mathcal{O}_{n-1}/(\varpi_{n-1}^{md})\right) \otimes_{\mathbb{Z}_p} \mathcal{O}_1 \\ &\simeq \left(\mathcal{O}_{n-1}/\left(\varpi_{n-1}^{md}\right)\right)^{\oplus (p-1)} \end{aligned}$$

For $p^{N_2-2} > md$ and $n > N_2$, the $\mathcal{O}_1$-module $Q_n[f(T)^m] \otimes_{\mathbb{Z}_p} \mathcal{O}_1$ is annihilated by ϖ_1. Hence, we obtain

$$\begin{aligned} \mathrm{Ann}_{\mathcal{O}_1}(M_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1) &\supseteq \mathrm{Ann}_{\mathcal{O}_1}(Q_n[f(T)^m] \otimes_{\mathbb{Z}_p} \mathcal{O}_1) \\ &\qquad \cdot \mathrm{Ann}_{\mathcal{O}_1}\left(M_{n-2} \otimes_{\mathbb{Z}_p} \mathcal{O}_1 \times \frac{\mathcal{O}_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1}{(\varpi_{n-1}^{md} \otimes 1)}\right) \\ &\supseteq \varpi_1 \left(\mathrm{Ann}_{\mathcal{O}_1}(M_{n-2} \otimes_{\mathbb{Z}_p} \mathcal{O}_1) \cap \varpi_1^{md}\mathcal{O}_1\right). \end{aligned}$$

Note that $k_{N_2} + n - 1 - N_2 > md$ for any $n \in \mathbb{Z}_{>2N_2}$. By induction on n, we obtain the assertion of Claim 2. $\square$

Now, let us complete the proof of Proposition 3.2. Take N_2 as in Claim 2, and let $N_3 \in \mathbb{Z}_{>2N_2}$ be an integer satisfying that $(p-1)N_3 > k_{N_2} + N_3 - 1 - N_2$. By Claim 2 above, for any $n \in \mathbb{Z}_{>N_3}$, it holds that

$$\mathrm{Ann}_{\mathcal{O}_1}(M_{n-1} \otimes_{\mathbb{Z}_p} \mathcal{O}_1) \supseteq \varpi_1^{k_{N_2}+n-1-N_2}\mathcal{O}_1 \supseteq \varpi_1^{n-N_3} p^{N_3}\mathcal{O}_1 \supseteq p^n\mathcal{O}_1,$$

and in particular $p^n \in \mathrm{Ann}_{\mathbb{Z}_p}(M_{n-1})$. For any $n \in \mathbb{Z}_{>N_3}$, we have $p^n M_{n-1} = 0$ and this implies that $M \otimes_\Lambda \Lambda_n \simeq M_{n-1}$. By (3.11), we obtain

$$\Phi_0(M \otimes_\Lambda \Lambda_n) = \Phi_0(M_{n-1}) = \Phi_0(M_{N_3-1}) + (n - N_3)\lambda(M)$$

for any $n > N_3$. Thus, the sequence

$$\{\Phi_0(M \otimes_\Lambda \Lambda_n) - n\lambda(M)\}_n$$

is bounded for the case (iii). This completes the proof of (3.2) $\square$

4. The conditions (C1) and (C2)

Until the end of this note, we use the following notation: Fix an *odd* prime number p. Let E be an elliptic curve over $\mathbb{Q}$. We denote by D_E the discriminant of the minimal Weierstrass model for E over $\mathbb{Z}$. We define the p-adic Tate module $T_p(E)$ by $T_p(E) := \varprojlim_n E[p^n]$, and put $V_p(E) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$. As in Section 1, for each $n \in \mathbb{Z}_{\geq 0}$, we define $K_n^E = \mathbb{Q}(E[p^n])$, and $K_n = \mathbb{Q}(\mu_{p^n})$. Put also $K_\infty^E = \bigcup_{n \geq 0} K_n^E$ and $K_\infty = \bigcup_{n\geq 0} K_n$.

In this section, we review some results on the conditions (C1) and (C2) referred in Theorem 1.1 under the additional assumption that E has *good reduction* at p. First, we recall the conditions:

(C1) The restriction

$$\rho_1^E \colon G_{K_\infty} \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

to G_{K_∞} of the mod p Galois representation $\rho_1^E : G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ is absolutely irreducible over $\mathbb{F}_p$.

(C2) For any $n \in \mathbb{Z}_{\geq 1}$ and any place v of K_n with the base change $E_{K_{n,v}}$ of E has potentially multiplicative reduction, we have $E(K_{n,v})[p] = 0$.

4.1. Remarks on (C1) and (C2). In this paragraph, we shall show some properties relating (C1) and (C2) mentioned in Section 1. First, let us verify the following property, which is noted in Remark 1.2.

Proposition 4.1. *The condition* (C1) *is satisfied if the Galois representation*

$$\rho^E \colon G_\mathbb{Q} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

is surjective.

Proof. It is enough to show that the image of $\rho_1^E\colon G_{K_\infty} \to \mathrm{GL}_2(\mathbb{F}_p)$ generates $\mathrm{End}_{\mathbb{F}_p}(E[p]) \simeq M_2(\mathbb{F}_p)$ over $\mathbb{F}_p$. By using the Weil pairing, the Galois group $G_{\mathbb{Q}}$ acts on $\bigwedge^2_{\mathbb{Z}_p} T_p(E) \simeq T_p(\boldsymbol{\mu})$ via the cyclotomic character χ, where $T_p(\boldsymbol{\mu}) := \varprojlim_n \mu_{p^n}$ (cf. [24, Chapter V, Section 2]). We obtain the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & G_{K_\infty} \arrow[r] \arrow[d] & G_{\mathbb{Q}} \arrow[r] \arrow[d, "\rho^E"] & \mathrm{Gal}(K_\infty/\mathbb{Q}) \arrow[r] \arrow[d, "\chi", "\simeq"'] & 0 \\
0 \arrow[r] & SL_2(\mathbb{Z}_p) \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_p) \arrow[r, "\det"] & \mathbb{Z}_p^\times \arrow[r] & 0.
\end{tikzcd}$$

The assumption implies that the image of the restriction $\rho^E|_{G_{K_\infty}}$ coincides with $SL_2(\mathbb{Z}_p)$. By taking the mod p reduction, $SL_2(\mathbb{F}_p) = \rho_1^E(G_{K_\infty})$ and this generates $M_2(\mathbb{F}_p)$ over $\mathbb{F}_p$. $\square$

Next, let us see the following property referred in Remark 1.3.

Proposition 4.2. *There exists a quadratic twist $E'/\mathbb{Q}$ of E which satisfies the condition* (C2).

Proof. For each prime number ℓ, put $L_\ell := \mathbb{Q}_\ell(\mu_{p^\infty})$. Suppose that E is defined by the Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$, and let $S(E)$ be the set of all the prime numbers at which E has potentially multiplicative reduction. As E has good reduction at p, we have $p \notin S(E)$. For each $\ell \in S(E)$, we fix an embedding $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, and regard μ_{p^∞} as a subgroup of $\overline{\mathbb{Q}}_\ell^\times$. Note that under these notations, the elliptic curve E satisfies the condition (C2) if and only if $E(L_\ell)[p] = 0$ for any $\ell \in S(E)$. In order to show the assertion of Proposition 4.2, we may suppose that E does not satisfy the condition (C2). In particular, the set $S(E)$ is not empty. We define

$$S_0(E) := \{\ell \in S(E) | E(L_\ell)[p] \neq 0,\ 2 \nmid [\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell]\},$$
$$S_1(E) := \{\ell \in S(E) | E(L_\ell)[p] \neq 0,\ 2 \mid [\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell]\}$$

and put $N_1^* := \prod_{\ell' \in S_1(E)} (\ell')^*$, where for each odd prime number ℓ, we write $\ell^* := (-1)^{\frac{\ell-1}{2}}\ell$, and put $2^* := 2$. For each odd $\ell \in S(E) \smallsetminus S_1(E)$, we put

$$\varepsilon_\ell := \prod_{\ell' \in S_1(E)} \left(\frac{(\ell')^*}{\ell}\right),$$

where $\left(\frac{\cdot}{\ell}\right)$ denotes the Legendre symbol modulo ℓ. For each odd prime $\ell \in S(E) \smallsetminus S_1(E)$, take a positive integer $a_\ell < \ell$ such that

$$\left(\frac{a_\ell}{\ell}\right) = \begin{cases} -\varepsilon_\ell & \text{if } \ell \in S_0(E), \\ \varepsilon_\ell & \text{if } \ell \notin S_0(E). \end{cases}$$

Furthermore, take a positive integer $a_8 < 8$ satisfying

$$a_8 N_1^* \equiv \begin{cases} 1 \bmod 8 & \text{if } 2 \in S(E) \smallsetminus (S_0(E) \cup S_1(E)), \\ 5 \bmod 8 & \text{if } 2 \in S_0(E). \end{cases}$$

By the Chinese remainder theorem, there exists a positive integer q_0 such that $q_0 \equiv a_\ell \bmod \ell$ for any odd $\ell \in S_0(E)$ and $q_0 \equiv a_8 \bmod 8$. Dirichlet's theorem on arithmetic progressions say that there exist infinitely many primes q such that

$$q \equiv q_0 \bmod 8 \prod_{\ell \in S(E) \smallsetminus S_1(E),\, \mathrm{odd}} \ell.$$

As a result, there exists an odd prime number q prime to p such that

$$\left(\frac{q}{\ell}\right) = \begin{cases} -\varepsilon_\ell & \text{if } \ell \in S_0(E), \\ \varepsilon_\ell & \text{if } \ell \notin S_0(E), \end{cases} \tag{4.1}$$

for any odd $\ell \in S(E) \smallsetminus S_1(E)$, and

$$q N_1^* \equiv \begin{cases} 1 \bmod 8 & \text{if } 2 \in S(E) \smallsetminus (S_0(E) \cup S_1(E)), \\ 5 \bmod 8 & \text{if } 2 \in S_0(E). \end{cases}$$

In fact, if $2 \notin S_1(E)$ then $N_1^* \equiv 1 \bmod 4$. This satisfies $q \equiv 1 \bmod 4$. Take such a prime number q, and let E' be a quadratic twist of E defined by the Weierstrass equation $qN_1^* y^2 = x^3 + ax + b$. We have an equality $S(E') = S(E)$ because E and E' are isomorphic over the field $\mathbb{Q}(\sqrt{qN_1^*})$.

Let us show that E' satisfies (C2). In the following, we prove $E'(L_\ell)[p] = 0$ for any $\ell \in S(E')$. Take any $\ell \in S(E')$.

The case $\ell \notin S_0(E) \cup S_1(E)$. First, we suppose that ℓ does not belong to $S_0(E) \cup S_1(E)$.

Claim 1. *The prime ℓ splits in $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$.*

Proof of Claim 1. When ℓ is odd, the prime ℓ is split in $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$ if and only if $\left(\frac{qN_1^*}{\ell}\right) = 1$ ([12, Chapter 1, Proposition 8.5]). By (4.1), we have

$$\left(\frac{qN_1^*}{\ell}\right) = \left(\frac{q}{\ell}\right)\left(\frac{N_1^*}{\ell}\right) = \varepsilon_\ell \prod_{\ell' \in S_1(E)} \left(\frac{(\ell')^*}{\ell}\right) = 1.$$

Next, consider the case $\ell = 2$. As $\ell \notin S_1(E)$ in this case, we know that N_1^* is odd. Since $qN_1^* \equiv 1 \bmod 8$, the prime $\ell = 2$ splits in $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$. □

From the above claim, the completion of $\mathbb{Q}(\sqrt{qN_1^*})$ at a place v above ℓ is $\mathbb{Q}_\ell$ and the base change to the local field $\mathbb{Q}_\ell$, we obtain $E'_{\mathbb{Q}_\ell} \simeq E_{\mathbb{Q}_\ell}$. As a result, we have

$$E'(L_\ell)[p] \simeq E'_{\mathbb{Q}_\ell}(L_\ell)[p] \simeq E_{\mathbb{Q}_\ell}(L_\ell)[p] \simeq E(L_\ell)[p] = 0.$$

The case $\ell \in S_0(E) \cup S_1(E)$. Next, we suppose that ℓ belongs to $S_0(E) \cup S_1(E)$. It holds that $E(L_\ell)[p] \neq 0$ and fix a non-zero $P \in E(L_\ell)[p]$.

Claim 2. *The action of G_{L_ℓ} on $E[p]$ is unipotent.*

Proof of Claim 2. Take a basis $\{P, Q\}$ of $E[p]$ as an $\mathbb{F}_p$-vector space with $Q \in E[p] \smallsetminus \mathbb{F}_p P$. Recall that the Weil pairing $e : E[p] \times E[p] \to \mu_p$ is alternating and G_{L_ℓ}-equivariant ([24, Chapter III, Section 8]). As $\mu_p \subseteq L_\ell$, we have $\sigma(e(P,Q)) = e(P,Q)$ for any $\sigma \in G_{L_\ell}$. On the other hand, $\sigma(e(P,Q)) = e(\sigma P, \sigma Q) = e(P, \sigma Q)$ implies $e(P, \sigma Q - Q) = 1$. Here, the element of the form $\sigma Q - Q$ is in the kernel of $E[p] \to \mu_p; T \mapsto e(P,T)$ which is generated by P so that $\sigma Q - Q = aP$ for some $a \in \mathbb{F}_p$. According to the fixed basis above, the action of σ is written as $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ which is unipotent. □

Claim 3. *The extension $L_\ell(\sqrt{qN_1^*})/L_\ell$ is quadratic.*

Proof of Claim 3. Let us show the claim by dividing into three cases.

(i) Suppose that $\ell \in S_0(E)$, and ℓ is odd. The equalities

$$\left(\frac{qN_1^*}{\ell}\right) \overset{(4.1)}{=} -\varepsilon_\ell \prod_{\ell' \in S_1(E)} \left(\frac{(\ell')^*}{\ell}\right) = -1$$

imply that the prime ℓ is inert in the extension $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$. For the prime 2 does not divide $[\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell]$, we have $\mathbb{Q}_\ell(\sqrt{qN_1^*}) \not\subseteq L_\ell$. Hence, the extension $L_\ell(\sqrt{qN_1^*})/L_\ell$ is non-trivial.

(ii) Suppose that $\ell = 2 \in S_0(E)$. The extension $L_2 = \mathbb{Q}_2(\mu_{p^\infty})/\mathbb{Q}_2$ does not contain quadratic extension fields of $\mathbb{Q}_2$. Since we have $qN_1^* \equiv 5 \bmod 8$, the prime 2 is inert in the extension $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$. Thus, the extension $L_2(\sqrt{qN_1^*})/L_2$ is non-trivial.

(iii) Suppose that $\ell \notin S_0(E)$. Then $\ell \in S_1(E)$ and thus $\ell \mid N_1^*$. This implies that the prime ℓ is ramified in the extension $\mathbb{Q}(\sqrt{qN_1^*})/\mathbb{Q}$. We also have $L_\ell(\sqrt{qN_1^*}) \neq L_\ell$ because $L_\ell/\mathbb{Q}_\ell$ is unramified.

In each case, the extension $L_\ell(\sqrt{qN_1^*})/L_\ell$ is quadratic. □

From Claim 2 above, there exists a basis $\{P, Q\}$ of $E[p]$ as $\mathbb{F}_p$-vector space such that G_{L_ℓ} acts trivially on $\mathbb{F}_p P$, and also $E[p]/\mathbb{F}_p P$ which is generated by the residue class represented by $Q \in E[p] \smallsetminus \mathbb{F}_p P$. We have an isomorphism $f \colon E[p] \otimes \mathbb{F}_p(\psi) \xrightarrow{\simeq} E'[p]$ of $\mathbb{F}_p[G_{L_\ell}]$-modules, where ψ denotes the quadratic character attached to $L_\ell(\sqrt{qN_1^*})/L_\ell$. Take a lift $\sigma \in G_{L_\ell}$ of the generator of $\mathrm{Gal}(L_\ell(\sqrt{qN_1^*})/L_\ell)$. This satisfies $\sigma P = P$ and $\sigma Q - Q \in \mathbb{F}_p P$. Thus, the element σ acts by $\psi(\sigma) = -1$ on both $\mathbb{F}_p f(P \otimes 1) \subseteq E'[p]$ and $E'[p]/\mathbb{F}_p f(P \otimes 1)$. Therefore, for any $\ell \in S(E') = S(E)$, we have $E'(L_\ell)[p] = 0$. □

4.2. Equivalent conditions of (C2). For later use in the proof of our main results, let us study some equivalent conditions of (C2).

Lemma 4.3. *Suppose that E has potentially multiplicative reduction at ℓ ($\neq p$). Then, the elliptic curve $E_{K_1^E}$ has split multiplicative reduction at every place of $K_1^E = \mathbb{Q}(E[p])$ above ℓ.*

Proof. We may assume that the j-invariant $j(E)$ is not equal to 0 or 1728 because E has potentially good reduction at all primes in such cases ([24, Chapter VII, Proposition 5.5]). By [25, Chapter V, Lemma 5.2], there exist elements $q, \gamma \in \mathbb{Q}_\ell^\times$ with $\mathrm{ord}_\ell(q) > 0$ such that $E_{\mathbb{Q}_\ell(\sqrt{\gamma})}$ has split multiplicative reduction, and we have a $G_{\mathbb{Q}_\ell}$-equivariant isomorphism

$$f\colon E[p^\infty] \xrightarrow{\simeq} (\overline{\mathbb{Q}}_\ell^\times/q^{\mathbb{Z}})[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi),$$

where $\chi\colon G_{\mathbb{Q}_\ell} \to \mathbb{Z}_p^\times$ is the trivial character or the quadratic character attached to the extension $\mathbb{Q}_\ell(\sqrt{\gamma})/\mathbb{Q}_\ell$. In order to prove the assertion, it is sufficient to show that $\sqrt{\gamma} \in \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$. If χ is trivial, then $\sqrt{\gamma} \in \mathbb{Q}_\ell$ and there is nothing to show. We may assume that χ is non-trivial. Since the Weil paring

$$E(\overline{\mathbb{Q}}_\ell)[p] \times E(\overline{\mathbb{Q}}_\ell)[p] \longrightarrow \boldsymbol{\mu}_p(\overline{\mathbb{Q}}_\ell) = \mu_p$$

preserves the action of $G_{\mathbb{Q}_\ell}$, we have $\mu_p \subseteq \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$. If $\sqrt{\gamma} \in \mu_p$, then $\sqrt{\gamma} \in \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$. Suppose that $\sqrt{\gamma} \notin \mu_p$. The fields $F_1 := \mathbb{Q}_\ell(\sqrt{\gamma})$ and $\mathbb{Q}_\ell(\mu_p)$ are linearly disjoint over $\mathbb{Q}_\ell$. Moreover, as p is odd, the fields F_1 and $F_2 := \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q})$ are linearly disjoint over $\mathbb{Q}_\ell$. Put $\widetilde{F} := \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}, \sqrt{\gamma}) = F_2F_1$. By the isomorphism f, we have $\mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p], \sqrt{\gamma}) = \widetilde{F}$. Recall that $\widetilde{F}/\mathbb{Q}_\ell(\mu_p)$ is an abelian extension whose degree divides $2p$, and p is odd. The extension $\widetilde{F}/\mathbb{Q}_\ell(\mu_p)$ has only one subextension F' with $[\widetilde{F} : F'] = 2$. It holds that $F_2 \subseteq \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$ because $[\widetilde{F} : F_2] = 2$ and $[\widetilde{F} : \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])] \leq 2$. Furthermore, by the isomorphism f, the group $\mathrm{Gal}(\widetilde{F}/F_2)$ ($\simeq \mathrm{Gal}(F_1/\mathbb{Q}_\ell)$) acts faithfully on $E(\overline{\mathbb{Q}}_\ell)[p]$. This implies that $\mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p]) = \widetilde{F}$, and especially $\sqrt{\gamma} \in \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$. Consequently, the elliptic curve $E_{K_1^E}$ has split multiplicative reduction at every place of K_1^E. $\square$

The following Lemma 4.4 gives some conditions equivalent to (C2).

Lemma 4.4. *Let ℓ be a prime number. Suppose that E has potentially multiplicative reduction at ℓ. Then, the following are equivalent:*

(a) *The condition* (C2) *holds, i.e., for any $n \in \mathbb{Z}_{\geq 1}$ and any place v of K_n above ℓ, we have $E(K_{n,v})[p] = 0$.*

(b) *For any $n \in \mathbb{Z}_{\geq 1}$ and any place w of K_n^E above ℓ where the base change $E_{K_{n,w}^E}$ of E has split multiplicative reduction, we have*

$$H^0\left(K_{n,v}, E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right) = 0.$$

Here, we denote by v the place of K_n below w. (Note that the absolute Galois group $G_{K_{n,v}}$ acts on $E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}$ because the extension $K_{n,w}^{E,\mathrm{ur}}/K_{n,v}$ is Galois.)

(c) *For any $n \in \mathbb{Z}_{\geq 1}$ and any place w of K_n^E above ℓ at where $E_{K_n^E}$ has split multiplicative reduction, we have*

$$H^0\left(K_{n,v}, E[p^\infty]/E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right) = 0,$$

where v denotes the place of K_n below w.

(d) *For any $n \in \mathbb{Z}_{\geq 1}$, any place v of K_n above ℓ and any subquotient $\mathbb{Z}_p[G_{K_{n,v}}]$-module M of $E[p^\infty]$, we have*

$$H^0\left(K_{n,v}, M\right) = 0.$$

Remark 4.5. Recall that the condition (C2) holds if and only if for any prime number ℓ with E has potentially multiplicative reduction, the condition (a) in Lemma 4.4 holds. As we are assuming E has good reduction at p, the prime number $\ell \neq p$.

Proof of Lemma 4.4. (a) $\Longrightarrow$ (b). Suppose that the base change $E_{K_{n,w}^E}$ has split multiplicative reduction for $n \geq 1$ and a place w of K_n^E above ℓ, we have

$$H^0(K_{n,v}, E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}) = E(K_{n,v})[p^\infty]_{\mathrm{div}} \subseteq E(K_{n,v})[p^\infty].$$

The latter group is trivial because of $E(K_{n,v})[p] = 0$.

(d) $\Longrightarrow$ (a). Take any $n \geq 1$, and any place v of K_n above ℓ. As $E[p]$ is a submodule of $E[p^\infty]$, the condition (d) implies $E(K_{n,v})[p] = H^0(K_{n,v}, E[p]) = 0$.

(b) $\Longleftrightarrow$ (c). Suppose that w is a place of K_n^E where $E_{K_n^E}$ has split multiplicative reduction, and let v be a place of K_n below w. The elliptic curve E is isomorphic to a Tate curve $\mathbb{G}_m/q_w^{\mathbb{Z}}$ ([25, Chapter V, Theorem 3.1]). Since $\ell \neq p$ and $K_{n,v}$ is an extension of $\mathbb{Q}_\ell$, the extension $K_{n,v}(\mu_{p^\infty})$ is unramified over $K_{n,v}$ ([20, Chapitre IV, §4, Proposition 16]) so that we have $E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}} \simeq \mu_{p^\infty}$ and

$$E[p^\infty]/E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}} \simeq \frac{\mu_{p^\infty} \times (q_w^{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p])}{\mu_{p^\infty} \times q_w^{\mathbb{Z}}}.$$

By the Weil pairing, we have a natural $G_{K_{n,v}}$-equivariant isomorphism

$$\left(E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right)[p] \simeq \mathrm{Hom}_{\mathbb{Z}_p}\left(\frac{E[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}[p], \mu_p\right)$$

for any $n \in \mathbb{Z}_{\geq 1}$. As $G_{K_{n,v}}$ acts trivially on μ_p, we deduce that (b) and (c) are equivalent.

(b)&(c) $\Longrightarrow$ (a). Take any $n \geq 1$, and any place v of K_n above ℓ. By Lemma 4.3, the base change $E_{K_{n,w}^E}$ of E has split multiplicative reduction for some place w of K_n^E above v. The short exact sequence

$$0 \longrightarrow E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}} \longrightarrow E(K_{n,w}^{E,\mathrm{ur}})[p^\infty] \longrightarrow \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}} \longrightarrow 0$$

induces the exact sequence

$$\begin{aligned}&H^0\left(K_{n,v}, E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right)\\ &\qquad\qquad \longrightarrow E(K_{n,v})[p^\infty] \longrightarrow H^0\left(K_{n,v}, \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right)\end{aligned}$$

by the equality $H^0(K_{n,v}, E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]) = E(K_{n,v})[p^\infty]$. From the condition (b), we have $H^0\left(K_{n,v}, E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right) = 0$. It is enough to show $H^0\left(K_{n,v}, \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right) = 0$. As the functor $H^0(K_{n,v}, -)$ is left exact, the condition (c) implies

$$H^0\left(K_{n,v}, \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right) \subseteq H^0\left(K_{n,v}, \frac{E[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right) = 0.$$

We obtain $E(K_{n,v})[p] \subseteq E(K_{n,v})[p^\infty] = 0$ and this implies the condition (a).

(b)&(c) $\Longrightarrow$ (d). For any $n \geq 1$ and any place v of K_n above ℓ, take any subquotient $\mathbb{Z}_p[G_{K_{n,v}}]$-module M of $E[p^\infty]$. From Lemma 4.3, the elliptic curve $E_{K_{n,w}^E}$ has split multiplicative reduction for some place w of K_n^E above v. We define a $\mathbb{Z}_p[G_{K_{n,v}}]$-submodule M_1 of $E[p]$ by $M_1 := \left(E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right)[p]$, and put

$$M_2 := E[p]/M_1 \simeq \left(E[p^\infty]/E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}\right)[p].$$

Since M_1 and M_2 are one dimensional vector spaces over $\mathbb{F}_p$, the $\mathbb{Z}_p[G_{K_{n,v}}]$-modules M_1 and M_2 are simple, and the filtration $0 \subsetneq M_1 \subsetneq E[p]$ becomes a Jordan–Hölder series of the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $E[p]$. The Jordan–Hölder theorem implies that for any $N \in \mathbb{Z}_{>0}$, every simple subquotient of the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $E[p]$ is isomorphic to M_1 or M_2 since the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $E[p^N]$ is written as a successive extension of copies of $E[p]$. (For the

Jordan–Hölder theorem in an abelian category, in particular, for $\mathbb{Z}_p[G_{K_{n,v}}]$-modules, see for instance, [27, Lemma 0FCK].) Hence every simple subquotient of the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $E[p^\infty] = \varinjlim_{N>0} E[p^N]$ is isomorphic to M_1 or M_2. As M is a subquotient $\mathbb{Z}_p[G_{K_{n,v}}]$-module of $E[p^\infty]$, every simple subquotient of M is isomorphic to M_1 or M_2. The conditions (b) and (c) imply (d). This completes the proof of Lemma 4.4 □

4.3. Example of (C2). It is obvious that if E has potentially good reduction everywhere, then (E,p) satisfies the condition (C2). Here, we introduce an example of (E,p) satisfying (C2) such that E has multiplicative reduction at some primes. The following proposition is useful to find such a pair (E,p).

Proposition 4.6. *Let ℓ be a prime number distinct from p. Suppose that E has non-split multiplicative reduction at ℓ. We also assume that* $p \equiv 3 \bmod 4$*, and $-p$ is quadratic residue modulo ℓ. Then, it holds that*

$$E(K_{n,v})[p] = 0$$

for any $n \in \mathbb{Z}_{\geq 0}$, and any place v of K_n above ℓ.

Proof. Fix any embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, and regard μ_{p^∞} as a subgroup of $\overline{\mathbb{Q}}_\ell^\times$. Let $q, \gamma \in \mathbb{Q}_\ell$ be as in the proof of Lemma 4.3. We have $\sqrt{\gamma} \notin \mathbb{Q}_\ell$ because E has non-split multiplicative reduction at ℓ. Let $\chi\colon G_{\mathbb{Q}_\ell} \to \mathbb{Z}_p^\times$ be the quadratic character attached to $\mathbb{Q}_\ell(\sqrt{\gamma})/\mathbb{Q}_\ell$. We have a $G_{\mathbb{Q}_\ell}$-equivariant isomorphism

$$f\colon E[p^\infty] \longrightarrow (\overline{\mathbb{Q}}_\ell^\times/q^{\mathbb{Z}})[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi).$$

In order to prove Proposition 4.6, it suffices to show that

$$H^0(\mathbb{Q}_\ell(\mu_{p^\infty}), (\overline{\mathbb{Q}}_\ell^\times/q^{\mathbb{Z}})[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi)) = 0. \tag{4.2}$$

It holds that $\sqrt{-p} \in \mathbb{Q}_\ell$, because $-p$ is quadratic residue modulo ℓ. As $p \equiv 3 \bmod 4$, the extension degree $[\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell]$ is odd. This implies that $\mathbb{Q}_\ell(\mu_{p^\infty})$ never contains any quadratic extension field of $\mathbb{Q}_\ell$ because p is odd. We obtain

$$H^0(\mathbb{Q}_\ell(\mu_{p^\infty}), \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi)) \simeq H^0(\mathbb{Q}_\ell(\mu_{p^\infty}), (\mathbb{Q}_p/\mathbb{Z}_p)(\chi)) = 0.$$

Suppose that (4.2) does not hold. There exists an element

$$P \in H^0(\mathbb{Q}_\ell(\mu_{p^\infty}), (\overline{\mathbb{Q}}_\ell^\times/q^{\mathbb{Z}})[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi))$$

of order p. Let ζ be a primitive p-th root of unity, and $\sigma \in G_{\mathbb{Q}_\ell(\mu_{p^\infty})}$ an element satisfying $\chi(\sigma) = -1$. Note that in $\mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi)$, we have $\sigma(\zeta \otimes 1) = \zeta \otimes (-1)$. By taking the Weil pairing $e\colon E[p] \times E[p] \to \mu_p$, we obtain

$$e(\zeta \otimes 1, P) = \sigma(e(\zeta \otimes 1, P)) = e\left(\sigma(\zeta \otimes 1), \sigma P\right) = e(\zeta \otimes 1, P)^{-1}.$$

As p is odd, this contradicts the fact that the Weil pairing e is non-degenerate. Consequently, the assertion (4.2) holds. $\square$

Example 4.7. Let (E,p) be as in Example 1.13. Then, the elliptic curve E has good reduction outside the prime 5077, and it has non-split multiplicative reduction at 5077. Since $p = 7 \equiv 3 \bmod 4$, and -7 is a quadratic residue modulo 5077, Proposition 4.6 implies that (E,p) satisfies the condition (C2).

5. Selmer Groups

In this section, we shall recall the definition of the fine Selmer groups of an elliptic curve, and introduce some preliminary results related to Selmer groups. In Section 5.2, we shall review preliminary results in the Iwasawa theoretical setting. We keep the notation and the assumptions in Section 4.

5.1. Definition of Selmer groups. Let K be a number field, that is, a finite extension field of $\mathbb{Q}$. First, let us recall Bloch–Kato's finite local conditions.

Definition 5.1 ([17, Definition 1.3.4, Remark 1.3.6])**.** Let v be any place of K. We define $H^1_f(K_v, V_p(E))$ to be the $\mathbb{Q}_p$-vector space

$$\begin{cases} H^1_{\mathrm{ur}}(K_v, V_p(E)) & \text{if } v \nmid p, \\ \mathrm{Ker}\left(H^1(K_v, V_p(E)) \to H^1(K_v, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V_p(E))\right) & \text{if } v \mid p, \\ 0 & \text{if } v \mid \infty, \end{cases}$$

where B_{cris} is Fontaine's p-adic period ring and $v \mid \infty$ we mean that v is an infinite place in K. We define

$$H^1_f(K_v, E[p^\infty]) \subseteq H^1(K_v, E[p^\infty]) \text{ and } H^1_f(K_v, T_p(E)) \subseteq H^1(K_v, T_p(E))$$

to be the image and the inverse image, respectively, of $H^1_f(K_v, V_p(E))$ under the natural maps $H^1(K_v, T_p(E)) \to H^1(K_v, V_p(E)) \to H^1(K_v, E[p^\infty])$. For each $n \in \mathbb{Z}_{>0}$, we define $H^1_f(K_v, E[p^n])$ to be the inverse image of $H^1_f(K_v, E[p^\infty])$ by the natural map

$$\iota_{n,v} \colon H^1(K_v, E[p^n]) \longrightarrow H^1(K_v, E[p^\infty]). \tag{5.1}$$

The subgroup $H^1_f(K_v, E[p^n])$ coincides with the image of $H^1_f(K_v, T_p(E))$ under the map $H^1(K, T_p(E)) \to H^1(K_v, E[p^n])$ induced by $T_p(E) \to T_p(E)/p^nT_p(E) \simeq E[p^n]$ ([17, Lemma 1.3.8]).

Remark 5.2. Let v be any finite place of K not above p. Suppose that E_K has good reduction at v. The p-adic Tate module $T_p(E)$ is unramified at v (from the "easy" direction of the Néron–Ogg–Shafarevich criterion [24, Chapter VII, Theorem 7.1]) so that $H^1_f(K_v, E[p^n])$ coincides with

$H^1_{\mathrm{ur}}(K_v, E[p^n])$ (cf. [17, Lemma 1.3.8]), for each $n \in \mathbb{Z}_{>0} \cup \{\infty\}$. Furthermore, the inflation-restriction exact sequence (e.g., [17, Proposition B.2.5]) gives a natural isomorphism

$$H^1(K_v^{\mathrm{ur}}/K_v, E[p^n]) \simeq H^1_f(K_v, E[p^n]).$$

Definition 5.3 (the fine Selmer group)**.** For each $n \in \mathbb{Z}_{>0} \cup \{\infty\}$, we define *the fine Selmer group* $\mathrm{Sel}_p(K, E[p^n])$ to be the kernel of

$$H^1(K, E[p^n]) \longrightarrow \prod_{u \mid p} H^1(K_v, E[p^n]) \times \prod_{v \nmid p} \frac{H^1(K_v, E[p^n])}{H^1_f(K_v, E[p^n])},$$

where u runs through all the places of K above p, and v runs through all the places of K not above p.

Remark 5.4. When v is an infinite place of K, the cohomology group $H^1(K_v, E[p^n])$ is annihilated by at most 2 for each $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$. Since we are considering the odd prime p, we have $H^1(K_v, E[p^n]) = 0$. Because of this, we may not care about infinite places in the following.

Remark 5.5. We denote by Σ_K the set of places of K above the prime divisors of pD_E and the all infinite places and by K_Σ the maximal algebraic extension field of K unramified outside Σ_K. Then, for each $n \in \mathbb{Z}_{>0} \cup \{\infty\}$, the kernel of the natural map

$$H^1(K, E[p^n]) \longrightarrow \prod_{v \notin \Sigma_K} \frac{H^1(K_v, E[p^n])}{H^1_f(K_v, E[p^n])}$$

coincides with $H^1(K_\Sigma/K, E[p^n])$ ([17, Lemma 1.5.3]). The fine Selmer group $\mathrm{Sel}_p(K, E[p^n])$ can be regarded as a subgroup of $H^1(K_\Sigma/K, E[p^n])$.

Remark 5.6. Here, we give a remark on the relation between $\mathrm{Sel}_p(K, E[p^n])$ and the classical Selmer group. Take any $n \in \mathbb{Z}_{>0}$. Recall that the classical Selmer group $\mathrm{Sel}(K, E[p^n])$ is defined by

$$\mathrm{Sel}(K, E[p^n]) := \mathrm{Ker}\left(H^1(K, E[p^n]) \longrightarrow \prod_{v} \frac{H^1(K_v, E[p^n])}{H^1_{\mathrm{cl}}(K_v, E[p^n])} \right),$$

where v runs through all the finite places of K, and $H^1_{\mathrm{cl}}(K_v, E[p^n])$ denotes the image of the homomorphism

$$\delta_{n,v} \colon E(K_v) = H^0(K_v, E(\overline{K}_v)) \longrightarrow H^1(K_v, E[p^n])$$

induced by the short exact sequence

$$0 \longrightarrow E[p^n] \xrightarrow{\subseteq} E(\overline{K}_v) \xrightarrow{\times p^n} E(\overline{K}_v) \longrightarrow 0.$$

For any $n \in \mathbb{Z}_{>0}$, there exists a short exact sequence

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathrm{Sel}(K, E[p^n]) \longrightarrow \text{Ш}(E_K/K)[p^n] \longrightarrow 0,$$

where Ш(E_K/K) denotes the Tate–Shafarevich group of E_K/K. By the well-known fact below (Proposition 5.7 which follows from the arguments in [1, Example 3.11]), it holds that

$$\mathrm{Sel}_p(K, E[p^n]) = \mathrm{Ker}\left(\mathrm{Sel}(K, E[p^n]) \longrightarrow \prod_{v\mid p} H^1(K_v, E[p^n])\right).$$

Proposition 5.7. *Let K be a number field. For any finite place v of K, it holds that*

$$H^1_{\mathrm{cl}}(K_v, E[p^n]) = H^1_f(K_v, E[p^n]). \tag{5.2}$$

Proof. The short exact sequence

$$0 \longrightarrow T_p(E) \longrightarrow V_p(E) \longrightarrow E(\overline{K}_v)[p^\infty] \longrightarrow 0$$

induces a natural isomorphism

$$\delta\colon E(K_v)[p^\infty] \xrightarrow{\simeq} H^1(K_v, T_p(E))_{\mathrm{tor}},$$

where $H^1(K_v, T_p(E))_{\mathrm{tor}}$ denotes the torsion part of $H^1(K_v, T_p(E))$ ([28, (2.3) Proposition]). Note that we have $H^1(K_v, T_p(E))_{\mathrm{tor}} \subseteq H^1_f(K_v, T_p(E))$ by definition. We also note that the diagram

$$\begin{tikzcd} E(K_v)[p^\infty] \arrow[r, "\delta", "\simeq"'] \arrow[d, hook, "\eta_1"'] & H^1(K_v, T_p(E))_{\mathrm{tor}} \arrow[d, "\eta_2"] \\ E(K_v)\otimes\mathbb{Z}_p \arrow[r, "\delta_{n,v}\otimes\mathbb{Z}_p"'] & H^1(K_v, E[p^n]) \end{tikzcd} \tag{5.3}$$

commutes, where η_1 and η_2 are natural homomorphisms.

First, suppose that v lies above a prime number ℓ distinct from p. As noted in [1, Example 3.11], we have

$$\begin{aligned} H^1_f(K_v, V_p(E)) &= H^1_{\mathrm{ur}}(K_v, V_p(E)) \\ &\xleftarrow[\simeq]{\mathrm{inf}} H^1(\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v), H^0(K_v^{\mathrm{ur}}, V_p(E))) = 0. \end{aligned}$$

By the Weil pairing, we have

$$\mathrm{Hom}_{\mathbb{Q}_p}(V_p(E), \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \mu_{p^n}) \simeq V_p(E).$$

The local duality ([1, Proposition 3.8]) implies that

$$H^1(K_v, V_p(E))/H^1_f(K_v, V_p(E)) \simeq H^1_f(K_v, V_p(E)) = 0.$$

Therefore, we obtain $H^1(K_v, V_p(E)) = 0$ and hence $H^1(K_v, T_p(E))$ is torsion. This implies the equalities

$$H^1(K_v, T_p(E))_{\mathrm{tor}} = H^1_f(K_v, T_p(E)) = H^1(K_v, T_p(E)).$$

Since $E(K_v)$ is a compact commutative ℓ-adic Lie group of dimension $[K_v : \mathbb{Q}_\ell]$, the group $E(K_v)$ is isomorphic to the direct sum of $\mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]}$ and a finite abelian group. This implies that η_1 in (5.3) becomes an isomorphism. Since $H^1_f(K_v, E[p^n])$ coincides with the image of $H^1_f(K_v, T_p(E))$ under the map $H^1(K_v, T_p(E)) \overset{\eta_2}{\to} H^1(K_v, E[p^n])$ ([17, Lemma 1.3.8]), the commutative diagram (5.3) above implies the equality $(\star)$ below

$$H^1_{\mathrm{cl}}(K_v, E[p^n]) = \mathrm{Im}(\delta_{n,v}) = \mathrm{Im}(\delta_{n,v} \otimes \mathbb{Z}_p) \overset{(\star)}{=} \mathrm{Im}(\eta_2) = H^1_f(K_v, E[p^n]).$$

Next, let us suppose that v lies above p. (Note that we do not use this case in this manuscript, but for the sake of the readers' convenience, we give a proof.) We denote by $H^1_{\mathrm{cl}}(K_v, T_p(E))$ the image of

$$(\delta_{m,v})_m \colon E(K_v) \longrightarrow \varprojlim_m H^1(K_v, E[p^m]) \simeq H^1(K_v, T_p(E)).$$

Claim. *The group $H^1_{\mathrm{cl}}(K_v, T_p(E))$ coincides with the inverse image of*

$$H^1_{\mathrm{cl}}(K_v, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

via the natural mapping $H^1(K_v, T_p(E)) \to H^1(K_v, T_p(E)) \otimes \mathbb{Q}_p$.

Proof. The torsion part $H^1_{\mathrm{cl}}(K_v, T_p(E))_{\mathrm{tor}}$ coincides with the image of δ in (5.3). We have $H^1_{\mathrm{cl}}(K_v, T_p(E))_{\mathrm{tor}} = H^1(K_v, T_p(E))_{\mathrm{tor}}$. There is a commutative diagram

$$\begin{tikzcd}
& H^1_{\mathrm{cl}}(K_v, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Z}/p\mathbb{Z} \arrow[d, hook, dotted, "(\mathrm{inclusion})\otimes\mathbb{Z}/p\mathbb{Z}"] \\
& H^1(K_v, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Z}/p\mathbb{Z} \arrow[d, hook, "\mathrm{inclusion}"] \\
E(K_v) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \arrow[uur, bend left, "(\delta_{n,v})_n\otimes\mathbb{Z}/p\mathbb{Z}"] \arrow[r, hook, "\delta_{1,v}\otimes\mathbb{Z}/p\mathbb{Z}"'] & H^1(K_v, E[p]).
\end{tikzcd}$$

Note that in the above commutative diagram, the injectivity of $\delta_{1,v} \otimes \mathbb{Z}/p\mathbb{Z}$ and the surjectivity of $(\delta_{n,v})_n \otimes \mathbb{Z}/p\mathbb{Z}$ imply that the vertical dotted arrow is injective. By Nakayama's lemma, a basis of the $\mathbb{Z}_p$-module $\frac{H^1_{\mathrm{cl}}(K_v,T_p(E))}{H^1(K_v,T_p(E))_{\mathrm{tor}}}$ extends to a basis of the $\mathbb{Z}_p$-module $\frac{H^1(K_v,T_p(E))}{H^1(K_v,T_p(E))_{\mathrm{tor}}}$. Hence, the quotient $\frac{H^1_{\mathrm{cl}}(K_v,T_p(E))}{H^1(K_v,T_p(E))_{\mathrm{tor}}}$ coincides with

$$\Big(H^1_{\mathrm{cl}}(K_v, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\Big) \cap \frac{H^1(K_v, T_p(E))}{H^1(K_v, T_p(E))_{\mathrm{tor}}}.$$

The claim follows from this. $\square$

The arguments in [1, Example 3.11] (the isomorphism ∂ in commutative diagram (3.11.1) and the first equality in (3.11.2)) imply the equality $H^1_{\mathrm{cl}}(K_v, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = H^1_f(K_v, V_p(E))$. The above claim gives

$$H^1_{\mathrm{cl}}(K_v, T_p(E)) = H^1_f(K_v, T_p(E)).$$

Both of the $\mathbb{Z}_p$-modules $H^1_{\mathrm{cl}}(K_v, E[p^n])$ and $H^1_f(K_v, E[p^n])$ coincide with the image of $H^1_{\mathrm{cl}}(K_v, T_p(E))$ and $H^1_f(K_v, T_p(E))$ respectively under the map $H^1(K_v, T_p(E)) \to H^1(K_v, E[p^n])$. Hence, we obtain the equality (5.2). $\square$

5.2. Preliminaries of Iwasawa theory. For each place v of K_1, we denote by D_v the decomposition subgroup of the Galois group $\Gamma := \mathcal{G}_{\infty,1} = \mathrm{Gal}(K_\infty/K_1)$ at v, and define

$$\mathcal{A}_v := \begin{cases} \mathrm{Ann}_{\mathbb{Z}_p[\![D_v]\!]}\left(\frac{E(K_{\infty,w})[p^\infty]}{E(K_{\infty,w})[p^\infty]_{\mathrm{div}}}\right) & \text{if } v \mid p, \\ \mathrm{Ann}_{\mathbb{Z}_p[\![D_v]\!]}\left(H^1\left(K^{\mathrm{ur}}_{\infty,w}/K_{\infty,w}, \frac{E(K^{\mathrm{ur}}_{\infty,w})[p^\infty]}{E(K^{\mathrm{ur}}_{\infty,w})[p^\infty]_{\mathrm{div}}}\right)\right) & \text{if } v \nmid p, \end{cases}$$

where w is a place of K_∞ above v. We set

$$\mathcal{A}_{\mathcal{N}} := \prod_{v \mid pD_E} \mathcal{A}_v \mathbb{Z}_p[\![\Gamma]\!].$$

Recall that, for each $m, n \in \mathbb{Z}_{\geq 1}$, we have

$$\Lambda_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,1}] \simeq \Lambda/(p^n, \gamma^{p^{m-1}} - 1),$$

where $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ and γ is the fixed topological generator of Γ. Write

$$\mathrm{Sel}_p(K_\infty, E[p^\infty]) := \varinjlim_m \mathrm{Sel}_p(K_m, E[p^\infty]).$$

For any $m, n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, we put $X_{m,n} := \mathrm{Sel}_p(K_m, E[p^n])^\vee$ and $X_n := X_{n,n}$.

Proposition 5.8 (Control theorem, [17, Proposition 7.4.4])**.** *Suppose that E satisfies the condition* (C1)*. Let $m, n \in \mathbb{Z}_{\geq 0}$ be any integers. Then, the following hold.*

(1) *The restriction map $H^1(K_m, E[p^\infty]) \to H^1(K_\infty, E[p^\infty])$ is injective.*
(2) *The natural map $H^1(K_m, E[p^n]) \to H^1(K_m, E[p^\infty])[p^n]$ is injective.*
(3) *The cokernel of the restriction map*

$$\mathrm{Sel}_p(K_m, E[p^\infty]) \longrightarrow H^0(K_m, \mathrm{Sel}_p(K_\infty, E[p^\infty]))$$

is finite, and annihilated by $\mathcal{A}_{\mathcal{N}}$.

(4) *The cokernel of the natural map*

$$\mathrm{Sel}_p(K_m, E[p^n]) \longrightarrow \mathrm{Sel}_p(K_m, E[p^\infty])[p^n]$$

is finite, and independent of n.

Remark 5.9. In [17, Proposition 7.4.4], the following two additional assumptions are assumed:

- (Assumption 7.1.4) For every sub extension $F \subset K_\infty$ with $[F : \mathbb{Q}] < \infty$, both $\Lambda_F/\operatorname{char}(X_\infty)\Lambda_F$ and $X_\infty \otimes \Lambda_F$ are finite, where $\Lambda_F = \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$.
- (Assumption 7.1.5) For every prime number ℓ dividing pD_E, the decomposition group of ℓ contains an element γ_ℓ with the property that
$$T_p(E)^{\gamma_\ell^{p^n}=1} = (T_p(E)^\vee)^{\gamma_\ell^{p^n}=1} = 0$$
for every $n \geq 0$, where the superscript $\gamma_\ell^{p^n} = 1$ stands for the fixed part by $\gamma_\ell^{p^n}$.

However, the arguments in the proof of [17, Proposition 7.4.4] do not need Assumption 7.1.4. In our setting, it follows from Hasse–Weil's theorem that the $\mathbb{Z}_p[G_{K_1}]$-module $T_p(E)$ satisfies Assumption 7.1.5. We also note that (C1) for E implies
$$\mathcal{A}_{\mathrm{glob}} := \mathrm{Ann}_{\mathbb{Z}_p[\![\Gamma]\!]}(E(K_\infty)) = \mathbb{Z}_p[\![\Gamma]\!]$$
(cf. [17, Definition 7.4.1]).

By Proposition 5.8, we immediately obtain the following corollary.

Corollary 5.10. *There exists an integer ν_X such that for any $m, n \in \mathbb{Z}_{>0}$, the orders of the kernel and the cokernel of $X_\infty \otimes_\Lambda \Lambda_{m,n} \to X_{m,n}$ are at most p^{ν_X}.*

Remark 5.11. Recall that $\Delta = \mathrm{Gal}(K_1/\mathbb{Q})$. Take any $n \in \mathbb{Z}_{>0}$. Since the order of Δ is prime to p, we have
$$H^0(\Delta, \mathrm{Sel}_p(K_1, E[p^n])) \simeq \mathrm{Sel}_p(\mathbb{Q}, E[p^n]),$$
and hence $(X_{1,n})_{\mathbf{1}} \simeq X_{0,n}$, where $\mathbf{1} \in \widehat{\Delta}$ denotes the trivial character. By Corollary 5.10, the orders of the kernel and the cokernel of
$$X_{\infty,\mathbf{1}} \otimes_\Lambda \Lambda_{1,n} \longrightarrow (X_{1,n})_{\mathbf{1}} \simeq X_{0,n}$$
are at most p^{ν_X}.

6. Proof of Main results

In this section, we shall prove our main results, in particular, Theorem 1.1. We keep the notation in Section 4 and we suppose that the elliptic curve E over $\mathbb{Q}$ has good reduction at an odd prime number p.

6.1. Boundedness of the order of Galois cohomology. In this paragraph, let us prove the following Proposition 6.1, which is related to the boundedness of the order of the kernel and the cokernel of the restriction map
$$H^1(K_n, E[p^n]) \longrightarrow H^1(K_n^E, E[p^n]).$$

Proposition 6.1. *Suppose that the elliptic curve E satisfies the conditions* (C1) *and* (C3)*. Then, for any $i \in \{1, 2\}$, the set*

$$\{\# H^i(K_n^E/K_n, E[p^n])\}_{n \geq 0}$$

is bounded.

In order to prove Proposition 6.1, we need the following lemmas.

Lemma 6.2. *We assume the condition* (C1) *and also E has complex multiplication by an order $\mathfrak{o}$ of an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Then, the fields $\mathbb{Q}(\sqrt{-d})$ and K_∞ are linearly disjoint over $\mathbb{Q}$.*

Proof. Assume $\mathbb{Q}(\sqrt{-d}) \subseteq K_\infty$ for the contradiction. As E is defined over $\mathbb{Q}$, every endomorphism of E is defined over $\mathbb{Q}(\sqrt{-d})$ ([25, Chapter II, Theorem 2.2 (b)]), hence over K_∞. Recall that $E[p]$ is a free $\mathfrak{o}/p\mathfrak{o}$-module of rank 1 ([25, Chapter II, Proposition 1.4]). The two dimensional representation $\rho_1^E \colon G_{K_\infty} \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ is given by a character $G_{K_\infty} \to \mathrm{Aut}_{\mathfrak{o}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(E[p]) \simeq (\mathfrak{o}/p\mathfrak{o})^\times$. This contradicts (C1). $\square$

Lemma 6.3. *Suppose that E satisfies* (C1) *and* (C3)*. Then, for any $i \in \mathbb{Z}_{\geq 0}$, it holds that $H^i(K_\infty^E/K_\infty, V_p(E)) = 0$.*

Proof. The case non CM. First, suppose that E does not have complex multiplication. Recall that $G_{\mathbb{Q}}$ acts on $\bigwedge^2_{\mathbb{Z}_p} T_p(E)$ via the cyclotomic character (cf. [24, Chapter V, Section 2]). By Serre's open image theorem ([22, 4.4, Théorème 3], [23, p. IV-11]), the image H of the Galois representation

$$\rho^E \colon \mathrm{Gal}(K_\infty^E/K_\infty) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

becomes an open subgroup of $SL_2(\mathbb{Z}_p)$. There exists an open normal standard pro-p subgroup U of H ([2, 8.29 Theorem]), because H is a p-adic Lie group. By [10, Chapter V, (2.4.9) Théorème], we have

$$H^q(U, V_p(E)) = H^q(\mathrm{Lie}(U), V_p(E))$$

for any $q \geq 0$. Since $\mathrm{Lie}(U)$ is an open Lie-subalgebra of

$$\mathfrak{sl}_2(\mathbb{Z}_p) := \{A \in pM_2(\mathbb{Z}_p) \mid \mathrm{Tr}\, A = 0\},$$

a matrix of the form $\left(\begin{smallmatrix} 1+p^n & 0 \\ 0 & -(1+p^n) \end{smallmatrix}\right)$ for some n belongs to $\mathrm{Lie}(U)$. By [21, Théorème 1], we obtain $H^q(\mathrm{Lie}(U), V_p(E)) = 0$. Hence, the Hochschild–Serre spectral sequence

$$E_2^{pq} = H^p(H/U, H^q(U, V_p(E))) \Longrightarrow H^{p+q}(H, V_p(E))$$

implies that $H^i(K_\infty^E/K_\infty, V_p(E)) = H^i(H, V_p(E)) = 0$ for any $i \geq 0$.

The case CM. Next, let us assume that E has complex multiplication. By the assumption (C3), the ring $\mathrm{End}(E)$ of endomorphisms of E defined over $\overline{\mathbb{Q}}$ is the maximal order $\mathfrak{o}$ of an imaginary quadratic field $L := \mathbb{Q}(\sqrt{-d})$.

Put $L^E_\infty = LK^E_\infty$. Since E is defined over $\mathbb{Q}$, every element of $\mathrm{End}(E)$ is defined over L ([25, Chapter II, Theorem 2.2 (b)]). Consider the representation $\rho\colon G_L \to \mathrm{Aut}(T_p(E))$ which is arising from the action of G_L on $T_p(E)$. This factors through an injective homomorphism $\mathrm{Gal}(L^E_\infty/L) \to \mathrm{Aut}(T_p(E))$ which is also denoted by ρ. The Tate module $T_p(E) = \varprojlim_n E[p^n]$ is a free $\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module of rank 1 because $E[p^n]$ is a free $\mathfrak{o}/p^n\mathfrak{o}$-module of rank 1 ([25, Chapter II, Proposition 1.4]). As we noted above, every endomorphism of E is defined over L, the action of $\mathrm{Gal}(L^E_\infty/L)$ commutes with the scalar multiplication by $\mathfrak{o}$, and we obtain the commutative diagram

$$
\begin{tikzcd}
\mathrm{Gal}(L^E_\infty/L) \arrow[r, hook, "\rho"] \arrow[dr, hook, "\rho_{\mathfrak{o}}"'] & \mathrm{Aut}(T_p(E)) \\
& \mathrm{Aut}_{\mathfrak{o}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_p(E)) \simeq (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times. \arrow[u, hook]
\end{tikzcd}
\tag{6.1}
$$

In particular, the extension L^E_∞/L is an abelian extension. The short exact sequence

$$0 \longrightarrow \mathrm{Gal}(L^E_\infty/L) \longrightarrow \mathrm{Gal}(L^E_\infty/\mathbb{Q}) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow 0$$

induces the action of $\mathrm{Gal}(L/\mathbb{Q})$ to $\mathrm{Gal}(L^E_\infty/L)$. In fact, let c be the unique generator of $\mathrm{Gal}(L/\mathbb{Q})$ and take $\widetilde{c} \in \mathrm{Gal}(L^E_\infty/\mathbb{Q})$ a lift of c. The action of $\mathrm{Gal}(L/\mathbb{Q})$ on $\mathrm{Gal}(L^E_\infty/L)$ is given by $\sigma \mapsto \widetilde{c}\sigma\widetilde{c}^{-1}$. The induced map $\rho_{\mathfrak{o}}$ preserves the action of $\mathrm{Gal}(L/\mathbb{Q})$. Let $\pi_{\mathfrak{o}^\times}\colon \mathrm{Aut}_{\mathfrak{o}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_p(E)) = (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \to (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times/\mathfrak{o}^\times$ be the natural surjection. We denote by H' the image of $\rho_{\mathfrak{o}}$, and by $\overline{H}'$ that of $\pi_{\mathfrak{o}^\times} \circ \rho_{\mathfrak{o}}$. Let $L_{\overline{H}'}$ be the maximal subfield of L^E_∞/L fixed by the kernel of $\pi_{\mathfrak{o}^\times} \circ \rho_{\mathfrak{o}}$. We have

$$
\begin{aligned}
\mathrm{Gal}(L^E_\infty/L) &\simeq H' \subset (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times, \text{ and} \\
\mathrm{Gal}(L_{\overline{H}'}/L) &\simeq \overline{H}' \subseteq (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times/\mathfrak{o}^\times.
\end{aligned}
\tag{6.2}
$$

Claim 1. *The extension $L_{\overline{H}'}/L$ is the maximal abelian extension unramified outside p.*

Proof of Claim 1. The elliptic curve E is defined over $\mathbb{Q}$ so that the class number of L is 1 ([25, Chapter II, Theorem 4.1]). We denote by $L_{\overline{H}'_n}$ be the fixed field of $L^E_n := L(E[p^n])$ by the kernel of the composition

$$\mathrm{Gal}(L^E_n/L) \hookrightarrow \mathrm{Aut}_{\mathfrak{o}\otimes\mathbb{Z}/p^n\mathbb{Z}}(E[p^n]) \twoheadrightarrow \frac{\mathrm{Aut}_{\mathfrak{o}\otimes\mathbb{Z}/p^n\mathbb{Z}}(E[p^n])}{\mathrm{Aut}(E)} \simeq (\mathfrak{o}/p^n\mathfrak{o})^\times/\mathfrak{o}^\times.$$

By the theory of complex multiplication ([25, Chapter II, Theorem 5.6]), $L_{\overline{H}'_n}$ is the ray class field of L modulo $p^n\mathfrak{o}$. The claim follows from $L_{\overline{H}'} = \bigcup_n L_{\overline{H}'_n}$. □

By the global class field theory, the above claim implies that the group $\overline{H}' \simeq \mathrm{Gal}(L_{\overline{H}'}/L)$ has a quotient isomorphic to $\mathbb{Z}_p^2$ (see, for instance, [29, Chapter 13, Proposition 13.2 and Theorem 13.4]). The subgroup H' is open in $(\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$, and in particular, the complex conjugate c acts non-trivially on H'.

Claim 2. *The field K_∞^E contains $L = \mathbb{Q}(\sqrt{-d})$.*

Proof of Claim 2. If K_∞^E and L are linearly disjoint over $\mathbb{Q}$, then the extension $L_\infty^E = LK_\infty^E/\mathbb{Q}$ becomes abelian. Therefore, the complex conjugate c acts on $\mathrm{Gal}(L_\infty^E/L)$ trivially, and it acts on H' via $\rho_{\mathfrak{o}}$. This contradicts the fact that c acts on H' non-trivially. $\square$

From the above claim, we have $L_\infty^E = LK_\infty^E = K_\infty^E$.

Claim 3. *There exists a lift $\widetilde{c} \in \mathrm{Gal}(K_\infty^E/\mathbb{Q})$ of c whose order is two such that*

$$\mathrm{Gal}(K_\infty^E/\mathbb{Q}) = \langle \widetilde{c} \rangle \ltimes \mathrm{Gal}(K_\infty^E/L) \simeq \langle \widetilde{c} \rangle \ltimes H'.$$

Proof of Claim 3. From Claim 2, we have $K_\infty^E \supseteq L$. Fix an embedding $\iota_{\mathbb{C}} \colon K_\infty^E \hookrightarrow \mathbb{C}$. Consider the following short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Gal}(K_\infty^E/L) \arrow[r] \arrow[d, "\rho_{\mathfrak{o}}^E"', "\simeq"] & \mathrm{Gal}(K_\infty^E/\mathbb{Q}) \arrow[r] & \mathrm{Gal}(L/\mathbb{Q}) \arrow[r] \arrow[d, equal] & 0. \\ & H' & & \langle c \rangle & \end{tikzcd}$$

The embedding $\iota_{\mathbb{C}}$ induces a splitting of this short exact sequence which sends c to the restriction $\widetilde{c} \in \mathrm{Gal}(K_\infty^E/\mathbb{Q})$ of the complex conjugation after regarding K_∞^E as a subfield of $\mathbb{C}$ via $\iota_{\mathbb{C}}$. This splitting gives $\mathrm{Gal}(K_\infty^E/\mathbb{Q}) \simeq \langle \widetilde{c} \rangle \ltimes H'$. $\square$

Claim 4. *Putting $L_\infty = LK_\infty$, we have $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}} = L_\infty$.*

Proof of Claim 4. By Lemma 6.2, the fields K_∞ and $L = \mathbb{Q}(\sqrt{-d})$ are linearly disjoint. The composition field $L_\infty = K_\infty L$ is an abelian extension of $\mathbb{Q}$ so that $L_\infty \subseteq \mathbb{Q}^{\mathrm{ab}}$. The extension $K_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_n \mathbb{Q}(\mu_{p^n})$ of $\mathbb{Q}$ is unramified outside p and hence the extension $L_\infty = K_\infty L/L$ is unramified outside p. Let us show that $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}} = L_\infty$. Claim 1 implies that $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}} \supseteq L_\infty$ because the extension L_∞/L is unramified outside p. Accordingly, it suffices to show that $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}} \subseteq L_\infty$. As E is defined over $\mathbb{Q}$, the class number of L is one. Put $p^* := (-1)^{(p-1)/2}p$. Lemma 6.2 implies that $\mathbb{Q}(\sqrt{p^*})$ and L are linearly disjoint over $\mathbb{Q}$ because $\mathbb{Q}(\sqrt{p^*})$ is contained in $K_1 = \mathbb{Q}(\mu_p)$. We deduce that p is unramified in $L/\mathbb{Q}$. In fact, if p were ramified in $L/\mathbb{Q}$, the Hilbert class field of L would contain the quadratic extension $L(\sqrt{p^*})/L$. Since L is the imaginary quadratic field of class number one, there exists a unique prime $q_L \in \{2, 3, 7, 11, 19, 43, 67, 163\}$ which is ramified in $L/\mathbb{Q}$.

For each prime ℓ, we denote by I_ℓ the inertia subgroup of $\mathrm{Gal}((L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}})/\mathbb{Q})$ at ℓ. We define L_1 to be the subfield of $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}}$ fixed by I_p, and L_2 to be that fixed by I_{q_L}. The extension $L_{\overline{H}'}/L$ is unramified outside p, and L has class number one. The extension $(L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}})/L$ does not contain the proper extension field of L where every place above p is unramified. As p is unramified in $L/\mathbb{Q}$, we obtain $L_1 = L$. The field L_2 coincides with the maximal intermediate field of $(L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}})/\mathbb{Q}$ unramified outside p because the extension $L_{\overline{H}'}/\mathbb{Q}$ is unramified outside $\{p, q_L\}$. The inclusion $L_2 \subseteq K_\infty$ holds, because $K_\infty/\mathbb{Q}$ is the maximal abelian extension unramified outside p. As a result, we obtain $L_1L_2 \subseteq L_\infty$. Additionally, the extension $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}}$ of $L_1 = L$ is unramified outside p. In particular, the extension $(L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}})/L_1$ is unramified at q_L. Because of this, we have

$$I_p \cap I_{q_L} = \mathrm{Gal}((L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}})/L_1) \cap I_{q_L} = \{1\}.$$

Consequently, we deduce that $L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}} = L_1L_2 \subseteq L_\infty$. □

By this Claim 4, the abelianization of the Galois group $\mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q})$ is

$$\mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q})^{\mathrm{ab}} = \mathrm{Gal}(L_{\overline{H}'} \cap \mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \mathrm{Gal}(L_\infty/\mathbb{Q}). \tag{6.3}$$

The abelianization $\mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q})^{\mathrm{ab}}$ is the maximal quotient of $\mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q})$ where c acts trivially, and we have $\mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q}) \simeq \langle \widetilde{c} \rangle \ltimes \overline{H}'$ by Claim 3. Therefore, we obtain

$$\begin{aligned}
\mathrm{Gal}(L_\infty/\mathbb{Q}) &\overset{(6.3)}{=} \mathrm{Gal}(L_{\overline{H}'}/\mathbb{Q})^{\mathrm{ab}} \\
&\simeq (\langle \widetilde{c} \rangle \ltimes \overline{H}')/(\langle \widetilde{c} \rangle \ltimes (1-c)\overline{H}') \\
&\simeq \overline{H}'/(1-c)\overline{H}'.
\end{aligned}$$

(Here, the group operation of $\overline{H}'$ is written in additive manner.) Let H'_∞ be the inverse image of $(1-c)\overline{H}'$ by $\pi_{\mathfrak{o}^\times}|_{H'} \colon H' \subseteq (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \to (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times/\mathfrak{o}^\times$. By (6.2), we have

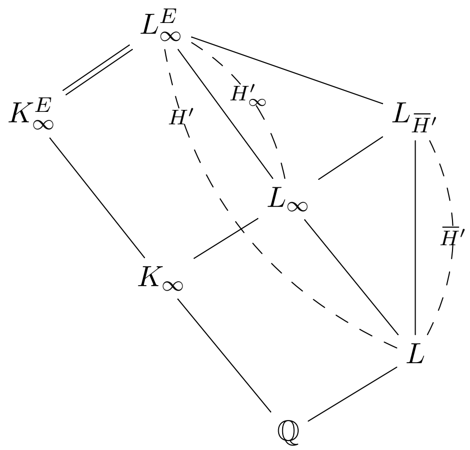
$$\begin{aligned}
\mathrm{Gal}(L_{\overline{H}'}/L_\infty) &\simeq (1-c)\overline{H}', \text{ and} \\
\mathrm{Gal}(L^E_\infty/L_\infty) &\overset{\text{Claim 2}}{=} \mathrm{Gal}(K^E_\infty/L_\infty) \simeq H'_\infty.
\end{aligned}$$

By Lemma 6.2, the fields K_∞ and L are linearly disjoint over $\mathbb{Q}$. We obtain an isomorphism $\mathrm{Gal}(L_\infty/K_\infty) \simeq \mathrm{Gal}(L/\mathbb{Q})$ and an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(K^E_\infty/L_\infty) \arrow[r] \arrow[d, "\rho^E_{\mathfrak{o}}"', "\simeq"] & \mathrm{Gal}(K^E_\infty/K_\infty) \arrow[r] & \mathrm{Gal}(L_\infty/K_\infty) \arrow[r] \arrow[d, "\simeq"] & 0. \\
& H'_\infty & & \langle c \rangle &
\end{tikzcd}$$

There exists a lift $\widetilde{c}' \in \mathrm{Gal}(K^E_\infty/K_\infty)$ of c. Note that $\widetilde{c}'$ and the isomorphism $\mathrm{Gal}(K^E_\infty/L_\infty) \simeq H'_\infty$ generate $\mathrm{Gal}(K^E_\infty/K_\infty)$, and we have $(\mathrm{Gal}(K^E_\infty/K_\infty) :$

$H'_\infty) = 2$.



Claim 5. *We have* $H'_\infty \subseteq H'[(1+c)^2]$. *Here, the* $(1+c)^2$*-torsion part of a* $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$*-module* M *is denoted by* $M[(1+c)^2]$.

Proof of Claim 5. Note that $(1-c)\overline{H}'$ is contained in $\overline{H}'[1+c]$ and $\mathfrak{o}^\times$ is contained in $H'[1+c]$. For any $x \in H'_\infty = \pi_{\mathfrak{o}^\times}^{-1}((1-c)\overline{H}')$, we have $\pi_{\mathfrak{o}^\times}(x) \in (1-c)\overline{H}' \subseteq \overline{H}'[1+c]$. For $(1+c)x \in \mathrm{Ker}(\pi_{\mathfrak{o}^\times}) = \mathfrak{o}^\times \subseteq H'[1+c]$, we obtain $(1+c)^2 x = (1+c)(1+c)x = 0$. $\square$

Put $V := (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p \simeq \mathbb{Q}_p^2$. Since c acts on V non-trivially, and $1+p \in V$ is a non-trivial element fixed by c, the eigenvalues of the action of c on V are 1 and -1. The group $(\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times[(1+c)^2]$ has a subgroup of finite index which is isomorphic to $\mathbb{Z}_p$. This implies that there exists an element $x \in H'_\infty$ of infinite order such that the closure H_∞ of $\langle x \rangle$ has finite index in H'_∞. Fix an embedding $\iota_p \colon L \hookrightarrow \overline{\mathbb{Q}}_p$. The embedding ι_p induces the ring homomorphism $\widetilde{\iota}_p \colon \mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \overline{\mathbb{Q}}_p$ sending $a \otimes b$ to $\iota_p(a)b$. The eigenvalues of the action of x on $V_p(E) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$ are $\widetilde{\iota}_p(x)$ and $\widetilde{\iota}_p(c(x)) = \widetilde{\iota}_p(x)^{-1}$. We obtain $V_p(E)[x-1] = 0$ and $V_p(E)/(1-x) = 0$. Note that H_∞ is topologically generated by x. By [13, (1.7.7) Proposition] combined with [28, (2.2) Corollary and (2.3) Proposition], it holds that $H^q(H_\infty, V_p(E)) = 0$ for any $q \geq 0$. Let us identify H'_∞ with $\mathrm{Gal}(K_\infty^E/L_\infty)$. We may regard H_∞ as a normal subgroup of $\mathrm{Gal}(K_\infty^E/K_\infty)$ because c acts on H_∞ by $x \mapsto x^{-1}$. Hence, by the Hochschild–Serre spectral sequence

$$E_2^{pq} = H^p(\mathrm{Gal}(K_\infty^E/K_\infty)/H_\infty, H^q(H_\infty, V_p(E))) \Longrightarrow H^{p+q}(K_\infty^E/K_\infty, V_p(E)),$$

we deduce that $H^i(K_\infty^E/K_\infty, V_p(E)) = 0$ for any $i \geq 0$. $\square$

In the proof of Proposition 6.1, we use a corollary of the following well-known lemma called topological Nakayama's lemma.

Lemma 6.4 (Topological Nakayama's lemma)**.** *Let* $(R, \mathfrak{m})$ *be a Noetherian complete local ring whose residue field is finite, and* M *a compact Hausdorff* R*-module. Suppose that* $\dim_{R/\mathfrak{m}} M/\mathfrak{m}M < \infty$*. Then, the* R*-module* M *is finitely generated.*

Proof. Since M is compact, for any neighborhood U of $0 \in M$, there exists an integer $n \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}^n M \subseteq U$. As M is Hausdorff, we obtain $\bigcap_{n \geq 0} \mathfrak{m}^n M = 0$. By [4, Exercise 7.2], we deduce that M is finitely generated over R if $\dim_{R/\mathfrak{m}} M/\mathfrak{m}M < \infty$. (See [29, Lemma 13.16] for the proof of Lemma 6.4 in the case when $R = \mathbb{Z}_p[\![T]\!]$.) □

Corollary 6.5. *Let* M *be a torsion* $\mathbb{Z}_p$*-module satisfying* $\dim_{\mathbb{F}_p} M[p] < \infty$*. Then, it holds that* M *is a cofinitely generated* $\mathbb{Z}_p$*-module.*

Proof. We regard M as a topological group equipped with the discrete topology. By applying Lemma 6.4 to the Pontrjagin dual of M, we obtain Corollary 6.5. □

Proof of Proposition 6.1. Take any $i \in \{1, 2\}$. Let $j \in \mathbb{Z}$ be any integer satisfying $0 \leq j \leq i$. The group $\mathrm{Gal}(K_\infty^E/K_\infty)$ is topologically finitely presented because it is isomorphic to a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. This implies that $H^j(K_\infty^E/K_\infty, E[p])$ is of finite order. The long exact sequence arising from the short exact sequence

$$0 \longrightarrow E[p] \longrightarrow E[p^\infty] \xrightarrow{p} E[p^\infty] \longrightarrow 0$$

induces the surjective homomorphism

$$H^j(K_\infty^E/K_\infty, E[p]) \longrightarrow\!\!\!\!\!\rightarrow H^j(K_\infty^E/K_\infty, E[p^\infty])[p].$$

In particular, we have

$$\dim_{\mathbb{F}_p} H^j(K_\infty^E/K_\infty, E[p^\infty])[p] \leq \dim_{\mathbb{F}_p} H^j(K_\infty^E/K_\infty, E[p]) < \infty.$$

By Corollary 6.5, it holds that $H^j(K_\infty^E/K_\infty, E[p^\infty])$ is cofinitely generated over $\mathbb{Z}_p$. Moreover, the short exact sequence

$$0 \longrightarrow T_p(E) \longrightarrow V_p(E) \longrightarrow E[p^\infty] \longrightarrow 0$$

induces

$$H^j(K_\infty^E/K_\infty, V_p(E)) \longrightarrow H^j(K_\infty^E/K_\infty, E[p^\infty]) \\ \longrightarrow H^{j+1}(K_\infty^E/K_\infty, T_p(E)).$$

From Lemma 6.3, we have $H^j(K_\infty^E/K_\infty, V_p(E)) = 0$. Since the $\mathbb{Z}_p$-module $H^{j+1}(K_\infty^E/K_\infty, T_p(E))$ does not have a non-trivial divisible $\mathbb{Z}_p$-submodule by [28, (2.1) Proposition], it follows from the above short exact sequence that $\# H^j(K_\infty^E/K_\infty, E[p^\infty]) < \infty$. Take any $n \in \mathbb{Z}_{\geq 0}$. As K_∞/K_n is a pro-cyclic extension, the Hochschild–Serre spectral sequence

$$E_2^{pq} = H^p(K_\infty/K_n, H^q(K_\infty^E/K_\infty, E[p^\infty])) \longrightarrow H^{p+q}(K_\infty^E/K_n, E[p^\infty])$$

implies that

$$\#H^i(K_\infty^E/K_n, E[p^\infty]) \leq \prod_{q \leq i} \{\#H^q(K_\infty^E/K_\infty, E[p^\infty])\} < \infty.$$

Therefore, the sequence $\{\#H^i(K_\infty^E/K_n, E[p^\infty])\}_{n\geq 0}$ is bounded. The exact sequence

$$\frac{H^{i-1}(K_\infty^E/K_n, E[p^\infty])}{p^n} \longrightarrow H^i(K_\infty^E/K_n, E[p^n]) \longrightarrow H^i(K_\infty^E/K_n, E[p^\infty])[p^n]$$

implies that $\{\#H^i(K_\infty^E/K_n, E[p^n])\}_{n\geq 0}$ is bounded. The inflation map

$$H^1(K_n^E/K_n, E[p^n]) \longrightarrow H^1(K_\infty^E/K_n, E[p^n])$$

is injective ([17, Proposition B.2.5]). The assertion of Proposition 6.1 for $i = 1$ follows from this. In order to prove Proposition 6.1 for $i = 2$, by considering the inflation-restriction sequence

$$\begin{aligned} H^1(K_\infty^E/K_n^E, E[p^n])^{\mathrm{Gal}(K_n^E/K_n)} \longrightarrow H^2(K_n^E/K_n, E[p^n]) \\ \longrightarrow H^2(K_\infty^E/K_n, E[p^n]) \end{aligned}$$

([17, Proposition B.2.5 (ii)]), it suffices to show that the order of

$$H^0(K_n, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_n^E), E[p^n]))$$

is bounded. Put $H_{n,m} := H^0(K_n, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_n^E), E[p^m]))$. The short exact sequence

$$0 \longrightarrow E[p] \longrightarrow E[p^n] \longrightarrow E[p^{n-1}] \longrightarrow 0$$

induces an exact sequence

$$0 \longrightarrow H_{n,1} \longrightarrow H_{n,m} \longrightarrow H_{n,m-1}.$$

The lemma below (Lemma 6.6) says that there exists an integer N such that

$$H_{n,1} = H^0(K_n, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_n^E), E[p])) = 0$$

for all $n \geq N$. Thus, we have a sequence of injective homomorphisms

$$H_{n,m} \hookrightarrow H_{n,m-1} \hookrightarrow \cdots \hookrightarrow H_{n,1}.$$

The lemma below again implies $H_{n,1} = 0$. In particular, we have

$$H_{n,n} = H^0(K_n, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_n^E), E[p^n])) = 0$$

for all $n \geq N$. Therefore, the sequence

$$\{\#H^0(K_n, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_n^E), E[p^n]))\}_{n\geq 0}$$

is bounded. $\square$

Lemma 6.6. *Suppose that E satisfies* (C1) *and* (C3)*. There exists an integer N such that*

$$H^0(K_m, \mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_m^E), E[p])) = 0$$

for any $m \in \mathbb{Z}_{\geq N}$.

Proof. The case non-CM. First, suppose that E does not have complex multiplication. The representation $\rho^E \colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$ factors through $\mathrm{Gal}(K_\infty^E/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ and is also denoted by ρ^E. In this non-CM case, Serre's open image theorem ([22, 4.4, Théorème 3], [23, p. IV-11]) implies that the group $\rho^E(\mathrm{Gal}(K_\infty^E/\mathbb{Q}))$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. We can take an integer $N \in \mathbb{Z}_{\geq 1}$ such that $\rho^E(\mathrm{Gal}(K_\infty^E/\mathbb{Q}))$ contains $1 + p^N M_2(\mathbb{Z}_p)$. Take any $m \in \mathbb{Z}_{\geq N}$. As we have

$$\mathrm{Hom}(\mathrm{Gal}(K_\infty^E/K_m^E), E[p])^{G_{K_m}} = \mathrm{Hom}_{\mathrm{Gal}(K_\infty^E/K_m)}(\mathrm{Gal}(K_\infty^E/K_m^E), E[p]),$$

it is enough to show that there is no non-trivial $\mathrm{Gal}(K_\infty^E/K_m)$-equivariant homomorphism $\mathrm{Gal}(K_\infty^E/K_m^E) \to E[p]$. The commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(K_\infty^E/\mathbb{Q}) & \xhookrightarrow{\rho^E} & \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_m^E/\mathbb{Q}) & \hookrightarrow & \mathrm{Aut}(E[p^m]) \simeq \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \end{array}$$

indicates that $\rho^E(\mathrm{Gal}(K_\infty^E/K_m^E)) \subseteq 1 + p^m M_2(\mathbb{Z}_p)$. As we have

$$1 + p^m M_2(\mathbb{Z}_p) \subseteq 1 + p^N M_2(\mathbb{Z}_p) \subseteq \rho^E(\mathrm{Gal}(K_\infty^E/\mathbb{Q})),$$

it holds

$$\rho^E(\mathrm{Gal}(K_\infty^E/K_m^E)) = \rho^E(\mathrm{Gal}(K_\infty^E/\mathbb{Q})) \cap (1 + p^m M_2(\mathbb{Z}_p)) = 1 + p^m M_2(\mathbb{Z}_p).$$

Hence, every group homomorphism $\mathrm{Gal}(K_\infty^E/K_m^E) \to E[p]$ factors through

$$\mathrm{Gal}(K_{m+1}^E/K_m^E) \simeq \mathfrak{gl}_2(\mathbb{F}_p) = M_2(\mathbb{F}_p).$$

The group $G := \rho^E(\mathrm{Gal}(K_\infty^E/K_m)) \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ acts on $M_2(\mathbb{F}_p)$ via the conjugate action, and we have $M_2(\mathbb{F}_p) = \mathbb{F}_p \oplus \mathfrak{sl}_2(\mathbb{F}_p)$ as $\mathbb{F}_p[G]$-modules, where we set

$$\mathfrak{sl}_2(\mathbb{F}_p) := \{A \in M_2(\mathbb{F}_p) \mid \mathrm{Tr}\, A = 0\}.$$

The condition (C1) for E implies that there is no non-trivial G-equivariant homomorphism $\mathbb{F}_p \to E[p]$. Now, we suppose that there is a non-trivial G-equivariant homomorphism $f \colon \mathfrak{sl}_2(\mathbb{F}_p) \to E[p]$, and show that this assumption leads to a contradiction. Put $V := \mathrm{Ker}(f)$. By (C1), we have $\dim_{\mathbb{F}_p} \mathrm{Im}(f) = 2$, and $\dim_{\mathbb{F}_p} V = 1$. Take any non-zero $A \in V$.

- First, let us suppose that A is nilpotent. In this case, there exists a matrix $P \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $A = P\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)P^{-1}$. Since G acts via the conjugate action on the space $V = \mathbb{F}_p A$, for any $B \in G$ there exists $a \in \mathbb{F}_p^\times$ such that $BAB^{-1} = aA$. This implies that if $v \in \mathbb{F}_p^2$ is an eigenvector of A, then Bv is also an eigenvector of A. As a result, the group G is contained in the Borel subgroup $P\begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}P^{-1}$ of $\mathrm{GL}_2(\mathbb{F}_p)$. This implies that G acts on the subspace $W \subseteq \mathfrak{sl}_2(\mathbb{F}_p)$ generated by $P\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)P^{-1}$ and A. In fact, for $Q = P\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)P^{-1} \in G$ with $a, d \in \mathbb{F}_p^\times (ad \neq 0), b \in \mathbb{F}_p$, we have
$$QP\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P^{-1}Q^{-1} = P\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P^{-1} + \frac{-b}{d}A \in W, \text{ and}$$
$$QAQ^{-1} = \frac{a}{d}A \in W.$$
Since $A \in V = \mathrm{Ker}(f)$, the image of W by f becomes a proper G-stable $\mathbb{F}_p$-subspace of $E[p]$. This contradicts (C1).
- Next, suppose that A is not nilpotent. If we assume the matrix $A \in \mathfrak{sl}_2(\mathbb{F}_p)$ has one eigenvalue α, then $0 = \mathrm{Tr}\, A = 2\alpha$. Since p is odd, we have $\alpha = 0$ and A is nilpotent. The matrix A has two distinct eigenvalues $\alpha, -\alpha$ in $\overline{\mathbb{F}}_p$. Since V is stable under the conjugate action of G, for any $B \in G$, there exists some $a \in \mathbb{F}_p^\times$ such that $BAB^{-1} = aA$. For each eigenvalue $\beta \in \{\alpha, -\alpha\}$ of A, we denote by $V_\beta \subseteq \overline{\mathbb{F}_p}^2$ the eigenspace associated with the eigenvalue β. Take any non-zero $v \in V_\alpha$. Note that Bv is also an eigenvector of A, for we have $BA = aAB$. Suppose that $Bv \in V_{-\alpha}$. The group G acts on $\{V_\alpha, V_{-\alpha}\}$ transitively, and G has a subgroup of index 2. This contradicts the fact that G is a pro-p-group. Because of this, we obtain $Bv \in V_\alpha$. This implies that V_α is G-stable. This contradicts (C1).

Hence, there is no non-trivial G-equivariant homomorphism $\mathfrak{sl}_2(\mathbb{F}_p) \to E[p]$, and the assertion for the non-CM case follows from this.

The case CM. Suppose that E has complex multiplication. By the assumption (C3), the ring $\mathrm{End}(E)$ is the maximal order $\mathfrak{o}$ of some imaginary quadratic field $L := \mathbb{Q}(\sqrt{-d})$. As we shall see below, in this case, we can take $N := 1$. Take any $m \in \mathbb{Z}_{\geq 1}$, and put $G := \mathrm{Gal}(K_\infty^E/K_m)$. Let H'_m be the subgroup of $(\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ corresponding to $\mathrm{Gal}(K_\infty^E/L_m)$ by
$$\rho_{\mathfrak{o}}^E\colon\ \mathrm{Gal}(K_\infty^E/L) \longrightarrow \mathrm{Aut}_{\mathfrak{o}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_p(E)) = (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times,$$
where $L_m = K_m L$ (cf. (6.1)). Recall that $L = \mathbb{Q}(\sqrt{-d})$ and K_∞ are linearly disjoint over $\mathbb{Q}$ (Lemma 6.2) and $LK_\infty^E = K_\infty^E$ by Claim 2 in the proof of Lemma 6.3. There exists a lift $\widetilde{c}_m \in G = \mathrm{Gal}(K_\infty^E/K_m)$ of the generator

$c \in \mathrm{Gal}(L/\mathbb{Q})$. Note that G is generated by $\widetilde{c}_m$ and H'_m, and H'_m is a normal subgroup of G of index two.

Claim. *There exists a non-trivial element of H'_m whose order is prime to p.*

Proof of the Claim. Suppose that H'_m has no non-trivial element whose order is prime to p for the contradiction. Then H'_m becomes a pro-p group, and hence there exists a non-zero element $a \in E[p]$ fixed by H'_m (cf. [20, Chapitre IX, §1, Lemme 2]).

- If a is an eigenvector of $\widetilde{c}_m$, then a spans a proper G-stable $\mathbb{F}_p$-subspace of $E[p]$.
- Let us suppose that a is not an eigenvector of $\widetilde{c}_m$. Note that H'_m acts trivially on both a and $\widetilde{c}_m(a)$, for H'_m is a normal subgroup of G. Since $E[p]$ is spanned by $\{a, \widetilde{c}_m(a)\}$ over $\mathbb{F}_p$, the action of H'_m on $E[p]$ is trivial. The action of G on $E[p]$ factors through the cyclic group G/H'_m of order two, especially prime to p, generated by the image of $\widetilde{c}_m$.

In any cases, it contradicts (C1). As a result, there exists a non-trivial element H'_m whose order is prime to p. □

Take any non-trivial element $x \in H'_m$ whose order is prime to p. Since $[K_m : K_1]$ and $[K_m^E : K_1^E]$ are powers of p, we may regard x as an element of $\mathrm{Gal}(K_\infty^E/K_m)$. Since the order of $x \in (\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ is prime to p, we also note that there is no non-trivial element of $E[p]$ fixed by x. However, the element x acts trivially on $\mathrm{Gal}(K_{m+1}^E/K_m^E)$ because $\mathrm{Gal}(K_{m+1}^E/K_m^E)$ is a subquotient of the abelian group H'_m which contains x. This implies that there is no non-trivial G-equivariant homomorphism $\mathrm{Gal}(K_{m+1}^E/K_m^E) \to E[p]$. This completes the proof of Lemma 6.6. □

6.2. The kernel and the cokernel of the restriction maps. The goal of this subsection is to show the following proposition which is a key of the proof of Theorem 1.1.

Proposition 6.7. *Suppose that E satisfies the conditions* (C1), (C2) *and* (C3). *Let*

$$\mathrm{res}_n^{\mathrm{Sel}} \colon \mathrm{Sel}_p(K_n, E[p^n]) \longrightarrow H^0(K_n, \mathrm{Sel}_p(K_n^E, E[p^n])).$$

be the restriction map. Then, the following hold.

(1) *There exists a non-negative integer $\nu_{\mathrm{res}}^{\mathrm{Ker}}$ such that*

$$\#\,\mathrm{Ker}(\mathrm{res}_n^{\mathrm{Sel}}) \leq p^{\nu_{\mathrm{res}}^{\mathrm{Ker}}}$$

for any $n \in \mathbb{Z}_{\geq 0}$.

(2) *There exists a non-negative integer $\nu_{\mathrm{res}}^{\mathrm{Coker}}$ such that*

$$\#\,\mathrm{Coker}(\mathrm{res}_n^{\mathrm{Sel}}) \leq p^{\nu_{\mathrm{res}}^{\mathrm{Coker}}}$$

for any $n \in \mathbb{Z}_{\geq 0}$.

In order to prove Proposition 6.7, we need the following theorem:

Theorem 6.8. *Let ℓ be a prime number, and $F/\mathbb{Q}_\ell$ a finite extension. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{F}$, and regard μ_{p^∞} as a subset of $\overline{F}$. If ℓ is distinct from p, suppose that $E_{F(\mu_{p^n})}$ has additive reduction for any $n \geq 1$. Then the sequence*

$$\{\#E(F(\mu_{p^n}))[p^\infty]\}_{n\geq 0}$$

is bounded.

Proof. For the case $\ell = p$, this follows from Imai's result [7]. Consider the case $\ell \neq p$. For every $n \geq 1$, put $F_n := F(\mu_{p^n})$ and we denote by κ_n the residue field of F_n. Following the notation in [24, Chapter VII, Section 2], we denote by $\pi\colon E_{F_n}(F_n) \to \widetilde{E}_{F_n}(\kappa_n)$ the reduction map. We define $\widetilde{E}_{F_n,\mathrm{ns}}$ to be the set of non-singular points in the reduction $\widetilde{E}_{F_n}$ and put $E_{F_n,0}(F_n) := \pi^{-1}(\widetilde{E}_{F_n,\mathrm{ns}}(\kappa_n))$ the group of rational points whose reduction is non-singular. The reduction map π induces a short exact sequence

$$0 \longrightarrow E_{F_n,1}(F_n) \longrightarrow E_{F_n,0}(F_n) \longrightarrow \widetilde{E}_{F_n,\mathrm{ns}}(\kappa_n) \longrightarrow 0, \tag{6.4}$$

where the left term $E_{F_n,1}(F_n)$ is defined by the exactness ([24, Chapter VII, Proposition 2.1]). From the assumption that E_{F_n} has additive reduction, the order of the quotient $E_{F_n}(F_n)/E_{F_n,0}(F_n)$ is at most 4 ([24, Chapter VII, Theorem 6.1]). Hence, it is enough to show that $\{\#E_{F_n,0}(F_n)[p^\infty]\}_{n\geq 0}$ is bounded. The above sequence (6.4) induces

$$0 \longrightarrow E_{F_n,1}(F_n)[p^m] \longrightarrow E_{F_n,0}[p^m] \longrightarrow \widetilde{E}_{F_n,\mathrm{ns}}(\kappa_n)[p^m] \longrightarrow \frac{E_{F_n,1}(F_n)}{p^m E_{F_n,1}(F_n)}$$

for any $m \geq 1$. Since $E_{F_n,1}(F_n)$ is written by the group associated to the formal group law and has no non-trivial points of order p^m ([24, Chapter VII, Proposition 3.1]), we obtain $E_{F_n,1}(F_n)[p^m] = E_{F_n,1}(F_n)/p^m E_{F_n,1}(F_n) = 0$. From the assumption that E_{F_n} has additive reduction again, it follows that $\widetilde{E}_{F_n,\mathrm{ns}}(\kappa_n)$ is isomorphic to the additive group κ_n ([24, Chapter III, Exercise 3.5]) so that $\widetilde{E}_{F_n,\mathrm{ns}}(\kappa_n)[p^m] = 0$. The assertion follows from this. □

Lemma 6.9. *Suppose that E has potentially multiplicative reduction at a prime number ℓ (distinct from p). Then, there exists an integer N_ℓ such that for any $n \in \mathbb{Z}_{\geq N_\ell}$ and any place w of K_n^E above ℓ, we have $p^n E(K_{n,w}^E)[p^\infty] = 0$.*

Proof. Suppose that E has potentially multiplicative reduction at a prime ℓ.

Claim. *There exists a finite Galois extension field L of $\mathbb{Q}$ contained in K_∞^E satisfying the following conditions:*

(a) *The elliptic curve E_L has split multiplicative reduction at every place of L above ℓ.*

(b) *Every place of L above ℓ is inert in $L_\infty := L(\mu_{p^\infty})/L$.*
(c) *There exists $N \in \mathbb{Z}_{\geq 1}$ such that $K_N \subseteq L \subseteq K_N^E$.*

Proof of the Claim. By Lemma 4.3, the base change $E_{K_1^E}$ has split multiplicative reduction at every place of K_1^E above ℓ. Take any integer $N \in \mathbb{Z}_{>0}$ satisfying $\mu_{p^N} \not\subseteq \mathbb{Q}_\ell(E(\overline{\mathbb{Q}}_\ell)[p])$, and put $L := K_1^E(\mu_{p^N})$. As $\mu_{p^N} \subset K_N^E$, the conditions (a) and (c) are satisfied. Note that $L_\infty := K_1^E(\mu_{p^\infty})/K_1^E$ is a (cyclotomic) $\mathbb{Z}_p$-extension, and our choice of N implies that the group $\mathrm{Gal}(L_\infty/L)$ becomes a proper subgroup of the decomposition group of $\mathrm{Gal}(L_\infty/K_1^E)$ at any place v of K_1^E above ℓ. The condition (b) is satisfied. $\square$

In order to prove Lemma 6.9, it suffices to show that there exists an integer $N' \in \mathbb{Z}_{>0}$ such that for any $n \in \mathbb{Z}_{\geq N'}$ and any place w of K_n^E above ℓ, it holds that $E(K_{n,w}^E)[p^\infty] = E[p^n]$. For the field L and $N \in \mathbb{Z}_{\geq 1}$ given in the above claim, take any $n \in \mathbb{Z}_{\geq N}$ and any place w of K_n^E above ℓ. Let u be the place of L below w. Since E_{L_u} has split multiplicative reduction, we have a G_{L_u}-invariant isomorphism

$$E(\overline{L}_u) \xrightarrow{\simeq} \overline{L}_u^\times/q^{\mathbb{Z}} \tag{6.5}$$

for some $q \in L_u$ with $\mathrm{ord}_u(q) > 0$. Recall that every place of L above ℓ is inert in L_∞/L. By the isomorphism (6.5), if $n \geq N_0 := N + \mathrm{ord}_u(q)$, then we have $E(K_{n,w}^E)[p^n] = E[p^n]$, and $E(K_{n,w}^{E,\mathrm{ur}})[p^\infty] \simeq \mu_{p^\infty} \times q^{p^{-n}\mathbb{Z}}/q^{\mathbb{Z}}$. $\square$

Lemma 6.10 ([1, Example 3.11])**.** *For any prime number ℓ distinct from p and any finite extension $F/\mathbb{Q}_\ell$, it holds that $H^1_f(F, E[p^\infty]) = 0$.*

For each $n \in \mathbb{Z}_{\geq 0}$, we denote by $\Sigma_{n,p}$ the set of all the finite places v of K_n above p, and $\Sigma_{n,\mathrm{bad}}$ by the set of all the finite places v of K_n where $E_{K_{n,v}}$ has bad reduction. We put $\Sigma_n := \Sigma_{n,p} \cup \Sigma_{n,\mathrm{bad}}$ and define Σ_n^0 to be the subset of $\Sigma_{n,\mathrm{bad}}$ consisting of all the places v which lies below some $w \in \Sigma_m$ for every $m \in \mathbb{Z}_{\geq n}$. Namely, we have

$$\Sigma_n^0 = \left\{ v \in \Sigma_{n,\mathrm{bad}} \;\middle|\; \begin{array}{l} \text{for any } m \geq 0, \text{ the elliptic curve} \\ E_{K_m} \text{ has bad reduction for some } w \mid v \end{array} \right\}. \tag{6.6}$$

Since the elliptic curve E has good reduction at p, the set of places $\Sigma_{n,p}$ is not contained in Σ_n^0.

Proof of Proposition 6.7. In this proof, once we fix $n \in \mathbb{Z}_{\geq 0}$ and simplify the notation $H^i(F'/F, E[p^n]) = H^i(F'/F)$ for an extension F'/F. We denote by K_{n,Σ_n} the maximal unramified extension of K_n outside Σ_n. As noted in Remark 5.5, the fine Selmer group $\mathrm{Sel}_p(K_n, E[p^n])$ is a subgroup of $H^1(K_{n,\Sigma_n}/K_n)$. The Hochschild–Serre spectral sequence gives the following commutative diagram with exact rows:

$$\begin{tikzcd}
\mathrm{Ker}(\mathrm{res}_n^{\mathrm{loc}}) \arrow[r, hook] & \mathrm{Coker}(\iota_n) \arrow[r, "\mathrm{res}_n^{\mathrm{loc}}"] & \mathrm{Coker}(\iota_n^E) & \\
H^1(K_n^E/K_n) \arrow[u] \arrow[r, hook, "\mathrm{Inf}_n"] & H^1(K_{n,\Sigma_n}/K_n) \arrow[u, two heads] \arrow[r, "\mathrm{res}_n"] & H^1(K_{n,\Sigma_n}/K_n^E)^{G_{K_n}} \arrow[u, two heads] \arrow[r] & H^2(K_n^E/K_n) \\
\mathrm{Ker}(\mathrm{res}_n^{\mathrm{Sel}}) \arrow[u, hook] \arrow[r, hook] & \mathrm{Sel}_p(K_n, E[p^n]) \arrow[u, hook, "\iota_n"] \arrow[r, "\mathrm{res}_n^{\mathrm{Sel}}"] & \mathrm{Sel}_p(K_n^E, E[p^n])^{G_{K_n}} \arrow[u, hook, "\iota_n^E"] \arrow[r] & \mathrm{Coker}(\mathrm{res}_n^{\mathrm{Sel}}). \arrow[u]
\end{tikzcd}$$

The snake lemma induces the exact sequence

$$\begin{aligned}(6.7)\quad 0 \longrightarrow \mathrm{Ker}(\mathrm{res}_n^{\mathrm{Sel}}) \longrightarrow H^1(K_n^E/K_n) \longrightarrow \mathrm{Ker}(\mathrm{res}_n^{\mathrm{loc}}) \\ \xrightarrow{\delta} \mathrm{Coker}(\mathrm{res}_n^{\mathrm{Sel}}) \longrightarrow H^2(K_n^E/K_n).\end{aligned}$$

By Proposition 6.1, the order of $H^1(K_n^E/K_n) = H^1(K_n^E/K_n, E[p^n])$ is bounded independently of n, and so is the kernel $\mathrm{Ker}(\mathrm{res}_n^{\mathrm{Sel}})$. We obtain the assertion (1).

Let us investigate the cokernel of $\mathrm{res}_n^{\mathrm{Sel}}$. By Proposition 6.1, the group $H^2(K_n^E/K_n) = H^2(K_n^E/K_n, E[p^n])$ is finite and its order is bounded independently of n. From the exact sequence (6.7), to show the assertion (2) it is enough to give a bound for $\{\#\,\mathrm{Ker}(\mathrm{res}_n^{\mathrm{loc}})\}_{n\geq 0}$.

For each finite place v in K_n, we define restriction maps

$$\mathrm{res}_{n,v}^{\mathrm{loc}} : H^1(K_{n,v}, E[p^n]) \longrightarrow H^0\left(K_n, \prod_{w|v} H^1(K_{n,w}^E, E[p^n])\right),$$

$$\mathrm{res}_{n,v}^{f} : H_f^1(K_{n,v}, E[p^n]) \longrightarrow H^0\left(K_n, \prod_{w|v} H_f^1(K_{n,w}^E, E[p^n])\right), \quad \text{and}$$

$$\overline{\mathrm{res}}_{n,v}^{\mathrm{loc}} : \frac{H^1(K_{n,v}, E[p^n])}{H_f^1(K_{n,v}, E[p^n])} \longrightarrow H^0\left(K_n, \prod_{w|v} \frac{H^1(K_{n,w}^E, E[p^n])}{H_f^1(K_{n,w}^E, E[p^n])}\right).$$

These maps induce the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & H_f^1(K_{n,v}) \arrow[r] \arrow[d, "\mathrm{res}_{n,v}^{f}"] & H^1(K_{n,v}) \arrow[r] \arrow[d, "\mathrm{res}_{n,v}^{\mathrm{loc}}"] & \frac{H^1(K_{n,v})}{H_f^1(K_{n,v})} \arrow[r] \arrow[d, "\overline{\mathrm{res}}_{n,v}^{\mathrm{loc}}"] & 0 \\
0 \arrow[r] & \left(\prod_{w|v} H_f^1(K_{n,w}^E))\right)^{G_{K_n}} \arrow[r] & \left(\prod_{w|v} H^1(K_{n,w}^E)\right)^{G_{K_n}} \arrow[r] & \left(\prod_{w|v} \frac{H^1(K_{n,w}^E)}{H_f^1(K_{n,w}^E)}\right)^{G_{K_n}}. &
\end{tikzcd}$$

By applying the snake lemma to the above diagram, there is an exact sequence

$$\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v}) \longrightarrow \mathrm{Ker}(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v}) \longrightarrow \mathrm{Coker}(\mathrm{res}^{f}_{n,v}). \tag{6.8}$$

By the definition of the fine Selmer groups (Definition 5.3), we obtain the commutative diagram

$$\begin{tikzcd}
\mathrm{Coker}(\iota_n) \arrow[r, hook] \arrow[d, "\mathrm{res}^{\mathrm{loc}}_n"] & \prod_{v\mid p} H^1(K_{n,v}) \times \prod_{v\nmid p} \frac{H^1(K_{n,v})}{H^1_f(K_{n,v})} \arrow[d, "(\mathrm{res}^{\mathrm{loc}}_{n,v})_{v\mid p}\times(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v})_{v\nmid p}"] \\
\mathrm{Coker}(\iota^E_n) \arrow[r, hook] & \prod_{v\mid p}\left(\prod_{w\mid v} H^1(K^E_{n,w})\right)^{G_{K_n}} \times \prod_{v\nmid p}\left(\prod_{w\mid v} \frac{H^1(K^E_{n,w})}{H^1_f(K^E_{n,w})}\right)^{G_{K_n}}.
\end{tikzcd}$$

This diagram induces an injective homomorphism

$$\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n}) \hookrightarrow \prod_{v\mid p} \mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v}) \times \prod_{v\nmid p} \mathrm{Ker}(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v}). \tag{6.9}$$

When E_{K_n} has good reduction at a finite place $v\nmid p$ of K_n, then the Tate module $T_\ell(E)$ for the prime number ℓ with $v \mid \ell$ is unramified ([24, Chapter VII, Theorem 7.1]). We have $H^1_f(K_{n,v}, E[p^n]) = H^1_{\mathrm{ur}}(K_{n,v}, E[p^n])$ and $H^1_f(K^E_{n,w}, E[p^n]) = H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])$ ([17, Lemma 1.3.8 (ii)]). Moreover, the extension $K^E_{n,w}/K_{n,v}$ is unramified for any $w \mid v$ as $E[p^n]$ is unramified. From the definition of the unramified cohomology (cf. Notation), we have a commutative diagram

$$\begin{tikzcd}
\frac{H^1(K_{n,v}, E[p^n])}{H^1_{\mathrm{ur}}(K_{n,v}, E[p^n])} \arrow[r, "\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v}"] \arrow[d, hook] & \prod_{w\mid v}\left(\frac{H^1(K^E_{n,w}, E[p^n])}{H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])}\right)^{G_{K_n}} \arrow[d, hook] \\
H^1(K^{\mathrm{ur}}_{n,v}, E[p^n]) \arrow[r, "\mathrm{res}^{\mathrm{ur}}_{n,v}"] & \prod_{w\mid v} H^1(K^{E,\mathrm{ur}}_{n,w}, E[p^n])^{G_{K_n}}.
\end{tikzcd}$$

From the inflation-restriction sequence ([17, Proposition B.2.5 (i)]), the kernel of the bottom horizontal map $\mathrm{res}^{\mathrm{ur}}_{n,v}$ equals to

$$\bigcap_{w\mid v} H^1(K^{E,\mathrm{ur}}_{n,w}/K^{\mathrm{ur}}_{n,v}, E[p^n]^{G_{K^{\mathrm{ur}}_{n,v}}}) = 0$$

and the map $\mathrm{res}^{\mathrm{ur}}_{n,v}$ is injective. In particular, we have $\mathrm{Ker}(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v}) = 0$ for any finite place $v \notin \Sigma_n$. This implies that the order of $\mathrm{Ker}(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v})$ is bounded independently of n for the case $v \nmid p$ and $v \notin \Sigma^0_n$. From (6.9), in order to prove Proposition 6.7 (2), it is left to show the following assertions.

- For $v \mid p$, the sequence $\{\#\,\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v})\}_{n\geq 0}$ is bounded.
- For $v \nmid p$, and $v \in \Sigma^0_n$, the sequence $\{\#\,\mathrm{Ker}(\overline{\mathrm{res}}^{\mathrm{loc}}_{n,v})\}_{n\geq 0}$ is bounded.

By the exact sequence (6.8), these assertions follow from Lemma 6.11 below. □

By definition (cf. (6.6)), we have

$$\Sigma_0^0 = \left\{ \ell\colon \text{prime number} \;\middle|\; \begin{array}{l} \text{for any } m \geq 0, \text{ the elliptic curve} \\ E_{K_m} \text{ has bad reduction at a place above } \ell \end{array} \right\}.$$

We are assuming E has good reduction at p, so that $p \notin \Sigma_0^0$.

Lemma 6.11.

(1) *For any prime number $\ell \in \Sigma_0^0$ (distinct from p), the set*

$$\left\{ \# \operatorname{Ker}(\operatorname{res}_{n,v}^{\mathrm{loc}}) \;\middle|\; n \geq 0, v \mid \ell \right\}$$

is bounded.

(2) *For the fixed prime p, the set*

$$\left\{ \# \operatorname{Ker}(\operatorname{res}_{n,v}^{\mathrm{loc}}) \;\middle|\; n \geq 0, v \mid p \right\}$$

is bounded.

(3) *For any prime number $\ell \in \Sigma_0^0$ (distinct from p), the set*

$$\left\{ \# \operatorname{Coker}(\operatorname{res}_{n,v}^{f}) \;\middle|\; n \geq 0, v \mid \ell \right\}$$

is bounded.

Proof. First, we prove the following claim.

Claim 1. *There exists a finite Galois extension field L of $\mathbb{Q}$ contained in $K_\infty^E = \mathbb{Q}(E[p^\infty])$ satisfying the following conditions.*

(a) *The elliptic curve E_L has semistable reduction everywhere.*

(b) *The elliptic curve E_L has split multiplicative reduction at every place u of L above a prime number q where E has potentially multiplicative reduction.*

(c) *Every place of L above every $\ell \in \Sigma_0^0$ is inert in $L_\infty := L(\mu_{p^\infty})/L$.*

(d) *There exists an integer $N \in \mathbb{Z}_{\geq 0}$ such that $K_N \subseteq L \subseteq K_N^E$.*

Proof of Claim 1. Let q_0 be a prime number where E has potentially good additive reduction. Since q_0 is distinct from p, the order of the image of $G_{\mathbb{Q}_{q_0}^{\mathrm{ur}}}$ in $\operatorname{Aut}_{\mathbb{Z}_p}(T_p(E))$ is finite ([24, Chapter VII, Theorem 7.1]). This implies that there exists an intermediate field $F_{\mathrm{pg}}^{(q_0)}$ of $K_\infty^E/\mathbb{Q}$ such that $F_{\mathrm{pg}}^{(q_0)}/\mathbb{Q}$ is a finite Galois extension, and $E_{F_{\mathrm{pg}}^{(q_0)}}$ has good reduction at every place above q_0. Let F_{pg} be the composite of the fields $F_{\mathrm{pg}}^{(q)}$ where q runs all the prime numbers where E has potentially good additive reduction. By Lemma 4.3, the composite field $L := F_{\mathrm{pg}} K_1^E$ satisfies the conditions (a) and (b). Moreover, take a sufficiently large $N \in \mathbb{Z}_{>0}$, and replace L with $L(\mu_{p^N})$, the additional conditions (c) and (d) follow from the similar arguments in the proof of Lemma 6.9. Note that $L = F_{\mathrm{pg}}K_1^E(\mu_{p^N})$ is a finite Galois extension field of $\mathbb{Q}$ contained in K_∞^E. $\square$

Put $L_n := L(\mu_{p^n})$ for each $n \geq 1$. Take any prime number $\ell \in \Sigma_0^0$. Fix a place w_∞ of K_∞^E above ℓ. For any $m \in \mathbb{Z}_{\geq N}$, denote by w_m the place of K_m^E below w_∞ and by u_m the place of L_m below w_∞ respectively.

Let us prove the assertion (1). Take any $n \in \mathbb{Z}_{\geq N}$, and let $v = v_n$ be the place of K_n below w_∞. For the fixed place w_n, by identifying $G_{K_{n,v}}$ with the decomposition subgroup of G_{K_n} at v, we consider $H^1(K_{n,w_n}^E, E[p^n])$ as an $G_{K_{n,v}}$-module and $\prod_{w|v} H^1(K_{n,w}^E, E[p^n])$ is isomorphic to the induced module $\mathrm{Ind}_{G_{K_n}}^{G_{K_{n,v}}}(H^1(K_{n,w_n}^E, E[p^n]))$. Shapiro's lemma gives an isomorphism

$$H^0\left(K_n, \prod_{w|v} H^1(K_{n,w}^E, E[p^n])\right) \simeq H^0\left(K_{n,v}, H^1(K_{n,w_n}^E, E[p^n])\right) \tag{6.10}$$

(cf. [13, (1.6.4) Proposition]). By the Hochschild–Serre exact sequence ([17, Proposition B.2.5 (ii)]), we obtain the following commutative diagram whose rows are exact:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}}) \arrow[r] \arrow[d] & H^1(K_{n,v}) \arrow[r, "\mathrm{res}_{n,v}^{\mathrm{loc}}"] \arrow[d, equal] & \left(\prod_{w|v} H^1(K_{n,w}^E)\right)^{G_{K_n}} \arrow[d, "(6.10)"', "\simeq"] \\
0 \arrow[r] & H^1(K_{n,w_n}^E/K_{n,v}) \arrow[r] & H^1(K_{n,v}) \arrow[r] & H^1(K_{n,w_n}^E)^{G_{K_{n,v}}}.
\end{tikzcd}$$

Here, we put $H^1(F'/F, E[p^n]) = H^1(F'/F)$ for an extension F'/F. It holds that

$$\mathrm{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}}) \xrightarrow{\simeq} H^1(K_{n,w_n}^E/K_{n,v}, E[p^n]). \tag{6.11}$$

The order of $\mathrm{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}})$ depends only on the prime number ℓ and the positive integer n (in particular, it is independent of the choice of the place w_∞ of K_∞^E above the fixed prime number ℓ). For any intermediate field M of $K_{n,w_n}^E/K_{n,v}$ which is Galois over $K_{n,v}$, we have an exact sequence

$$0 \longrightarrow Y_n(M) \longrightarrow \mathrm{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}}) \longrightarrow Z_n(M),$$

where we put

$$\begin{aligned} Y_n(M) &:= H^1(M/K_{n,v}, E(M)[p^n]), \text{ and} \\ Z_n(M) &:= H^0(K_{n,v}, H^1(K_{n,w_n}^E/M, E[p^n])). \end{aligned}$$

First, let us study the cases when $\ell \neq p$. Recall that $E_{L_{n,u_n}}$ has good or split multiplicative reduction and $E_{K_{n,v}}$ has bad reduction from the very definition of Σ_0^0.

The case: Potentially good reduction with $\ell \neq p$. Suppose that $\ell \neq p$, and E has potentially good reduction at ℓ. Let M_n be the maximal subfield of K^E_{n,w_n} which is unramified above $K_{n,v}$. As the extension $M_n/K_{n,v}$ is cyclic, we have

$$\begin{aligned} H^1(M_n/K_{n,v}, E(M_n)[p^n]) &\simeq \widehat{H}^{-1}(M_n/K_{n,v}, E(M_n)[p^n]) \\ &= \frac{\operatorname{Ker}\left(N_{M_n/K_{n,v}} \colon E(M_n)[p^n] \to E(K_{n,v})[p^n]\right)}{\langle \operatorname{Forb}_v -1\rangle}, \end{aligned}$$

where $\widehat{H}^*$ stands for the Tate cohomology group, $N_{M_n/K_{n,v}}$ is the norm map and Forb_v is the Frobenius automorphism at v which is a generator of the cyclic group $\operatorname{Gal}(M_n/K_{n,v})$ (cf. [20, Chapitre VIII, §4]). There are (in)equalities below:

$$\begin{aligned} \#Y_n(M_n) &= \#H^1(M_n/K_{n,v}, E(M_n)[p^n]) \\ &= \#\widehat{H}^{-1}(M_n/K_{n,v}, E(M_n)[p^n]) \\ &\leq \#\left(\frac{E(M_n)[p^n]}{\langle \operatorname{Forb}_v -1\rangle}\right) \\ &= \#(E(M_n)[p^n])[\operatorname{Forb}_v -1] \\ &= \#E(K_{n,v})[p^n] \\ &\leq \#E(K_{n,v})[p^\infty]. \end{aligned}$$

From Theorem 6.8, the sequence $\{\#Y_n(M_n)\}_{n\geq 0}$ is bounded. Let us study $Z_n(M_n)$. Note that $K^E_{n,w_n}/L_{n,u_n}$ is unramified because $E_{L_{n,u_n}}$ has good reduction. Since $K^E_{n,w_n}/M_n$ is totally ramified, we have

$$[K^E_{n,w_n} : M_n] = [L_{n,u_n} : L_{n,u_n} \cap M_n] \leq [L_{n,u_n} : K_{n,v}] \leq [L : K_N].$$

This implies that

$$\sup_{n\geq N} \#Z_n(M_n) \leq \sup_{n\geq N} \#H^1(K^E_{n,w_n}/M_n, E[p^n]) < \infty.$$

Consequently, the set $\{\# \operatorname{Ker}(\operatorname{res}^{\mathrm{loc}}_{n,v}) | n \geq 0, v \mid \ell\}$ is bounded.

The case: Potentially multiplicative reduction with $\ell \neq p$. Suppose that $\ell \neq p$, and E has potentially multiplicative reduction at ℓ. Put $Y_n := Y_n(L_{n,u_n})$ and $Z_n := Z_n(L_{n,u_n})$. Let $u := u_N$ be the place of L below u_n. The elliptic curve E_{L_u} is isomorphic to a Tate curve $\mathbb{G}_m/q_u^{\mathbb{Z}}$, and in particular, we have a G_{L_u}-equivariant isomorphism

$$E[p^\infty] \simeq \mu_{p^\infty} \times q_u^{\mathbb{Z}[p^{-1}]}/q_u^{\mathbb{Z}}. \tag{6.12}$$

This implies that $K^E_{\infty,w_\infty}/L_{\infty,u_\infty}$ is a totally ramified cyclic extension, where u_∞ is the place of L_∞ below w_∞. Fix a topological generator $\tau \in$

$\mathrm{Gal}(K^E_{\infty,w_\infty}/L_{\infty,u_\infty})$. Since $L_{\infty,u_\infty}/L_u$ is unramified, the homomorphism

$$\mathrm{Gal}(K^E_{\infty,w_\infty}/L_{\infty,u_\infty}) \longrightarrow \mathrm{Gal}(K^E_{n,w_n}/L_{n,u_n});\ \sigma \longmapsto \sigma|_{K^E_{n,w_n}}$$

is surjective. Firstly, we show that $\{\# Y_n\}_{n\geq 0}$ is bounded. We define

$$E'_n := \left(E(K^{E,\mathrm{ur}}_{n,w_n})[p^\infty]_{\mathrm{div}}\right)[p^n].$$

The isomorphism (6.12) implies that E'_n is isomorphic to μ_{p^n} as a $\mathbb{Z}_p[G_{L_u}]$-module. Note that E'_n is $G_{K_{n,v}}$-stable as $K^{E,\mathrm{ur}}_{n,w_n}/K_{n,v}$ is a Galois extension. We obtain an exact sequence

$$Y'_n \longrightarrow Y_n \longrightarrow Y''_n, \tag{6.13}$$

where we put

$$Y'_n := H^1(L_{n,u_n}/K_{n,v}, E'_n), \quad \text{and}$$
$$Y''_n := H^1(L_{n,u_n}/K_{n,v}, E(L_{n,u_n})[p^n]/E'_n).$$

Let us study Y''_n. Note that τ acts on $T_p(E)$ non-trivially and unipotently. Putting $\nu_\tau := \mathrm{ord}_p(\#(T_p(E)/\langle \tau-1\rangle)_{\mathrm{tor}})$, we have

$$\#(E(L_{n,u_n})[p^n]/E'_n) \leq \#(E(L_{\infty,u_\infty})[p^\infty]/E'_\infty) = p^{\nu_\tau}.$$

It follows that the sequence $\{\# Y''_n\}_{n\geq 0}$ is bounded, because of the inequality $[L_{n,u_n} : K_{n,v}] \leq [L:\mathbb{Q}]$.

Let us consider Y'_n. Recall that we have $E'_n \simeq \mu_{p^n}$ as $\mathbb{Z}_p[G_{L_u}]$-modules. We define H_n to be the maximal subgroup of $\mathrm{Gal}(L_{n,u_n}/K_{n,v})$ acting trivially on E'_n, and L'_n the maximal subfield of L_{n,u_n} fixed by H_n. Now, we consider an exact sequence

$$0 \longrightarrow H^1(L'_n/K_{n,v}, E'_n) \longrightarrow Y'_n \longrightarrow H^1(L_{n,u_n}/L'_n, E'_n).$$

By (C2) for E, we know $H^0(K_{n,v}, E'_n) = 0$ (Lemma 4.4). Since $L'_n/K_{n,v}$ is cyclic, we have

$$H^1(L'_n/K_{n,v}, E'_n) \simeq \widehat{H}^{-1}(L'_n/K_{n,v}, E'_n)$$

(cf. [20, Chapitre VIII, §4]). For E'_n is finite, its Herbrand quotient is trivial so that

$$\#\widehat{H}^{-1}(L'_n/K_{n,v}, E'_n) = \#\widehat{H}^0(L'_n/K_{n,v}, E'_n)$$

([20, Chapitre VIII, §4, Proposition 8]). Therefore, we have

$$\# H^1(L'_n/K_{n,v}, E'_n) = \#\widehat{H}^0(L'_n/K_{n,v}, E'_n) \leq \# H^0(K_{n,v}, E'_n) = 1.$$

Since $L_{n,u_n}/L'_n$ is a cyclic extension whose order is at most $[L:\mathbb{Q}]$, we have

$$\# H^1(L_{n,u_n}/L'_n, E'_n) = \#\operatorname{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(L_{n,u_n}/L'_n), \mathbb{Z}/p^n\mathbb{Z}) \leq [L:\mathbb{Q}].$$

The sequence $\{\# Y'_n\}_{n\geq 0}$ is bounded. This implies that $\{\# Y_n\}_{n\geq 0}$ is bounded by (6.13).

Secondly, let us show that $\{\#Z_n\}_{n\geq 0}$ is bounded. Recall that $Z_n = Z_n(L_{n,u_n}) = H^0(K_{n,v}, H^1(K^E_{n,w_n}/L_{n,u_n}, E[p^n]))$. We have an exact sequence

$$\begin{aligned}(6.14)\quad & H^0(L_{n,u_n}, E[p^n]/E'_n) \xrightarrow{\delta_n} H^1(K^E_{n,w_n}/L_{n,u_n}, E'_n) \\ & \longrightarrow H^1(K^E_{n,w_n}/L_{n,u_n}, E[p^n]) \longrightarrow H^1(K^E_{n,w_n}/L_{n,u_n}, E[p^n]/E'_n).\end{aligned}$$

We put

$$\begin{aligned} Z'_n &:= H^0(K_{n,v}, \mathrm{Coker}(\delta_n)), \text{ and} \\ Z''_n &:= H^0(K_{n,v}, H^1(K^E_{n,w_n}/L_{n,u_n}, E[p^n]/E'_n)).\end{aligned}$$

In order to prove that $\{\#Z_n\}_{n\geq 0}$ is bounded, considering the exact sequence (6.14) it suffices to show that

$$\{\#Z'_n\}_{n\geq 0} \quad \text{and} \quad \{\#Z''_n\}_{n\geq 0}$$

are bounded. Let us show that the sequence $\{\#Z'_n\}_{n\geq 0}$ is bounded. The extension $K^E_{n,w_n}/L_{n,u_n}$ is non-trivial and totally ramified. The Galois group $\mathrm{Gal}(K^E_{n,w_n}/L_{n,u_n})$ acts trivially on E'_n. By the Weil pairing, we have $E'_n \simeq \mathrm{Hom}\,(E[p^n]/E'_n, \mu_{p^n})$. The Galois group $\mathrm{Gal}(K^E_{n,w_n}/L_{n,u_n})$ also acts trivially on $E[p^n]/E'_n$. It holds that

$$H^0(L_{n,u_n}, E[p^n]/E'_n) = E[p^n]/E'_n \simeq \mathbb{Z}/p^n.$$

Put $\tau_n := \tau|_{K^E_{n,w_n}}$. Note that τ_n generates $\mathrm{Gal}(K^E_{n,w_n}/L_{n,u_n})$. We have an isomorphism

$$H^1(K^E_{n,w_n}/L_{n,u_n}, E'_n) = \mathrm{Hom}(\mathrm{Gal}(K^E_{n,w_n}/L_{n,u_n}), E'_n) \xrightarrow{\simeq} E'_n[p^{M_n}]$$

given by the evaluation at τ_n, where $M_n := \mathrm{ord}_p([K^E_{n,w_n} : L_{n,u_n}])$. We denote by $\overline{E}'_n$ the image of E'_n in $E[p^n]/\langle \tau - 1\rangle$. Its order is bounded as $\#\overline{E}'_n \leq p^{\nu_\tau}$. By definition, the coboundary map δ_n is given by

$$\delta_n \colon E[p^n]/E'_n \longrightarrow E'_n[p^{M_n}];\ (P \bmod E'_n) \longmapsto (\tau - 1)P.$$

We obtain

$$\#Z'_n \leq \#\,\mathrm{Coker}(\delta_n) \leq \#\overline{E}'_n \leq p^{\nu_\tau}.$$

Finally, let us show that $\{\#Z''_n\}_{n\geq 0}$ is bounded. Note that we have an isomorphism

$$H^1(K^E_{n,w_n}/L_{n,u_n}, E[p^n]/E'_n) \xrightarrow{\simeq} \frac{E[p^n]/E'_n}{\langle \tau - 1\rangle} = E[p^n]/E'_n.$$

By (C2) for E and Lemma 4.4, it holds that $Z''_n = H^0(K_{n,v}, E[p^n]/E'_n) = 0$. This implies that $\{\#Z_n\}_{n\geq 0}$ is bounded. Hence, we deduce that $\{\#\,\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v}) | n \geq 0, v \mid \ell\}$ is bounded.

Now, suppose that $\ell \neq p$, and let us show the assertion (3) of Lemma 6.11. Again, take any $n \in \mathbb{Z}_{\geq N}$, and let $v = v_n$ be the place of K_n below w_∞. The order of $\mathrm{Coker}(\mathrm{res}^f_{n,v})$ depends only on ℓ and n. By the short exact sequence $0 \to E[p^n] \to E[p^\infty] \xrightarrow{\times p^n} E[p^\infty] \to 0$, there is a short exact sequence

$$0 \longrightarrow A_n^0 \xrightarrow{\delta} H^1(K_{n,v}, E[p^n]) \xrightarrow{\iota_{n,v}} H^1(K_{n,v}, E[p^\infty])[p^n],$$

where $A_n^0 := E(K_{n,v})[p^\infty] \otimes_{\mathbb{Z}_p} (\mathbb{Z}/p^n\mathbb{Z})$. Recall that $H^1_f(K_{n,v}, E[p^n])$ is defined to be the inverse image of $H^1_f(K_{n,v}, E[p^\infty])$ by $\iota_{n,v}$ (cf. (5.1)). Thus, the map $\iota_{n,v}$ induces the short exact sequence $0 \to A_n^0 \to B_n^0 \to C_n^0$, where

$$B_n^0 := H^1_f(K_{n,v}, E[p^n]), \text{ and } C_n^0 := H^1_f(K_{n,v}, E[p^\infty])[p^n].$$

Furthermore, we obtain a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A_n^0 \arrow[r] \arrow[d, "a_n"] & B_n^0 \arrow[r] \arrow[d, "b_n"] & C_n^0 \arrow[d, "c_n"] \\ 0 \arrow[r] & A_n^1 \arrow[r] & B_n^1 \arrow[r] & C_n^1 \end{tikzcd}$$

whose rows are exact, where

$$A_n^1 := H^0\left(K_n, \prod_{w|v} E(K_{n,w}^E)[p^\infty] \otimes_{\mathbb{Z}_p} (\mathbb{Z}/p^n\mathbb{Z})\right),$$

$$B_n^1 := H^0\left(K_n, \prod_{w|v} H^1_f(K_{n,w}^E, E[p^n])\right),$$

$$C_n^1 := H^0\left(K_n, \prod_{w|v} H^1_f(K_{n,w}^E, E[p^\infty])[p^n]\right),$$

and the arrows a_n and c_n are restriction maps, and $b_n = \mathrm{res}^f_{n,v}$. By Lemma 6.10, we have $C_n^0 = C_n^1 = 0$. In order to prove Lemma 6.11 (3), it suffices to show that the sequence $\{\#\,\mathrm{Coker}(a_n)\}_{n \geq N}$ is bounded. By the exact sequence

$$0 \longrightarrow p^n E(K_{n,w}^E)[p^\infty] \longrightarrow E(K_{n,w}^E)[p^\infty] \longrightarrow E(K_{n,w}^E)[p^\infty] \otimes_{\mathbb{Z}_p} (\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow 0,$$

using Shapiro's lemma as in (6.10), we obtain an exact sequence

$$E(K_{n,v})[p^\infty] \xrightarrow{a_n} A_n^1 \longrightarrow H^1\left(K_n^E/K_n, \prod_{w|v} p^n E(K_{n,w}^E)[p^\infty]\right) =: \Xi_n.$$

In order to prove that $\{\#\,\mathrm{Coker}(a_n) \mid n \in \mathbb{Z}_{\geq N}\}$ is bounded, it suffices to show that $\{\#\Xi_n\}_n$ is bounded. Fix a place w_n of K_n^E. We have

$$\Xi_n \simeq H^1(K_{n,w_n}^E/K_{n,v}, p^n E(K_{n,w_n}^E)[p^\infty]).$$

For any intermediate field M of $K^E_{n,w_n}/K_{n,v}$ which is Galois over $K_{n,v}$, we have the inflation-restriction exact sequence

$$0 \longrightarrow \Xi'_n(M) \longrightarrow \Xi_n \longrightarrow \Xi''_n(M),$$

where we put

$$\begin{aligned}\Xi'_n(M) &:= H^1\big(M/K_{n,v}, H^0(M, p^n E(K^E_{n,w_n})[p^\infty])\big), \text{ and}\\ \Xi''_n(M) &:= H^0\big(K_{n,v}, H^1(K^E_{n,w_n}/M, p^n E(K^E_{n,w_n})[p^\infty])\big).\end{aligned}$$

Recall that K^E_n contains L, the elliptic curve $E_{K^E_n}$ has semistable reduction everywhere. Let u_n be the place of $L_n := L(\mu_{p^n})$ below w_n.

The case: Good reduction. Suppose that $E_{L_{n,u_n}}$ has good reduction. Let M_n be the maximal subfield of K^E_{n,w_n} which is unramified over $K_{n,v}$. By similar arguments of the boundedness of $\{\#Y_n(M_n)\}_{n\geq 0}$ for *The case: Potentially good reduction with* $\ell \neq p$ in the proof of (1), we have

$$\begin{aligned}\#\Xi'_n(M_n) &= \#H^1(M_n/K_{n,v}, p^n E(K^E_{n,w_n})[p^\infty])\\ &\leq \#\left(\frac{p^n E(M_n)[p^\infty]}{\langle \mathrm{Forb}_v - 1\rangle}\right)\\ &= \#p^n E(K_{n,v})[p^\infty]\\ &\leq \#E(K_{n,v})[p^\infty].\end{aligned}$$

Theorem 6.8 implies that $\{\#\Xi'_n(M_n)\}_{n\geq 0}$ is bounded. Moreover, as noted in the proof of the boundedness of $\{\#Z_n(M_n)\}_{n\geq 0}$ in *The case: Potentially good reduction with* $\ell \neq p$, the sequence $\{[K^E_n : M_n]\}_{n\geq N}$ is bounded, and hence $\{\#\Xi''_n(M_n)\}_{n\geq N}$ is bounded.

The case: Multiplicative reduction. Suppose that $E_{L_{n,u_n}}$ has multiplicative reduction. Put $\Xi'_n := \Xi'_n(L_{n,u_n})$ and $\Xi''_n := \Xi''_n(L_{n,u_n})$. In this case, Lemma 6.9 implies that $\Xi'_n = 0$ and $\Xi''_n = 0$ for sufficiently large n, and in particular, the sequences $\{\#\Xi''_n\}_{n\geq N}$ and $\{\#\Xi''_n\}_{n\geq N}$ is bounded.

By the above arguments, we deduce that in any case, the set $\{\#\Xi''_n\}_{n\geq N}$ is bounded and so is $\{\#\Xi_n\}_{n\geq N}$. Accordingly, the assertion Lemma 6.11 (3) is proved.

Let us show the assertion (2). Here, we study the case when $\ell = p$. Recall that by our assumption, the elliptic curve E has good reduction at p.

The case: Good ordinary reduction. Suppose that the elliptic curve E has good ordinary reduction at p. In this case, there exists a $G_{\mathbb{Q}_p}$-stable $\mathbb{Z}/p^n\mathbb{Z}$-submodule $\mathrm{Fil}\, E[p^n]$ of $E[p^n]$ of rank one such that the inertia group $I_{\mathbb{Q}_p}$ of $G_{\mathbb{Q}_p}$ acts via the cyclotomic character on $\mathrm{Fil}\, E[p^n]$, and trivially on $E[p^n]/\mathrm{Fil}\, E[p^n]$. Fix a generator P_n of the cyclic $\mathbb{Z}_p$-module $\mathrm{Fil}\, E[p^n]$ and a lift $Q_n \in E[p^n]$ of a generator of the cyclic $\mathbb{Z}_p$-module $\overline{Q}_n \in E[p^n]/\mathrm{Fil}\, E[p^n]$. The pair (P_n, Q_n) becomes a basis of the free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank two.

Let M_n be the maximal subfield of K^E_{n,w_n} which is unramified over $K_{n,v}$, and put $I_n := \mathrm{Gal}(K^E_{n,w_n}/M_n)$. Since I_n acts trivially on $\mathrm{Fil}\, E[p^n]$ and $E[p^n]/\mathrm{Fil}\, E[p^n]$, the group I_n is a cyclic group which is generated by an element acting on $E[p^n]$ via a unipotent matrix

$$U = \begin{pmatrix} 1 & x_n \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z}/p^n\mathbb{Z})$$

under the basis (P_n, Q_n). Fix a lift $\tau \in \mathrm{Gal}(K^E_{n,w_n}/K_{n,v})$ of the Frobenius $\mathrm{Forb}_v \in \mathrm{Gal}(M_n/K_{n,v})$. The filtration $\mathrm{Fil}\, E[p^n]$ is stable under the action of $\mathrm{Gal}(K^E_{n,w_n}/K_{n,v})$, and the Weil pairing $e\colon E[p^n]\times E[p^n] \to \mu_{p^n}$ is an alternative pairing preserving the action of $\mathrm{Gal}(K^E_{n,w_n}/K_{n,v})$ ([24, Chapter III, Section 8]). Accordingly, the fixed lift τ acts on $E[p^n]$ by a matrix

$$A = \begin{pmatrix} a_n & b_n \\ 0 & a_n^{-1} \end{pmatrix} \in M_2(\mathbb{Z}/p^n\mathbb{Z}) \tag{6.15}$$

for some $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b_n \in \mathbb{Z}/p^n\mathbb{Z}$. We can define $a := (a_n)_n \in \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$. Since E has good reduction at p, Theorem 6.8 implies that $a^k \neq 1$ for any $k \in \mathbb{Z}_{>0}$. In fact, if $a^k = 1$, then for any $m \in \mathbb{Z}_{\geq 0}$, the group $\mathrm{Fil}\, E[p^m]$ of order p^m is contained in $E(\mathbb{Q}_{p^k}(\mu_{p^m}))$, and contradicts Theorem 6.8. Here, we denote by $\mathbb{Q}_{p^k}$ the unramified extension field of $\mathbb{Q}_p$ of degree k. It holds that

$$AUA^{-1} = \begin{pmatrix} 1 & a_n^2 x_n \\ 0 & 1 \end{pmatrix} = U^{a_n^2}. \tag{6.16}$$

By the short exact sequence

$$0 \longrightarrow \mathrm{Fil}\, E[p^n] \longrightarrow E[p^n] \longrightarrow E[p^n]/\mathrm{Fil}\, E[p^n] \longrightarrow 0$$

and (6.11), we obtain an exact sequence

$$Y_n \longrightarrow \mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v}) \longrightarrow Z_n, \tag{6.17}$$

where

$$\begin{aligned} Y_n &:= H^1(K^E_{n,w_n}/K_{n,v_n}, \mathrm{Fil}\, E[p^n]), \text{ and} \\ Z_n &:= H^1(K^E_{n,w_n}/K_{n,v_n}, E[p^n]/\mathrm{Fil}\, E[p^n]). \end{aligned}$$

In order to show that $\{\#\,\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v})\}_{n\geq 0}$ is bounded, it is sufficient to prove that both $\{\#Y_n\}_{n\geq 0}$ and $\{\#Z_n\}_{n\geq 0}$ are bounded.

First, let us study the order of Z_n. Since I_n acts trivially on the quotient $E[p^n]/\mathrm{Fil}\, E[p^n]$, we have an exact sequence

$$0 \longrightarrow Z'_n \longrightarrow Z_n \longrightarrow Z''_n, \tag{6.18}$$

where

$$\begin{aligned} Z_n' &:= H^1(M_n/K_{n,v_n}, E[p^n]/\operatorname{Fil} E[p^n]), \text{ and} \\ Z_n'' &:= H^0(K_{n,v}, H^1(K_{n,w_n}^E/M_n, E[p^n]/\operatorname{Fil} E[p^n])) \\ &= H^0(K_{n,v}, \operatorname{Hom}(I_n, E[p^n]/\operatorname{Fil} E[p^n])). \end{aligned}$$

Since $a \neq 1$, we have $\#(E[p^\infty]/\operatorname{Fil} E[p^\infty])[a^{-1}-1] < \infty$, and

$$\begin{aligned} \# Z_n' &\leq \# \left(\frac{E[p^n]/\operatorname{Fil} E[p^n]}{\langle \tau - 1 \rangle} \right) \\ &= \# \left(\frac{E[p^n]/\operatorname{Fil} E[p^n])}{\langle a^{-1} - 1 \rangle} \right) \\ &= \#(E[p^n]/\operatorname{Fil} E[p^n])[a^{-1}-1] \\ &\leq \#(E[p^\infty]/\operatorname{Fil} E[p^\infty])[a^{-1}-1]. \end{aligned}$$

The sequence $\{\# Z_n'\}_{n \geq 0}$ is bounded. Let us consider the order of Z_n''. The matrix presentation (6.15) implies that the Galois group $\operatorname{Gal}(M_n/K_{n,v}) = \langle \operatorname{Forb}_v \rangle$ acts on $E[p^n]/\operatorname{Fil} E[p^n]$ via the character $\operatorname{Forb}_v \mapsto a_n^{-1}$, and (6.16) implies that $\operatorname{Forb}_v \in \operatorname{Gal}(M_n/K_{n,v})$ acts on I_n via the character $\operatorname{Forb}_v \mapsto a_n^2$. Recall that $a = (a_n)_n$ satisfies $a^3 \neq 1$, namely $a^2 \neq a^{-1}$. There exists an integer $m_0 \in \mathbb{Z}_{>0}$ such that $a_{m_0}^2 \neq a_{m_0}^{-1}$. We have

$$Z_n'' \subseteq \operatorname{Hom}(I_n, E[p^{m_0-1}]/\operatorname{Fil} E[p^{m_0-1}]).$$

Since I_n is cyclic, the sequence $\{\# \operatorname{Hom}(I_n, E[p^{m_0-1}]/\operatorname{Fil} E[p^{m_0-1}])\}_{n \geq 0}$ is bounded and so is $\{\# Z_n''\}_{n \geq 0}$. As a result, the sequence $\{\# Z_n\}_{n \geq 0}$ is bounded from (6.18).

The boundedness of $\{\# Y_n\}$ follows from the arguments in the previous paragraph just by replacing $E[p^n]/\operatorname{Fil} E[p^n]$ with $\operatorname{Fil} E[p^n]$, where the Galois group $\operatorname{Gal}(M_n/K_{n,v}) = \langle \operatorname{Forb}_v \rangle$ acts via the character $\operatorname{Forb}_v \mapsto a_n$. By the short exact sequence (6.17) we deduce that $\{\# \operatorname{Ker}(\operatorname{res}_{n,v}^{\mathrm{loc}})\}_{n \geq 0}$ is bounded.

The case: Good supersingular reduction. Suppose that E has good supersingular reduction at p. In order to prove that the sequence

$$\{\# \operatorname{Ker}(\operatorname{res}_{n,v}^{\mathrm{loc}}) | n \geq 0, v \mid p\}$$

is bounded, by (6.11) it suffices to show that $H^1(K_{n,w_n}^E/K_{n,v}, E[p^n]) = 0$ for any $n \geq 0$. The short exact sequence

$$0 \longrightarrow E[p] \longrightarrow E[p^{m+1}] \xrightarrow{\times p} E[p^m] \longrightarrow 0$$

induces the exact sequence

$$H^1(K^E_{n,w_n}/K_{n,v}, E[p]) \longrightarrow H^1(K^E_{n,w_n}/K_{n,v}, E[p^{m+1}]) \longrightarrow H^1(K^E_{n,w_n}/K_{n,v}, E[p^m]).$$

By induction on m, it is enough to show that $H^1(K^E_{n,w_n}/K_{n,v}, E[p]) = 0$. We denote the inertia subgroup of $G_{\mathbb{Q}_p}$ by $I_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\mathrm{ur}})$, and the wild inertia subgroup by $I^w_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\mathrm{tame}}) \subseteq I_{\mathbb{Q}_p}$, where $\mathbb{Q}_p^{\mathrm{tame}}$ is the maximal tamely ramified extension of $\mathbb{Q}_p$. Let $I^t_{\mathbb{Q}_p} := I_{\mathbb{Q}_p}/I^w_{\mathbb{Q}_p} \simeq \varprojlim_n \mathbb{F}^\times_{p^n}$ be the tame inertia group of $G_{\mathbb{Q}_p}$ (cf. [22, 1.3, Proposition 2]), and $\psi\colon I^t_{\mathbb{Q}_p} \to \mathbb{F}^\times_{p^2}$ the character induced by the natural projection $\varprojlim_n \mathbb{F}^\times_{p^n} \to \mathbb{F}^\times_{p^2}$. The characters ψ and ψ^p form the fundamental characters of level 2 (cf. [22, 1.7]). By [22, 1.11, Proposition 12], the following hold.

- The action of the wild inertia subgroup $I^w_{\mathbb{Q}_p}$ on $E[p]$ is trivial, so that the action of the inertia group $I_{\mathbb{Q}_p}$ of $G_{\mathbb{Q}_p}$ on $E[p]$ factors through $I^t_{\mathbb{Q}_p}$.
- The group $E[p]$ has a structure of $\mathbb{F}_{p^2}$-vector space of dimension 1.
- The image of $I_{\mathbb{Q}_p}$ in $\mathrm{Aut}(E[p])$ is a cyclic group of order $p^2 - 1$.
- The action of $I^t_{\mathbb{Q}_p}$ on $E[p]$ is given by the fundamental character ψ of level 2.

Let us regard $E[p]$ as an $\mathbb{F}_p$-vector space, and consider the $\mathbb{F}_{p^2}$-vector space $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$, which is the extension of scalar of $E[p]$. By the properties of $E[p]$ noted above, the action of $I^t_{\mathbb{Q}_p}$ on $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is given by the matrix

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi^p \end{pmatrix} \tag{6.19}$$

after taking a suitable $\mathbb{F}_{p^2}$-basis $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ (cf. [22, 1.9, Corollaire 3], see also [3, 2.6 Theorem] which is a result on modulo p Galois representations attached to modular forms with coefficients in $\overline{\mathbb{F}}_p$). Let F be the maximal unramified extension field of $\mathbb{Q}_p$ contained in K^E_{1,w_1}. Put $F_n := F(\mu_{p^n})$. We have the following inflation-restriction exact sequences:

$$H^1(F_n/\mathbb{Q}_p(\mu_{p^n}), H^0(F_n, E[p])) \longrightarrow H^1(K^E_{n,w_n}/K_{n,v}, E[p]) \longrightarrow H^1(K^E_{n,w_n}/F_n, E[p]) \tag{6.20}$$

and

$$H^1(K^E_{1,w_1}(\mu_{p^n})/F_n, E[p]) \longrightarrow H^1(K^E_{n,w_n}/F_n, E[p]) \longrightarrow H^1(K^E_{n,w_n}/K^E_{1,w_1}(\mu_{p^n}), E[p])^{G_{F_n}}, \tag{6.21}$$

where F'_n is the maximal abelian extension field of $K^E_{1,w_1}(\mu_{p^n})$ contained in K^E_{n,w_n}. Note also that the last term in (6.21) is written as

$$H^1(K^E_{n,w_n}/K^E_{1,w_1}(\mu_{p^n}), E[p])^{G_{F_n}} = \mathrm{Hom}_{\mathbb{Z}[G_{F_n}]}(\mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n})), E[p]).$$

Claim 2. *We have $H^0(F_n, E[p]) = 0$ and $H^1(K^E_{1,w_1}(\mu_{p^n})/F_n, E[p]) = 0$.*

Proof of Claim 2. We may assume $n \geq 1$. Since $F/\mathbb{Q}_p$ is unramified, the ramification index of $F_n/\mathbb{Q}_p$ is $(p-1)p^{n-1}$, which is not divisible by $[K^E_{1,w_1} : F] = p^2 - 1$. This implies that the restrictions of ψ and ψ^p on $I_{\mathbb{Q}_p} \cap G_{F_n}$ are non-trivial, and by (6.19), we have

$$H^0(F_n, E[p]) \subseteq H^0(F_n, E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}) = 0.$$

Furthermore, the extension $K^E_{1,w_1}(\mu_{p^n})/F_n$ is finite cyclic. By using the Herbrand quotient of the Tate cohomology groups ([20, Chapitre VIII, §4, Proposition 8]), we have

$$\begin{aligned} \# H^1(K^E_{1,w_1}(\mu_{p^n})/F_n, E[p]) &= \# \widehat{H}^1(K^E_{1,w_1}(\mu_{p^n})/F_n, E[p]) \\ &= \# \widehat{H}^0(K^E_{1,w_1}(\mu_{p^n})/F_n, E[p]) \\ &\leq \# H^0(F_n, E[p]) = 1. \end{aligned}$$

Because of this, we obtain the claim. $\square$

Applying Claim 2, the exact sequences (6.20) and (6.21) give

$$\begin{aligned} \# H^1(K^E_{n,w_n}/K_{n,v}, E[p]) &\leq \# H^1(K^E_{n,w_n}/F_n, E[p]) \\ &\leq \# \mathrm{Hom}_{\mathbb{Z}[G_{F_n}]}(\mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n})), E[p]). \end{aligned}$$

Now, we shall show that

$$\mathrm{Hom}_{\mathbb{Z}[G_{F_n}]}(\mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n})), E[p]) = 0. \tag{6.22}$$

For each $m \in \mathbb{Z}$ with $1 \leq m \leq n$, we define the subgroup

$$\mathrm{Fil}^m \subset \mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n}))$$

to be the image of $\mathrm{Gal}(K^E_{n,w_n}/K^E_{m,w_m}(\mu_{p^n}))$ by the natural map

$$\mathrm{Gal}(K^E_{n,w_n}/K^E_{1,w_1}(\mu_{p^n})) \longrightarrow \mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n})).$$

Note that the family $\{\mathrm{Fil}^m\}_m$ becomes a G_{F_n}-stable descending filtration of $\mathrm{Gal}(F'_n/K^E_{1,w_1}(\mu_{p^n}))$. In order to show (6.22), it suffices to show that

$$\mathrm{Hom}_{\mathbb{Z}[G_{F_n}]}(\mathrm{Fil}^m / \mathrm{Fil}^{m+1}, E[p] \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}) = 0.$$

Take an $\mathbb{F}_{p^2}$-basis B_1 of $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ which gives the presentation of the action of $I^t_{\mathbb{Q}_p}$ by the matrix given in (6.19), and for each $m \in \mathbb{Z}$ with $2 \leq m \leq n$, fix a basis B_m of $E[p^m] \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$ which is a lift of B_1. Since $\mathrm{Gal}(K^E_{m+1,w_{m+1}}/K^E_{m,w_m})$ is a normal subgroup of $\mathrm{Gal}(K^E_{m+1,w_{m+1}}/\mathbb{Q}_p)$, it is stable under the conjugate action of G_{F_n}. Recall that we have a G_{F_n}-stable injection from $\mathrm{Gal}(K^E_{m+1,w_{m+1}}/K^E_{m,w_m})$ into

$$\begin{aligned}\mathrm{Ker}\Big(&\mathrm{Aut}(E[p^{m+1}]\otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2})\twoheadrightarrow \mathrm{Aut}(E[p^m]\otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2})\Big)\\ &= 1+p^m M_2(\mathbb{Z}_{p^2}/p^{m+1}\mathbb{Z}_{p^2})\simeq M_2(\mathbb{F}_{p^2}),\end{aligned}$$

where the action of $\sigma\in G_{F_n}$ on $M_2(\mathbb{F}_{p^2})$ is defined by the conjugate action of the matrix

$$\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}.$$

Since $\mathrm{Fil}^m/\mathrm{Fil}^{m+1}$ is a quotient of $\mathrm{Gal}(K^E_{m+1,w_{m+1}}(\mu_{p^n})/K^E_{m,w_m}(\mu_{p^n}))$ by definition, and the restriction

$$\mathrm{Gal}(K^E_{m+1,w_{m+1}}(\mu_{p^n})/K^E_{m,w_m}(\mu_{p^n}))\longrightarrow \mathrm{Gal}(K^E_{m+1,w_{m+1}}/K^E_{m,w_m})$$

is an injective homomorphism, we can regard $\mathrm{Fil}^m/\mathrm{Fil}^{m+1}$ as a G_{F_n}-stable subquotient of $M_2(\mathbb{F}_{p^2})$. Let us study the $\mathbb{F}_{p^2}[G_F]$-module structure of $M_2(\mathbb{F}_{p^2})$. Take any $\sigma\in G_{F_n}$. It holds that

$$\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}^{-1}=\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}\ \text{for any } a,b\in\mathbb{F}_{p^2},$$

$$\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}^{-1}=\psi^{1-p}(\sigma)\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix},$$

and

$$\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}\psi(\sigma) & 0\\ 0 & \psi^p(\sigma)\end{pmatrix}^{-1}=\psi^{p-1}(\sigma)\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

Note that $\psi\neq\psi^{p-1}$, and $\psi\neq\psi^{1-p}$. It holds that $M_2(\mathbb{F}_{p^2})$ is a semisimple $\mathbb{F}_{p^2}[G_{F_n}]$-module, and there is no simple $\mathbb{F}_{p^2}[G_{F_n}]$-submodule of $M_2(\mathbb{F}_{p^2})$ which is isomorphic to an $\mathbb{F}_{p^2}[G_{F_n}]$-submodule of $E[p]\otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2}$. This implies

$$\mathrm{Hom}_{\mathbb{Z}[G_{F_n}]}(\mathrm{Fil}^m/\mathrm{Fil}^{m+1}, E[p]\otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2})=0,$$

and we obtain (6.22). Consequently, we have

$$\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v})=H^1(K^E_{n,w_n}/K_{n,v}(\mu_{p^n}),E[p^n])=0.$$

By the above arguments, we deduce that $\{\#\,\mathrm{Ker}(\mathrm{res}^{\mathrm{loc}}_{n,v})\}_{n\geq 0,v\mid p}$ is bounded. This completes the proof of Lemma 6.11 (2). □

6.3. Proof of Theorem 1.1. In this paragraph, we show our main theorem Theorem 1.1 (Theorem 6.16).

Recall that $\Sigma_{0,\mathrm{bad}}$ denotes the set of prime numbers where E has bad reduction. As E has good reduction at p the prime p does not belong to $\Sigma_{0,\mathrm{bad}}$.

Lemma 6.12. *Suppose that E satisfies* (C2)*. Let $\ell \in \Sigma_{0,\mathrm{bad}}$. For each $n \in \mathbb{Z}_{\geq 0}$ and $i \in \{0,1,2\}$, we put*

$$\mathcal{H}^i_f(\ell,n) := H^i\left(K_n, \prod_{w\mid\ell} \frac{H^1_f(K^E_{n,w}, E[p^n])}{H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n]) \cap H^1_f(K^E_{n,w}, E[p^n])}\right), \text{ and}$$

$$\mathcal{H}^i_{\mathrm{ur}}(\ell,n) := H^i\left(K_n, \prod_{w\mid\ell} \frac{H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])}{H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n]) \cap H^1_f(K^E_{n,w}, E[p^n])}\right).$$

Then, there exists an integer $N'_\ell \in \mathbb{Z}_{\geq 1}$ such that for any $n \in \mathbb{Z}_{\geq N'_\ell}$ and $i \in \{0,1,2\}$, it holds that $\mathcal{H}^i_f(\ell,n) = 0$ and $\mathcal{H}^i_{\mathrm{ur}}(\ell,n) = 0$.

Proof. The case: Potentially good reduction at ℓ. First, suppose that E has potentially good reduction at ℓ. There exists an integer $n_0 \in \mathbb{Z}_{\geq 1}$ such that $E_{K^E_{n_0}}$ has good reduction at every place above ℓ ([25, Chapter IV, Proposition 10.3]). For any $n \in \mathbb{Z}_{\geq n_0}$ and any place w of K^E_n, we have $H^1_f(K^E_{n,w}, E[p^n]) = H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])$ (cf. Remark 5.2). We obtain $\mathcal{H}^i_f(\ell,n) = 0$ and $\mathcal{H}^i_{\mathrm{ur}}(\ell,n) = 0$ for any $n \in \mathbb{Z}_{\geq n_0}$ and $i \in \{0,1,2\}$.

The case: Potentially multiplicative reduction at ℓ. Next, suppose that E has potentially multiplicative reduction at ℓ. Let $N_\ell \in \mathbb{Z}_{\geq 1}$ be as in Lemma 6.9. By Lemma 4.3, the base change $E_{K^E_{N_\ell}}$ has split multiplicative reduction at every $w \mid \ell$. Take any $n \in \mathbb{Z}_{\geq N_\ell}$, and let v be any place of K_n above ℓ. For any place w of K^E_n above v, $E_{K^E_{n,w}}$ is isomorphic to a Tate curve $\mathbb{G}_m/q_w^{\mathbb{Z}}$. By Shapiro's lemma as in (6.10), for each $\mathcal{F} \in \{f, \mathrm{ur}\}$ and $i \in \{0,1,2\}$, we have

$$\mathcal{H}^i_{\mathcal{F}}(\ell,n) \simeq H^i\left(K_{n,v}, M_{\mathcal{F}}(w,n)\right),$$

where

$$M_{\mathcal{F}}(w,n) := \frac{H^1_{\mathcal{F}}(K^E_{n,w}, E[p^n])}{H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n]) \cap H^1_f(K^E_{n,w}, E[p^n])}. \tag{6.23}$$

Let us show that $\mathcal{H}^i_f(\ell,n) = 0$ for each i. The natural surjective homomorphism $T_p(E) \to T_p(E)/p^nT_p(E) \simeq E[p^n]$ induces a map

$$\pi_{n,w}\colon H^1(K^E_{n,w}, T_p(E)) \longrightarrow H^1(K^E_{n,w}, E[p^n]).$$

We note that $H^1_{\mathrm{ur}}(K^E_{n,w}, T_p(E))$ is contained in the inverse image of the unramified cohomology $H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])$ by $\pi_{n,w}$. By [17, Lemma 1.3.8], the image of $H^1_f(K^E_{n,w}, T_p(E))$ by $\pi_{n,w}$ coincides with $H^1_f(K^E_{n,w}, E[p^n])$. From [17, Lemma 1.3.5 (ii)], we have $H^1_{\mathrm{ur}}(K^E_{n,w}, T_p(E)) \subseteq H^1_f(K^E_{n,w}, T_p(E))$

with finite index. The map $\pi_{n,w}$ induces a surjection

$$\pi_{n,w}^f \colon \frac{H_f^1(K_{n,w}^E, T_p(E))}{H_{\mathrm{ur}}^1(K_{n,w}^E, T_p(E))} \longrightarrow M_f(w,n). \tag{6.24}$$

By [17, Lemma 1.3.5 (iii)], we have

$$\frac{H_f^1(K_{n,w}^E, T_p(E))}{H_{\mathrm{ur}}^1(K_{n,w}^E, T_p(E))} = \left(\frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right)^{\mathrm{Forb}_w=1}, \tag{6.25}$$

where $\mathrm{Forb}_w \in \mathrm{Gal}(K_{n,w}^{E,\mathrm{ur}}/K_{n,w}^E)$ is the Frobenius automorphism. Note that the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $H_f^1(K_{n,w}^E, T_p(E))/H_{\mathrm{ur}}^1(K_{n,w}^E, T_p(E))$ is written as a successive extension of copies of a simple $\mathbb{Z}_p[G_{K_{n,v}}]$-module

$$\frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}[p] \simeq (\mu_p \times q_w^{p^{-1}\mathbb{Z}})/(\mu_p \times q_w^{\mathbb{Z}}). \tag{6.26}$$

Here, (6.26) is valid because of the inclusion $E(K_{n,w}^{E,\mathrm{ur}}) \supseteq E[p^n]$ and the isomorphism $E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}} \simeq \mu_{p^\infty}$ induced by (6.12). Since $\pi_{n,w}^f$ is surjective, all the (simple) quotients J_i/J_{i-1} of a Jordan–Hölder series

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_t := M_f(w,n)$$

as $\mathbb{Z}_p[G_{K_{n,v}}]$-modules are isomorphic to (6.26) (cf. [27, Lemma 0FCK]). It follows from the condition (C2) for E and Lemma 4.4 that

$$H^0\left(K_{n,v}, \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}[p]\right) \subseteq H^0\left(K_{n,v}, \frac{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]}{E(K_{n,w}^{E,\mathrm{ur}})[p^\infty]_{\mathrm{div}}}\right) = 0.$$

By induction on i, we have $H^0(K_{n,v}, J_i) = 0$. In particular, we obtain

$$H^0(K_{n,v}, J_t) = \mathcal{H}_f^0(\ell, n) = 0.$$

By (6.24) and (6.25), the module $M_f(w,n)$ defined in (6.23) is a subquotient $\mathbb{Z}_p[G_{K_{n,v}}]$-module of $E[p^\infty]$. The condition (C2) for E and Lemma 4.4 ((a) $\Rightarrow$ (d)) also imply the equality

$$H^0\left(K_{n,v}, \mathrm{Hom}_{\mathbb{Z}_p}\left(M_f(w,n), \mu_{p^n}\right)\right) = 0.$$

By the local duality of the Galois cohomology ([13, (7.2.6) Theorem]), we also have $\mathcal{H}_f^2(\ell, n) = 0$. Moreover, as we have $\ell \neq p$, the local Euler–Poincaré characteristic

$$\frac{\#\mathcal{H}_f^0(\ell,n)\#\mathcal{H}_f^2(\ell,n)}{\#\mathcal{H}_f^1(\ell,n)}$$

is equal to 1 ([13, (7.3.1) Theorem]). We obtain $\mathcal{H}_f^1(\ell, n) = 0$.

Next, let us show that $\mathcal{H}_{\mathrm{ur}}^i(\ell, n) = 0$ for each i. The inclusion $E[p^n] \subseteq E[p^\infty]$ induces a homomorphism

$$\iota_{n,w} : H^1(K_{n,w}^E, E[p^n]) \longrightarrow H^1(K_{n,w}^E, E[p^\infty]).$$

Recall that $H^1_f(K^E_{n,w}, E[p^n])$ is the inverse image of $H^1_f(K^E_{n,w}, E[p^\infty])$ by the natural map $\iota_{n,w}$ (cf. [17, Remark 1.3.9]). From Lemma 6.10, we have

$$H^1_f(K^E_{n,w}, E[p^n]) = \mathrm{Ker}(\iota_{n,w}). \tag{6.27}$$

By [17, Lemma 1.3.2 (i)], we have

$$H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n]) \simeq \frac{E(K^{E,\mathrm{ur}}_{n,w})[p^n]}{\langle \mathrm{Forb}_w - 1\rangle}.$$

The latter group is isomorphic to $E[p^n] = E(K^E_{n,w})[p^n]$ because of $K^E_n = \mathbb{Q}(E[p^n])$. The image of $H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])$ by $\iota_{n,w}$ is contained in

$$H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^\infty]) \simeq \frac{E(K^{E,\mathrm{ur}}_{n,w})[p^\infty]}{\langle \mathrm{Forb}_w - 1\rangle},$$

and we have

$$\iota_{n,w}(H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])) = \left(\frac{E(K^{E,\mathrm{ur}}_{n,w})[p^\infty]}{\langle \mathrm{Forb}_w - 1\rangle} \right)[p^n].$$

By (6.27), the map $\iota_{n,w}$ induces

$$M_{\mathrm{ur}}(w,n) \xrightarrow{\simeq} \left(\frac{E(K^{E,\mathrm{ur}}_{n,w})[p^\infty]}{\langle \mathrm{Forb}_w - 1\rangle} \right)[p^n].$$

In particular, the $\mathbb{Z}_p[G_{K_{n,v}}]$-module $M_{\mathrm{ur}}(w,n)$ is a subquotient of $E[p^\infty]$. Therefore, by (C2) and Lemma 4.4, we have $\mathcal{H}^0_{\mathrm{ur}}(\ell,n) = 0$. Moreover, similar to the proof of $\mathcal{H}^i_f(\ell,n) = 0$, by using the local duality theorem and the local Euler–Poincaré characteristic formula, we deduce that $\mathcal{H}^1_{\mathrm{ur}}(\ell,n) = 0$ and $\mathcal{H}^2_{\mathrm{ur}}(\ell,n) = 0$. This completes the proof of Lemma 6.12. □

Corollary 6.13. *Suppose that E satisfies* (C2). *Let ℓ be a prime number (distinct from p) at which E has bad reduction. Then, there exists an integer $N'_\ell \in \mathbb{Z}_{\geq 1}$ such that for any $n \in \mathbb{Z}_{\geq N'_\ell}$ and any $\mathcal{F} \in \{f, \mathrm{ur}\}$, the natural map*

$$\left(\prod_{w \mid \ell} \frac{H^1(K^E_{n,w}, E[p^n])}{H^1_f(K^E_{n,w}, E[p^n]) \cap H^1_{\mathrm{ur}}(K^E_{n,w}, E[p^n])} \right)^{G_{K_n}} \longrightarrow \left(\prod_{w \mid \ell} \frac{H^1(K^E_{n,w}, E[p^n])}{H^1_{\mathcal{F}}(K^E_{n,w}, E[p^n])} \right)^{G_{K_n}}$$

is an isomorphism.

Proof. Take $N'_\ell \in \mathbb{Z}_{\geq 1}$ as in Lemma 6.12. For $n \geq N'_\ell$, to simplify the notation, we put $H^i_{\mathcal{F}'}(K^E_{n,w}) := H^i_{\mathcal{F}'}(K^E_{n,w}, E[p^n])$ $(\mathcal{F}' \in \{\emptyset, \mathrm{ur}, f\})$. The short exact sequences

$$0 \longrightarrow \frac{H^1_{\mathcal{F}}(K^E_{n,w})}{H^1_f(K^E_{n,w}) \cap H^1_{\mathrm{ur}}(K^E_{n,w})} \longrightarrow \frac{H^1(K^E_{n,w})}{H^1_f(K^E_{n,w}) \cap H^1_{\mathrm{ur}}(K^E_{n,w})} \longrightarrow \frac{H^1(K^E_{n,w})}{H^1_{\mathcal{F}}(K^E_{n,w})} \longrightarrow 0$$

for all place w above ℓ induce the cohomological long exact sequence

$$\mathcal{H}^0_{\mathcal{F}}(\ell, n) \longrightarrow \left(\prod_{w \mid \ell} \frac{H^1(K^E_{n,w})}{H^1_f(K^E_{n,w}) \cap H^1_{\mathrm{ur}}(K^E_{n,w})} \right)^{G_{K_n}} \xrightarrow{h} \left(\prod_{w \mid \ell} \frac{H^1(K^E_{n,w})}{H^1_{\mathcal{F}}(K^E_{n,w})} \right)^{G_{K_n}} \longrightarrow \mathcal{H}^1_{\mathcal{F}}(\ell, n).$$

Lemma 6.12 implies that the map h is an isomorphism. $\square$

As we referred in Section 1, we introduce a quotient A^E_n of $\mathrm{Cl}(\mathcal{O}_{K^E_n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for each $n \in \mathbb{Z}_{\geq 1}$ as follows: We fix a basis of the free $\mathbb{Z}/p^n\mathbb{Z}$-module $E[p^n]$ of rank 2, and identify $E[p^n]$ with the $\mathbb{Z}/p^n\mathbb{Z}$-module

$$M_{2,1}(\mathbb{Z}/p^n\mathbb{Z}) = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z}/p^n\mathbb{Z} \right\}$$

consisting of column vectors of degree two. Via this identification, we can identify the Pontrjagin dual $E[p^n]^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(E[p^n], \mathbb{Z}/p^n\mathbb{Z})$ of $E[p^n]$ with the $\mathbb{Z}/p^n\mathbb{Z}$-module

$$M_{1,2}(\mathbb{Z}/p^n\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \end{pmatrix} \mid a, b \in \mathbb{Z}/p^n\mathbb{Z} \right\}$$

consisting of row vectors of degree two. Let

$$\rho^E_n \colon \mathrm{Gal}(K^E_n/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

be the natural left action of $\mathrm{Gal}(K^E_n/\mathbb{Q})$ on $E[p^n]$, and

$$(\rho^E_n)^\vee \colon \mathrm{Gal}(K^E_n/\mathbb{Q})^{\mathrm{op}} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]^\vee) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

be the right action of $\mathrm{Gal}(K^E_n/\mathbb{Q})$ on the Pontrjagin dual $E[p^n]^\vee$. Note that for each $\sigma \in \mathrm{Gal}(K^E_n/\mathbb{Q})$, the automorphism $(\rho^E_n)^\vee(\sigma) \in \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]^\vee)$ is given by

$$E[p^n]^\vee = M_{1,2}(\mathbb{Z}/p^n\mathbb{Z}) \ni \begin{pmatrix} a & b \end{pmatrix} \longmapsto (\rho^E_n)^\vee(\sigma)\Big(\begin{pmatrix} a & b \end{pmatrix}\Big) = \begin{pmatrix} a & b \end{pmatrix} \rho^E_n(\sigma).$$

We define A^E_n by

$$A^E_n := (M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho^E_n)^\vee) \otimes_{\mathbb{Z}[\mathrm{Gal}(K^E_n/K_n)]} \mathrm{Cl}(\mathcal{O}_{K^E_n}[1/p]) \tag{6.28}$$

as a $\mathbb{Z}_p$-module, where $(M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee)$ denotes the matrix algebra $M_2(\mathbb{Z}/p^n\mathbb{Z}) = M_{2,2}(\mathbb{Z}/p^n\mathbb{Z})$ of degree two over $\mathbb{Z}/p^n\mathbb{Z}$ equipped with the right action of $\mathrm{Gal}(K_n^E/\mathbb{Q})$ given by

$$M_2(\mathbb{Z}/p^n\mathbb{Z}) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} (\rho_n^E)^\vee(\sigma)((a\ b)) \\ (\rho_n^E)^\vee(\sigma)((c\ d)) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rho_n^E(\sigma).$$

We define a $\mathbb{Z}_p$-linear left action of $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on A_n^E by

$$\sigma(A \otimes [\mathfrak{a}]) := A\rho_n^E(\sigma^{-1}) \otimes [\sigma\mathfrak{a}]$$

for each $\sigma \in G_\mathbb{Q}$, $A \in M_2(\mathbb{Z}/p^n\mathbb{Z})$ and $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])$. Since every $\sigma \in G_{K_n}$ acts trivially on A_n^E, we may regard A_n^E as an R_n-module, where $R_n = \mathbb{Z}/p^n\mathbb{Z}[\mathrm{Gal}(K_n/\mathbb{Q})]$. As noted in Remark 1.4, under the condition (C1), one can regard the R_n-module A_n^E as a quotient of the ideal class group $\mathrm{Cl}(\mathcal{O}_{K_n^E})$. We denote by $(A_n^E)^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(A_n^E, \mathbb{Z}/p^n\mathbb{Z})$ the Pontrjagin dual of A_n^E. We also define an R_n-module

$$S_n := \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_n^E/K_n)]}(\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) \otimes_\mathbb{Z} \mathbb{Z}_p, E[p^n])$$

Lemma 6.14. *For each $n \in \mathbb{Z}_{\geq 1}$, there exists a* $\mathrm{Gal}(K_n/\mathbb{Q})$*-equivariant isomorphism*

$$(A_n^E)^\vee \xrightarrow{\simeq} S_n^{\oplus 2}.$$

Proof. By the fixed basis above, we identify the isomorphism $E[p^n] \simeq M_{2,1}(\mathbb{Z}/p^n\mathbb{Z})$. Since we have a natural isomorphism

$$M_2(\mathbb{Z}/p^n\mathbb{Z}) \simeq M_{2,1}(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2},$$

our identification induces a $\mathrm{Gal}(K_n^E/\mathbb{Q})$-equivariant isomorphism

$$(M_2(\mathbb{Z}/p^n\mathbb{Z}), \rho_n^E) \simeq E[p^n]^{\oplus 2}, \tag{6.29}$$

where $(M_2(\mathbb{Z}/p^n\mathbb{Z}), \rho_n^E)$ denotes $M_2(\mathbb{Z}/p^n\mathbb{Z})$ equipped with the left action of $\mathrm{Gal}(K_n^E/\mathbb{Q})$ given by

$$M_2(\mathbb{Z}/p^n\mathbb{Z}) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left(\rho_n^E(\sigma) \begin{pmatrix} a \\ c \end{pmatrix}\ \rho_n^E(\sigma) \begin{pmatrix} b \\ d \end{pmatrix} \right) = \rho_n^E(\sigma) \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for each $\sigma \in \mathrm{Gal}(K_n^E/\mathbb{Q})$. We have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}_p}((M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee), \mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\simeq} (M_2(\mathbb{Z}/p^n\mathbb{Z}), \rho_n^E) \tag{6.30}$$

as $\mathrm{Gal}(K_n^E/\mathbb{Q})$-modules. We obtain $\mathrm{Gal}(K_n/\mathbb{Q})$-equivariant isomorphisms

$$\begin{aligned}
&(A_n^E)^\vee \\
&\underset{(6.28)}{=} \mathrm{Hom}_{\mathbb{Z}_p}\big((M_2(\mathbb{Z}/p^n\mathbb{Z}),(\rho_n^E)^\vee)\otimes_{\mathbb{Z}[\mathrm{Gal}(K_n^E/K_n)]}\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]),\mathbb{Z}/p^n\mathbb{Z}\big) \\
&\xrightarrow[\substack{\text{adjoint}\\ \&\ (6.30)}]{\simeq} \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_n^E/K_n)]}\left(\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])\otimes_{\mathbb{Z}}\mathbb{Z}_p,(M_2(\mathbb{Z}/p^n\mathbb{Z}),\rho_n^E)\right) \\
&\xrightarrow[(6.29)]{\simeq} S_n^{\oplus 2}.
\end{aligned}$$

This shows the assertion. $\square$

Lemma 6.15. *There exists an integer $N\in\mathbb{Z}_{\geq 1}$ such that, for any $n\in\mathbb{Z}_{\geq N}$, we have an isomorphism*

$$S_n\simeq H^0(K_n,\mathrm{Sel}_p(K_n^E,E[p^n])).$$

Proof. Let H_n^E be the maximal subextension of the p-Hilbert class field of K_n^E which is completely split at primes above p. From the global class field theory, the ideal class group $\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])\otimes_{\mathbb{Z}}\mathbb{Z}_p$ is isomorphic to the Galois group $\mathrm{Gal}(H_n^E/K_n^E)$. We have

$$\begin{aligned}
&\mathrm{Hom}(\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])\otimes_{\mathbb{Z}}\mathbb{Z}_p,E[p^n]) \\
&\simeq \mathrm{Hom}(\mathrm{Gal}(H_n^E/K_n^E),E[p^n]) \\
&= \mathrm{Ker}\left(\begin{aligned}&\mathrm{Hom}(G_{K_n^E},E[p^n]) \\ &\quad\longrightarrow \prod_{w\mid p}\mathrm{Hom}(G_{K_{n,w}^E},E[p^n])\times\prod_{w\nmid p}\mathrm{Hom}(G_{K_{n,w}^{E,\mathrm{ur}}},E[p^n])\end{aligned}\right) \\
&\simeq \mathrm{Ker}\left(\begin{aligned}&H^1(K_n^E,E[p^n]) \\ &\quad\longrightarrow \prod_{w\mid p}H^1(K_{n,w}^E,E[p^n])\times\prod_{w\nmid p}H^1(K_{n,w}^{E,\mathrm{ur}},E[p^n])\end{aligned}\right).
\end{aligned}$$

Therefore, the R_n-module S_n is isomorphic to

$$\begin{aligned}
&\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_n^E/K_n)]}(\mathrm{Gal}(H_n^E/K_n^E),E[p^n]) \\
&\simeq \mathrm{Hom}(\mathrm{Gal}(H_n^E/K_n^E),E[p^n])^{G_{K_n}} \\
&= \mathrm{Ker}\left(\begin{aligned}&H^1(K_n^E,E[p^n])^{G_{K_n}} \\ &\quad\longrightarrow \left(\prod_{w\mid p}H^1(K_{n,w}^E,E[p^n])\times\prod_{w\nmid p}H^1(K_{n,w}^{E,\mathrm{ur}},E[p^n])\right)^{G_{K_n}}\end{aligned}\right).
\end{aligned}$$

By the very definition of H^1_{ur}, there exists an injective homomorphism

$$H^1(K_{n,w}^E,E[p^n])/H^1_{\mathrm{ur}}(K_{n,w}^E,E[p^n])\hookrightarrow H^1(K_{n,w}^{E,\mathrm{ur}},E[p^n])$$

and hence we have

$$S_n \simeq \operatorname{Ker}\left(\begin{array}{l} H^1(K_n^E, E[p^n])^{G_{K_n}} \\ \quad \longrightarrow \left(\prod_{w|p} H^1(K_{n,w}^E, E[p^n]) \times \prod_{w\nmid p} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \end{array}\right). \tag{6.31}$$

It follows from Corollary 6.13 that, for each prime $\ell \in \Sigma_{0,\mathrm{bad}}$, there exists an integer $N'_\ell \in \mathbb{Z}_{\geq 1}$ such that

$$\left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_f(K_{n,w}^E, E[p^n]) \cap H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \simeq \left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_f(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}},$$

$$\left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_f(K_{n,w}^E, E[p^n]) \cap H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \simeq \left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}}$$

for any $n \geq N'_\ell$. We have an isomorphism

$$\left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_f(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \simeq \left(\prod_{w|\ell} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \tag{6.32}$$

for any $n \geq N'_\ell$. Now, we put $N := \max\{N'_\ell | \ell \in \Sigma_{0,\mathrm{bad}}\}$. For any $n \geq N$, we have

$$\begin{aligned} & H^0(K_n, \mathrm{Sel}_p(K_n^E, E[p^n])) \\ & = \operatorname{Ker}\left(\begin{array}{l} H^1(K_n^E, E[p^n])^{G_{K_n}} \\ \quad \longrightarrow \left(\prod_{w|p} H^1(K_{n,w}^E, E[p^n]) \times \prod_{w\nmid p} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_f(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \end{array}\right) \\ & \overset{(\diamondsuit)}{=} \operatorname{Ker}\left(\begin{array}{l} H^1(K_n^E, E[p^n])^{G_{K_n}} \\ \quad \longrightarrow \left(\prod_{w|p} H^1(K_{n,w}^E, E[p^n]) \times \prod_{w\nmid p} \frac{H^1(K_{n,w}^E, E[p^n])}{H^1_{\mathrm{ur}}(K_{n,w}^E, E[p^n])}\right)^{G_{K_n}} \end{array}\right) \\ & \overset{(6.31)}{\simeq} S_n. \end{aligned}$$

Here, the second equality $(\diamondsuit)$ follows from (6.32) for a bad prime $\ell \neq p$ and Remark 5.2 for a good prime $\ell \neq p$. $\square$

Theorem 6.16. *Suppose that E satisfies the conditions* (C1), (C2) *and* (C3). *Then, there exists a family of R_n-homomorphisms*

$$r_n \colon \mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \longrightarrow (A_n^E)^\vee$$

such that the kernel $\mathrm{Ker}(r_n)$ *and the cokernel* $\mathrm{Coker}(r_n)$ *are finite with order bounded independently of n.*

Proof. By Proposition 6.7 and Lemma 6.15, there exists $N \in \mathbb{Z}_{\geq 1}$, the order of the kernel and that of the cokernel of the map

$$\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \xrightarrow{\left(\mathrm{res}_n^{\mathrm{Sel}}\right)^{\oplus 2}} H^0(K_n, \mathrm{Sel}_p(K_n^E, E[p^n]))^{\oplus 2} \simeq S_n^{\oplus 2}$$

are at most $p^{2\nu_{\mathrm{res}}^{\mathrm{Ker}}}$ and $p^{2\nu_{\mathrm{res}}^{\mathrm{Coker}}}$ respectively for all $n \geq N$. By Lemma 6.14, there is an isomorphism $S_n^{\oplus 2} \simeq (A_n^E)^\vee$. Since $\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2}$ and $(A_n^E)^\vee$ are finite for any $n < N$, this completes the proof of Theorem 6.16. $\square$

References

[1] S. BLOCH & K. KATO, "L-functions and Tamagawa numbers of motives", in *The Grothendieck Festschrift. Vol. I*, Progress in Mathematics, vol. 86, Birkhäuser, 1990, p. 333-400.

[2] J. D. DIXON, M. P. F. DU SAUTOY, A. MANN & D. SEGAL, *Analytic pro-p groups*, Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, 2003.

[3] B. EDIXHOVEN, "The weight in Serre's conjectures on modular forms", *Invent. Math.* **109** (1992), no. 3, p. 563-594.

[4] D. EISENBUD, *Commutative Algebra. With a View Toward Algebraic Theory*, Graduate Texts in Mathematics, vol. 150, Springer, 1995.

[5] J. GARNEK, "On class numbers of division fields of abelian varieties", *J. Théor. Nombres Bordeaux* **31** (2019), no. 1, p. 227-242.

[6] T. HIRANOUCHI, "Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$", *Hiroshima Math. J.* **49** (2019), no. 1, p. 117-128.

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

[8] K. IWASAWA, "On $\mathbb{Z}_\ell$-extensions of algebraic number fields", *Ann. Math.* **98** (1973), p. 246-326.

[9] K. KATO, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.

[10] M. LAZARD, "Groupes analytiques p-adiques", *Publ. Math., Inst. Hautes Étud. Sci.* **26** (1965), p. 389-603.

[11] THE LMFDB COLLABORATION, "The L-functions and Modular Forms Database", `http://www.lmfdb.org`, accessed 21 March 2022.

[12] J. NEUKIRCH, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, 1999.

[13] J. NEUKIRCH, A. SCHMIDT & K. WINGBERG, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2008.

[14] T. OHSHITA, "Asymptotic lower bound of class numbers along a Galois representation", *J. Number Theory* **211** (2020), p. 95-112.

[15] ———, "On higher Fitting ideals of certain Iwasawa modules associated with Galois representations and Euler systems", *Kyoto J. Math.* **61** (2021), no. 1, p. 1-95.

[16] D. PRASAD & S. SHEKHAR, "Relating the Tate–Shafarevich group of an elliptic curve with the class group", *Mathematics* **312** (2021), no. 1, p. 203-218.

[17] K. RUBIN, *Euler systems*, Annals of Mathematics Studies, vol. 147, Hermann, 2000, Hermann Weyl lectures.

[18] F. SAIRAIJI & T. YAMAUCHI, "On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$", *J. Number Theory* **156** (2015), p. 277-289.

[19] ———, "On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$", *J. Théor. Nombres Bordeaux* **30** (2018), no. 3, p. 893-915.

[20] J.-P. SERRE, *Corps locaux*, 2nd ed., Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 8, Hermann, 1968.

[21] ———, “Sur les groupes de congruence des variétés abéliennes. II”, *Izv. Akad. Nauk SSSR, Ser. Mat.* **35** (1971), no. 4, p. 731-737.

[22] ———, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15** (1972), p. 259-331.

[23] ———, *Abelian l-adic representations and elliptic curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Group, 1989.

[24] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2009.

[25] ———, *Advanced topic in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 2013.

[26] C. Skinner & E. Urban, “The Iwasawa Main Conjectures for GL_2”, *Invent. Math.* **195** (2014), no. 1, p. 1-277.

[27] The Stacks Project Authors, “Stacks Project”, 2022, `http://stacks.math.columbia.edu`.

[28] J. Tate, “Relation between K_2 and Galois cohomology”, *Invent. Math.* **36** (1976), p. 257-274.

[29] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer, 1997.

[30] C. Wuthrich, “The fine Selmer group and height pairings”, PhD Thesis, University of Cambridge, UK, 2004.

Toshiro Hiranouchi
Department of Basic Sciences
Graduate School of Engineering
Kyushu Institute of Technology
1-1 Sensui-cho, Tobata-ku, Kitakyushu-shi
Fukuoka 804-8550, Japan
E-mail: `hira@mns.kyutech.ac.jp`

Tatsuya Ohshita
Department of Mathematics
Cooperative Faculty of Education
Gunma University, Maebashi
Gunma 371-8510, Japan
E-mail: `ohshita@gunma-u.ac.jp`