ON THE MOD p IWASAWA THEORY FOR ELLIPTIC CURVES

CHAN-HO KIM AND R. SUJATHA

ABSTRACT. In this note, we study the mod p behavior of Kato's Euler systems and fine Selmer groups for an elliptic curve with good reduction at a prime $p \geq 5$. We show that we observe a version of the λ-invariant formula for fine Selmer groups for congruent elliptic curves holds, as in the work of Greenberg–Vatsal, and formulate a mod p version of Kato's main conjecture.

1. INTRODUCTION

The goal of this article is to understand a refined aspect of Iwasawa theory of elliptic curves with good reduction from the point of view of the associated residual representations.

1.1. **Variation of Iwasawa invariants in congruent families.** Let E_1 and E_2 be elliptic curves defined over $\mathbb{Q}$ such that $E_1[p] \simeq E_2[p]$ as *irreducible* Galois modules, where p is an odd prime. The curves E_1 and E_2 are then said to be congruent modulo p. Consider the following question.

Question 1.1. Which properties and invariants in Iwasawa theory of elliptic curves depend only on the mod p representation?

From now on, we assume that every mod p representation is a surjective Galois representation throughout this article (Assumption 2.1).

In the case when the elliptic curves have good ordinary reduction at p, Greenberg–Vatsal [GV00] prove the following statements for elliptic curves. Let μ^{an} and λ^{an} be the μ-invariant and λ-invariant of the p-adic L-function, respectively, while μ^{alg} and λ^{alg} are those of the characteristic power series of the dual Selmer group.

(1) If $\mu^{\mathrm{an}} = 0$ for one elliptic curve, then $\mu^{\mathrm{an}} = \mu^{\mathrm{alg}} = 0$ for all congruent elliptic curves.
(2) Under $\mu^{\mathrm{an}} = 0$, the difference of the analytic and the algebraic λ-invariants, $\lambda^{\mathrm{an}} - \lambda^{\mathrm{alg}}$ is invariant for congruent elliptic curves. Further, the variation of each of the invariants, λ^{an} and λ^{alg} for congruent elliptic curves can be computed in terms of Euler factors.
(3) Under $\mu^{\mathrm{an}} = 0$, the validity of the main conjecture is invariant for congruent elliptic curves. This uses the one-sided divisibility result of Kato.

This work has been generalized to Hida families in [EPW06].

When the elliptic curves have supersingular reduction at $p \geq 5$, the $\pm$-Iwasawa theory for elliptic curves with supersingular reduction à la Kobayashi–Pollack [Kob03, Pol03] is available, and similar results for $\pm$-Selmer groups and $\pm$-p-adic L-functions are proved in [Kim09] and [GIP]. Let $\mu^{\mathrm{an},\pm}$ and $\lambda^{\mathrm{an},\pm}$ be the Iwasawa invariants of the $\pm$-p-adic L-function, and $\mu^{\mathrm{alg},\pm}$ and $\lambda^{\mathrm{alg},\pm}$ be those of the characteristic power series of the dual $\pm$-Selmer group.

($1_\pm$) If $\mu^{\mathrm{an},\pm} = 0$ for one elliptic curve, then $\mu^{\mathrm{an},\pm} = \mu^{\mathrm{alg},\pm} = 0$ for all congruent elliptic curves.
($2_\pm$) Under $\mu^{\mathrm{an},\pm} = 0$, $\lambda^{\mathrm{an},\pm} - \lambda^{\mathrm{alg},\pm}$ is invariant for congruent elliptic curves. Further, even the variation of each $\lambda^{\mathrm{an},\pm}$ and $\lambda^{\mathrm{alg},\pm}$ can be computed in terms of Euler factors, for congruent elliptic curves.

Date: July 25, 2023.
2010 *Mathematics Subject Classification.* 11R23 (Primary); 11G05, 11G40, 11F67 (Secondary).
Key words and phrases. Iwasawa theory, elliptic curves, supersingular primes.

($3_\pm$) Under $\mu^{\mathrm{an},\pm} = 0$, the validity of the $\pm$-main conjecture is invariant for congruent elliptic curves. Again, this is proved using the one-sided divisibility result of Kato.

In this article, the focus is on Kato's formulation of the Iwasawa main conjecture [Kat04, Conjecture 12.10] for elliptic curves with good reduction. Indeed, the first-named author has also studied the behavior of the Iwasawa modules in Kato's main conjecture for congruent elliptic curves in [KLP]. Let μ^{Kato} and λ^{Kato} be the Iwasawa μ- and λ-invariants of the quotient of the first Iwasawa cohomology by Kato's zeta element [Kat04, Theorem 12.5.(4)], and μ^{fine} and λ^{fine} be those of the characteristic power series of the dual fine Selmer group. See [CS06] for the study of μ^{fine} and [Suj11] for a more general description of the μ-invariants. The following (slightly weaker) results are proved for elliptic curves with good reduction in [KLP].

(1_{Kato}) If $\mu^{\mathrm{Kato}} = 0$ for one elliptic curve, then $\mu^{\mathrm{Kato}} = \mu^{\mathrm{fine}} = 0$ for all congruent elliptic curves.

(2_{Kato}) Under $\mu^{\mathrm{Kato}} = 0$, $\lambda^{\mathrm{Kato}} - \lambda^{\mathrm{fine}}$ is invariant for congruent elliptic curves.

(3_{Kato}) Under $\mu^{\mathrm{Kato}} = 0$, the validity of Kato's main conjecture is invariant for congruent elliptic curves. Again, this is proved using the one-sided divisibility result of Kato.

As we see, (2_{Kato}) does not fully capture the information on how each λ-invariant varies for congruent elliptic curves although the result in [KLP] is enough to deduce an application to the Iwasawa main conjecture. *The goal of this paper is to study the explicit variation of both λ^{Kato} and λ^{fine}, i.e. the λ-invariants that occur in* (2_{Kato})*,* see (Theorem 2.9). In other words, we study an explicit comparison of the variation of λ^{Kato} and λ^{fine} for congruent elliptic curves under $\mu^{\mathrm{Kato}} = 0$. This points towards a "mod p Iwasawa theory for elliptic curves" and "mod p main conjectures", and this conjectural framework is outlined below. Although the comparison contains an "error" term coming from possibly non-trivial finite Iwasawa submodules of the dual fine Selmer group, we also analyze the error term in terms of Coleman maps.

1.2. **The formulation of the mod p main conjecture "with mod p L-functions".** In this subsection, we review how the mod p main conjecture "with mod p L-functions" is formulated in order to motivate our formulation of the mod p main conjecture "without mod p L-functions".

The following *mod p main conjecture for Hida families* is formulated in [EPW06, §1.4].

Let p be a prime ≥ 5. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\mathbb{Q}_n$ the subextension of $\mathbb{Q}$ in $\mathbb{Q}_\infty$ of degree p^n. Denote by $\Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$ the Iwasawa algebra.

Let Y be a branch of the Hida family of a given (irreducible) mod p representation $\overline{\rho}$ and fixed tame level N. Let $f \in Y$ be a newform, π a chosen p-adic uniformizer of the Hecke field of f, and A_f the corresponding discrete Galois representation. Following [EPW06, §4.2], there exists the residual Selmer structure $\mathcal{S}(f)$ characterized by $\mathrm{Sel}_{\mathcal{S}(f)}(\mathbb{Q}_\infty, \overline{\rho}) \simeq \mathrm{Sel}(\mathbb{Q}_\infty, A_f)[\pi]$. The residual Selmer structure $\mathcal{S}(f)$ depends on both $\overline{\rho}$ and N in general. Under the vanishing of μ-invariant of Selmer groups, it is known that the algebraic λ-invariants of all members of Y are all the same, and equal to $\dim_{\mathbb{F}_p}\mathrm{Sel}_{\mathcal{S}(f)}(\mathbb{Q}_\infty, \overline{\rho})$, which we denote by $\lambda^{\mathrm{alg}}(Y)$. See [EPW06, Corollary 2].

On the other hand, the existence of the "mod p L-function" is expected. See [Maz79, §3.4]. The mod p L-function is defined by the mod p reduction of the integral p-adic L-function constructed in [EPW06, §1.4]. Henceforth, by mod p L-functions, we shall always mean "mod p, p-adic L-functions". Note that the mod p L-functions also depend on both $\overline{\rho}$ and N, in general.

Let us now set the notation that will be used in the article.

Notation 1.2. (1) For an ordinary elliptic curve E (resp. an ordinary modular form f), denote by $L_p(E)$ (resp. $L_p(f)$) the p-adic L-function of E (resp. f), respectively.

(2) For a branch of the Hida family, denote by $L_p(Y)$ the "two-variable" p-adic L-function of Y.

(3) For the ordinary mod p representation $E[p]$ (resp. $\overline{\rho}$), denote by $L_p(E[p])$ (resp. $L_p(\overline{\rho})$) the mod p L-function of $E[p]$ (resp. $\overline{\rho}$) which is obtained by the mod p reduction of the p-adic L-functions.

Under the vanishing of μ-invariant, it is also known that the analytic λ-invariants are constant along a branch, and we write $\lambda^{\mathrm{an}}(Y) = \lambda(L_p(Y))$.

Conjecture 1.3 (Mod p main conjecture for Hida families). *With notation as above, the following statement holds.*

(1) *the mod p L-function $L_p(\overline{\rho})$ of Y is non-zero (i.e. $\mu^{\mathrm{an}}(Y) = 0$),*
(2) *$\lambda^{\mathrm{alg}}(Y)$ is finite, and*
(3) *$\lambda^{\mathrm{an}}(Y) = \lambda^{\mathrm{alg}}(Y)$.*

Remark 1.4. The first statement corresponds to the $\mu = 0$ conjecture for p-adic L-functions. In the case of elliptic curves, it corresponds to Greenberg's conjecture [Gre99, Conjecture 1.11], which says that there exists an elliptic curve in its $\mathbb{Q}$-isogeny class such that the μ-invariant of the elliptic curve vanishes. The second one is the Λ-torsionness of the dual Selmer group for all members of Y. The last one is equivalent to the Iwasawa main conjecture for all members of Y. The key feature is that all these conjectures depend only on the residual representation $\overline{\rho}$ and the fixed tame level N.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with supersingular reduction at a prime $p \geq 5$. Following [EPW06, §4.2] and [Kim09, Definition 2.8], it is easy to see that there exist the residual Selmer structure $\mathcal{S}^{\pm}(E)$ characterized by $\mathrm{Sel}_{\mathcal{S}^{\pm}(E)}(\mathbb{Q}_\infty, E[p]) \simeq \mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])[p]$. For a cofinitely generated module M, denote by $M^\vee$ the Pontryagin dual of M.

Motivated by Conjecture 1.3, the mod p $\pm$-main conjecture for elliptic curves can be formulated without too much effort.

Conjecture 1.5 (Mod p $\pm$-main conjecture). *Write $L^{\pm}_p(E[p]) = L^{\pm}_p(E) \pmod p$.*

(1) *the mod p $\pm$-L-function $L^{\pm}_p(E[p])$ is non-zero (i.e. $\mu(L^{\pm}_p(E)) = 0$),*
(2) *$\lambda(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee) = \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathcal{S}^{\pm}(E)}(\mathbb{Q}_\infty, E[p])$ is finite, and*
(3) *$\lambda(L^{\pm}_p(E)) = \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathcal{S}^{\pm}(E)}(\mathbb{Q}_\infty, E[p])$.*

Remark 1.6. As before, the first statement corresponds to the $\mu = 0$ conjecture for $\pm$-p-adic L-functions. The second one is the Λ-cotorsionness of $\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])$. The last one is equivalent to the usual $\pm$-main conjecture for all elliptic curves whose residual representations are isomorphic to $E[p]$. All these conjectures depend only on the residual representation $E[p]$ and the conductor N again.

We briefly summarize how a variety of earlier congruence results fit naturally in the framework of the mod p L-functions. Consider two normalized Hecke eigenforms whose Fourier coefficients are congruent modulo p. Then the congruence properties between the special values of their associated L-functions have been studied. Greenberg and Vatsal consider the special case of elliptic curves. Suppose E is an elliptic curve over $\mathbb{Q}$ and ρ_1, ρ_2 are two Dirichlet characters that are congruent modulo p. The congruence properties between the twisted L-values $L(E, \rho_i, 1)$ for $i = 1, 2$ have also been studied [Vat99]. In [SS15], this was extended to the setting of two new, normalized Hecke eigenforms of weight 2 with residually isomorphic Galois representations and the twisted L-values obtained by considering twists by Artin representations that arise from a dihedral extension, and are congruent modulo p. These methods were extended to the case of Selmer groups of Galois representations associated with ordinary Hilbert modular forms by Delbourgo and Lei [DL18].

Viewed through the lens of the mod p L-functions, it becomes clear that in all these cases the objects of study are the Selmer groups associated with Galois representations that have the property that the associated residual Galois representations are isomorphic. One may then work with this single residual Galois representation and the congruence results may be interpreted via the associated mod p L-function.

One may want to formulate the mod p version of Kato's main conjecture, i.e. the "mod p main conjecture without mod p L-functions" and relate it to these mod p main conjectures with mod p L-functions. However, it is trickier to formulate the main conjectures with (signed) p-adic L-functions, since the naïve mod p reduction of the first Iwasawa cohomology of T and the first Iwasawa cohomology of T/pT differ by the p-torsion of the second Iwasawa cohomology of T. This requires a more delicate analysis, which is the key feature of §4.3.

Here is the plan of the paper. In §2, we quickly review some preliminaries, recall the relevant setting, and give the statement of the main theorem (Theorem 2.9). In §3, we give a proof of Theorem 2.9 on the first and the second invariants. In §4, we recall the relevant results of B.D. Kim on Selmer groups and present the corresponding results on p-adic L-functions (c.f. [GIP]). Then we complete the proof of Theorem 2.9 by applying the techniques from $\pm$-Iwasawa theory.

2. The main result and related topics

2.1. **Iwasawa cohomology and Selmer groups.** Throughout this article, it is assumed that an elliptic curve E over $\mathbb{Q}$ and a prime $p > 3$ satisfy the following properties.

Assumption 2.1. *For any elliptic curve E over $\mathbb{Q}$, we assume that*

(1) *the mod p representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_p}(E[p])$ is surjective, and*
(2) *p does not divide the conductor of E.*

For a mod p representation $\overline{\rho}$, denote by $N(\overline{\rho})$ the prime-to-p Artin conductor of $\overline{\rho}$. We say that the conductor N of an elliptic curve E is *minimal* with respect to p if $N = N(E[p])$.

Let Σ be a finite set of places of $\mathbb{Q}$ containing p, ∞ and all the bad reduction primes for E. For a number field F, denote by F_Σ the maximal extension of F unramified outside the primes of F lying above the primes in Σ.

Denote by T the p-adic Tate module of E. For $a = 1, 2$, the global and local Iwasawa cohomologies without any restriction are defined by $\mathrm{H}^a_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T) := \varprojlim_n \mathrm{H}^a(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T)$ and $\mathrm{H}^a_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T) := \varprojlim_n \mathrm{H}^a(\mathbb{Q}_{n,p}, T)$ where the inverse limit are taken with respect to the corestriction maps. Note that $\mathrm{H}^a_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)$ depends on the choice of Σ.

Let $j : \mathrm{Spec}(\mathbb{Q}_n) \to \mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p])$ be the natural map and we use the same notation for $\mathbb{Q}_\infty$. For $a = 1, 2$, the **a-th Iwasawa cohomology for T** is defined by $\mathrm{H}^a_{\mathrm{Iw}}(j_*T) := \varprojlim_n \mathrm{H}^a_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_{n,*}T)$ where $\mathrm{H}^a_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_{n,*}T)$ is the étale cohomology group and the inverse limit is taken with respect to the corestriction map. This definition is independent of the choice of Σ. It is well-known that $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T) \simeq \mathrm{H}^1_{\mathrm{Iw}}(j_*T)$. See [Kur02] and [Kob03] for details.

Theorem 2.2 (Kato). (1) *$\mathrm{H}^2_{\mathrm{Iw}}(j_*T)$ is a finitely generated torsion module over Λ.*
(2) *$\mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ is free of rank one over Λ under Assumption 2.1.(1).*

Proof. See [Kat04, Theorem 12.4]. □

Let $\Sigma_0 \subseteq \Sigma$ be a subset of Σ not containing p or ∞. We recall that the **Σ_0-imprimitive Selmer group of E over F** is defined by

$$\mathrm{Sel}^{\Sigma_0}(F, E[p^\infty]) = \ker\left(\mathrm{H}^1(F_\Sigma/F, E[p^\infty]) \to \prod_{\ell \in \Sigma \setminus \Sigma_0} \frac{\mathrm{H}^1(F \otimes \mathbb{Q}_\ell, E[p^\infty])}{E(F \otimes \mathbb{Q}_\ell) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$$

where $\mathrm{H}^1(F_\Sigma/F, E[p^\infty]) = \mathrm{H}^1(\mathrm{Gal}(F_\Sigma/F), E[p^\infty])$. Since p is odd, the local cohomology at the infinite place is trivial; thus, the use of $\Sigma \setminus \Sigma_0$ is equivalent to the use of $\Sigma \setminus (\Sigma_0 \cup \{\infty\})$ in the product of local conditions.

The Σ_0**-imprimitive fine Selmer group of** E **over** F is defined by $\mathrm{Sel}_0^{\Sigma_0}(F,E[p^\infty]) = \ker\left(\mathrm{Sel}^{\Sigma_0}(F,E[p^\infty]) \to \mathrm{H}^1(F\otimes\mathbb{Q}_p,E[p^\infty])\right)$. Over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$, we have

$$\mathrm{Sel}^{\Sigma_0}(\mathbb{Q}_\infty,E[p^\infty]) := \varinjlim_n \mathrm{Sel}^{\Sigma_0}(\mathbb{Q}_n,E[p^\infty]), \qquad \mathrm{Sel}_0^{\Sigma_0}(\mathbb{Q}_\infty,E[p^\infty]) := \varinjlim_n \mathrm{Sel}_0^{\Sigma_0}(\mathbb{Q}_n,E[p^\infty]).$$

When $\Sigma_0=\emptyset$, we recover the usual Selmer groups and remove Σ_0 in the notation. It will be shown later (Proposition 3.1) that the dual fine Selmer group $\mathrm{Sel}_0(\mathbb{Q}_\infty,E[p^\infty])^\vee$ and $\mathrm{H}^2_{\mathrm{Iw}}(j_*T)$ are isomorphic.

2.2. **Kato's main conjecture and Kobayashi's main conjecture.** For an elliptic curve E over $\mathbb{Q}$, let $\mathbf{z}_{\mathrm{Kato}}(E)\in \mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ be Kato's zeta element for E [Kur02, Theorem 5.1] such that

$$\exp^*(\mathrm{loc}_p z_{\mathbb{Q}}(E)) = \frac{L^{(p)}(E,1)}{\Omega_E^+}\cdot\omega_E$$

where

- $\exp^* : \mathrm{H}^1(\mathbb{Q}_p,T)\to \cot(E/\mathbb{Q}_p) = \mathbb{Q}_p\omega_E$ is the Bloch–Kato dual exponential map [Kat93, §II.1.2],
- $\mathrm{loc}_p : \mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q},T)\to\mathrm{H}^1(\mathbb{Q}_p,T)$ is the natural restriction map,
- $z_{\mathbb{Q}}(E)$ is the image of $\mathbf{z}_{\mathrm{Kato}}(E)$ in $\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q},T)$ via the corestriction map,
- $L^{(p)}(E,1) = (1-a_p(E)\cdot p^{-1}+p^{-1})\cdot L(E,1)$ is the L-value of E at $s=1$ whose Euler factor at p is removed,
- ω_E is a generator of the global differentials of a minimal Weierstrass model of E, and
- Ω_E^+ is the real period of E (depending on ω_E).

For a finitely generated torsion Λ-module M, we denote by $\mathrm{char}_\Lambda(M)$ the associated characteristic ideal, and by $\mu(M)=\mu(\mathrm{char}_\Lambda(M))$ and $\lambda(M)=\lambda(\mathrm{char}_\Lambda(M))$, the Iwasawa invariants of M.

We consider the Iwasawa main conjecture à la Kato [Kur02, Conjecture 6.1], [Kat04].

Conjecture 2.3 (Kato's main conjecture)**.** *Under Assumption 2.1.(1),*

$$\mathrm{char}_\Lambda \mathrm{H}^1_{\mathrm{Iw}}(j_*T)/\mathbf{z}_{\mathrm{Kato}}(E) = \mathrm{char}_\Lambda \mathrm{H}^2_{\mathrm{Iw}}(j_*T)$$

Theorem 2.4 (Kato)**.** *Under Assumption 2.1.(1),*

$$\mathrm{char}_\Lambda \mathrm{H}^1_{\mathrm{Iw}}(j_*T)/\mathbf{z}_{\mathrm{Kato}}(E) \subseteq \mathrm{char}_\Lambda \mathrm{H}^2_{\mathrm{Iw}}(j_*T).$$

Notably, $\mu(\mathrm{H}^2_{\mathrm{Iw}}(j_*T))\le\mu(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)/\mathbf{z}_{\mathrm{Kato}}(E))$ *and* $\lambda(\mathrm{H}^2_{\mathrm{Iw}}(j_*T))\le\lambda(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)/\mathbf{z}_{\mathrm{Kato}}(E))$.

Proof. See [Kat04, Theorem 12.5.(4)]. □

Corollary 2.5. *If the inequalities of Iwasawa invariants in Theorem 2.4 are equalities, then Kato's main conjecture holds.*

In the good ordinary case, it is known that Conjecture 2.3 is equivalent to the usual main conjecture with p-adic L-functions

$$\mathrm{char}_\Lambda \Lambda/L_p(E) = \mathrm{char}_\Lambda \mathrm{Sel}(\mathbb{Q}_\infty,E[p^\infty])^\vee$$

and one inclusion $\subseteq$ holds by using Theorem 2.4.

In the supersingular case, it is well-known that $\mathrm{Sel}(\mathbb{Q}_\infty,E[p^\infty])$ is never Λ-cotorsion. Kobayashi [Kob03] introduced the notion of $\pm$-Selmer groups, which are Λ-cotorsion, and formulated the $\pm$-main conjecture, recalled in §4.

Conjecture 2.6 (Kobayashi's main conjecture)**.** *Under Assumption 2.1, if E has supersingular reduction at $p>3$, then*

$$\mathrm{char}_\Lambda \Lambda/L_p^{\pm}(E) = \mathrm{char}_\Lambda \mathrm{Sel}^{\pm}(\mathbb{Q}_\infty,E[p^\infty])^\vee,$$

respectively.

Theorem 2.7 (Kobayashi)**.** *Suppose that E has supersingular reduction at $p > 3$.*

(1) $\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee$ *is a finitely generated torsion Λ-module.*
(2) *The following three statements are equivalent:*
   (a) *Conjecture 2.3.*
   (b) *The $+$-part of Conjecture 2.6.*
   (c) *The $-$-part of Conjecture 2.6.*
(3) *Under Assumption 2.1.(1),*
$$\mathrm{char}_\Lambda \Lambda/L_p^{\pm}(E) \subseteq \mathrm{char}_\Lambda \mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee.$$

2.3. **Iwasawa theoretic Euler factors.** Let ℓ be a rational prime with $\ell \neq p$. Let γ_ℓ be the arithmetic Frobenius at ℓ in $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Following [GV00, (15)], the **Iwasawa theoretic Euler factor $\mathcal{P}_\ell(E)$ of E at ℓ** is defined by
$$\mathcal{P}_\ell(E) := \begin{cases} 1 - a_\ell(E)\ell^{-1}\gamma_\ell + \ell^{-1}\gamma_\ell^2 & \text{if } \ell \nmid N \\ 1 - a_\ell(E)\ell^{-1}\gamma_\ell & \text{if } \ell \| N \\ 1 & \text{if } \ell^2 | N \end{cases}$$
in Λ and it satisfies the following equality of ideals in Λ.

Lemma 2.8 (Greenberg–Vatsal)**.** *We have*
$$(\mathcal{P}_\ell(E)) = \mathrm{char}_\Lambda \left((\prod_{\eta|\ell} \mathrm{H}^1(\mathbb{Q}_{\infty,\eta}, E[p^\infty]))^\vee \right) = \mathrm{char}_\Lambda \left(\prod_{\eta|\ell} \mathrm{H}^2(\mathbb{Q}_{\infty,\eta}, T) \right)$$
and its μ-invariant is zero.

Proof. See [GV00, Proposition 2.4]. □

2.4. **Main results and applications.** We obtain the following result towards the formulation of the mod p Kato's main conjecture.

Theorem 2.9 (Main Theorem)**.** *Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ satisfying Assumption 2.1. Let T_i be the p-adic Tate module for E_i for $i = 1, 2$. Let Σ be a finite set of primes containing p, ∞, and all the bad reduction primes for E_1 and E_2. Denote by $\Sigma_0 = \Sigma \setminus \{p, \infty\}$. Assume that $E_1[p] \simeq E_2[p]$ as Galois modules.*

(1) *If E_i has good ordinary reduction at p and $\mu(L_p(E_i)) = 0$ for one of $i = 1, 2$, then the following three invariants*
$$\lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T_i)\right) + \sum_{\ell\in\Sigma_0} \lambda\left(\mathcal{P}_\ell(E_i)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_i)[p]\right), \tag{2.1}$$
$$\lambda\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T_i)}{\mathbf{z}_{\mathrm{Kato}}(E_i)}\right) + \sum_{\ell\in\Sigma_0} \lambda\left(\mathcal{P}_\ell(E_i)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_i)[p]\right), \text{ and} \tag{2.2}$$
$$\dim_{\mathbb{F}_p}\left(\Lambda/(\mathrm{Col}\circ\mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T_i)), p)\right) - \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_i)[p]\right) \tag{2.3}$$
are independent of i where Col *is the Coleman map. In other words, all these invariants depend only on the residual representation and Σ_0.*

(2) *If E_i has good supersingular reduction at p and $\mu(L_p^{\pm}(E_i)) = 0$ for one of $i = 1, 2$, then the same conclusion holds but the third invariant is replaced by*
$$\dim_{\mathbb{F}_p}\left(\Lambda/(\mathrm{Col}^{\pm}\circ\mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T_i)), p)\right) - \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_i)[p]\right)$$
where $\mathrm{Col}^{\pm}$ is the $\pm$-Coleman map, respectively.

Proof. The proof for the first two invariants is given in §3. Regarding the third invariant, we give a proof for the supersingular case only since the ordinary case is easier. See §4 for the proof. □

Although the independence of i result for the first two invariants in Theorem 2.9 looks similar to that in [GV00] and [Kim09], the "error" term $\dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)$ appears due to the possible existence of non-trivial finite Λ-submodules of $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)$. We need to be more careful in stating an analogue of Conjecture 1.3.(2) and Conjecture 1.5.(2), since the λ-invariants and the $\mathbb{F}_p$-dimensions should be clearly distinguished in our setting. More precisely, we will see that

$$\dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)\right) = \lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)$$

depends only on $E[p]$ and Σ provided that $\mu\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) = 0$. It seems difficult to know that $\lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T)\right)$ is constant for congruent elliptic curves of conductor $N(E[p])$. In other words, we do not know whether the Iwasawa invariants themselves vary well under congruences.

Although the error term looks mysterious, we also give an interpretation of this error term in terms of (signed) Coleman maps by looking at the third invariant. An explicit example is illustrated in §5.

Thanks to Theorem 2.9, we are ready to formulate the following conjecture.

Conjecture 2.10 (Mod p Kato's main conjecture)**.** *Let $\mathbf{z}_{\mathrm{Kato}}(E[p])$ be the image of $\mathbf{z}_{\mathrm{Kato}}(E)$ in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)$. With notation as above, the following statement holds.*

(1) *$\mathbf{z}_{\mathrm{Kato}}(E[p])$ is non-zero,*
(2) *$\lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)$ is finite, and*
(3) $\dim_{\mathbb{F}_p}\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)}{\mathbf{z}_{\mathrm{Kato}}(E[p])}\right) = \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)\right).$

Conjecture 2.10 depends only on the residual representation and Σ. By choosing Σ_0 as the set of the primes dividing the conductor N of E, the dependence on N in Conjectures 1.3 and 1.5 and the dependence of Σ in Conjecture 2.10 are equivalent.

Theorem 2.9 recovers the main result of [KLP] for elliptic curves with supersingular reduction, but Theorem 2.9 *does not follow* from the main result of [KLP]. More precisely, the stability of the difference between (2.1) and (2.2) is only considered in [KLP].

Notably, under the assumptions of Theorem 2.9, Kato's main conjectures for E_1 and E_2 are equivalent.

2.5. **Conjecture A and related conjectures.** In this subsection, we assume that E *has supersingular reduction at $p > 3$.* Since the vanishing of μ-invariants of the $\pm$-p-adic L-functions is assumed in Theorem 2.9, we clarify the relation among the vanishing of various μ-invariants and other conjectures.

Conjecture 2.11 (Coates–Sujatha [CS05, Conjecture A])**.** $\mu\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) = 0$.

Remark 2.12. We have $\mu\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) = \mu\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T)\right) = \mu\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}, T)\right)$ where the first equality will be explained in Proposition 3.1 and the second one is due to [CS05, (45) and Lemma 3.1]. Although $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}, T)$ depends on Σ, $\mathrm{H}^2_{\mathrm{Iw}}(j_*T)$ is independent of Σ. It is known that Conjecture 2.11 depends only on $E[p]$. See [KLP, Proposition 6.2.(1)], for example.

Let $\omega_n = (1+X)^{p^n} - 1$ and then $\Phi_n(1+X) = \omega_n/\omega_{n-1}$ where and Φ_n is the p^n-th cyclotomic polynomial. Denote by $e_0 = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q})$ and $e_n = \dfrac{\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}_n) - \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}_{n-1})}{p^{n-1}(p-1)} \in \mathbb{Z}_{\geq 0}$ for $n \geq 1$.

Conjecture 2.13 (Greenberg [KP07, Problem 0.7])**.**

$$\mathrm{char}_\Lambda(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee) = \prod_{e_n \geq 1, n \geq 0} \left(\Phi_n(X+1)^{e_n - 1}\right).$$

Conjecture 2.14 (Kurihara–Pollack [KP07, Problem 3.2])**.**

$$\gcd\left(L_p^+(E), L_p^-(E)\right) = X^{e_0} \cdot \prod_{e_n \geq 1, n \geq 0} \left(\Phi_n(X+1)^{e_n - 1}\right)$$

Proposition 2.15 (Kurihara–Pollack [KP07, Proposition 3.3])**.** *The conjectures of Coates–Sujatha and Kurihara–Pollack (Conjectures 2.11 and 2.14) together imply the conjecture of Greenberg (Conjecture 2.13).*

Remark 2.16. If $E[p]$ is a surjective Galois representation, then the conjecture of Kurihara–Pollack (Conjecture 2.14) also implies the conjecture of Coates–Sujatha (Conjecture 2.11) due to the Euler system argument following [Kat04, Theorem 13.4]. See the comment right after [KP07, Proposition 3.3].

The second named author has obtained the following result with A. Lei [LS21].

Theorem 2.17 (Lei–Sujatha)**.** *Suppose that Kato's main conjecture holds. Then* $\mu\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) = 0$ *if and only if* $\mu\left(\Lambda / L_p^{\pm}(E)\right) = 0$ *for at least one sign.*

To sum up, we have the following implications

$$\begin{tikzcd}
\begin{array}{c}\text{Coates–Sujatha's conjecture A}\\ \text{(Conjecture 2.11)}\end{array} \arrow[rrdd, Rightarrow, dotted, "\text{[LS21]}"] & + \arrow[d, Rightarrow] & \begin{array}{c}\text{Kurihara–Pollack's conjecture}\\ \text{(Conjecture 2.14)}\end{array} \arrow[ll, Rightarrow, bend right, "\text{Euler system argument when } E[p] \text{ is surj. [Kat04, Kob03]}"'] \arrow[dd, Rightarrow] \\
 & \begin{array}{c}\text{Greenberg's conjecture}\\ \text{(Conjecture 2.13)}\end{array} \arrow[ul, Rightarrow] & \\
\mu\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{\mathbf{z}_{\mathrm{Kato}}(E)}\right) = 0 \arrow[uu, Rightarrow, "\text{Thm 2.4}"] & \mu(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee) = 0 \text{ for one of } \pm \arrow[uul, Rightarrow] & \mu(\Lambda/L_p^{\pm}(E)) = 0 \text{ for one of } \pm \arrow[l, Rightarrow, "\text{[Kob03]}"] \arrow[ll, Rightarrow, bend left, "\text{Construction of Col}^{\pm} \text{ [Kob03]}"]
\end{tikzcd}$$

The *dotted* implication means that it requires Kato's main conjecture. The implication of

$$\mu(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee) = 0 \text{ for one of } \pm \Rightarrow \text{Conjecture A of Coates–Sujatha}$$

follows immediately from the comparison between $\pm$-Selmer groups and fine Selmer groups.

3. Proof of Theorem 2.9: the first two invariants

3.1. **Fine Selmer groups and the second Iwasawa cohomology.** We recall the following result on the relation between dual fine Selmer groups and $\mathrm{H}^2(j_*T)$.

Proposition 3.1 (Kurihara, Kobayashi)**.** *Suppose that E has good reduction at p and $E[p]$ is surjective. As Λ-modules,* $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ *and* $\mathrm{H}^2_{\mathrm{Iw}}(j_*T)$ *are isomorphic.*

Proof. See [Kur02, §6] and [Kob03, Proposition 7.1.ii)]. □

It is immediate to observe the Σ_0-imprimitive version of Proposition 3.1.

Corollary 3.2. *Put $\Sigma_0 = \Sigma \setminus \{p, \infty\}$. As Λ-modules,* $\mathrm{Sel}_0^{\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])^\vee$ *and* $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)$ *are isomorphic.*

Remark 3.3. It is known that $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ and $(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee)_{\Lambda\text{-tor}}$ are pseudo-isomorphic in our setting [Win89, KP07, Mat20]. See [Gre16] for the triviality of the finite Λ-submodule of the latter.

From now on, we freely interchange the dual Σ_0-imprimitive fine Selmer groups and the second Iwasawa cohomology groups with $\Sigma_0 = \Sigma \setminus \{p, \infty\}$.

3.2. **Proof of Theorem 2.9: the first invariant.** By Theorem 2.4, $\mathrm{H}^2_{\mathrm{Iw}}(j_*T)$ is a torsion Λ-module. From this, It is easy to see that $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)$ is also a torsion Λ-module. If we assume that $\mu\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) = 0$, then we have equality

$$\dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)/p\right) = \lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)$$

and both sides are finite.

Considering the p-cohomological dimension of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$, we have $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)/p \simeq \mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)$, so we obtain the following equality

$$\dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)\right) = \lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right). \tag{3.1}$$

Thus, the independence of i of the first invariant (2.1) in Theorem 2.9 follows from Lemma 2.8 and (3.1).

3.3. **Proof of Theorem 2.9: the second invariant.** We briefly review the construction of Kato's zeta elements and sketch some results from [KLP]. Let $f = \sum_{n\geq 1} a_n(E)q^n$ be the newform corresponding to E. For convenience, write $T_N = \mathrm{H}^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)$ and denote by $\mathrm{Frac}(\Lambda)$ the total quotient ring of Λ. Define the map $\mathbf{z}_{\mathrm{Kato},N} \otimes \mathbb{Q}_p : T_N \otimes \mathbb{Q}_p \to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_N(1)) \otimes_\Lambda \mathrm{Frac}(\Lambda)$ by the composition

$$\begin{tikzcd} T_N \otimes \mathbb{Q}_p \arrow[r] & \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}(\zeta_{p^\infty}), j_*T_N) \otimes_\Lambda \mathrm{Frac}(\Lambda) \arrow[d, "\simeq"] & \\ & \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}(\zeta_{p^\infty}), j_*T_N(1)) \otimes_\Lambda \mathrm{Frac}(\Lambda) \arrow[r] & \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_N(1)) \otimes_\Lambda \mathrm{Frac}(\Lambda) \end{tikzcd}$$

where the first map is the zeta morphism for the space of modular forms of tame level N following [Kat04, §8.9], [FK23, §3], and [KLP], the second isomorphism is the Tate twist, and the last map is the projection to the trivial Teichmüller component. Denote by $\mathbf{z}_{\mathrm{Kato},N}$ the restriction of $\mathbf{z}_{\mathrm{Kato},N} \otimes \mathbb{Q}_p$ to T_N. It is not known that the image of $\mathbf{z}_{\mathrm{Kato},N}$ lies in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_N(1))$ in general. Indeed, we will see that it is true after the localization of $\mathbf{z}_{\mathrm{Kato},N}$ at a certain maximal ideal (Proposition 3.4 below).

Let $\mathbb{T}(N)$ be the full Hecke algebra over $\mathbb{Z}_p$ acting faithfully on $S_2(\Gamma_0(N))$ and $\wp_f$ be the height one prime ideal of $\mathbb{T}(N)$ generated by $T_\ell - a_\ell(f)$ for all ℓ. Since all the objects in the map $\mathbf{z}_{\mathrm{Kato},N}$ are $\mathbb{T}(N)$-modules, we may take the quotient of $\mathbf{z}_{\mathrm{Kato},N}$ by $\wp_f$. By [Kat04, Theorem 12.5], we obtain

$$\mathbf{z}_{\mathrm{Kato},E} : V_pE(-1) \to \mathrm{H}^1_{\mathrm{Iw}}(j_*V_pE) = \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*V_pE) \subseteq \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_pE) \otimes_\Lambda \mathrm{Frac}(\Lambda)$$

where $V_pE = T_pE \otimes \mathbb{Q}_p$ and T_pE is the p-adic Tate module of E. Let $\gamma^\pm_E$ be a $\mathbb{Z}_p$-basis of $T_pE(-1)^\pm$, the eigenspace of $T_pE(-1)$ with respect to complex conjugation with eigenvalue ± 1, respectively. Then $\mathbf{z}_{\mathrm{Kato}}(E)$ is defined by $\mathbf{z}_{\mathrm{Kato},E}(\gamma^+_E + \gamma^-_E)$.

Let $\Sigma_0 = \Sigma \setminus \{p, \infty\}$. Let $N^{\Sigma_0} = N(E[p]) \cdot \prod_\ell \ell \cdot \prod_q q^2$ where $N(E[p])$ is the prime-to-p conductor of $E[p]$, ℓ runs over the primes in Σ_0 exactly dividing $N(E[p])$, and q runs over the primes in Σ_0 not dividing $N(E[p])$. Let $\mathfrak{m}$ be the maximal ideal of $\mathbb{T}(N^{\Sigma_0})$ generated by p, $T_\ell - a_\ell(E)$ for all $\ell \notin \Sigma_0$, and U_q for all $q \in \Sigma_0$. In this case, we say that $\mathfrak{m}$ **is non-Eisenstein** if $E[p]$ is irreducible. Note that Σ_0 contains all prime divisors of N.

Proposition 3.4. *Suppose that $\mathfrak{m}$ is non-Eisenstein. Then the image of the localization of $\mathbf{z}_{\mathrm{Kato},N^{\Sigma_0}}$ at $\mathfrak{m}$ lies in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_{N^{\Sigma_0}}(1))_\mathfrak{m}$. In other words, we have the map*

$$\mathbf{z}_{\mathrm{Kato},N^{\Sigma_0},\mathfrak{m}} : (T_{N^{\Sigma_0}})_\mathfrak{m} \to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_{N^{\Sigma_0}}(1))_\mathfrak{m}$$

Proof. See [KLP] for a detailed proof. The fundamental input is the mod p multiplicity one result [Wil95, Theorem 2.1] since it implies that $(T_{N^{\Sigma_0}})_\mathfrak{m}$ is free of rank two over $\mathbb{T}(N^{\Sigma_0})_\mathfrak{m}$. This result applies when E has good reduction or multiplicative reduction with the p-distinguished property. □

For convenience, denote by T_f an integral Galois-stable lattice in $(T_N/\wp_f) \otimes \mathbb{Q}_p$. Let $f^{\Sigma_0} = \sum_{n\geq 1} a_n(f^{\Sigma_0})q^n = \sum_{n\geq 1,(n,N^{\Sigma_0})=1} a_n(E)q^n$ be the Σ_0-imprimitive eigenform of level N^{Σ_0} and $T_{f^{\Sigma_0}}$ is defined similarly. We also compare two maps

$$\begin{aligned} \mathbf{z}_{\mathrm{Kato},E} = \mathbf{z}_{\mathrm{Kato},f} : T_f &\to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_f(1)), \\ \mathbf{z}_{\mathrm{Kato},f^{\Sigma_0}} : T_{f^{\Sigma_0}} &\to \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, j_*T_{f^{\Sigma_0}}(1)). \end{aligned}$$

As before, $\mathbf{z}_{\mathrm{Kato}}(f^{\Sigma_0}) := \mathbf{z}_{\mathrm{Kato},f^{\Sigma_0}}(\gamma^+_{f^{\Sigma_0}} + \gamma^-_{f^{\Sigma_0}})$ where $\gamma^\pm_{f^{\Sigma_0}}$ is a basis of $T^\pm_{f^{\Sigma_0}}$, respectively. Note that the zeta morphism for one modular form is given in [Kat04, Theorem 12.5].

Proposition 3.5. *Suppose that $\mathfrak{m}$ is non-Eisenstein. Then*

$$\mathbf{z}_{\mathrm{Kato}}(f^{\Sigma_0}) = \left(\prod_{\ell\in\Sigma_0} \mathcal{P}_\ell(E) \right) \cdot \mathbf{z}_{\mathrm{Kato}}(E)$$

up to a p-adic unit.

Proof. See [KLP] for a detailed proof. The Iwasawa theoretic Euler factors appear naturally from the interpolation formula of Kato's zeta elements [Kat04, Theorem 12.5]. The non-trivial part is to show the equivalence between $\mathbf{z}_{\mathrm{Kato}}(f^{\Sigma_0}) \not\equiv 0 \pmod p$ and $\mathbf{z}_{\mathrm{Kato}}(E) \not\equiv 0 \pmod p$, and Ihara's lemma [Rib84] is essential to prove this equivalence. □

Thanks to Proposition 3.5, we define the **Σ_0-imprimitive Kato's zeta element for** E by

$$\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E) := \left(\prod_{\ell\in\Sigma_0} \mathcal{P}_\ell(E) \right) \cdot \mathbf{z}_{\mathrm{Kato}}(E)$$

and its mod p variant $\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])$ by the image of $\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)$ in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)$. By using Proposition 3.4, $\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])$ is also realized as the image of $\mathbf{z}_{\mathrm{Kato},N^{\Sigma_0},\mathfrak{m}}(\gamma^+_{\mathfrak{m}} + \gamma^-_{\mathfrak{m}}) \pmod{\mathfrak{m}}$ in $\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)$ where $\gamma^\pm_{\mathfrak{m}}$ is a basis of $(T_{N^{\Sigma_0}})^\pm_{\mathfrak{m}}$, respectively. Thus, $\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])$ depends only on $E[p]$ and Σ_0.

Lemma 3.6. *Let Σ be a finite set of primes containing the bad reduction primes for E, p, and ∞. Let $\Sigma_0 = \Sigma \setminus \{p, \infty\}$. Suppose that $\mu\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)}\right) = 0$. Then we have*

(1) $\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)}$, $\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])}$, *and* $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]$ *are finite, and*

(2) $\dim_{\mathbb{F}_p}\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)}\right) - \dim_{\mathbb{F}_p}\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])}\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right) = 0.$

Proof. Since $\mu\left(\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)}\right) = 0$, we see that $\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)}$ is finite. By Kato's divisibility (Theorem 2.4), it is not difficult to observe that $\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]$ is also finite. The conclusion follows from the exact sequence

$$0 \longrightarrow \frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)} \longrightarrow \frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])} \longrightarrow \mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p] \longrightarrow 0. \tag{3.2}$$

□

Thanks to Lemma 2.8 and Lemma 3.6, the second invariant (2.2) in Theorem 2.9 is equal to

$$\dim_{\mathbb{F}_p} \frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\infty, T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)} + \dim_{\mathbb{F}_p} \mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]$$

if $E[p] \simeq E_1[p] \simeq E_2[p]$ and Σ contains all the bad reduction primes of E, E_1, and E_2.

4. The $\pm$-Iwasawa theory and congruences

We review $\pm$-Iwasawa theory for elliptic curves with supersingular reduction. The corresponding results for elliptic curves with good ordinary reduction can be found in [GV00,Kat04].

4.1. **The $\pm$-Selmer groups and congruences.** We recall the notion of $\pm$-Selmer groups and their behavior for congruent elliptic curves due to B.D. Kim [Kob03, Kim07, Kim13, Kim09]. In [NS23], more general results are obtained without recourse to the imprimitive Selmer groups and directly working with the residual representations by the second-named author.

Following [Kob03], we define the $\mathbb{Z}_p$-submodules of $E(\mathbb{Q}_{n,p})$ by

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

respectively, where $\mathrm{Tr}_{n/m+1} : E(\mathbb{Q}_{n,p}) \to E(\mathbb{Q}_{m+1,p})$ is the trace map. Let $\Sigma_0 \subseteq \Sigma$ be a subset of Σ not containing p or ∞. Then the **Σ_0-imprimitive $\pm$-Selmer group of E over $\mathbb{Q}_n$** is defined by

$$\mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_n, E[p^\infty]) := \ker\left(\mathrm{Sel}^{\Sigma_0}(\mathbb{Q}_n, E[p^\infty]) \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right).$$

We have $\mathrm{Sel}^{\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty]) = \varinjlim_n \mathrm{Sel}^{\Sigma_0}(\mathbb{Q}_n, E[p^\infty])$ and $\mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty]) = \varinjlim_n \mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_n, E[p^\infty])$, respectively. When $\Sigma_0 = \emptyset$, we recover usual Selmer groups and remove Σ_0 in the notation, as before.

The following result can be found in [Kim13] and [Kim09].

Theorem 4.1 (B.D.Kim)**.** (1) *If $\mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])$ is Λ-cotorsion, then $\mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])$ has no proper Λ-submodule of finite index.*

(2) *Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ satisfying Assumption 2.1. Let Σ_0 be a finite set of primes containing all the bad reduction primes for E_1 and E_2 and not containing p or ∞. Assume that $E_1[p] \simeq E_2[p]$ as Galois modules. If $\mu(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E_1[p^\infty])^\vee) = 0$, then $\mu(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E_2[p^\infty])^\vee) = 0$ and*

$$\lambda(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E_1[p^\infty])^\vee) + \sum_{\ell \in \Sigma_0} \lambda(\mathcal{P}_\ell(E_1)) = \lambda(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E_2[p^\infty])^\vee) + \sum_{\ell \in \Sigma_0} \lambda(\mathcal{P}_\ell(E_2)).$$

Remark 4.2. The Λ-cotorsion property of Σ_0-imprimitive signed Selmer groups follows easily from Theorem 2.7.

4.2. **The $\pm$-p-adic L-functions and congruences.** We recall the notion of $\pm$-p-adic L-functions following [Pol03]. Note that our sign convention is compatible with that of [Kob03], not that of [Pol03].

Recall that $\omega_n = (1+X)^{p^n} - 1$ and $\Phi_n(1+X) = \omega_n/\omega_{n-1}$ where and Φ_n is the p^n-th cyclotomic polynomial. Let $\omega^{\pm}_0(X) := X$, $\widetilde{\omega}^{\pm}_0(X) := 1$, and

$$\omega^+_n = \omega^+_n(X) := X \cdot \prod_{2 \leq m \leq n, m\text{: even}} \Phi_m(1+X), \qquad \omega^-_n = \omega^-_n(X) := X \cdot \prod_{1 \leq m \leq n, m\text{: odd}} \Phi_m(1+X),$$

$$\widetilde{\omega}^+_n = \widetilde{\omega}^+_n(X) := \prod_{2 \leq m \leq n, m\text{: even}} \Phi_m(1+X), \qquad \widetilde{\omega}^-_n = \widetilde{\omega}^-_n(X) := \prod_{1 \leq m \leq n, m\text{: odd}} \Phi_m(1+X).$$

Then we have $\omega_n(X) = \omega_n^{\pm}(X)\cdot\widetilde{\omega}_n^{\mp}(X)$, respectively. We also regard $\omega_n^{\pm}$, $\widetilde{\omega}_n^{\pm}$ as elements in Λ_n or Λ via fixed isomorphisms. Also, we identify $\Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_{n,p}/\mathbb{Q}_p)]$ if necessary. Here, $\mathbb{Q}_{n,p}$ is the completion of $\mathbb{Q}_n$ at the (unique) prime lying above p.

We fix an isomorphism $\mathbb{Z}_p[\![X]\!] \simeq \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$ sending $1+X \mapsto \gamma$ where γ is a topological generator of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

We also identify $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ by sending c to $\sigma_c : \zeta_{p^{n+1}} \mapsto \zeta_{p^{n+1}}^c$, and then we have the following commutative diagram

$$\begin{tikzcd}
(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \arrow[r, "\simeq"] \arrow[d, "\simeq"] & (\mathbb{Z}/p\mathbb{Z})^\times \times \left(\dfrac{1+p^{n+1}\mathbb{Z}}{1+p\mathbb{Z}}\right) \arrow[r, two heads] & \left(\dfrac{1+p^{n+1}\mathbb{Z}}{1+p\mathbb{Z}}\right) \arrow[d, "\simeq"] \\
\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \arrow[rr, two heads] & & \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}).
\end{tikzcd}$$

Definition 4.3. By using the above diagram, the **Mazur–Tate element of E over $\mathbb{Q}_n$** is defined by $\theta_n(E) := \sum_{a\in\mathbb{Z}/p^n\mathbb{Z}} \left[\dfrac{1+ap}{p^{n+1}}\right]\cdot\sigma_{1+ap} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$ where $\left[\dfrac{1+ap}{p^{n+1}}\right]$ are the normalized modular symbols associated to E.

The **$\pm$-p-adic L-function $L_p^{\pm}(E)$ of E** can be characterized by the following proposition.

Proposition 4.4 (Pollack)**.** *$\theta_n(E) \equiv \widetilde{\omega}_n^{\mp}\cdot L_p^{\pm}(E) \pmod{\omega_n}$ in Λ_n if n is even/odd, respectively.*

Proof. See [Pol03, Proposition 6.18]. □

See also [PR04, (10), (11), and (12)] for the interpolation property of the $\pm$-p-adic L-functions.

The following construction of $\pm$-p-adic L-functions, using the Coleman map is due to S. Kobayashi [Kob03, Theorem 6.2, Theorem 6.3, and §8].

Theorem 4.5 (Kobayashi)**.** *There exist the 'n-th layer $\pm$-Coleman maps'*

$$\mathrm{Col}_n^{\pm} : \mathrm{H}^1(\mathbb{Q}_{n,p}, T) \to \Lambda_n/\omega_n^{\pm}$$

such that $\mathrm{Col}_n^{\pm} : \mathrm{H}^1(\mathbb{Q}_{n,p}, T)/\ker \mathrm{Col}_n^{\pm} \simeq \Lambda_n/\omega_n^{\pm}$ and $\mathrm{Col}_n^{\pm}(\mathrm{loc}_p\mathbf{z}_{\mathrm{Kato},n}(E)) = \theta_n^{\pm}(E)$ where $\mathbf{z}_{\mathrm{Kato},n} \in \mathrm{H}^1(\mathbb{Q}_n, T)$ is Kato's zeta element over $\mathbb{Q}_n$ and $\theta_n^{\pm}(E) = L_p^{\pm}(E) \pmod{\omega_n^{\pm}} \in \Lambda_n/\omega_n^{\pm}$. By taking the inverse limit with respect to n, we have the $\pm$-Coleman maps

$$\mathrm{Col}^{\pm} : \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T) \to \Lambda$$

such that $\mathrm{Col}^{\pm}$ are surjective and $\mathrm{Col}^{\pm}(\mathrm{loc}_p\mathbf{z}_{\mathrm{Kato}}(E)) = L_p^{\pm}(E)$.

We briefly sketch how analytic Iwasawa invariants of modular forms at supersingular primes vary for congruent elliptic curves. Although the results here are well-known to the experts (e.g. [GIP]), we include the full details as they are not easily available in the existing literature.

Let $f_1 \in S_2(\Gamma_0(N_1))$ and $f_2 \in S_2(\Gamma_0(N_2))$ be the newforms corresponding to E_1 and E_2, respectively. Let Σ_0 be the set of finite places dividing N_1 and N_2. Let Σ_0 be the set of primes dividing N_1 and N_2 and write $N^{\Sigma_0} = N(\overline{\rho})\cdot\prod_\ell \ell\cdot\prod_q q^2$ where ℓ runs over the primes in Σ_0 exactly dividing $N(\overline{\rho})$ and q runs over the primes in Σ_0 not dividing $N(\overline{\rho})$. Let f^{Σ_0} and g^{Σ_0} be the Σ_0-imprimitive eigenforms of f and g of level N^{Σ_0}, respectively. Then *all* the Fourier coefficients of f^{Σ_0} and g^{Σ_0} are congruent modulo p. The $\mathbb{F}_p$-valued Hecke eigensystem induces the maximal ideal $\mathfrak{m}$ of the full Hecke algebra $\mathbb{T}(N^{\Sigma_0})$ acting faithfully on $S_2(\Gamma_0(N^{\Sigma_0}))$. We recall the mod p multiplicity one result.

Theorem 4.6. *If $\mathfrak{m}$ is non-Eisenstein, then $S_2(\Gamma_0(N^{\Sigma_0}), \mathbb{F}_p)_{\mathfrak{m}}[\mathfrak{m}] \simeq \mathbb{F}_p$.*

Proof. See [Wil95, Theorem 2.1]. □

One consequence of Theorem 4.6 and the integral Eichler–Shimura isomorphism is that the values of the normalized modular symbols associated to f^{Σ_0} and g^{Σ_0} are congruent modulo p. Since Mazur–Tate elements are directly built out of the values of modular symbols, we obtain congruence between Mazur–Tate elements

$$\theta_n(f^{\Sigma_0}) \equiv \theta_n(g^{\Sigma_0}) \pmod{p}, \tag{4.1}$$

In other words, they are same in $\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$. Here, $\theta_n(f^{\Sigma_0})$ are $\theta_n(g^{\Sigma_0})$ are defined as in Definition 4.3 with values of modular symbols associated to f^{Σ_0} and g^{Σ_0}, respectively.

By using Definition 4.3 and Proposition 4.4, $L^{\pm}_p(f^{\Sigma_0})$ and $L^{\pm}_p(g^{\Sigma_0})$ can be defined easily.

Proposition 4.7. *Suppose that $\mathfrak{m}$ is non-Eisenstein. Then $L^{\pm}_p(f^{\Sigma_0}) = L^{\pm}_p(g^{\Sigma_0}) \pmod{p}$, respectively.*

Proof. This follows immediately from Proposition 4.4 and (4.1), which is a consequence of Theorem 4.6. □

The Σ_0**-imprimitive** $\pm$**-p-adic L-functions of** f is defined by $L^{\pm,\Sigma_0}_p(f) := \left(\prod_{\ell\in\Sigma_0}\mathcal{P}_\ell(f)\right)\cdot L^{\pm}_p(f)$. Using Ihara's lemma [Rib84], the following proposition can be easily obtained.

Proposition 4.8. *If $\mathfrak{m}$ is non-Eisenstein, then $L^{\pm}_p(f^{\Sigma_0}) \equiv u\cdot L^{\pm,\Sigma_0}_p(f) \pmod{p}$ in $\mathbb{F}_p[\![X]\!]$, respectively, and $u\in\mathbb{Z}_p^{\times}$.*

Proof. See [Kim17, §5, especially Remark 5.8]. Replacing quaternionic modular forms therein by modular symbols, the proof is verbatim. □

The following corollary is the analytic counterpart of Theorem 4.1.(3).

Corollary 4.9. *Assume $\mathfrak{m}$ is non-Eisenstein and $\mu(L^{\pm}_p(E_1)) = 0$. Then $\mu(L^{\pm}_p(E_2)) = 0$, and*

$$\lambda(L^{\pm}_p(E_1)) + \sum_{\ell\in\Sigma_0}\lambda(\mathcal{P}_\ell(E_1)) = \lambda(L^{\pm}_p(E_2)) + \sum_{\ell\in\Sigma_0}\lambda(\mathcal{P}_\ell(E_2)).$$

In particular, the Iwasawa invariants depend only on the residual representation and conductors.

Proof. By using Proposition 4.7 and Proposition 4.8, we have

$$L^{\pm,\Sigma_0}_p(f) \equiv L^{\pm}_p(f^{\Sigma_0}) \equiv L^{\pm}_p(g^{\Sigma_0}) \equiv L^{\pm,\Sigma_0}_p(g) \pmod{p}$$

in $\mathbb{F}_p[\![\Gamma]\!]$ up to multiplication by an element in $\mathbb{F}_p^{\times}$. □

Since the mod p L-function $L^{\pm}_p(E[p])$ depend only on $E[p]$ and N, we obtain the congruence between the complex twisted L-values from the mod p L-function as we now explain. Fix an isomorphism $\mathbb{F}_p[\![\Gamma]\!] \simeq \mathbb{F}_p[\![X]\!]$ by sending a generator γ of $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ to $X+1$. If $L^{\pm}_p(E[p]) \neq 0$ in $\mathbb{F}_p[\![X]\!]$, then the mod p L-function $L^{\pm}_p(E[p])$ is just X^{λ} where $\lambda = \lambda(L^{\pm}_p(E))$.

In terms of p-adic measures, we have the following interpretation of congruences. Let $\mathcal{C}(\Gamma,\mathbb{F}_p)$ be the space of $\mathbb{F}_p$-valued continuous functions on Γ and define the space of $\mathbb{F}_p$-valued measures on Γ by $\mathrm{Meas}(\Gamma,\mathbb{F}_p) := \mathrm{Hom}_{\mathrm{cts}}(\mathcal{C}(\Gamma,\mathbb{F}_p),\mathbb{F}_p)$. It is easy to see that $\mathrm{Meas}(\Gamma,\mathbb{F}_p)\simeq\mathbb{F}_p[\![\Gamma]\!]$. Let $\overline{\chi}$ be a $\mathbb{F}_p$-valued finite order character on Γ. Let $\mu^{\pm}_{f^{\Sigma_0}}$, $\mu^{\pm}_{g^{\Sigma_0}}$ be the p-adic measures corresponding to the signed p-adic L-functions of f^{Σ_0} and g^{Σ_0}, respectively. Then the congruence $f^{\Sigma_0}\equiv g^{\Sigma_0} \pmod{p}$ yields

$$\mu^{\pm}_{f^{\Sigma_0}}(\overline{\chi}) = \int_\Gamma \overline{\chi}\mu^{\pm}_{f^{\Sigma_0}} = \int_\Gamma \overline{\chi}\mu^{\pm}_{g^{\Sigma_0}} = \mu^{\pm}_{g^{\Sigma_0}}(\overline{\chi}).$$

By using the interpolation formula of signed p-adic L-functions and Mazur–Tate elements [Vat99, Pol03] and Proposition 4.4, the congruence between the complex twisted L-values follows

$$\tau(\chi^{-1})\cdot\frac{L^{\Sigma_0}(f,\chi,1)}{2\pi i\cdot\Omega_f} \equiv \tau(\chi^{-1})\cdot\frac{L^{\Sigma_0}(g,\chi,1)}{2\pi i\cdot\Omega_g} \pmod{p}$$

where $\tau(\chi^{-1})$ is the Gauss sum of χ^{-1} and Ω_f^+, Ω_g^+ are the real canonical periods of f and g.

4.3. **The connection with the $\pm$-Iwasawa theory.** We prove the independence of i for the third invariant for the supersingular case of Theorem 2.9, which describes the p-torsion of the second Iwasawa cohomology in terms of the $\pm$-Coleman maps.

Assumption 4.10. *Suppose that $\mu(L_p^{\pm}(E)) = 0$.*

By the Coleman map construction of $\pm$-p-adic L-functions (Theorem 4.5), we have

$$L_p^{\pm,\Sigma_0}(E) = \mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)). \tag{4.2}$$

Consider the following commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1_{\mathrm{Iw}}(j_*T) \arrow[r, "\mathrm{loc}_p"] \arrow[d] & \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T) \arrow[r, two heads, "\mathrm{Col}^{\pm}"] \arrow[d] & \Lambda \arrow[d, two heads] \\
\dfrac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)} \arrow[r] & \dfrac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T)}{(\mathrm{loc}_p(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)), p)} \arrow[r, two heads] & \dfrac{\Lambda}{(L_p^{\pm,\Sigma_0}(E), p)}
\end{tikzcd}$$

and the surjectivity of the maps in the diagram follows from the surjectivity of $\pm$-Coleman maps (Theorem 4.5). By (4.2) and the surjectivity of $\pm$-Coleman maps, we have

$$\frac{\Lambda}{(L_p^{\pm,\Sigma_0}(E), p)} = \frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)), p)} = \frac{\mathrm{Col}^{\pm}(\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T))}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)), p)}.$$

It is known that $\mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ is free of rank one over Λ under the irreducibility of $E[p]$ [Kat04, Theorem 12.4]. We identify $\mathrm{H}^1_{\mathrm{Iw}}(j_*T) \simeq \Lambda$ and denote by $w \in \mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ the Λ-generator of $\mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ mapping to 1 under the identification and by $f_z \in \Lambda$ the image of $\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)$ under the identification. Then we have equality

$$\begin{aligned}
\frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E)), p)} &= \frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(f_z \cdot w), p)} \\
&= \frac{\Lambda}{(f_z \cdot \mathrm{Col}^{\pm} \circ \mathrm{loc}_p(w), p)}.
\end{aligned}$$

Considering the $\mathbb{F}_p$-dimension of $\dfrac{\Lambda}{(f_z \cdot \mathrm{Col}^{\pm} \circ \mathrm{loc}_p(w), p)}$, we have

$$\dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(f_z \cdot \mathrm{Col}^{\pm} \circ \mathrm{loc}_p(w), p)}\right) = \dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(w), p)}\right) + \dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(f_z, p)}\right).$$

Then we have

$$\begin{aligned}
&\dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(L_p^{\pm,\Sigma_0}(E), p)}\right) \\
&= \dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)), p)}\right) + \dim_{\mathbb{F}_p}\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T)}{(\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E), p)}\right) \\
&= \dim_{\mathbb{F}_p}\left(\frac{\Lambda}{(\mathrm{Col}^{\pm} \circ \mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)), p)}\right) + \dim_{\mathbb{F}_p}\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)}{\mathbf{z}^{\Sigma_0}_{\mathrm{Kato}}(E[p])}\right) - \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)
\end{aligned} \tag{4.3}$$

where the first equality follows from the above computation and the second equality follows from (3.2). Following [Kob03, Theorem 7.3], we have an exact sequence

$$0 \longrightarrow \frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p}, T)}{\mathrm{H}^1_{\mathrm{Iw},\pm}(\mathbb{Q}_{\infty,p}, T) + \mathrm{loc}_p\left(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)\right)} \longrightarrow \mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])^\vee \longrightarrow \mathrm{Sel}_0^{\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])^\vee \longrightarrow 0$$

where $\mathrm{H}^1_{\mathrm{Iw},\pm}(\mathbb{Q}_{\infty,p},T) = \ker(\mathrm{Col}^{\pm})$ and $\mathrm{loc}_p\left(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)\right)$ is the image of $\mathrm{H}^1_{\mathrm{Iw}}(j_*T)$ under the localization map. Following [Kob03, Theorem 6.2], the $\pm$-Coleman maps induce isomorphisms

$$\frac{\mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_{\infty,p},T)}{\mathrm{H}^1_{\mathrm{Iw},\pm}(\mathbb{Q}_{\infty,p},T) + \mathrm{loc}_p\left(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)\right)} \simeq \Lambda/\mathrm{Col}^{\pm} \circ \mathrm{loc}_p\left(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)\right).$$

Thus, we also have

$$\begin{aligned}
&\dim_{\mathbb{F}_p}\left(\mathrm{Sel}^{\pm,\Sigma_0}(\mathbb{Q}_\infty, E[p^\infty])[p]^\vee\right) \\
&= \dim_{\mathbb{F}_p}\left(\Lambda/(\mathrm{Col}^{\pm}\circ \mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)), p)\right) + \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T/pT)\right) \\
&\quad - \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right).
\end{aligned} \tag{4.4}$$

Since all the terms in (4.3) and (4.4) except

$$\dim_{\mathbb{F}_p}\left(\Lambda/(\mathrm{Col}^{\pm}\circ \mathrm{loc}_p(\mathrm{H}^1_{\mathrm{Iw}}(j_*T)), p)\right) - \dim_{\mathbb{F}_p}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T)[p]\right)$$

depend only on T/pT and Σ.

5. An example

We examine how Theorem 2.9 applies to a numerical example in [Hat17, §5.1]. Fix a prime $p = 5$. Let

- $E_1 : y^2 + xy + y = x^3 - x - 1$ (LMFDB label 69.a1)
- $E_2 : y^2 + xy + y = x^3 + 130884x - 59725523$ (LMFDB label 897.f2)

Then both elliptic curves have supersingular reduction at 5. Also, $E_1[5] \simeq E_2[5]$ and it is a surjective mod 5 Galois representation. We put $\Sigma_0 = \{3, 13, 23\}$. For an elliptic curve E, $\mathrm{Tam}(E)$ means the product of all Tamagawa factors of E. Since we have

$$5 \nmid \frac{L(E_1,1)}{\Omega^+_{E_1}} \cdot \mathrm{Tam}(E_1),$$

both $\mathrm{Sel}_0(\mathbb{Q}, E_1[p^\infty])$ and $\mathrm{Sel}_0(\mathbb{Q}_\infty, E_1[p^\infty])$ are trivial by applying [Kur02, Proposition 5.2]. From this, we obtain $\mu\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T_1)\right) = \lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T_1)\right) = 0$ and

$$\dim_{\mathbb{F}_5}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_1)[5]\right) = 0.$$

Since the conductors only differ by 13, it suffices to observe the behavior of $\mathcal{P}_{13}(E_1)$ and $\mathcal{P}_{13}(E_2)$. Since $13 \equiv 3 \pmod 5$, 13 is inert in $\mathbb{Q}_\infty/\mathbb{Q}$. Also, E_1 has a good reduction at 13 and E_2 has a split multiplicative reduction at 13. By using [GV00, Proposition 2.4], we have $\lambda(\mathcal{P}_{13}(E_1)) = 2$ and $\lambda(\mathcal{P}_{13}(E_2)) = 1$. On the other hand, E_2 has analytic rank one and the Tamagawa factor is (exactly) divisible by 5. By using Theorem 2.9, we are still able to obtain

$$\lambda\left(\mathrm{H}^2_{\mathrm{Iw}}(j_*T_2)\right) + \dim_{\mathbb{F}_5}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_2)[5]\right) = 1.$$

In this setting, the Iwasawa main conjecture holds for E_1, so the same holds for E_2. Thus, we also have

$$\lambda\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(j_*T_2)}{\mathbf{z}_{\mathrm{Kato}}(E_2)}\right) + \dim_{\mathbb{F}_5}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_2)[5]\right) = 1.$$

Regarding the third invariant, [Kur02, Proposition 5.2] also shows that

$$\dim_{\mathbb{F}_5}\left(\Lambda/(\mathrm{Col}^{\pm}\circ \mathrm{loc}_5(\mathrm{H}^1_{\mathrm{Iw}}(j_*T_1)), 5)\right) = 0$$

since $\mathrm{H}^1_{\mathrm{Iw}}(j_*T_1)$ is generated by $\mathbf{z}_{\mathrm{Kato}}(E_1)$. Thus, we have

$$\dim_{\mathbb{F}_5}\left(\Lambda/(\mathrm{Col}^{\pm}\circ \mathrm{loc}_5(\mathrm{H}^1_{\mathrm{Iw}}(j_*T_1)), 5)\right) - \dim_{\mathbb{F}_5}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_1)[5]\right) = 0.$$

Theorem 2.9 shows that

$$\dim_{\mathbb{F}_5}\left(\Lambda/(\mathrm{Col}^{\pm}\circ \mathrm{loc}_5(\mathrm{H}^1_{\mathrm{Iw}}(j_*T_2)), 5)\right) - \dim_{\mathbb{F}_5}\left(\mathrm{H}^2_{\mathrm{Iw}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T_2)[5]\right) = 0.$$

Acknowledgement

This project grew out from considering how to deal with a gap in an earlier version of [KLP]. We would like to thank Takenori Kataoka for pointing out it and providing various helpful comments. Chan-Ho Kim was partially supported by a KIAS Individual Grant (SP054102) via the Center for Mathematical Challenges at Korea Institute for Advanced Study and by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2018R1C1B6007009).

References

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), 809–839.

[CS06] ———, *Cyclotomic Fields and Zeta Values*, Springer Monogr. Math., Springer-Verlag, 2006.

[DL18] D. Delbourgo and A. Lei, *Congruences modulo p between ρ-twisted Hasse–Weil L-values*, Trans. Amer. Math. Soc. **370** (2018), 8047–8080.

[EPW06] M. Emerton, R. Pollack, and T. Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), no. 3, 523–580.

[FK23] T. Fukaya and K. Kato, *On conjectures of Sharifi*, Kyoto J. Math. (2023), to appear.

[GIP] R. Greenberg, A. Iovita, and R. Pollack, *On the Iwasawa invariants for elliptic curves with supersingular reduction*, in preparation, July 2008.

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

[Gre16] ———, *On the structure of Selmer groups*, Elliptic Curves, Modular Forms and Iwasawa Theory (D. Loeffler and S. L. Zerbes, eds.), Springer Proc. Math. Stat., vol. 188, Springer, 2016, In Honour of John H. Coates' 70th Birthday, Cambridge, UK, March 2015, pp. 225–252.

[GV00] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.

[Hat17] J. Hatley, *Rank parity for congruent supersingular elliptic curves*, Proc. Amer. Math. Soc. **145** (2017), no. 9, 3775–3786.

[Kat93] K. Kato, *Lectures on the approach to Iwasawa theory for Hasse–Weil L-functions via* $\mathbf{B}_{\mathrm{dR}}$*. Part I*, Arithmetic Algebraic Geometry (Heidelberg) (E. Ballico, ed.), Lecture Notes in Math., vol. 1553, Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, Springer-Verlag, 1993, Lectures given at the 2nd Session of the Centro Internazionale Matematico Estivo (C.I.M.E.) held in Trento, Italy, June 24-July 2, 1991, pp. 50–163.

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

[Kim07] B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. **143** (2007), no. 1, 47–72.

[Kim09] ———, *The Iwasawa invariants of the plus/minus Selmer groups*, Asian J. Math. **13** (2009), no. 2, 181–190.

[Kim13] ———, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc. **95** (2013), no. 2, 189–200.

[Kim17] C.-H. Kim, *Anticyclotomic Iwasawa invariants and congruences of modular forms*, Asian J. Math. **21** (2017), no. 3, 499–530.

[KLP] C.-H. Kim, J. Lee, and G. Ponsinet, *On the Iwasawa invariants of Kato's zeta elements for modular forms*, submitted, arXiv:1909.01764.

[Kob03] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[KP07] M. Kurihara and R. Pollack, *Two p-adic L-functions and rational points on elliptic curves with supersingular reduction*, L-functions and Galois representations (Cambridge) (D. Burns, K. Buzzard, and J. Nekovář, eds.), London Math. Soc. Lecture Note Ser., vol. 320, Cambridge University Press, 2007, pp. 300–332.

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

[LS21] A. Lei and R. Sujatha, *On fine Selmer groups and the greatest common divisor of signed and chromatic p-adic L-functions*, Proc. Amer. Math. Soc. **149** (2021), no. 8, 3235–3243.

[Mat20] A. Matar, *On the* Λ*-cotorsion subgroup of the Selmer group*, Asian J. Math. **24** (2020), no. 3, 437–456.

[Maz79] B. Mazur, *On the arithmetic of special values of L functions*, Invent. Math. **55** (1979), 207–240.

[NS23] F. A. E. Nuccio Mortarino Majno di Capriglio and R. Sujatha, *Residual supersingular Iwasawa theory and signed Iwasawa invariants*, Rend. Sem. Mat. Univ. Padova **149** (2023), 83–129.

[Pol03] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PR04] R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.

[Rib84] K. Ribet, *Congruence relations between modular forms*, Proceedings of the International Congress of Mathematicians (Warsaw, 1983) (Warsaw), vol. 1, 1984, pp. 503–514.

[SS15] S. Shekhar and R. Sujatha, *Congruence formula for certain dihedral twists*, Trans. Amer. Math. Soc. **367** (2015), no. 5, 3579–3598.

[Suj11] R. Sujatha, *On the μ-invariant in iwasawa theory*, WIN–women in numbers, Fields Inst. Commun., vol. 60, Amer. Math. Soc., 2011, pp. 265–276.

[Vat99] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

[Win89] K. Wingberg, *Duality theorems for Abelian varieties over $\mathbb{Z}_p$-extensions*, Algebraic Number Theory – in honor of Kenkichi Iwasawa (J. Coates, R. Greenberg, B. Mazur, and I. Satake, eds.), Adv. Stud. Pure Math., Academic Press, 1989, pp. 471–492.

(Chan-Ho Kim) Center for Mathematical Challenges, Korea Institute for Advanced Study, 85 Hoegiro, Dongdaemun-gu, Seoul 02455, Republic of Korea

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

(R. Sujatha) University of British Columbia, Vancouver, BC, V6T1Z2, Canada

E-mail address: `sujatha@math.ubc.ca`