ON FINE SELMER GROUPS AND THE GREATEST COMMON DIVISOR OF SIGNED AND CHROMATIC p-ADIC L-FUNCTIONS

ANTONIO LEI AND R. SUJATHA

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime where E has good supersingular reduction. Let F_1 denote the characteristic power series of the Pontryagin dual of the fine Selmer group of E over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let F_2 denote the greatest common divisor of Pollack's plus and minus p-adic L-functions or Sprung's sharp and flat p-adic L-functions attached to E, depending on whether $a_p(E) = 0$ or $a_p(E) \neq 0$. We study a link between the divisors of F_1 and F_2 in the Iwasawa algebra. This gives new insights into problems posed by Greenberg and Pollack–Kurihara on these elements.

AMS Subject Classification: 11R23, 11G05
Keywords and phrases: Elliptic curves, supersingular primes, Selmer groups

1. INTRODUCTION

Let p a fixed odd prime number. We write $\mathbb{Q}_{\text{cyc}}$ for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let Γ denote the Galois group $\text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$. The Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]]$ is defined to be $\varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$, where the connecting maps are projections. After fixing a topological generator γ of Γ, there is an isomorphism of rings $\Lambda \cong \mathbb{Z}_p[[X]]$, sending γ to $X + 1$.

Let $E/\mathbb{Q}$ be an elliptic curve and write $\text{Sel}_0(E/\mathbb{Q}_{\text{cyc}})$ for the fine Selmer group of E over $\mathbb{Q}_{\text{cyc}}$ as defined in [CS05] (whose precise definition is reviewed in (2.2) below). It has been shown by Kato in [Kat04] that $\text{Sel}_0(E/\mathbb{Q}_{\text{cyc}})^\vee$ is a finitely generated Λ-torsion module. Conjecture A in [CS05] further predicts that it should be a finitely generated $\mathbb{Z}_p$-module, which is equivalent to saying that its μ-invariant is zero. Examples validating this conjecture can be found in a recent work of Kundu and the second named author [KS20].

For an integer $n \geq 1$, we write

$$\Phi_n = \frac{(1+X)^{p^n} - 1}{(1+X)^{p^{n-1}} - 1} \in \Lambda$$

for the p^n-th cyclotomic polynomial in $1 + X$. Let K_n denote the unique sub-extension of $\mathbb{Q}_{\text{cyc}}$ such that $[K_n : \mathbb{Q}] = p^n$. Define

$$e_n = \frac{\text{rank}E(K_n) - \text{rank}E(K_{n-1})}{p^{n-1}(p-1)}.$$

When $n = 0$, we define $\Phi_0 = X$ and $e_0 = \mathrm{rank}E(\mathbb{Q})$. We recall from [KP07, Problem 0.7] that the following problem was posed by Greenberg:

$$\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \stackrel{?}{=} \Big(\prod_{e_n \geq 1, n \geq 0} \Phi_n^{e_n - 1} \Big). \tag{Gr}$$

Here, $\mathrm{Char}_\Lambda M$ denotes the Λ-characteristic ideal of a finitely generated torsion Λ-module M. In particular, if (Gr) holds, then Conjecture A of [CS05] holds as well.

We now turn our attention to the case where E has supersingular reduction at p. The classical p-adic L-functions attached to E are p-adic power series with unbounded denominators (in particular, they are not elements of Λ). In [Pol03], under the hypothesis that $a_p(E) = 0$, Pollack introduced the so-called plus and minus p-adic L-functions $L_p^+(E)$ and $L_p^-(E)$, which are non-zero elements of Λ, interpolating complex L-values of E twisted by Dirichlet characters factoring through Γ. They can be regarded as the analytic analogues of certain cotorsion Selmer groups $\mathrm{Sel}^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ defined by Kobayashi [Kob03]. In fact, Kobayashi formulated the following main conjecture

$$\mathrm{Char}_\Lambda \mathrm{Sel}^\pm(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \stackrel{?}{=} \big(L_p^\pm(E)\big). \tag{Ko}$$

When $a_p(E) \neq 0$, Sprung [Spr12] generalized the works of Pollack and Kobayashi by introducing the sharp and flat p-adic L-functions $L_p^\sharp(E)$ and $L_p^\flat(E)$ as well as the corresponding Selmer groups $\mathrm{Sel}^\sharp(E/\mathbb{Q}_{\mathrm{cyc}})$ and $\mathrm{Sel}^\flat(E/\mathbb{Q}_{\mathrm{cyc}})$. He showed that there exists $\star \in \{\sharp, \flat\}$ such that $L_p^\star(E) \neq 0$ and that $\mathrm{Sel}^\star(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ is Λ-torsion (see Proposition 6.14 and Theorem 7.14 of [Spr12]). Moreover, he formulated the analogue of (Ko): If $\star \in \{\sharp, \flat\}$ is such that $L_p^\star(E) \neq 0$, then

$$\mathrm{Char}_\Lambda \mathrm{Sel}^\star(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \stackrel{?}{=} \big(L_p^\star(E)\big). \tag{Sp}$$

Furthermore, by [Kob03, Theorem 7.4] and [Spr12, discussion on P.1505] respectively, (Ko) and (Sp) are equivalent to Kato's main conjecture in [Kat04], which can be expressed as

$$\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \stackrel{?}{=} \mathrm{Char}_\Lambda H^1_{\mathrm{Iw}}(\mathbb{Q}, T)/\mathcal{Z}, \tag{Ka}$$

where T is the p-adic Tate module of E, $H^1_{\mathrm{Iw}}(\mathbb{Q}, T)$ is the inverse limit of certain global Galois cohomological groups over K_n and $\mathcal{Z}$ is the Λ-module generated by certain zeta elements (we will review the definition of these objects in the main part of the article).

Kato showed that there exists an integer n such that

$$\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \supset p^n \mathrm{Char}_\Lambda H^1_{\mathrm{Iw}}(\mathbb{Q}, T)/\mathcal{Z}$$

using the theory of Euler systems. Furthermore, if the Galois representation $G_\mathbb{Q} \to \mathrm{GL}_{\mathbb{Z}_p}(T)$ is surjective, then we may take $n = 0$. In other words, the inclusion $\supset$ holds in (Ka). This has the consequence that one inclusion in the main conjectures (Ko) and (Sp) also holds, namely:

$$\big(L_p^\star(E)\big) \subset \mathrm{Char}_\Lambda \mathrm{Sel}^\star(E/\mathbb{Q}_{\mathrm{cyc}})^\vee, \tag{1.1}$$

where $\star \in \{+,-\}$ or $\{\sharp,\flat\}$, depending on whether $a_p(E)=0$ or $a_p(E)\neq 0$.

When E has complex multiplication (in which case $a_p(E)$ is always 0), Pollack and Rubin [PR04] showed that (Ko) holds. Consequently, (Ka) holds as well. In the non-CM case, recent progress on these conjectures has been made by Wan [Wan14] and Sprung [Spr16].

It follows from their definitions that $\mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})$ is a subgroup of both plus and minus (or sharp and flat) Selmer groups. In particular, we have the inclusions

$$\mathrm{Char}_\Lambda \mathrm{Sel}^\star(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \subset \mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee. \tag{1.2}$$

Pollack has written a MAGMA program which computes numerically the p-adic L-functions $L_p^\star(E)$ for a given E (see `http://math.bu.edu/people/rpollack/Data/data.html`)[1]. One can observe that the μ-invariants of $L_p^\star(E)$ turn out to be zero in all the examples that have been considered by Pollack. Therefore, on combining (1.1) and (1.2), we deduce that the μ-invariant of $\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ is also zero. In particular, this gives evidence towards the validity of Conjecture A in [CS05]. In this article, we are interested in the following question:

Question 1.1. *What can* [CS05, Conjecture A] *tell us about the μ-invariants of $L_p^\pm(E)$ and $L_p^{\sharp/\flat}(E)$?*

In [KP07, Problem 3.2], under the assumption that $a_p(E)=0$, the following problem was posed by Kurihara and Pollack:

$$\gcd\left(L_p^+(E), L_p^-(E)\right) \stackrel{?}{=} X^{e_0} \prod_{e_n\geq 1, n\geq 1} \Phi_n^{e_n-1}. \tag{KP}$$

Here, we express the greatest common divisor of two elements in Λ in the form $p^\mu h \in \Lambda$, where h is a distinguished polynomial. The two problems (Gr) and (KP) are intimately linked. Indeed, Kurihara and Pollack showed in [KP07, §3] that under certain hypotheses, they are equivalent to each other. Furthermore, they have found several numerical examples where the answers to both (Gr) and (KP) are affirmative. We observe that the problems (Gr) and (KP) suggest that the following equality holds

$$\left(\gcd\left(L_p^+(E), L_p^-(E)\right)\right) \stackrel{?}{=} X^{\delta_E} \mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee, \tag{1.3}$$

where $\delta_E \in \{0,1\}$. The appearance of the term X^δ on the right-hand side originates from the discrepancy[2] of the exponents of X in (Gr) and (KP).

[1] Even though Pollack's algorithm was written before Sprung's p-adic L-functions $L_p^{\sharp/\flat}(E)$ were defined, it in fact computes the Iwasawa invariants considered by Perrin-Riou in [PR03] when $a_3(E)=\pm 3$. These in turn give the Iwasawa invariants of $L_p^{\sharp/\flat}(E)$ (see [Spr13, §5]). We thank Robert Pollack and Florian Sprung for explaining this to us.

[2] This discrepancy seems to be related to the fact that

$$E^+(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}}) \bigcap E^-(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}}) = E(\mathbb{Q}_p),$$

where $E^\pm(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}})$ are Kobayashi's plus and minus norm groups which are used to define $\mathrm{Sel}^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ (see §2.2 for more details). This suggests that the plus and minus Selmer groups might capture more information on the Mordell-Weil group $E(\mathbb{Q})$ than the fine Selmer group.

The main result of the present article is the following theorem which gives evidence towards (1.3). It can also be regarded as partial evidence towards (Gr) and (KP).

Theorem 1.2. *Suppose that $E/\mathbb{Q}$ is an elliptic curve with supersingular reduction at p. In the case where $a_p(E) \neq 0$, we assume that both $L_p^\sharp(E)$ aand $L_p^\flat(E)$ are non-zero. Furthermore, assume that* (Ka) *holds (in particular,* (Ko) *and* (Sp) *also hold). Let $f \in \Lambda$ be an irreducible element that is coprime to X. If $a_p(E) = 0$, then f divides* $\gcd\left(L_p^+(E), L_p^-(E)\right)$ *if and only if f divides* $\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$. *Likewise, if $a_p(E) \neq 0$, then f divides* $\gcd\left(L_p^\sharp(E), L_p^\flat(E)\right)$ *if and only if f divides* $\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$.

In particular, Theorem 1.2 gives the following answer to Question 1.1 on taking $f = p$: If (Ka) holds, then [CS05, Conjecture A] (which says that p does not divide $\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$) is equivalent to $p \nmid \gcd\left(L_p^+(E), L_p^-(E)\right)$ (or $p \nmid \gcd\left(L_p^\sharp(E), L_p^\flat(E)\right)$), which is the same as saying that the μ-invariant of at least one of the two p-adic L-functions $L_p^\pm(E)$ (or $L_p^{\sharp/\flat}(E)$) is zero.

Outline of the article. We review general definitions and preliminary results on Iwasawa modules and Selmer groups in Section 2. The proof of Theorem 1.2 is then given in Section 3. At the end of the article (Section 4), we discuss some numerical examples.

Acknowledgment. This work was initiated during the first named author's visit to PIMS in March 2020. He would like to thank PIMS for the hospitality. We would like to thank Filippo Nuccio, Robert Pollack, Florian Sprung and Chris Wuthrich for helpful discussions during the preparation of this article. Both authors also gratefully acknowledge support of their respective NSERC Discovery Grants. Finally, we thank the anonymous referee for very helpful comments and suggestions that led to many improvements to the presentation of the article.

2. Notation and preliminary results

2.1. **Generalities on Λ-modules.** Let M be a Λ-module, we write $M^\vee$ for its Pontryagin dual

$$\mathrm{Hom}_{\mathrm{conts}}(M, \mathbb{Q}_p/\mathbb{Z}_p).$$

We let M_{tor} denote the maximal torsion submodule of M.

If M is a finitely generated Λ-module, there is a pseudo-isomorphism of Λ-modules

$$M \sim \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{a_i} \oplus \bigoplus_{i=1}^{t} \Lambda/(F_i^{b_i}), \tag{2.1}$$

where r, s, t, a_i, b_i are non-negative integers and F_i are irreducible distinguished polynomials. We define the μ- and λ-invariants of M by

$$\mu(M) := \sum_{i=1}^{s} a_i,$$
$$\lambda(M) := \sum_{i=1}^{t} \deg(F_i).$$

In the case where M is Λ-torsion, we have $r = 0$ and the characteristic ideal of M is defined to be

$$\mathrm{Char}_\Lambda(M) = \left(p^{\mu(M)} \prod_{i=1}^{t} F_i^{b_i} \right) \Lambda.$$

Given any irreducible element $f \in \Lambda$, we write $M[f]$ for the Λ-submodule of M defined by

$$\{m \in M : f \cdot m = 0\}.$$

The following lemmas will be employed in our proof of Theorem 1.2.

Lemma 2.1. *Let M be a finitely generated Λ-module and $f \in \Lambda$ an irreducible element. Then, $M[f]$ is finite if and only if $f \nmid \mathrm{Char}_\Lambda(M_{\mathrm{tor}})$.*

Proof. We can see from the the pseudo-isomorphism (2.1) that $M[f]$ is finite if and only if $(\Lambda/(g^n))[f]$ is finite for all $\Lambda/(g^n)$ that appear on the right-hand side of (2.1). Therefore, without loss of generality, we may assume that $M = \Lambda/(g^n)$ for some irreducible element g of Λ and $n \geq 1$. It is clear that $M[f] = 0$ if $\gcd(f, g) = 1$ and $M[f] = f^{n-1}\Lambda/(f^n)$ if $f = g$, which is of infinite cardinality. Therefore, our lemma follows. □

Lemma 2.2. *Let*

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of finitely generated Λ-modules and $f \in \Lambda$ an irreducible element.

(a) Suppose that $f \nmid \mathrm{Char}_\Lambda B_{\mathrm{tor}}$, then $f \nmid \mathrm{Char}_\Lambda A_{\mathrm{tor}}$.
(b) Suppose that $f \nmid \mathrm{Char}_\Lambda A_{\mathrm{tor}}$ and $f \nmid \mathrm{Char}_\Lambda C_{\mathrm{tor}}$, then $f \nmid \mathrm{Char}_\Lambda B_{\mathrm{tor}}$.
(c) Suppose that A is a torsion Λ-module, then we have the equality

$$\mathrm{Char}_\Lambda(A)\mathrm{Char}_\Lambda(C_{\mathrm{tor}}) = \mathrm{Char}_\Lambda(B_{\mathrm{tor}}).$$

Proof. Part (a) follows from Lemma 2.1 and the fact that $A[f]$ injects into $B[f]$. Part (b) follows from the exact sequence

$$0 \to A[f] \to B[f] \to C[f] \to \cdots$$

and Lemma 2.1. Finally, part (c) follows from [HL19, proof of Proposition 2.1]. □

2.2. **Galois cohomology and Selmer groups.** As in the introduction, T denotes the p-adic Tate module of E. Let S be a finite set of primes of $\mathbb{Q}$ including the bad primes of E, the prime p and the archimedean prime. Given a finite extension of F, we write $G_{F,S}$ for the Galois group of the maximal extension of F that is unramified outside S. We define

$$H^1_{\mathrm{Iw}}(\mathbb{Q},T)=\varprojlim H^1(G_{K_n,S},T),$$

where K_n is the unique sub-extension of $\mathbb{Q}_{\mathrm{cyc}}$ such that $[K_n:\mathbb{Q}]=p^n$ and the connecting maps in the inverse limit are given by corestrictions. It has been shown in [Kat04] that there exists a so-called zeta element $z_{\mathrm{Kato}}\in H^1_{\mathrm{Iw}}(\mathbb{Q},T)$, which, when localized at p, interpolates complex L-values of E twisted by Dirichlet characters factoring through Γ under the dual exponential map of Bloch-Kato as defined in [BK90]. We define $\mathcal{Z}\subset H^1_{\mathrm{Iw}}(\mathbb{Q},T)$ to be the Λ-submodule generated by z_{Kato}.

Locally, we define

$$H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T)=\varprojlim H^1(K_{n,v_n},T),$$

where v_n denotes the unique prime of K_n lying above p and the connecting maps in the inverse limit are again given by corestrictions. The restriction maps $H^1(K_n,T)\to H^1(K_{n,v_n},T)$ give

$$\mathrm{loc}_p: H^1_{\mathrm{Iw}}(\mathbb{Q},T)\hookrightarrow H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T),$$

where the injectivity follows from [Kob03, Theorem 7.3] and [Spr12, (3) on P.1504]. Let us write $\mathcal{Z}_{\mathrm{loc}}$ for the image of $\mathcal{Z}$ under the localization map, that is

$$\mathcal{Z}_{\mathrm{loc}}=\mathrm{loc}_p(\mathcal{Z}).$$

We finish this section by defining the various Selmer groups of E over $\mathbb{Q}_{\mathrm{cyc}}$ studied in this article. Recall that if K is a number field, the classical p-primary Selmer group of E over K is given by

$$\mathrm{Sel}_{p^\infty}(E/K)=\ker\left(H^1(G_{K,S},E_{p^\infty})\to\bigoplus_{v\in S}J_v(K)\right),$$

where $J_v(K)$ is defined to be $\displaystyle\bigoplus_{w|v}\frac{H^1(K_w,E_{p^\infty})}{E(K_w)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$ (here, the direct sum runs over all places of K above v). The classical p-primary Selmer group of E over $\mathbb{Q}_{\mathrm{cyc}}$ is given by

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})=\varinjlim_n \mathrm{Sel}_{p^\infty}(E/K_n),$$

where the connecting maps are given by restrictions.

The fine Selmer group of E over $\mathbb{Q}_{\mathrm{cyc}}$ is given by

$$\mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})=\ker\left(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})\to H^1(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}},E_{p^\infty})\right),\tag{2.2}$$

where $\mathfrak{p}$ denotes the unique prime of $\mathbb{Q}_{\mathrm{cyc}}$ above p (see [CS05, (58) on P.828]). When $a_p(E)=0$, Kobayashi's plus and minus Selmer groups are defined by

$$\mathrm{Sel}^{\pm}(E/\mathbb{Q}_{\mathrm{cyc}})=\ker\left(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})\to\frac{H^1(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}},E_{p^\infty})}{E^{\pm}(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where $E^{\pm}(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}})$ are certain subgroups in E defined by some "jumping conditions" (see [Kob03, Definition 1.1]). When $a_p(E) \neq 0$, Sprung's sharp and flat Selmer groups are defined by

$$\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_{\mathrm{cyc}}) = \ker\left(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}) \to \frac{H^1(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}}, E_{p^\infty})}{E^{\sharp/\flat}(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where $E^{\sharp/\flat}(\mathbb{Q}_{\mathrm{cyc},\mathfrak{p}})$ are given by the exact annihilators of certain Coleman maps (see [Spr12, Definition 7.9]).

3. Proof of Theorem 1.2

This section is dedicated to the proof of the main theorem of this article. We remark that some of the ingredients of the proof were also utilized in [KP07, proof of Proposition 3.4].

Throughout this section, $f \in \Lambda$ is a fixed irreducible element that is coprime to X. We write $(\circ, \bullet) = (+, -)$ or $(\sharp, \flat)$, depending on whether $a_p(E) = 0$ or $a_p(E) \neq 0$. Suppose that f does not divide $\gcd(L_p^{\circ}(E), L_p^{\bullet}(E))$. Then it does not divide $\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ by (1.2). This gives one of the two implications of Theorem 1.2. The rest of this section will be dedicated to the proof of the opposite implication, which is less straightforward. From now on, we assume that

$$f \nmid \mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee. \tag{3.1}$$

If we combine this with (Ka), we have

$$f \nmid \mathrm{Char}_\Lambda H^1_{\mathrm{Iw}}(\mathbb{Q}, T)/\mathcal{Z}. \tag{3.2}$$

The following proposition is one of the key ingredients of the proof of Theorem 1.2.

Proposition 3.1. *We have*

$$f \nmid \mathrm{Char}_\Lambda \left(H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)/\mathcal{Z}_{\mathrm{loc}}\right)_{\mathrm{tor}}.$$

Proof. The injectivity of loc_p gives the following short exact sequence

$$0 \to H^1_{\mathrm{Iw}}(\mathbb{Q}, T)/\mathcal{Z} \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)/\mathcal{Z}_{\mathrm{loc}} \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)/\mathrm{loc}_p\left(H^1_{\mathrm{Iw}}(\mathbb{Q}, T)\right) \to 0.$$

Since the Λ-module $H^1_{\mathrm{Iw}}(\mathbb{Q}, T)$ is of rank one (see [Kat04, Theorem 12.4]), the first term of the short exact sequence is Λ-torsion. Therefore, thanks to Lemma 2.2(c), it is enough to show that

$$f \nmid \mathrm{Char}_\Lambda H^1_{\mathrm{Iw}}(\mathbb{Q}, T)/\mathcal{Z} \quad \text{and} \quad f \nmid \mathrm{Char}_\Lambda \left(H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)/\mathrm{loc}_p\left(H^1_{\mathrm{Iw}}(\mathbb{Q}, T)\right)\right)_{\mathrm{tor}}.$$

The first indivisibility is a direct consequence of our hypothesis that both (Ka) and (3.1) hold. For the second indivisibility, we consider the Poitou-Tate exact sequence

$$0 \to H^1_{\mathrm{Iw}}(\mathbb{Q}, T) \xrightarrow{\mathrm{loc}_p} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \to \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee \to 0 \tag{3.3}$$

(which is obtained by taking inverse limit in [Kob03, (7.18)]). By [Win89, Corollary 2.5], we have the equality

$$\mathrm{Char}_\Lambda \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee_{\mathrm{tor}} = \mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee.$$

Therefore, our hypothesis (3.1) tells us that

$$f \nmid \mathrm{Char}_\Lambda \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee_{\mathrm{tor}}.$$

We may therefore apply Lemma 2.2(a) to (3.3) to deduce that

$$f \nmid \mathrm{Char}_\Lambda \left(H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T)/\mathrm{loc}_p\left(H^1_{\mathrm{Iw}}(\mathbb{Q},T)\right)\right)_{\mathrm{tor}}$$

as required. □

We recall from [Kob03, §§8.5-8.6] and [Spr12, §7] that there are two surjective Λ-homomorphisms

$$\mathrm{Col}^{\circ/\bullet} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T) \to \Lambda,$$

which are called the plus and minus (or sharp and flat) Coleman maps of E. Furthermore, [Kob03, Theorem 6.3] and [Spr12, Definition 6.1] tell us that

$$L_p^{\circ/\bullet}(E) = \mathrm{Col}^{\circ/\bullet}\left(\mathrm{loc}_p\left(z_{\mathrm{Kato}}\right)\right). \tag{3.4}$$

(Note that we are taking η to be the trivial character in the notation of op. cit.)

If we write

$$\begin{aligned}\widetilde{\mathrm{Col}} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T) &\to \Lambda^{\oplus 2}\\ z &\mapsto \mathrm{Col}^\circ(z)\oplus\mathrm{Col}^\bullet(z),\end{aligned}$$

then we have a short exact sequence of Λ-modules

$$0 \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T) \xrightarrow{\widetilde{\mathrm{Col}}} \Lambda^{\oplus 2} \to \mathbb{Z}_p \to 0 \tag{3.5}$$

as given by [KP07, Proposition 1.2] and [Spr12, Proposition 4.7].

If we combine (3.4) and (3.5), we deduce the short exact sequence

$$0 \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T)/\mathcal{Z}_{\mathrm{loc}} \to \Lambda^{\oplus 2}/(L_p^\circ(E)\oplus L_p^\bullet(E))\Lambda \to \mathbb{Z}_p \to 0. \tag{3.6}$$

But $\mathrm{Char}_\Lambda \mathbb{Z}_p = (X)$, which is coprime to f by assumption. Hence, we deduce from Proposition 3.1 and Lemma 2.2(b) that

$$f \nmid \mathrm{Char}_\Lambda\left(\Lambda^{\oplus 2}/(L_p^\circ(E)\oplus L_p^\bullet(E))\Lambda\right)_{\mathrm{tor}}.$$

In particular, $f \nmid \gcd(L_p^\circ(E), L_p^\bullet(E))$, which concludes the proof of Theorem 1.2.

4. Numerical examples

We discuss the two elliptic curves studied in [Wut07, §10], namely, $37A1$ and $53A1$, both of which are of rank one over $\mathbb{Q}$ with $L(E/\mathbb{Q},1)=0$.

$E = 37A1$. According to [Wut07, Proposition 10.1], the fine Selmer group of E over $\mathbb{Q}_{\mathrm{cyc}}$ is finite for all primes $p < 1000$. In particular,

$$\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee = \Lambda$$

for these primes. Note that E has supersingular reduction at the primes $p = 3, 17, 19$ with $a_3(E) = -3$ and $a_{17}(E) = a_{19}(E) = 0$. Theorem 1.2 tells that if $f \in \Lambda$ is an irreducible element dividing $\gcd\left(L_p^\sharp(E), L_p^\flat(E)\right)$ (resp. $\gcd\left(L_p^+(E), L_p^-(E)\right)$) when $p = 3$ (resp. $p = 17$ or 19), then f has to be (up to a unit) equal to X. In fact, we can even work out the greatest common divisors explicitly in these cases.

Since $L(E/\mathbb{Q},1)=0$, it follows from the interpolation formulae of the p-adic L-functions given in [Spr12, Page 14980] and [Kob03, Page 7] that X divides $L_p^{\sharp/\flat}(E)$ (when $p=3$) and $L_p^{\pm}(E)$ (when $p=17$ or 19). According to Pollack's table `http://math.bu.edu/people/rpollack/Data/37A.p` (see also [Spr17, Example 7.12] where the case $p=3$ is discussed), one of the two p-adic L-functions has λ-invariant equal to 1. This implies that

$$\gcd\left(L_p^{\sharp}(E), L_p^{\flat}(E)\right) = X$$

if $p=3$ and

$$\gcd\left(L_p^{+}(E), L_p^{-}(E)\right) = X$$

if $p=17$ or 19. Note in particular that the equation (1.3) holds for this curve when $p=17$ and 19. Furthermore, the μ-invariants of $\mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$, $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee_{\mathrm{tor}}$, $\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ (when $p=3$) and $\mathrm{Sel}^{\pm}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ (when $p=17,19$) are all zero.

$E=53A1$**.** Once again, E is supersingular at $p=3$ with $a_3(E)=-3$. Wuthrich showed that the fine Selmer group over $\mathbb{Q}_{\mathrm{cyc}}$ is finite when $p=3$ and Pollack's table `http://math.bu.edu/people/rpollack/Data/curves1-5000` tells us that $L_p^{\sharp/\flat}(E)=X$ (up to a unit). Therefore, we can deduce once more that

$$\mathrm{Char}_\Lambda \mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee = \Lambda,$$
$$\gcd\left(L_p^{\sharp}(E), L_p^{\flat}(E)\right) = X,$$

illustrating Theorem 1.2.

Note that E has supersingular reduction at $p=5,11$ and $a_5(E)=a_{11}(E)=0$. Pollack's table tells us that $L_p^{\pm}(E)=X$ (up to a unit) in these cases. We may apply the argument in [Wut07, §10] to deduce that the fine Selmer group of E over $\mathbb{Q}_{\mathrm{cyc}}$ is finite. This again illustrates Theorem 1.2 and gives examples where the equality (1.3) holds. Furthermore, the μ-invariants of $\mathrm{Sel}_0(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$, $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee_{\mathrm{tor}}$, $\mathrm{Sel}^{\sharp/\flat}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ (when $p=3$) and $\mathrm{Sel}^{\pm}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ (when $p=5,11$) vanish.

References

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[CS05] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), no. 4, 809–839.

[HL19] Jeffrey Hatley and Antonio Lei, *Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms*, Math. Res. Lett. **26** (2019), no. 4, 1115–1144.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, no. 295, 2004, Cohomologies p-adiques et applications arithmétiques. III, pp. ix, 117–290.

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

[KP07] Masato Kurihara and Robert Pollack, *Two p-adic L-functions and rational points on elliptic curves with supersingular reduction*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 300–332.

[KS20] Debanjana Kundu and R. Sujatha, *Structure of fine selmer groups in p-adic Lie extensions*, 2020, preprint.

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

[PR03] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186.

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

[Spr12] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.

[Spr13] ———, *The Šafarevič-Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes*, J. Reine Angew. Math. **681** (2013), 199–218.

[Spr16] ———, *The Iwasawa main conjecture for elliptic curves at odd supersingular primes*, arXiv: 1610.10017, 2016.

[Spr17] ———, *On pairs of p-adic L-functions for weight-two modular forms*, Algebra Number Theory **11** (2017), no. 4, 885–928.

[Wan14] Xin Wan, *Iwasawa main conjecture for supersingular elliptic curves and bsd conjecture*, 2014, Preprint, arXiv: 1411.6352.

[Win89] Kay Wingberg, *Duality theorems for abelian varieties over $\mathbf{Z}_p$-extensions*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 471–492.

[Wut07] Christian Wuthrich, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (2007), no. 1, 83–108.

(A. Lei) Département de Mathématiques et de Statistiques, Université Laval, Pavillon Alexandre-Vachon, 1045 Avenue de la Médecine, Québec, QC, Canada G1V 0A6

Email address: antonio.lei@mat.ulaval.ca

(R. Sujatha) Mathematics Department, 1984, Mathematics Road, University of British Columbia, Vancouver, Canada V6T 1Z2

Email address: sujatha@math.ubc.ca