NON-COMMUTATIVE p-ADIC L-FUNCTIONS FOR SUPERSINGULAR PRIMES

ANTONIO LEI

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at p with $a_p(E) = 0$. We give a conjecture on the existence of analytic plus and minus p-adic L-functions of E over the $\mathbb{Z}_p$-cyclotomic extension of a finite Galois extension of $\mathbb{Q}$ where p is unramified. Under some technical conditions, we adopt the method of Bouganis and Venjakob for p-ordinary CM elliptic curves to construct such functions for a particular non-abelian extension.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at an odd prime p. Coates *et al.* [CFK+05, CH01] have recently developed the framework of the Iwasawa theory of E over a p-adic Lie extension $\mathcal{F}$ of $\mathbb{Q}$ that contains the $\mathbb{Z}_p$-cyclotomic extension $\mathbb{Q}_\infty$. Let $\mathcal{G} = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. It is predicted that there exists a p-adic L-function $\mathcal{L}_{\mathcal{G},E} \in K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$, where $\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*}$ is an appropriate localisation of an Iwasawa algebra of $\mathcal{G}$ and $\mathcal{L}_{\mathcal{G},E}$ interpolates the complex L-values of E in the following sense. For all Artin representations ρ of $\mathcal{G}$, $\mathcal{L}_{\mathcal{G},E}$ is expected to satisfy

$$\mathcal{L}_{\mathcal{G},E}(\rho) = \frac{e_p(\rho)}{u^{\mathfrak{f}_p(\rho)}} \times \frac{P_p(\rho, u^{-1})}{P_p(\rho^\vee, w^{-1})} \times \frac{L_R(E, \rho^\vee, 1)}{\Omega_+^{d^+(\rho)}\Omega_-^{d^-(\rho)}}. \tag{1}$$

Here, e_p denotes the local epsilon factor at p, u and w are respectively the p-adic unit and non-unit roots of the quadratic $X^2 - a_p(E)X + p$, $P_p(\star, X)$ is the polynomial describing the Euler factor of $\star$ at p and R is the set consisting of the prime p and all primes at which E has multiplicative reduction. We shall review some of the notation in §2. The main conjecture predicts that such a p-adic L-function, should it exist, generates the characteristic ideal of the dual Selmer group $X(E/\mathcal{F})$, which is conjectured to lie in the $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$-category (see §2.4 below).

The existence of $\mathcal{L}_{\mathcal{G},E}$ would generalise the work of Mazur and Swinnerton-Dyer [MSD74], where they constructed an element $\mathcal{L}_{\Gamma,E} \in \Lambda(\Gamma)$ that interpolates the L-values of E twisted by finite characters of Γ. More precisely, if χ is a character on Γ with conductor $p^n > 1$, then

$$\mathcal{L}_{\Gamma,E}(\chi) = \frac{\tau(\chi)}{u^n} \times \frac{L(E, \chi^{-1}, 1)}{\Omega_+},$$

where $\tau(\chi)$ denotes the Gauss sum of χ.

When E has good supersingular reduction, no such element exists. Instead, Amice and Vélu [AV75] constructed two admissible p-adic L-functions $\mathcal{L}_{E,\Gamma}^u$ and $\mathcal{L}_{E,\Gamma}^w$, one for each of the two roots, u and w, to $X^2 - a_p(E)X + p$. Even though they have similar interpolating properties as their counterpart in the ordinary case, they do not lie in $\Lambda(\Gamma)$. Pollack [Pol03] resolved this by decomposing $\mathcal{L}_{E,\Gamma}^u$ and $\mathcal{L}_{E,\Gamma}^w$ into linear combinations of two elements $\mathcal{L}_{E,\Gamma}^\pm \in \Lambda(\Gamma)$ when $a_p(E) = 0$ and it has been generalised to the case where $a_p(E) \neq 0$ by Sprung [Spr09]. We shall concentrate on the former case in this paper. Pollack's p-adic L-functions exhibit the following interpolating properties. Let χ be a character on Γ of conductor $p^n > 1$. If n is even,

$$\mathcal{L}_{\Gamma,E}^+(\chi) = \frac{\tau(\chi)}{\omega^+(\chi)} \times \frac{L(E, \chi^{-1}, 1)}{\Omega_+}, \tag{2}$$

2000 *Mathematics Subject Classification.* 11R23 (primary), 11F67 (secondary).
Key words and phrases. non-commutative Iwasawa theory; elliptic curves; supersingular primes; p-adic L-functions.
The author is supported by a CRM-ISM fellowship.

whereas if n is odd,

$$\mathcal{L}^-_{\Gamma,E}(\chi) = \frac{\tau(\chi)}{\omega^-(\chi)} \times \frac{L(E,\chi^{-1},1)}{\Omega_+}. \tag{3}$$

Here, $\omega^+(\chi)$ and $\omega^-(\chi)$ are some non-zero factors that come from the plus and minus logarithms $\log^\pm$ defined in [Pol03]. It is shown in *op. cit.* that $\mathcal{L}^\pm_{\Gamma,E}$ are uniquely determined by (2) and (3) respectively. We shall review some of the details of Pollack's work in §3.1.

The main goal of this paper is to formulate a conjecture on the existence of two elements $\mathcal{L}^\pm_{\mathcal{G},E} \in K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$ with interpolating properties similar to (2) and (3) for $\mathcal{G} = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$, where $\mathcal{F}$ is the $\mathbb{Z}_p$-cyclotomic extension of a finite Galois extension of $\mathbb{Q}$ in which p is unramified. Let ρ be an irreducible Artin representation of $\mathcal{G}$ with $\mathfrak{f}_p(\rho) = n$. We define in §3.2 the factors $\omega^+(\rho)$ and $\omega^-(\rho)$, depending on the parity of n. We then go on to predict that there exist $\mathcal{L}^\pm_{\mathcal{G},E} \in K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$ that satisfy

$$\mathcal{L}^+_{\mathcal{G},E}(\rho) = \frac{e_p(\rho)}{\omega^+(\rho)} \times \frac{L_R(E,\rho^\vee,1)}{\Omega_+^{d^+(\rho)}\Omega_-^{d^-(\rho)}} \tag{4}$$

if n is even, whereas for odd n,

$$\mathcal{L}^-_{\mathcal{G},E}(\rho) = \frac{e_p(\rho)}{\omega^-(\rho)} \times \frac{L_R(E,\rho^\vee,1)}{\Omega_+^{d^+(\rho)}\Omega_-^{d^-(\rho)}}. \tag{5}$$

Here R is the set of primes as defined in the ordinary case above. Note that the Euler factors at p are trivial for the representations which we consider, which explains why they are not present in our conjectural formulae. Roughly speaking, $\mathcal{L}^+_{\mathcal{G},E}$ and $\mathcal{L}^-_{\mathcal{G},E}$ are each interpolating the L-values of E twisted by "half" of all irreducible Artin representations of $\mathcal{G}$. Despite these seemingly weaker properties, we show that, as in the ordinary case, if $\mathcal{L}^\pm_{\mathcal{G},E}$ exist, they are uniquely determined by (4) and (5) respectively as elements of $K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$ modulo the kernel of a determinant map.

Kobayashi [Kob03] defined the plus and minus Selmer groups $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty)$ for E over $\mathbb{Q}_\infty$ and formulate a main conjecture predicting that the characteristic ideals of their Pontryagin duals $X^\pm(E/\mathbb{Q}_\infty)$ should be generated by $\mathcal{L}^\pm_{\Gamma,E}$ (this has been proved by Pollack and Rubin [PR04] when E has complex multiplication). In [LZ11], we have generalised Kobayashi's construction to arbitrary p-adic Lie extensions. Therefore, analogous to the ordinary case, the existence of $\mathcal{L}^\pm_{\mathcal{G},E}$ would allow us to formulate a main conjecture for these plus and minus Selmer groups, which relates the characteristic ideals of $X^\pm(E/\mathcal{F})$ to $\mathcal{L}^\pm_{\mathcal{G},E}$. See §3.3 for details.

In [BV10], Bouganis and Venjakob proved the existence of the p-adic L-function $\mathcal{L}_{\mathcal{G},E} \in K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$ that satisfies (1), where E is an elliptic curve with complex multiplication that has good ordinary reduction at p and $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ assuming that the Selmer group satisfies the $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$-conjecture. Their construction makes use of the 2-variable p-adic L-function of Yager [Yag82], which does not exists in the supersingular case. We have nonetheless managed to adopt their method, together with some of the ideas from [KPZ10], to construct two elements $\mathcal{L}^\pm_{\mathcal{G},E}$ that satisfy (4) and (5) respectively under some technical assumptions when E is an elliptic curve with complex multiplication by K which has good supersingular reduction at p and $\mathcal{G}$ is the Galois group of the extension of $\mathbb{Q}$ by $\mathbb{Q}_\infty \cdot F$, where F is an abelian extension of K in which p is unramified. Note that $\mathcal{G}$ could be abelian, but there do exist examples for which this is not the case, e.g. $K = \mathbb{Q}(\sqrt{-3})$ and $F = K(\sqrt[3]{2})$. The details of our construction are given in §4.

Acknowledgement

The idea of this paper was originally developed when the author was a member of Monash University. He is extremely grateful for many helpful discussions with Daniel Delbourgo and Lloyd Peters on the subject while he was there. He is also indebted to David Loeffler for pointing out a few mistakes in an earlier version of this paper and to Henri Darmon and Alex Bartel for answering many of his questions. Finally, the author would like to thank the anonymous referee for suggestions that help improving the paper.

2. Notation and setup

2.1. **p-adic Lie extension.** Throughout this paper, p is an odd prime. If K is a field of characteristic 0, either local or global, G_K denotes its absolute Galois group, κ the p-cyclotomic character on G_K and $\mathcal{O}_K$ the ring of integers of K. We write c for the complex conjugation in $G_{\mathbb{Q}}$.

We let K_∞ denote the $\mathbb{Z}_p$-cyclotomic extension of K. The Galois group $\mathrm{Gal}(K_\infty/K)$ is written as Γ_K. When $K=\mathbb{Q}$, we simply write Γ for $\Gamma_{\mathbb{Q}}$. We fix a topological generator γ of Γ.

From now on, we fix a finite Galois extension F of $\mathbb{Q}$ with Galois group $\mathcal{H}$. We assume that p is unramified in F. Let $\mathcal{F}=F_\infty$. Our assumption on F implies that $F\cap\mathbb{Q}_\infty=\mathbb{Q}$. Hence, $F_\infty/\mathbb{Q}$ is Galois. We write $\mathcal{G}$ for its Galois group. Then

$$\mathcal{G}\cong\mathcal{H}\times\Gamma, \tag{6}$$

which allows us to view both $\Gamma=\Gamma_{\mathbb{Q}}$ and $\mathcal{H}$ as subgroups of $\mathcal{G}$ (e.g. $\mathcal{G}$ could be the Galois group studied in [Har10], where $\mathcal{H}$ is the group of 4×4 upper-triangular unipotent matrices over $\mathbb{F}_p$). We fix a family of subgroups of $\mathcal{H}$, written as $\{U_i\}_{i\in I}$, such that the following is true.

Condition 2.1. *For all irreducible representations ρ of $\mathcal{H}$, the trace of ρ is equal to a $\mathbb{Z}$-linear combinaton of representations of the form $\mathrm{Ind}_{U_i}^{\mathcal{H}}\chi_{\rho,i}$ where $i\in I$ and $\chi_{\rho,i}$ is an one-dimensional character on U_i.*

Remark 2.2. *Note that such a family exists by Brauer's theorem on induced characters.*

By (6), for all irreducible representations ρ of $\mathcal{G}$, there exists an one-dimensional character ρ_0 of Γ such that the trace of ρ is equal to a $\mathbb{Z}$-linear combinaton of representations of the form

$$\mathrm{Ind}_{U_i\times\Gamma}^{\mathcal{G}}(\chi_{\rho,i}\otimes\rho_0)\cong\left(\mathrm{Ind}_{U_i}^{\mathcal{G}}\chi_{\rho,i}\right)\otimes\rho_0$$

where $i\in I$ and $\chi_{\rho,i}$ is an one-dimensional character on U_i.

We write $V_i=[U_i,U_i]$ for all $i\in I$.

2.2. **Iwasawa algebras and power series.** Given a finite extension K of $\mathbb{Q}_p$ and a p-adic Lie group G, $\Lambda_{\mathcal{O}_K}(G)$ denotes the Iwasawa algebra of G over $\mathcal{O}_K$, i.e.

$$\varprojlim_N \mathcal{O}_K[G/N],$$

where the inverse limit runs over the open normal subgroups of G. When $K=\mathbb{Q}_p$ (so $\mathcal{O}_K=\mathbb{Z}_p$), we suppress $\mathbb{Z}_p$ from the notation and write $\Lambda(G)$ for $\Lambda_{\mathbb{Z}_p}(G)$. We denote $\Lambda_{\mathcal{O}_K}(G)\otimes_{\mathcal{O}_K}K$ by $\Lambda_K(G)$.

Let $r\in\mathbb{R}_{\geq 0}$. We define

$$\mathcal{H}_r=\left\{\sum_{n\geq 0}c_nX^n\in\mathbb{C}_p[[X]]:\sup_n\frac{|c_n|_p}{n^r}<\infty\right\},$$

where $|\cdot|_p$ is the p-adic norm on $\mathbb{C}_p$ such that $|p|_p=p^{-1}$. We write $\mathcal{H}_r(\Gamma)=\{f(\gamma-1):f\in\mathcal{H}_r\}$. In other words, the elements of $\mathcal{H}_r$ (respectively $\mathcal{H}_r(\Gamma)$) are the power series in X (respectively $\gamma-1$) over $\mathbb{C}_p$ with growth rate $O(\log_p^r)$.

Given a subfield K of $\mathbb{C}_p$, we write $\mathcal{H}_{r,K}=\mathcal{H}_r\cap K[[X]]$ and similarly for $\mathcal{H}_{r,K}(\Gamma)$. In particular, $\mathcal{H}_{0,K}(\Gamma)=\Lambda_K(\Gamma)$.

If $h=\sum_{n\geq 0}c_n(\gamma-1)^n\in\mathcal{H}_r(\Gamma)$ and $\lambda\in\mathrm{Hom}_{\mathrm{cts}}(\Gamma,\mathbb{C}_p^\times)$, we write

$$h(\lambda)=\sum_{n\geq 0}c_n(\lambda(\gamma)-1)^n\in\mathbb{C}_p.$$

More generally, if ρ is an Artin representation on Γ, then ρ may be decomposed into a finite sum of characters on Γ, say

$$\rho\cong\bigoplus_{i=1}^r\chi_i.$$

We then write

$$h(\rho)=\prod_{i=1}^{r}h(\chi_i).$$

2.3. **Artin representations.** Let V be a finite dimensional vector space over $\mathbb{C}$. If $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_{\mathbb{C}}(V)$ is an Artin representation, we write $d(\rho)$ (respectively $d^{\pm}(\rho)$) for the dimension of V (respectively the subspace of V on which the complex conjugation acts as ± 1). The contragredient representation of ρ is denoted by $\rho^\vee$.

We now review the definition of the local epsilon factor $e_p(\rho)=e_p(\rho|_{G_{\mathbb{Q}_p}})$ at p (see [Tat79, §3] and [DD07, §6.10] for details). It depends on a choice of Haar measure and an additive character on $\mathbb{Q}_p$. In this article, we take the canonical measure μ on $\mathbb{Q}_p$ with $\mu(\mathbb{Z}_p)=1$ and the additive character that sends ap^{-n} to $e^{2a\pi i/p^n}$ for $a\in\mathbb{Z}_p$. It is multiplicative in the sense that $e_p(\rho_1\oplus\rho_2)=e_p(\rho_1)e_p(\rho_2)$, so it is enough to define $e_p(\rho)$ for irreducible ρ.

If ρ is one-dimensional, we may factor $\rho|_{G_{\mathbb{Q}_p}}$ into $\rho_0\rho'$, where ρ_0 is an unramified character and ρ' is a Dirichlet character of conductor p^n. In this case, the epsilon factor is defined to be

$$e_p(\rho)=\rho_0(p)^n\times\tau(\rho'),$$

where $\tau(\rho')$ denotes the Gauss sum of ρ'. If $\rho=\mathrm{Ind}_F^{\mathbb{Q}}(\chi)$ for some character χ on G_F, where F is a number field, we may define $e_{\mathfrak{p}}(\chi)$ for each place $\mathfrak{p}$ of F above p in a similar way. The epsilon factor of ρ at p is then defined to be

$$e_p(\rho)=e_p(\mathrm{Ind}_F^{\mathbb{Q}}(\mathbf{1}))\prod_{\mathfrak{p}|p}\frac{e_{\mathfrak{p}}(\chi)}{e_{\mathfrak{p}}(\mathbf{1})}.$$

2.4. **A canonical Ore set.** We recall the definition of an Ore set S from [CFK+05]. Let $\mathcal{O}$ be the ring of integer of a finite extension of $\mathbb{Q}_p$. If $\mathcal{G}$ and $\mathcal{H}$ are as in §2.1, we define

$$S(\mathcal{O})=\{f\in\Lambda_{\mathcal{O}}(\mathcal{G}):\Lambda_{\mathcal{O}}(\mathcal{G})/\Lambda_{\mathcal{O}}(\mathcal{G})f\text{ is a finitely generated }\Lambda_{\mathcal{O}}(\mathcal{H})\text{-module}\}$$

and $S(\mathcal{O})^*=\cup_{n\geq 0}p^nS(\mathcal{O})$. We write $\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*}$ for the localisation of $\Lambda_{\mathcal{O}}(\mathcal{G})$ at $S(\mathcal{O})^*$.

Let U_i be the subgroups as fixed in Section 2.1. For each $i\in I$, we have a natural map

$$\theta_i : K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})\to K_1(\Lambda_{\mathcal{O}}(U_i\times\Gamma)_{S^*})\to K_1(\Lambda_{\mathcal{O}}(U_i/V_i\times\Gamma)_{S^*})=\Lambda_{\mathcal{O}}(U_i/V_i\times\Gamma)_{S^*}^{\times}.$$

Let $\mathrm{Irr}_p(\mathcal{G})$ be the additive group generated by isomorphic classes of p-adic representations of $\mathcal{G}$. There is a determinant map

$$\begin{aligned}\mathrm{Det} : K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*}) &\to \mathrm{Maps}\left(\mathrm{Irr}_p(\mathcal{G}),\overline{\mathbb{Q}_p}\cup\{\infty\}\right)\\ x &\mapsto (\rho\mapsto x(\rho)).\end{aligned}$$

We write $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ for the category of all finitely generated $\Lambda(\mathcal{G})$-modules which are $S^*(\mathbb{Z}_p)$-torsion. There is a connecting map

$$\partial_{\mathcal{G}} : K_1(\Lambda(\mathcal{G})_{S^*})\to K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})).$$

It is surjective when $\mathcal{G}$ has no p-torsion. Given an element M in $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$, a characteristic element for M is any $\xi_M\in K_1(\Lambda(\mathcal{G})_{S^*})$ such that $\partial_{\mathcal{G}}(\xi_M)=[M]$.

3. Conjectures

3.1. **Pollack's plus and minus p-adic L-functions.** We first recall Pollack's construction of plus and minus p-adic L-functions for the $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{Q}$ in [Pol03]. The plus and minus logarithms are defined as follows.

Definition 3.1. *Let $r\geq 0$ be an integer, define*

$$\begin{aligned}\log_r^+ &= \prod_{s=0}^{r}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(\kappa(\gamma)^{-s}\gamma)}{p},\\ \log_r^- &= \prod_{s=0}^{r}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(\kappa(\gamma)^{-s}\gamma)}{p},\end{aligned}$$

where Φ_m denotes the p^m-cyclotomic polynomial.

Lemma 3.2. *Let λ be a character on Γ. Then $\log_r^+(\lambda) = 0$ if and only if $\lambda = \kappa^s\theta$, where $s \in [0, r]$ and θ is a Dirichlet character whose conductor is an odd power of p. Similarly, $\log_r^-(\lambda) = 0$ if and only if $\lambda = \kappa^s\theta$, where $s \in [0, r]$ and θ is a Dirichlet character whose conductor is an even power of p.*

Proof. [Pol03, Lemma 4.1]. □

Remark 3.3. *Both $\log_r^+$ and $\log_r^-$ are elements of $\mathcal{H}_{r/2,\mathbb{Q}_p}(\Gamma)$ as given by* [Pol03, Lemma 4.5].

Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geq 2$, level N and Nebentypus character ϵ. Throughout, we assume $p \nmid N$. We write $F_p(f)$ for the completion of the coefficient field $\mathbb{Q}(a_n : n \geq 1)$ at a prime above p. Let α be a root of $X^2 - a_p X + \epsilon(p)p^{k-1} = 0$ with $h := \mathrm{ord}_p(\alpha) < k - 1$. Amice and Vélu [AV75] constructed $L_{f,\alpha} \in \mathcal{H}_{h,F_p(f)}(\Gamma)$ (written as $\mathcal{L}^{\alpha}_{\Gamma,E}$ in the introduction) with the following interpolating properties. For all integers $j \in [0, k-2]$ and Dirichlet characters θ of conductor p^n,

$$L_{p,\alpha}(\theta\kappa^j) = e_\alpha(\theta, j) \times \frac{p^{n(j+1)} j!}{\tau(\theta^{-1})(-2\pi i)^j} \times \frac{L(f, \theta^{-1}, j+1)}{\Omega_f^\delta}, \tag{7}$$

where $\delta = (-1)^j$, $\tau(\theta^{-1})$ denotes the Gauss sum of θ^{-1},

$$e_\alpha(\theta, j) = \frac{1}{\alpha^n}\left(1 - \frac{\theta^{-1}(p)\epsilon(p)p^{k-2-j}}{\alpha}\right)\left(1 - \frac{\theta(p)p^j}{\alpha}\right)$$

and $\Omega_f^\pm$ are some choice of periods. Moreover, $L_{f,\alpha}$ is uniquely determined by its values at $\theta\kappa^j$ as given by (7).

Remark 3.4. *We are only considering the $\mathbb{Z}_p$-cyclotomic extension here, rather than the whole extension by p-power roots of unity as studied in* [AV75]. *In particular, $\theta(-1)$ is always 1.*

Theorem 3.5. *Let f and α be as above with $a_p = 0$. There exist $L_f^\pm \in \Lambda_{F_p(f)}(\Gamma)$ (written as $\mathcal{L}^{\pm}_{\Gamma,E}$ in the introduction) such that*

$$L_{f,\alpha} = \log_{k-1}^+ L_f^+ + \alpha \log_{k-1}^- L_f^-.$$

Proof. This is the main result of [Pol03]. □

In particular, if α_1 and α_2 are the two roots to $X^2 + \epsilon(p)p^{k-1} = 0$, we have $\alpha_1 = -\alpha_2$ and

$$L_f^+ = \frac{L_{p,\alpha_1} + L_{p,\alpha_2}}{2\log_{k-1}^+}, \tag{8}$$

$$L_f^- = \frac{L_{p,\alpha_2} - L_{p,\alpha_1}}{(\alpha_2 - \alpha_1)\log_{k-1}^-}. \tag{9}$$

Therefore, we can readily combine (7) with (8) and (9) to obtain the interpolating formulae of L_f^+ and L_f^- respectively as given below.

Lemma 3.6. *Let $j \in [0, k-2]$ be an integer and θ a Dirichlet conductor $p^n > 1$. Write δ as in (7). If n is even, then*

$$L_f^+(\theta\kappa^j) = \frac{1}{(-\epsilon(p)p^{k-1})^{n/2}\log_{k-1}^+(\theta\chi^j)} \times \frac{p^{n(j+1)} j!}{\tau(\theta^{-1})(-2\pi i)^j} \times \frac{L(f, \theta^{-1}, j+1)}{\Omega_f^\delta},$$

whereas $\theta\kappa^j(L_f^+) = 0$ if $n = 1$. For all odd n, we have

$$L_f^-(\theta\kappa^j) = \frac{1}{(-\epsilon(p)p^{k-1})^{(n+1)/2}\log_{k-1}^-(\theta\chi^j)} \times \frac{p^{n(j+1)} j!}{\tau(\theta^{-1})(-2\pi i)^j} \times \frac{L(f, \theta^{-1}, j+1)}{\Omega_f^\delta}.$$

Moreover,

$$\begin{aligned} L_f^+(\kappa^j) &= \frac{1-p^{-1}}{\log_{k-1}^+(\chi^j)} \times \frac{j!}{(-2\pi i)^j} \times \frac{L(f,j+1)}{\Omega_f^\delta}, \\ L_f^-(\kappa^j) &= \frac{p^{-j-1}+\epsilon(p)^{-1}p^{j-k+1}}{\log_{k-1}^-(\chi^j)} \times \frac{j!}{(-2\pi i)^j} \times \frac{L(f,j+1)}{\Omega_f^\delta}. \end{aligned}$$

Definition 3.7. *Let θ be a Dirichlet character of conductor p^n. For even n, define*

$$\omega^+(\theta) = (-p)^{n/2} \log_1^+(\theta).$$

For odd n, define

$$\omega^-(\theta) = (-p)^{(n+1)/2} \log_1^-(\theta).$$

For a weight 2 modular form, we have the following simplified version of Lemma 3.6.

Lemma 3.8. *Assume that f is of weight 2. Let θ be a Dirichlet conductor $p^n > 1$. If n is even, then*

$$L_f^+(\theta) = \frac{\tau(\theta)}{\epsilon(p)^{n/2}\omega^+(\theta)} \times \frac{L(f,\theta^{-1},1)}{\Omega_f^+},$$

whereas $L_f^+(\theta) = 0$ if $n = 1$. For all odd n, we have

$$L_f^-(\theta) = \frac{\tau(\theta)}{\epsilon(p)^{(n+1)/2}\omega^-(\theta)} \times \frac{L(f,\theta^{-1},1)}{\Omega_f^+}.$$

Moreover,

$$\begin{aligned} L_f^+(\mathbf{1}) &= (p-1) \times \frac{L(f,1)}{\Omega_f^+}, \\ L_f^-(\mathbf{1}) &= (1+\epsilon(p)^{-1}) \times \frac{L(f,1)}{\Omega_f^+}. \end{aligned}$$

Proof. Recall from Remark 3.4 that $\theta(-1) = 1$, so we have $\tau(\theta)\tau(\theta^{-1}) = \theta(-1)p^n = p^n$. The result is then immediate from Lemma 3.6. See also [Kob03, (3.4)-(3.7)]. □

3.2. **Conjectural analytic p-adic L-functions.** In this section, we fix an elliptic curve E defined over $\mathbb{Q}$. We assume that E has good supersingular reduction at p with $a_p(E) = 0$. As in the introduction, we write R for the set consisting of the prime p and the primes where E has multiplicative reduction. Let Ω_+ and Ω_- denote the real and complex periods of E respectively. Let $\mathcal{F}$ and $\mathcal{G}$ be as defined in Section 2.1.

Definition 3.9. *Let ρ be an Artin representation on $\mathcal{G}$. We say that ρ is of even (respectively odd) Γ-conductor if, via* (6),

$$\rho \cong \rho_0 \otimes \rho'$$

for some representation ρ_0 of $\mathcal{H}$ and some one-dimensional character $\rho' \neq \mathbf{1}$ of Γ whose conductor is an even (respectively odd) power of p.

Remark 3.10. *By* (6), *an irreducible representation ρ of $\mathcal{G}$ is of the form $\rho_0 \otimes \rho'$ where ρ_0 is an irreducible representation of $\mathcal{H}$ and ρ' is an one-dimensional character of Γ. In particular, if $\rho' \neq \mathbf{1}$, it has either even or odd Γ-conductor. Moreover, all Artin representations of $\mathcal{G}$ that have even (respectively odd) Γ-conductors are direct sums of such irreducible representations.*

Lemma 3.11. *Let ρ be an Artin representation on $\mathcal{G}$. If ρ is of even Γ-conductor, then*

$$\omega^+(\rho|_\Gamma) = \omega^+(\rho')^{d(V)} \neq 0.$$

Similarly, if ρ is of odd Γ-conductor,

$$\omega^-(\rho|_\Gamma) = \omega^-(\rho')^{d(V)} \neq 0.$$

Proof. If ρ is of even or odd Γ-conductor, we have

$$\rho|_\Gamma \cong (\rho')^{\oplus d(V)}.$$

By definition, $\omega^\pm(\rho')$ and $\log_1^\pm(\rho')$ differ by a power of p. Hence the result by Lemma 3.2. □

As in Definition 3.7, we make the following definition to simplify our notation.

Definition 3.12. *Let ρ be an Artin representation on $\mathcal{G}$ that is of even Γ-conductor, we write*

$$\omega^+(\rho) = \omega^+(\rho|_\Gamma),$$

which is non-zero by Lemma 3.11. If on the other hand ρ is of odd Γ-conductor, we write

$$\omega^-(\rho) = \omega^-(\rho|_\Gamma),$$

which again is non-zero by Lemma 3.11.

We now formulate our conjecture on the existence of plus and minus p-adic L-functions of E over $\mathcal{G}$.

Conjecture 3.13. *There exist two elements $\mathcal{L}^\pm_{\mathcal{G},E} \in K_1(\Lambda_\mathcal{O}(\mathcal{G})_{S^*})$ for the ring of integer $\mathcal{O}$ of some finite unramified extension of $\mathbb{Q}_p$ such that $\mathcal{L}^\nu_{\mathcal{G},E}(\rho) \neq \infty$ and*

$$\mathcal{L}^\nu_{\mathcal{G},E}(\rho) = \frac{e_p(\rho)}{\omega^\nu(\rho)} \times \frac{L_R(E,\rho^\vee,1)}{\Omega_+^{d^+(\rho)}\Omega_-^{d^-(\rho)}} \tag{10}$$

for all Artin representations ρ on $\mathcal{G}$ that has even (respectively odd) Γ-conductor with $\nu = +$ (respectively $\nu = -$).

This is analogous to [CFK+05, Conjecture 5.7].

Remark 3.14. *Remark 3.10 implies that we might assume that the representations considered in the statement of Conjecture 3.13 are irreducible.*

We now show that despite having much weaker interpolating properties than their counterpart in the good ordinary case, (10) uniquely determines $\mathcal{L}^\pm_{\mathcal{G},E}$ modulo ker(Det).

Theorem 3.15. *If Conjecture 3.13 holds, $\mathcal{L}^\pm_{\mathcal{G},E}$ are uniquely determined by* (10) *modulo the kernel of Det.*

Proof. For all $\xi \in K_1(\Lambda_\mathcal{O}(\mathcal{G})_{S^*})$ and monomial representations ρ on $\mathcal{G}$, with $\rho = \mathrm{Ind}^{\mathcal{G}}_{U_i\times\Gamma}\chi_\rho$, we have

$$\mathrm{Det}(\xi)(\rho) = \xi(\rho) = \theta_i(\xi)(\chi_\rho).$$

Hence, by Condition 2.1, Det(ξ) is uniquely determined by its image under the map $\prod_{i\in I}\theta_i(\xi)$. In other words,

$$\ker(\mathrm{Det}) = \ker\left(\prod_{i\in I}\theta_i\right).$$

Therefore, it suffices to show that (10) uniquely determines an element in

$$K_1(\Lambda_\mathcal{O}(\mathcal{G})_{S^*})/\ker\left(\prod_{i\in I}\theta_i\right).$$

A character χ on $U_i/V_i \times \Gamma$ decomposes into $\chi_0 \otimes \chi'$, where $\chi_0 = \chi|_{U_i/V_i}$ and $\chi' = \chi|_\Gamma$. Therefore, by Weierstrass' preparation theorem, an element in $\Lambda_\mathcal{O}(U_i/V_i\times\Gamma)^\times_{S^*}$ is uniquely determined by its values at characters of the form $\chi_0\otimes\chi'$ for all χ_0 and an infinite number of χ'. Artin representations ρ induced from characters on $U_i\times\Gamma$ that have even (or odd) Γ-conductor provide such a set of characters χ_ρ because Definition 3.9 does not impose any restrictions on χ_0 and χ' can send γ to an infinite number of primitive roots of unity. The values predicted by (10) therefore uniquely determine $\theta_i(\mathcal{L}^\pm_{\mathcal{G},E})$ for all $i\in I$, hence the result.

□

3.3. **Main conjecture.** In [LZ11], we have defined the signed Selmer groups $\mathrm{Sel}_p^\pm(E/\mathcal{F})$, which are subgroups of the usual Selmer group $\mathrm{Sel}_p(E/\mathcal{F})$. Let $X^\pm(E/\mathcal{F})$ be their respective Pontryagin duals. We conjecture that the following holds.

Conjecture 3.16. *The dual Selmer groups $X^\pm(E/\mathcal{F})$ belong to the category $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$.*

This corresponds to [CFK+05, Conjecture 5.1]. If Conjecture 3.16 holds and $\mathcal{G}$ contains no p-torsion, then there exist characteristic elements $\xi_{X^\pm(E/\mathcal{F})} \in K_1(\Lambda(\mathcal{G})_{S^*})$ as discussed in § 2.4. We may then formulate a main conjecture that relates these characteristic elements to the conjectural analytic p-adic L-functions predicted by Conjecture 3.13.

Conjecture 3.17 (Main conjecture)**.** *Let $i : K_1(\Lambda(\mathcal{G})_{S^*}) \to K_1(\Lambda_{\mathcal{O}}(\mathcal{G})_{S^*})$ be the natural homomorphism. Assume that $\mathcal{G}$ does not contain an element of order p and both Conjectures 3.13 and 3.16 hold. Then*

$$\mathcal{L}^\pm_{\mathcal{G},E} \equiv i(\xi_{X^\pm(E/\mathcal{F})}) \mod i(K_1(\Lambda_{\mathcal{O}}(\mathcal{G}))).$$

This is analogous to [CFK+05, Conjecture 5.8].

4. A special case

In this section, we assume that our elliptic curve E has complex multiplication by $\mathcal{O}_K$, where K is an imaginary quadratic extension of $\mathbb{Q}$. If ψ is a character on G_K, we write ψ^c for the character that sends g to $\psi(cgc^{-1})$.

We recall that a Grossencharacter of K is simply a continuous homomorphism $\phi : C_K \to \mathbb{C}^\times$, where C_K is the idele class group of K. It has complex L-function

$$L(\phi, s) = \prod_v (1 - \phi(v)N(v)^{-s})^{-1},$$

where the product runs through the finite places v of K at which ϕ is unramified, $\phi(v)$ is the image of the uniformiser of K_v under ϕ and $N(v)$ is the norm of v. We say that ϕ is of type (m, n) for some $m, n \in \mathbb{Z}$ if the restriction of ϕ to the archimedean part $\mathbb{C}^\times$ of C_K is of the form $z \mapsto z^m \bar{z}^n$. By Class Field Theory, we may equally view ϕ as a character on the Galois group G_K.

Since we assume that E has complex multiplication, we have $R = \{p\}$. Moreover, there exist a Grossencharacter ϕ be of type $(-1, 0)$ over K and a weight 2 modular form f_ϕ such that

$$L(E, s) = L(\phi, s) = L(f_\phi, s).$$

Then $L(E/K, s) = L(\phi, s)L(\phi^c, s)$. We continue to assume that E has good supersingular reduction at p. This implies that p is inert in K and $a_p(E)$ is automatically 0.

Let F be a finite abelian extension of K in which p is unramified. Then, $K_\infty \cap F = K$. Moreover, F_∞/K is abelian and

$$\mathrm{Gal}(F_\infty/K) \cong \mathrm{Gal}(F/K) \times \mathrm{Gal}(K_\infty/K).$$

Let $A = \mathrm{Gal}(F/K)$, $G = \mathrm{Gal}(F_\infty/K)$ and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. We further assume that $F_\infty/\mathbb{Q}$ is Galois and write $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbb{Q})$. Then

$$\mathcal{G} \cong \Delta \ltimes G. \tag{11}$$

As remarked in the introduction, $\mathcal{G}$ can be either abelian or non-abelian, depending on whether Δ acts on G trivially.

For the rest of this section, we shall show under some technical conditions that there exist two elements $\mathcal{L}^\pm_{\mathcal{G},E} \in K_1(\Lambda_{\mathcal{O}_{F_A}}(\mathcal{G})_{S^*})$ satisfying the interpolating properties predicted by Conjecture 3.13 for some finite extension F_A of $\mathbb{Q}_p$. Let us briefly outline our strategy here. In [BV10], Bouganis and Venjakob constructed a non-commutative p-adic L-function over the extension $\mathbb{Q}(E[p^\infty])/\mathbb{Q}$ for a p-ordinary elliptic curve with complex multiplication by $\mathcal{O}_K$. They made use of the 2-variable p-adic L-function of Yager [Yag82] for the extension $\mathbb{Q}(E[p^\infty])/K$ and consider its image in $K_1(\Lambda_{\mathcal{O}}(\mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})))$ under a natural map, which turns out to satisfy (1) up to some correction factor $\mathcal{L}_\Omega$. In the supersingular case, a corresponding 2-variable p-adic L-function has not yet been constructed. We instead construct plus and minus p-adic L-functions for the extension F_∞/K using ideas from [KPZ10]. Once this is done, we can apply the machineries developed by Bouganis and Venjakob to construct our desired elements for the extension $F_\infty/\mathbb{Q}$.

4.1. **Analytic p-adic L-functions.** Let η be an one-dimensional character on A. We write F_η for the field $\mathbb{Q}_p(\eta(g) : g \in A)$. Note that $\phi\eta$ is once again a Grossencharacter of type $(-1, 0)$ over K. Hence, by [Rib77, Theorem 3.4], there exists a CM modular form $f_{\phi\eta}$ such that $L(f_{\phi\eta}, s) = L(\phi\eta, s)$. Its conductor is coprime to p by our assumption on F, so the plus and minus p-adic L-functions $L^{\pm}_{f_{\phi\eta}} \in \Lambda_{F_\eta}(\Gamma)$ exist, as given by Theorem 3.5. Note that the periods $\Omega^{\pm}_{f_{\phi\eta}}$ are not unique, but we may choose $\Omega^{+}_{f_{\phi\eta}}$ to be Ω_+ for all η by the following lemma.

Lemma 4.1. *For any choice of $\Omega^{+}_{f_{\phi\eta}}$, there exists a constant $C \in F_\eta^\times$ such that $C\Omega_+ = \Omega^{+}_{f_{\phi\eta}}$.*

Proof. Given a modular form f, let L_f be the $\mathbb{Q}$-vector space generated by the L-values $L(f, \chi, 1)$ where χ runs through the set of Dirichlet characters.

By the algebraicity property of the periods, the lemma would follow from the inclusion

$$L_{f_{\phi\eta}} \subset F_\eta \cdot L_{f_\phi},$$

which is a consequence of the Fourier inversion formula for η and Birch's lemma (c.f. [Har87, §4]). □

Under our choice of periods, we define the following.

Definition 4.2. *Let $\nu \in \{+, -\}$ and $\delta = 0$ if $\nu = +$, whereas $\delta = 1/2$ if $\nu = -$. Define*

$$L^\nu_{G,\phi} = \sum_{\eta \in \hat{A}} e_\eta \cdot \overline{\eta}(p)^\delta L^\nu_{f_{\phi\bar{\eta}}} \in \Lambda_{F_A}(\Gamma)[A],$$

where $F_A = \cup_{\eta \in \hat{A}} F_\eta(\eta(p)^{1/2})$ and e_η is the idempotent $|A|^{-1} \sum_{g \in A} \overline{\eta}(g) g$.

If we identify Γ_K with Γ, we can treat $L^{\pm}_{G,\phi}$ as elements of $\Lambda_{F_A}(A \times \Gamma_K) \cong \Lambda_{F_A}(G)$. We shall do so from now on without further notice.

Lemma 4.3. *Let χ be a one-dimensional character on G with $\chi_0 = \chi|_A$ and $\chi' = \chi|_{\Gamma_K}$ with conductor $p^n > 1$, then*

$$L^\nu_{G,\phi}(\chi) = \frac{\chi_0(p)^{n/2}\tau(\chi')}{\omega^\nu(\chi')} \times \frac{L(\phi, \overline{\chi}, 1)}{\Omega_+}$$

where $\nu = +$ if n is even and $\nu = -$ if n is odd.

Proof. For any $\eta \in \hat{A}$, $\chi(e_\eta) = 0$ if $\chi_0 \neq \eta$ and $\chi(e_\eta) = 1$ otherwise. This implies

$$L^\nu_{G,\phi}(\chi) = \overline{\chi_0}(p)^\delta L^\nu_{f_{\phi\overline{\chi_0}}}(\chi').$$

Since $f_{\phi\overline{\chi_0}}$ is of weight 2 and its Nebentypus character takes value $\overline{\chi_0}(p)$ at p, Lemma 3.8 implies that

$$\begin{aligned} L^\nu_{f_{\phi\overline{\chi_0}}}(\chi') &= \overline{\chi_0}(p)^\delta \times \frac{\tau(\chi')}{\overline{\chi_0}(p)^{\lfloor (n+1)/2 \rfloor}\omega^\nu(\chi')} \times \frac{L(\phi\overline{\chi_0}, \overline{\chi'}, 1)}{\Omega^+_\phi} \\ &= \frac{\chi_0(p)^{\lfloor (n+1)/2 \rfloor - \delta}\tau(\chi')}{\omega^\nu(\chi')} \times \frac{L(\phi\overline{\chi_0}, \overline{\chi'}, 1)}{\Omega_+} \end{aligned}$$

for the appropriate parity of n. But $\lfloor (n+1)/2 \rfloor - \delta = n/2$, so we are done. □

Let us recall from [Pol03, Corollary 5.11] and [Lei11, Lemma 6.5] that $L^{\pm}_{f_{\phi\eta}} \neq 0$ for all $\eta \in \hat{A}$. It therefore makes sense to talk about the μ-invariants of $L^{\pm}_{f_{\phi\eta}}$. We from now on assume that the following is true.

Technical assumption. *Under our choice of periods, the μ-invariant of $L^{\pm}_{f_{\phi\eta}}$ is independent of $\eta \in \hat{A}$ (but may depend on the sign $\pm$).*

Lemma 4.4. *Under our technical assumption, $L^\nu_{G,\phi} \in \Lambda_{\mathcal{O}_{F_A}}(G)^\times_{S^*} = K_1(\Lambda_{\mathcal{O}_{F_A}}(G)_{S^*})$.*

Proof. Since we assume that $L^{\pm}_{f_{\phi\eta}}$ have the same μ-invariant, there exists an integer n (depends on the sign $\pm$) such that

$$\Lambda_{\mathcal{O}_{F_A}}(G)/\Lambda_{\mathcal{O}_{F_A}}(G)p^n L^{\pm}_{f_{\phi\eta}}$$

is finitely generated over $\mathbb{Z}_p$, and hence over $\mathcal{O}_{F_A}[A]$. In particular,

$$p^n L^{\pm}_{f_{\phi\eta}} \in S(\mathcal{O}_{F_A})^*,$$

which proves the lemma. □

Let ι be the inclusion map

$$\iota : \Lambda_{\mathcal{O}_{F_A}}(G)_{S^*} \to \Lambda_{\mathcal{O}_{F_A}}(\mathcal{G})_{S^*}.$$

This induces a map

$$\iota_* : K_1(\Lambda_{\mathcal{O}_{F_A}}(G)_{S^*}) \to K_1(\Lambda_{\mathcal{O}_{F_A}}(\mathcal{G})_{S^*}).$$

Thanks to Lemma 4.4, we may now make the following definition.

Definition 4.5. *Under the notation above, we define*

$$L^{\pm}_{\mathcal{G},\phi} := (\iota)_* \left(L^{\pm}_{G,\phi}\right) \in K_1(\Lambda_{\mathcal{O}_{F_A}}(\mathcal{G})_{S^*}).$$

The following lemma allows us to relate the interpolating properties of $L^{\pm}_{G,\phi}$ to those of $L^{\pm}_{\mathcal{G},\phi}$.

Lemma 4.6. *For all Artin representations ρ of $\mathcal{G}$, one has*

$$L^{\pm}_{\mathcal{G},\phi}(\rho) = L^{\pm}_{G,\phi}\left(\mathrm{Res}^{\mathcal{G}}_{G}\,\rho\right).$$

Proof. This follows from the same proof as [BV10, Lemma 2.9]. □

Proposition 4.7. *Let ρ be an irreducible Artin representation on $\mathcal{G}$. Then*

$$L^{\nu}_{\mathcal{G},\phi}(\rho) = \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^{d(\rho)}},$$

where $\nu = +$ (respectively $\nu = -$) if the ρ has even (respectively odd) Γ-conductor.

Proof. By [Ser78, §8.2] and (11), all irreducible Artin representations ρ of $\mathcal{G}$ are either one-dimensional or isomorphic $\mathrm{Ind}^{\mathcal{G}}_{G}\,\chi$ for some one-dimensional character χ on G with $\chi \neq \chi^c$ (the latter case occurs if and only if $\mathcal{G}$ is non-abelian).

If ρ is one-dimensional, write $\chi = \mathrm{Res}^{\mathcal{G}}_{G}(\rho)$ and we factor χ into $\chi_0 \otimes \chi'$ as in Lemma 4.3. We have $\chi' = \rho|_{\Gamma}$. Let p^n be the conductor of χ'. Via the identification of Γ with Γ_K, we see that ρ has even (respectively odd) Γ-conductor if and only if n is even (respectively odd). Therefore, we can combine Lemmas 4.3 and 4.6 to deduce that

$$L^{\nu}_{\mathcal{G},\phi}(\rho) = \frac{\chi_0(p)^{n/2}\tau(\chi')}{\omega^{\nu}(\chi')} \times \frac{L(\phi,\overline{\chi},1)}{\Omega_+}. \tag{12}$$

By Frobenius reciprocity, we have

$$L(\phi,\overline{\chi},1) = L(E,\overline{\rho},1) = L(E,\rho^{\vee},1). \tag{13}$$

Let ρ_0 be the unramified part of $\rho|_{G_{\mathbb{Q}_p}}$. Then, $e_p(\rho) = \rho_0(p)^n\tau(\chi')$ by definition. But $K_p/\mathbb{Q}_p$ is an unramified extension of degree 2, so $\rho_0(p)^2 = \chi_0(p)$. Hence, $e_p(\rho) = \chi_0(p)^{n/2}\tau(\chi')$. Together with (12) and (13), we can therefore conclude that

$$L^{\nu}_{\mathcal{G},\phi}(\rho) = \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+}$$

as required.

We now study the case when ρ is 2-dimensional, should it occur. In this case, we have $\rho = \mathrm{Ind}^{\mathcal{G}}_{G}\,\chi$ for some character χ on G. Then $\mathrm{Res}^{\mathcal{G}}_{G}\,\rho = \chi \oplus \chi^c$. As before, we decompose χ and χ^c into $\chi_0 \otimes \chi'$ and $\chi_0^c \otimes (\chi^c)'$ respectively. As we assume that ρ has even or odd Γ-conductor, we have $\chi' = (\chi^c)' \neq \mathbf{1}$. In particular,

$$\rho|_{\Gamma} = \chi' \oplus (\chi^c)' = (\chi')^{\oplus 2}. \tag{14}$$

We can once again apply Lemmas 4.3 and 4.6 to deduce that

$$\begin{aligned} L^{\nu}_{\mathcal{G},\phi}(\rho) &= L^{\nu}_{G,\phi}(\chi)L^{\nu}_{G,\phi}(\chi^c) \\ &= (\chi_0\chi_0^c(p))^{n/2} \times \left(\frac{\tau(\chi')}{\omega^{\nu}(\chi')}\right)^2 \times \frac{L(\phi,\overline{\chi},1)L(\phi,\overline{\chi^c},1)}{\Omega_+^2}, \end{aligned}$$

where ν depends on the parity of the Γ-conductor of ρ as in the statement of the proposition.

As in the one-dimensional case, Frobenius reciprocity implies that

$$L(\phi,\overline{\chi},1)L(\phi,\overline{\chi^c},1) = L(\phi,\overline{\chi}\oplus\overline{\chi^c},1) = L(E,\rho^{\vee},1).$$

By our assumption on the non-ramification of p in F, $\rho|_{G_{\mathbb{Q}_p}}$ in fact decomposes into the direct sum of two one-dimensional characters, say ρ_1 and ρ_2. On restricting to G_{K_p}, they coincide with χ and χ^c. Hence, as above, we may deduce that $e_p(\rho_1)$ and $e_p(\rho_2)$ are given by $\chi_0^{n/2}(p)\tau(\chi')$ and $\chi_0^c(p)^{n/2}\tau(\chi')$. This implies that

$$e_p(\rho) = e_p(\rho_1)e_p(\rho_2) = \chi_0\chi_0^c(p)^{n/2}(\tau(\chi'))^2.$$

Putting all these together, we conclude that

$$\begin{aligned} L^{\nu}_{\mathcal{G},\phi}(\rho) &= \frac{e_p(\rho)}{(\omega^{\nu}(\chi'))^2} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^2} \\ &= \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^2}, \end{aligned}$$

where the second equality follows from (14). □

We can now define our plus and minus p-adic L-functions of E over $\mathcal{G}$.

Definition 4.8. *Let $\mathcal{L}_{\Omega} = \frac{1+c}{2} + \frac{\Omega_+}{\Omega_-} \times \frac{1-c}{2} \in \Lambda(\mathcal{G})^{\times}$ (c.f.* [BV10, Lemma 2.10]*). We define*

$$\mathcal{L}^{\pm}_{\mathcal{G},E} := L^{\pm}_{\mathcal{G},\phi}\mathcal{L}_{\Omega} \in K_1(\Lambda_{\mathcal{O}_{F_A}}(\mathcal{G})_{S^*}).$$

Theorem 4.9. *Let ρ be an irreducible Artin representation of $\mathcal{G}$. Then*

$$\mathcal{L}^{\nu}_{\mathcal{G},E}(\rho) = \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^{d^+(\rho)}\Omega_-^{d^-(\rho)}},$$

where $\nu = +$ (respectively $\nu = -$) if the ρ has even (respectively odd) Γ-conductor.

Proof. If ρ is 1-dimensional, then $d^+(\rho) = 1$ and $\mathcal{L}_{\Omega}(\rho) = 1$. Hence, by Proposition 4.7,

$$\begin{aligned} \mathcal{L}^{\nu}_{\mathcal{G},E}(\rho) &= L^{\nu}_{\mathcal{G},\phi}(\rho) \\ &= \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^{d(\rho)}}, \end{aligned}$$

where ν corresponds to the parity of the Γ-conductor of ρ as usual. If ρ is 2-dimensional, then $d^+(\rho) = d^-(\rho) = 1$ and $\mathcal{L}_{\Omega}(\rho) = \Omega_+/\Omega_-$. Therefore, we deduce from Proposition 4.7 that

$$\begin{aligned} \mathcal{L}^{\nu}_{\mathcal{G},E}(\rho) &= L^{\nu}_{\mathcal{G},\phi}(\rho) \\ &= \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+^2} \times \frac{\Omega_+}{\Omega_-} \\ &= \frac{e_p(\rho)}{\omega^{\nu}(\rho)} \times \frac{L(E,\rho^{\vee},1)}{\Omega_+\Omega_-}. \end{aligned}$$

□

Remark 4.10. *As remarked above, $R = \{p\}$ because E has complex multiplication. Since the Euler factor of $L(E,\rho^{\vee},1)$ at p is trivial, Theorem 4.9, together with Remark 3.14, give an affirmative answer to Conjecture 3.13 in this particular setting.*

4.2. **Remarks on the main conjecture.** Since p is unramified in F, p splits into distinct primes $\mathfrak{p}_1 \cdots \mathfrak{p}_d$ in F. Results in [LZ11, §4] imply that the signed Selmer groups $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ can be explicitly described as follows. For $n \geq 0$, let

$$\mathrm{Sel}_p^{\pm}(E/F_n) = \ker\left(\mathrm{Sel}_p(E/F_n) \to \bigoplus_{i=1}^{d} \frac{H^1(F_{\mathfrak{p}_i,n}, E[p^\infty])}{E(F_{\mathfrak{p}_i,n})^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where

$$E(F_{\mathfrak{p}_i,n})^{\pm} = \left\{x \in E(F_{\mathfrak{p}_i,n}) : \mathrm{Tr}_{n/m+1}(x) \in E(F_{\mathfrak{p}_i,m}) \forall m \in S_n^{\pm}\right\}.$$

Here, $\mathrm{Tr}_{n/m+1}$ denotes the trace map $E(F_{\mathfrak{p}_i,n}) \to E(F_{\mathfrak{p}_i,m+1})$ with respect to the group law on E and

$$\begin{aligned} S_n^+ &= [0, n-1] \cap 2\mathbb{Z}; \\ S_n^- &= [0, n-1] \cap (2\mathbb{Z}+1). \end{aligned}$$

Then we have

$$\mathrm{Sel}_p^{\pm}(E/F_\infty) = \varinjlim \mathrm{Sel}_p^{\pm}(E/F_n).$$

Note that this is the same definition as given in [KPZ10], where p is assumed to split completely in F.

The main conjecture (Conjecture 3.17) relates our p-adic L-functions $\mathcal{L}_{\mathcal{G},E}^{\pm}$ to the dual Selmer groups $X^{\pm}(E/F_\infty)$. In [BV10, §2], it has been shown that the main conjecture for the extension $\mathbb{Q}(E[p^\infty])/\mathbb{Q}$ follows from the $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$-conjecture and the 2-variable main conjecture in the ordinary case. Unfortunately, we do not have the corresponding 2-variable main conjecture in our current setting, so we cannot adopt the method of Bouganis and Venjakob directly here.

References

[AV75] Yvette Amice and Jacques Vélu, *Distributions p-adiques associées aux séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), Soc. Math. France, Paris, 1975, pp. 119–131. Astérisque, Nos. 24–25.

[BV10] Thanasis Bouganis and Otmar Venjakob, *On the non-commutative main conjecture for elliptic curves with complex multiplication*, Asian J. Math. **14** (2010), no. 3, 385–416.

[CFK+05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob, *The* GL_2 *main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. **101** (2005), 163–208.

[CH01] John Coates and Susan Howson, *Euler characteristics and elliptic curves. II*, J. Math. Soc. Japan **53** (2001), no. 1, 175–235.

[DD07] Tim Dokchitser and Vladimir Dokchitser, *Computations in non-commutative Iwasawa theory*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272, With an appendix by J. Coates and R. Sujatha.

[Har87] Shai Haran, *p-adic L-functions for modular forms*, Compositio Math. **62** (1987), no. 1, 31–46.

[Har10] Takashi Hara, *Iwasawa theory of totally real fields for certain non-commutative p-extensions*, J. Number Theory **130** (2010), no. 4, 1068–1097.

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

[KPZ10] Byoung Du Kim, Jeehoon Park, and Bei Zhang, *Iwasawa main conjecture for CM elliptic curves over abelian extensions at supersingular primes*, preprint, 2010.

[Lei11] Antonio Lei, *Iwasawa theory for modular forms at supersingular primes*, Compositio Math. **147** (2011), no. 03, 803–838.

[LZ11] Antonio Lei and Sarah Livia Zerbes, *Signed Selmer groups over p-adic Lie extensions*, arXiv:1104.2168, 2011.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[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.

[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.

[Rib77] Kenneth A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 17–51. Lecture Notes in Math., Vol. 601.

[Ser78] Jean-Pierre Serre, *Représentations linéaires des groupes finis*, revised ed., Hermann, Paris, 1978.

[Spr09] Florian Sprung, *Iwasawa theory for elliptic curves at supersingular primes: beyond the case* $a_p = 0$, arXiv: 0903.3419, 2009.

[Tat79] John Tate, *Number theoretic background*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.

[Yag82] Rodney Yager, *On two variable p-adic L-functions*, Ann. of Math. (2) **115** (1982), no. 2, 411–449.

Department of Mathematics and Statistics, Burnside Hall, McGill University, Montreal QC, Canada H3A 0B9
E-mail address: antonio.lei@mcgill.ca