Journal of Algebra 342 (2011) 197–211

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Plus/minus p-adic L-functions for Hilbert modular forms

Jeehoon Park[a,*], Shahab Shahabi[b]

[a] Department of Mathematics, POSTECH (Pohang University of Science and Technology), San 31, Hyoja-Dong, Nam-Gu, Pohang, Gyeongbuk, 790-784, South Korea
[b] Department of Mathematics, McGill University, Montreal, QC H3A 2K6, Canada

ARTICLE INFO

Article history:
Received 14 April 2011
Communicated by Eva Bayer-Fluckiger

MSC:
primary 11R23
secondary 11F67

Keywords:
Hilbert modular forms
p-Adic L-functions at supersingular primes
Selmer groups
Elliptic curves

ABSTRACT

R. Pollack constructed in Pollack (2003) [13] plus/minus p-adic L-functions for elliptic modular forms, which are p-adically bounded, when the Hecke eigenvalues at p are zero (the most supersingular case). The goal of this work is to generalize his construction to Hilbert modular forms. We find a suitable condition for Hilbert modular forms corresponding to the vanishing of p-th Hecke eigenvalue in elliptic modular form case, which guarantees the existence of plus/minus p-adic L-functions which are p-adically bounded. As an application, we construct cyclotomic plus/minus p-adic L-functions for modular elliptic curves over a totally real field F under the assumption that $a_{\mathfrak{p}}(E) = 0$ for each prime $\mathfrak{p}$ dividing p. We formulate a cyclotomic plus/minus Iwasawa main conjecture for such elliptic curves.

Contents

[*] Corresponding author.
E-mail addresses: jeehoonpark@postech.ac.kr (J. Park), shahabi@math.mcgill.ca (S. Shahabi).

0021-8693/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2011.04.033

1. Introduction

Analytic cyclotomic p-adic L-functions of modular forms are p-adic continuous functions on a p-adic rigid analytic space (called the weight space) which interpolate the critical values of modular forms twisted by powers of the p-adic cyclotomic character at the arithmetic points. (Since we will only consider cyclotomic p-adic L-functions in this article, we omit the term *cyclotomic* from now on.) Mazur and Swinnerton-Dyer [9] constructed the analytic p-adic L-functions $L_p(f,\alpha,\chi)$ for a weight k elliptic modular form f and an allowable root α of the p-Hecke polynomial, where χ is a p-adic character and α is said to be allowable if $\mathrm{ord}_p(\alpha) < k-1$, using the theory of modular symbols. Then Manin [8] extended this result to Hilbert modular forms. These p-adic L-functions depend on several things: a prime p, a choice of appropriate periods, and a root of the Hecke polynomial at p (call it *p-Frobenius root*). In particular, a choice of a prime p and a p-Frobenius root influences the behavior of the p-adic L-functions. For example, if p is an ordinary prime for a modular form, then one can show that the p-adic L-function for a p-Frobenius root which is a p-adic unit is an Iwasawa function, i.e. it comes from a p-adic measure. But if p is not an ordinary prime, then the p-adic L-function is not anymore p-adically bounded, which makes it harder to study. For example, it does have infinitely many zeros.

For non-ordinary primes p, Višik [15] (and Dabrowski [2] respectively) analyzed the growth conditions for p-adic L-functions of elliptic modular forms (Hilbert modular forms respectively). Then Pollack [13] realized how to remove certain trivial zeros from the supersingular p-adic L-functions of elliptic modular forms when its Hecke eigenvalue a_p vanishes and consequently constructed the so-called plus/minus p-adic L-functions which are p-adically bounded at such a supersingular (non-ordinary) prime p. Soon after, Kobayashi [7] constructed algebraic plus/minus p-adic L-functions for elliptic curves over $\mathbb{Q}$ and formulated the plus/minus Iwasawa main conjecture in the framework of Iwasawa algebras, which turns out to be equivalent to Kato's Iwasawa main conjecture at supersingular primes. In [7], Kobayashi also proved one divisibility of the plus/minus Iwasawa main conjecture, showing that the algebraic p-adic L-function divides the analytic p-adic L-function.

The goal of this paper is to construct plus/minus p-adic L-functions for Hilbert modular forms for certain non-ordinary primes p (Theorem 2.7) generalizing Pollack's work and to study the supersingular (or non-ordinary) p-adic L-functions for CM theta series as explicit such examples. Section 2 is devoted to carrying out such constructions and study their properties after reviewing briefly Dabrowski's result in [2]. The main idea, which is not that different from Pollack's idea, is to analyze the growth conditions of Dabrowski's p-adic L-functions for Hilbert modular forms for different choices of p-Frobenius roots. Then in Section 3, the Iwasawa main conjecture for modular elliptic curves over a totally real field is formulated (under certain technical conditions) using the analytic plus/minus p-adic L-functions and the plus/minus p-Selmer groups given in [5] (Conjecture 3.7). Since the definition of the plus/minus p-Selmer groups for Hilbert modular forms are not known in general, we limit ourselves to discuss only modular elliptic curves over a totally real field when we deal with the main conjecture.

2. *p*-Adic *L*-functions

Throughout we fix a rational *odd* prime p and embeddings $\overline{\mathbb{Q}} \to \mathbb{C}$ and $\overline{\mathbb{Q}} \to \mathbb{C}_p$ where $\mathbb{C}_p$ is the p-adic completion of $\overline{\mathbb{Q}}_p$. We normalize the valuation val_p and the absolute value $|\cdot|_p$ on $\mathbb{C}_p$ by assuming $\mathrm{val}_p(p) = 1$ and $|p|_p = p^{-1}$.

2.1. Basic notations for Hilbert modular forms

Let F be a totally real number field of degree d over $\mathbb{Q}$. For notational simplicity, we assume that F has the strict ideal class number one (hence a Hilbert modular form will be given by only one holomorphic function on $\mathbb{H}^d$; $\mathbb{H}$ being the upper half plane). Let $\mathcal{O}_F$ be the ring of integers of F. Let $\mathcal{D}_F$ be the different ideal of F and D_F the absolute discriminant of F. Let $J_F = \{\sigma_1, \ldots, \sigma_d\}$ be the set of embeddings of F into $\mathbb{R} \subset \mathbb{C}$, and let $\mathrm{sgn}_F \subset F_\infty^\times := (F \otimes \mathbb{R})^\times \simeq (\mathbb{R}^\times)^d$ be the group of signs of F, i.e. the group of elements of order 2 in $F_\infty^\times$.

Let f be a Hilbert cuspidal newform of weight $k = (k_1, \ldots, k_d)$ and character ω whose conductor divides a fixed integral ideal $\mathfrak{a}$ prime to p. We assume that each k_i is a positive integer ($i = 1, \ldots, d$) and $k_1 \equiv k_2 \equiv \cdots \equiv k_d \pmod 2$. Let $k_* = \min_i\{k_i\}$ and $k^* = \max_i\{k_i\}$. We fix the complex periods $c^\pm(\sigma, f)$, $\sigma \in J_F$, which are explained in [17] and [11] (also see Remark (i) on p. 1027 in [2]). Let $T(\mathfrak{n})$ be the Hecke operator associated to an ideal $\mathfrak{n}$ of F, so that $T(\mathfrak{n})f = \mathcal{C}(f, \mathfrak{n})f$ for each $\mathfrak{n}$. The field K_f generated over $\mathbb{Q}$ by $\{\mathcal{C}(f, \mathfrak{n})\}$, as $\mathfrak{n}$ ranges over all integral ideals of $\mathcal{O}_F$, is known to be a number field (i.e., $[K_f : \mathbb{Q}] < \infty$) and contains the values $\omega(\mathfrak{n})$ for any integral ideal $\mathfrak{n}$ of F. The complex L-function of f twisted by a Hecke character ψ of finite order is defined to be

$$\begin{aligned} L(f, \psi, s) &= \sum_{0 \neq \mathfrak{n} \subset F} \frac{\psi(\mathfrak{n})\mathcal{C}(f, \mathfrak{n})}{N\mathfrak{n}^s} \\ &= \prod_{\mathfrak{p}} \bigl(1 - \psi(\mathfrak{p})\mathcal{C}(f, \mathfrak{p})N\mathfrak{p}^{-s} + \psi^2(\mathfrak{p})\omega(\mathfrak{p})N\mathfrak{p}^{k^*-1-2s}\bigr)^{-1}, \quad \mathrm{Re}(s) \gg 0 \end{aligned}$$

where the sum (respectively the product) is taken over all nonzero integral (respectively prime) ideals of $\mathcal{O}_F$. Let $\Lambda(f, \psi, s) = (\prod_{i=1}^n \Gamma_\mathbb{C}(s - \frac{k^*-k_i}{2})) \cdot L(f, \psi, s)$ be the completed L-function of f twisted by ψ. Let $\mathfrak{p}$ be a prime ideal of F lying above p. Let

$$1 - \mathcal{C}(f, \mathfrak{p})X + \omega(\mathfrak{p})N\mathfrak{p}^{k^*-1}X^2 = \bigl(1 - \alpha(\mathfrak{p})X\bigr)\bigl(1 - \alpha'(\mathfrak{p})X\bigr) \in \mathbb{C}_p[X]$$

where $\alpha(\mathfrak{p}) = \alpha(\mathfrak{p}, f), \alpha'(\mathfrak{p}) = \alpha'(\mathfrak{p}, f)$ are the inverse roots of the Hecke polynomial at $\mathfrak{p}$ (note that p is prime to $\mathfrak{a}$). We will always assume $\mathrm{val}_p(\alpha(\mathfrak{p})) \leqslant \mathrm{val}_p(\alpha'(\mathfrak{p}))$ throughout the article. For given $\sigma \in J_F$, one can associate the embeddings $F \to \overline{\mathbb{Q}}, F \to \mathbb{C}_p$ and also define a prime divisor $\mathfrak{p} = \mathfrak{p}(\sigma)$ of p in F.

Let $[m_*, m^*]$ be the critical strip for $L(f, \psi, s)$, where

$$m_* = 1 + \max_i\left\{\frac{k^* - k_i}{2}\right\}, \qquad m^* = -1 + \min_i\left\{\frac{k^* + k_i}{2}\right\}.$$

Note that $m^* - m_* + 1 = -1 + \frac{k^*+k_*}{2} - (1 + \frac{k^*-k_*}{2}) + 1 = k_* - 1$.

2.2. Conductors of Hecke characters

We assume that the Leopoldt conjecture holds for F. This conjecture is known to be true for all abelian totally real number fields (see, for example, [16]).

Let $F_\infty = F(\mu_{p^\infty})$ be the field obtained by joining all the p-power roots of unity to F. Let $\chi : \mathrm{Gal}(F_\infty/F) \hookrightarrow \mathbb{Z}_p^\times$ be the p-adic cyclotomic character (which is injective) and denote the image of χ by Γ. Then the free part of Γ is topologically generated by $1 + p^e$ for some positive integer $e \geqslant 1$, i.e. $\Gamma/\mathrm{Tor}(\Gamma) = 1 + p^e\mathbb{Z}_p$ where $\mathrm{Tor}(\Gamma)$ is the torsion subgroup of Γ. Note that $\mathrm{Tor}(\Gamma)$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Let $F_{cyc} \subset F_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of F so that $\mathrm{Gal}(F_{cyc}/F) \simeq \chi^{-1}(1 + p\mathbb{Z}_p)$.

Class field theory provides an isomorphism (cf. Corollary 13.6 in [16])

$$\mathrm{rec}: (\mathcal{O}_F \otimes \mathbb{Z}_p)^\times / \overline{E_F^+} \to \mathrm{Gal}\big(F(p,\infty)/F(1)\big)$$

where $F(p,\infty)$ is the maximal abelian extension of F unramified outside all the primes of F above p and ∞, where $F(1)$ is the Hilbert class field of F, and where $\overline{E_F^+}$ is the p-adic closure of the totally positive unit group $E_F^+ = \mathcal{O}_F^{\times,+}$. Note that the strict ideal class number one assumption implies that

$$\mathrm{rec}: (\mathcal{O}_F \otimes \mathbb{Z}_p)^\times / \overline{E_F^+} \simeq \mathrm{Gal}\big(F(p,\infty)/F\big).$$

One can decompose the Galois group $\mathrm{Gal}(F(p,\infty)/F)$ as

$$\mathrm{Gal}\big(F(p,\infty)/F\big) \simeq \mathrm{Gal}(F_{cyc}/F) \times T$$

where T is an abelian group. The Leopoldt conjecture for F implies that T is a finite abelian group. The domain of definition for p-adic L-functions of Hilbert modular forms is the p-adic analytic group

$$\mathcal{X} := \mathrm{Hom}_{cts}\big(\mathrm{Gal}\big(F(p,\infty)/F\big), \mathbb{C}_p^\times\big).$$

Each element ϕ in $\mathcal{X}$ can be uniquely written as $\psi \cdot \epsilon$ where $\psi \in \mathrm{Hom}_{cts}(\mathrm{Gal}(F_{cyc}/F), \mathbb{C}_p^\times)$ and $\epsilon \in \mathrm{Hom}_{cts}(T, \mathbb{C}_p^\times)$. We fix a topological generator γ of $\mathrm{Gal}(F_{cyc}/F)$. If we fix a character ϵ of T, then ϕ is determined by the image $\psi(\gamma)$ which belongs to the open unit disc centered at 1 in $\mathbb{C}_p^\times$.

Note that $\phi \in \mathcal{X}$ can be thought of as a Hecke character of F. If $\phi = \psi \cdot \epsilon$ (as above) is of finite order, then $\psi(\gamma) = \zeta_{p^n}$ for some $n \geqslant 0$, where ζ_{p^n} is a primitive p^n-th root of unity. Viewing ϕ as a Hecke character, we want to determine its conductor $\mathfrak{c}(\phi)$ as an ideal of F. Define ψ_n by the condition $\psi_n(\gamma) := \zeta_{p^n}$ for $n \geqslant 0$.

Proposition 2.1. *If ϕ has the form $\psi_n \cdot \epsilon \in \mathcal{X}$, then $\mathfrak{c}(\psi_0 \cdot \epsilon) = \mathfrak{c}(\epsilon)$ and*

$$\mathfrak{c}(\phi) = lcm\big(\mathfrak{c}(\epsilon), p^{n+e}\mathcal{O}_F\big) = lcm\left(\mathfrak{c}(\epsilon), \prod_{i=1}^{\kappa} \mathfrak{p}_i^{e_i(e+n)}\right), \quad \textit{for } n \geqslant 1,$$

where $\mathfrak{c}(\epsilon)$ is the conductor of ϵ and $p\mathcal{O}_F = \prod_{i=1}^{\kappa} \mathfrak{p}_i^{e_i}$.

Proof. If $n = 0$, then $\mathfrak{c}(\psi_n) = \mathcal{O}_F$ and $\mathfrak{c}(\psi_0 \cdot \epsilon) = \mathfrak{c}(\epsilon)$. Now we assume that $n \geqslant 1$. Since $\psi_n(\gamma) = \zeta_{p^n}$, the character ψ_n factors through a finite cyclic group whose generator has order p^n. In fact, we can regard ψ_n as a Dirichlet character mod p^{n+e} via the p-adic cyclotomic character χ and the reduction modulo p^{n+e} map $1 + p^e\mathbb{Z}_p \to (\mathbb{Z}_p/p^{n+e}\mathbb{Z}_p)^\times$, i.e. the character ψ_n is the composition of the following maps:

$$\mathrm{Gal}(F_{cyc}/F) \xrightarrow{\chi} 1 + p^e\mathbb{Z}_p \overset{(\mathrm{mod}\ p^{n+e})}{\longrightarrow} 1 + p^e \cdot \big(\mathbb{Z}/p^n\mathbb{Z}\big) \hookrightarrow \big(\mathbb{Z}/p^{n+e}\mathbb{Z}\big)^\times \longrightarrow \mathbb{C}_p^\times$$

for $n \geqslant 1$. Therefore $\mathfrak{c}(\psi_n)$ is the smallest (in the sense of divisibility) ideal $\mathfrak{c}$ of F divisible by all the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_\kappa$ such that

$$\big(1 + p^e\big)^{p^n} = 1 + \sum_{i=1}^{p^n} \binom{p^n}{i} p^{ei} \equiv 1 \pmod{\mathfrak{c}}.$$

Because $\mathrm{val}_p(\sum_{i=1}^{p^n}\binom{p^n}{i}p^{ei}) = n+e$, which follows from $\mathrm{val}_p(\binom{p^n}{i}) = n - \mathrm{val}_p(i)$ for $1 \leqslant i \leqslant p^n$, such a smallest ideal $\mathfrak{c}$ should be $p^{n+e}\mathcal{O}_F$ and so $\mathfrak{c}(\psi_n) = p^{n+e}\mathcal{O}_F$. Since $\phi = \psi_n \cdot \epsilon$, the result follows. □

Remark 2.2. It is mostly for notational simplicity that we assume the Leopoldt conjecture. Without the Leopoldt conjecture we just need to use the norm character from $\mathrm{Gal}(F(p,\infty)/F)$ to $\mathbb{Z}_p^\times$ instead of the cyclotomic character above.

2.3. *h-Admissibility and growth conditions*

For a positive integer M prime to p, we let $\mathbb{Z}_{p,M}^\times = \mathbb{Z}_p^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$, and write $x_p : \mathbb{Z}_{p,M}^\times \twoheadrightarrow \mathbb{Z}_p^\times$ for the canonical projection. Let $\Sigma \subseteq \mathbb{Z}_{p,M}^\times$ be an open subgroup of finite index. Then $\Sigma/\Sigma_{tor} \simeq 1 + p^e\mathbb{Z}_p$ for some $e \geqslant 1$. For any nonnegative real number h, we shall denote by $P^h(\Sigma)$ the space of $\mathbb{C}_p$-valued functions on Σ which are locally polynomials in x_p of degree $\leqslant h$. A $\mathbb{C}_p$-valued distribution μ on $P^h(\Sigma)$ is said to be *h-admissible* if for each integer $0 \leqslant i < h$,

$$\sup_{a\in\mathbb{Z}_p^\times}\left|\int\limits_{(a+p^m\mathbb{Z}_p)\cap\Sigma}(x_p - a_p)^i\,d\mu\right|_p = O\bigl(|p^m|_p^{i-h}\bigr), \quad \text{as } m \to \infty.$$

Višik has proved in [15] that every $\mathbb{C}_p$-valued locally analytic function on Σ can be integrated against such μ, and that for any fixed character ϵ on $(\mathbb{Z}/pM\mathbb{Z})^\times \cap \Sigma$—viewed of course as a locally analytic function on Σ—the mapping $\psi \mapsto \int_\Sigma \epsilon\psi\,d\mu$ (defined on the group $\mathrm{Hom}_{cts}(1+p^e\mathbb{Z}_p, \mathbb{C}_p^\times)$ endowed with the analytic structure of the open unit disc in $\mathbb{C}_p$ via the identification $\psi \mapsto u = \psi(1+p^e)$) is p-adic analytic and is $O(\log_p(\ )^h)$.

We now review the result of Dabrowski in [2], which is a generalization of Višik's work [15] (on elliptic modular forms) to Hilbert modular forms. Recall that γ is a topological generator of $\mathrm{Gal}(F_{cyc}/F)$. We fix an isomorphism $\mathbb{Z}_p[\![\mathrm{Gal}(F_{cyc}/F)]\!] \simeq \mathbb{Z}_p[\![T]\!]$ by sending the class of γ to $1+T$. We will just reformulate Dabrowski's result in terms of power series in T with certain coefficient ring, using the fixed isomorphism $\mathbb{Z}_p[\![\mathrm{Gal}(F_{cyc}/F)]\!] \simeq \mathbb{Z}_p[\![T]\!]$. More precisely, his p-adic L-function $L_{(p)}^{\epsilon_0}$ defined on $\mathrm{Hom}_{cts}(\mathrm{Gal}(F(p,\infty)/F), \mathbb{C}_p^\times)$ and indexed by $\epsilon_0 \in \mathrm{sgn}_F \simeq \{\pm 1\}^d$ (see Theorem 1 of [2]) comes from a distribution $\mu_{f,\alpha}^{\epsilon_0}$ on $\mathrm{Gal}(F(p,\infty)/F)$ (where $\alpha = \{\alpha(\mathfrak{p}(\sigma))\}_{\sigma\in J_F}$) via

$$L_{(p)}^{\epsilon_0}(\phi) = \int\limits_{\mathrm{Gal}(F(p,\infty)/F)} \phi(x)\,d\mu_{f,\alpha}^{\epsilon_0}(x), \quad \phi \in \mathcal{X} = \mathrm{Hom}_{cts}\bigl(\mathrm{Gal}\bigl(F(p,\infty)/F\bigr), \mathbb{C}_p^\times\bigr).$$

Note that the integration on the right-hand side makes sense, since Dabrowski proves that $\mu_{f,\alpha}^{\epsilon_0}$ is h-admissible for certain h. For the actual value of h, see Theorem 2.3 below.

From now on we fix a finite order character

$$\epsilon \in \mathrm{Hom}_{cts}\bigl(T, \mathbb{C}_p^\times\bigr) \tag{2.1}$$

and set $\alpha = \{\alpha(\mathfrak{p}(\sigma))\}_{\sigma\in J_F}$. Then we define

$$L_p(f,\alpha,\phi) := \int\limits_{\mathrm{Gal}(F(p,\infty)/F)} \phi(x)\,d\mu_{f,\alpha}^{\mathrm{sgn}(\phi)}(x)$$

where $\phi = \psi \cdot \epsilon$ (using the previous notation). So $L_p(f,\alpha,\phi)$ corresponds to $L_{(p)}^{\mathrm{sign}(\psi\cdot\epsilon)}(\phi)$, with ϵ fixed.

We now choose a prime of K_f above p and let K be the completion of K_f at our chosen prime over p. Let K_ϵ be the field generated by the values of ϵ over K, and let $\mathcal{O}_\epsilon$ be its ring of integers (for a Hecke character ϵ of finite order). Since $L_p(f,\alpha,\phi)$ is p-adic analytic in ϕ (cf. [15, Theorem 2.3]), $L_p(f,\alpha,\phi)$ can be expanded in a power series in T around ϵ with identification $T=\psi(\gamma)-1$, giving rise to $L_p(f,\alpha,\epsilon,T)\in K_\epsilon\llbracket T\rrbracket$. Finally, let $\Lambda_\epsilon=\mathcal{O}_\epsilon\llbracket T\rrbracket$ be the associated Iwasawa algebra. We summarize Dabrowski's result [2, Theorem 1]:

Theorem 2.3. *Assume* $\mathrm{val}_p(\alpha(\mathfrak{p}))\leqslant\mathrm{val}_p(\alpha'(\mathfrak{p}))$ *for each* $\mathfrak{p}\mid p$. *Put* $h=h_\alpha:=\max_i\{\mathrm{val}_p(\alpha(\mathfrak{p}(\sigma_i)))-\frac{k^*-k_i}{2}\}$ *where* $J_F=\{\sigma_1,\sigma_2,\dots,\sigma_d\}$. *Then for a fixed character* $\epsilon\in\mathrm{Hom}_{cts}(T,\mathbb{C}_p^\times)$ *and* $\alpha=\{\alpha(\mathfrak{p}(\sigma))\}_{\sigma\in J_F}$ *the* p*-adic L-function* $L_p(f,\alpha,\epsilon,T)\in K_\epsilon\llbracket T\rrbracket$ *introduced above has the growth* $O(\log_p^h(1+T))$ *and satisfies the following properties*:

(1) *For each* $m\in\mathbb{Z}$, $m_*\leqslant m\leqslant m^*$, *and for all Hecke characters of finite order* $\phi=\psi_n\cdot\epsilon\in\mathrm{Tor}(\mathcal{X})$ *the following interpolation property holds*

$$L_p\bigl(f,\alpha,\epsilon,\bigl(1+p^e\bigr)^m\zeta_{p^n}-1\bigr)=\frac{D_F^m\cdot(\sqrt{-1})^{dm}}{G(\phi)}\prod_{\mathfrak{p}\mid p}\mathcal{A}_\mathfrak{p}(f,\phi,m)\cdot\frac{\Lambda(f,\phi,m)}{\Omega(\epsilon_0,f)},$$

where

$$\mathcal{A}_\mathfrak{p}(f,\phi,m)=\begin{cases}(1-\alpha'(\mathfrak{p})N\mathfrak{p}^{-m})(1-\alpha(\mathfrak{p})^{-1}N\mathfrak{p}^{m-1}) & \text{if } \mathfrak{p}\nmid\mathfrak{c}(\phi),\\ (\frac{N\mathfrak{p}^m}{\alpha(\mathfrak{p})})^{\mathrm{val}_\mathfrak{p}\,\mathfrak{c}(\phi)} & \text{if } \mathfrak{p}\mid\mathfrak{c}(\phi),\end{cases}$$

and

$$\Omega(\epsilon_0,f)=(2\pi i)^{-dm_*}\cdot D_F^{\frac{1}{2}}\cdot\prod_{\sigma\in J_F}c^{\epsilon_{0,\sigma}}(\sigma,f),$$

$$\epsilon_0=\{\epsilon_{0,\sigma}\}_\sigma:=\mathrm{sgn}\bigl(\epsilon\cdot\psi_n\cdot\bigl(x_p\mapsto\chi(x_p)^m\bigr)\bigr)\in\mathrm{sgn}_F,$$

and where $G(\phi)$ *is the Gauss sum of* ϕ.

(2) *If* $h\leqslant m^*-m_*=k_*-2$, *then* $L_p(f,\alpha,\epsilon,T)$ *is uniquely determined by the interpolation property of* (1) *and the growth condition* $O(\log_p^h(1+T))$.

(3) *If* $h=0$, *then the function* $L_p(f,\alpha,\epsilon,T)$ *is* p*-adically bounded on* $\mathcal{X}$, *i.e.* $L_p(f,\alpha,\epsilon,T)\in\mathcal{O}_\epsilon\llbracket T\rrbracket\otimes K_\epsilon$.

2.4. Infinitude of zeros of non-ordinary p-adic L-functions

We keep the notation from the previous section. The following proposition follows directly from Proposition 2.1 and the interpolation property (1) of Theorem 2.3:

Proposition 2.4. *Let* $\{\mathfrak{p}_j\colon j=1,2,\dots,\kappa\}$ *be the set of distinct prime ideals of* F *lying above* p. *Write* $p\mathcal{O}_F=\prod_{j=1}^\kappa\mathfrak{p}_j^{e_j}$ *and* $\mathfrak{c}(\epsilon)=\mathfrak{c}\prod_j\mathfrak{p}_j^{r_j}$ *for an ideal* $\mathfrak{c}$ *relatively prime to* p, *where* $e_j\geqslant 1$, $r_j\geqslant 0$ *for* $j=1,2,\dots,\kappa$. *Then we have*

$$L_p\bigl(f,\alpha,\epsilon,\bigl(1+p^e\bigr)^m\zeta_{p^n}-1\bigr)=\frac{c_n}{\prod_j\alpha(\mathfrak{p}_j)^{\max(r_j,e_j(e+n))}},\quad n\geqslant 1 \text{ and } m_*\leqslant m\leqslant m^*,$$

for some constant c_n *independent of* $\alpha=\{\alpha(\mathfrak{p}(\sigma))\}_{\sigma\in J_F}$ (*but obviously depending on* n, m *and* ϵ).

Suppose that $k_* - 2 \geqslant h = h_\alpha > 0$. Let $S_p := \{\mathfrak{p}(\sigma)\colon\ \mathfrak{p}(\sigma) \mid p,\ \sigma \in J_F\}$ be the set of prime ideals of F over p indexed by J_F (note that the cardinality of S_p is same as the one of J_F) and let $S = \{\mathfrak{p} \in S_p\colon\ \alpha'(\mathfrak{p}) = -\alpha(\mathfrak{p})\}$. For an arbitrary subset $R \subseteq S$, put

$$\alpha'_R = \bigl\{\alpha'(\mathfrak{p})\colon\ \mathfrak{p} \in R\bigr\} \cup \bigl\{\alpha(\mathfrak{p})\colon\ \mathfrak{p} \in S_p \setminus R\bigr\}. \tag{2.2}$$

Then, for a fixed character ϵ on T with $\mathfrak{c}(\epsilon) = \mathfrak{c}\prod_j \mathfrak{p}_j^{r_j}$, we can consider Dabrowski's p-adic L-function $L_p(f, \alpha'_R, \epsilon, \cdot)$, where R varies over subsets of S, because each root $\alpha \in \alpha'_R$ satisfies the assumption $\mathrm{val}_{\mathfrak{p}}(\alpha) \leqslant \mathrm{val}_{\mathfrak{p}}(\alpha')$ of Theorem 2.3. To simplify the notation, from now on we assume

$$r_j \leqslant e_j(e+1), \quad j = 1, \ldots, \kappa, \tag{2.3}$$

and remark that the case $r_j > e_j(e+1)$ can be easily dealt with by slightly modifying the plus/minus log functions below.

Proposition 2.5. *Let R_0 be a nonempty subset of S such that $(-1)^{\sum_{\mathfrak{p}_i \in R_0} e_i} = -1$. Then for any subset $R \subset S$ which is disjoint from R_0, one of $L_p^{\epsilon_0}(f, \alpha'_R, \epsilon, \cdot)$ and $L_p^{\epsilon_0}(f, \alpha'_{R \cup R_0}, \epsilon, \cdot)$ has infinitely many zeros in the open unit disc centered at 0.*

Proof. Let

$$G_\epsilon^+(R, R_0, T) := \frac{L_p(f, \alpha'_R, \epsilon, T) + L_p(f, \alpha'_{R \cup R_0}, \epsilon, T)}{2}$$

and

$$G_\epsilon^-(R, R_0, T) := \frac{L_p(f, \alpha'_R, \epsilon, T) - L_p(f, \alpha'_{R \cup R_0}, \epsilon, T)}{2\prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p})}.$$

Then we have

$$L_p\bigl(f, \alpha'_R, \epsilon, T\bigr) = G_\epsilon^+(R, R_0, T) + \prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p}) \cdot G_\epsilon^-(R, R_0, T),$$
$$L_p\bigl(f, \alpha'_{R \cup R_0}, \epsilon, T\bigr) = G_\epsilon^+(R, R_0, T) - \prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p}) \cdot G_\epsilon^-(R, R_0, T).$$

By Proposition 2.4 we have

$$L_p\bigl(f, \alpha'_R, \epsilon, \zeta_{p^n} - 1\bigr) = \frac{c_n}{(-1)^{\sum_{\mathfrak{p}_i \in R} \max(r_i, e_i(e+n))} \prod_j \alpha(\mathfrak{p}_j)^{\max(r_j, e_j(e+n))}} \tag{2.4}$$

and therefore

$$G_\epsilon^+(R, R_0, \zeta_{p^n} - 1) = 0$$

for $n \geqslant 1$ such that $\sum_{\mathfrak{p}_i \in R_0} \max(r_i, e_i(e+n)) = \sum_{\mathfrak{p}_i \in R_0} e_i(e+n)$ is odd. Since the condition $(-1)^{\sum_{\mathfrak{p}_i \in R_0} e_i} = -1$ implies that $e+n$ is odd, there are infinitely many such integers n. In the same way we see

$$G^-_\epsilon(R, R_0, \zeta_{p^n} - 1) = 0$$

when $n \geqslant 1$ satisfies that $\sum_{\mathfrak{p}_i \in R_0} \max(r_i, e_i(e+n)) = \sum_{\mathfrak{p}_i \in R_0} e_i(e+n)$ is even. There are also infinitely many such n's.

Assume now that both $L_p(f, \alpha'_R, \epsilon, T)$ and $L_p(f, \alpha'_{R \cup R_0}, \epsilon, T)$ have finitely many zeros. Then Lemma 3.2 in [13] would guarantee that both of these p-adic L-functions would have bounded coefficients. Hence $G^+_\epsilon(R, R_0, T)$ and $G^-_\epsilon(R, R_0, T)$ also would have bounded coefficients. But $G^\pm_\epsilon(R, R_0, T)$ have infinitely many zeros, which is a contradiction. □

2.5. Bounded p-adic L-functions at supersingular primes

Let $\Phi_k(T)$ be the k-th cyclotomic polynomial. For any positive integer m, we define

$$\log^+_{p,m}(F, T) := \frac{1}{p} \cdot \prod_{\substack{n=1 \\ e+n:\ \text{odd}}}^{\infty} \left(\frac{\Phi_{p^n}((1+p^e)^{-m}(1+T))}{p} \right),$$

and

$$\log^-_{p,m}(F, T) := \frac{1}{p} \cdot \prod_{\substack{n=1 \\ e+n:\ \text{even}}}^{\infty} \left(\frac{\Phi_{p^n}((1+p^e)^{-m}(1+T))}{p} \right).$$

Then Lemma 4.1 in [13] says that $\log^+_{p,m}(F, T)$ (respectively $\log^-_{p,m}(F, T)$) defines a power series in $\mathbb{Q}_p[\![T]\!]$ which is convergent on the open unit disc centered at 0, and that the zeros of $\log^+_{p,m}(F, T)$ (respectively $\log^-_{p,m}(F, T)$) are precisely $(1+p^e)^m \cdot \zeta_{p^n} - 1$ such that $e+n$ is even (respectively odd) for $n \geqslant 1$. Now we define

$$\log^+_p(F, T) := \prod_{m=m_*}^{m^*} \log^+_{p,m}(F, T),$$

and

$$\log^-_p(F, T) := \prod_{m=m_*}^{m^*} \log^-_{p,m}(F, T).$$

Then Corollary 4.2 in [13] implies that $\log^+_p(F, T)$ (respectively $\log^-_p(F, T)$) defines a power series in $\mathbb{Q}_p[\![T]\!]$ (depending on $k = (k_1, \ldots, k_d)$ and our chosen generator $1 + p^e$) which is convergent on the open unit disc centered at 0, and that the only zeros of $\log^+_p(F, T)$ (respectively $\log^-_p(F, T)$) are simple zeros at $(1+p^e)^m \cdot \zeta_{p^n} - 1$ such that $e+n$ is even (respectively odd) for $m_* \leqslant m \leqslant m^*$ and $n \geqslant 1$. Pollack has also proved (note that $m^* - m_* + 1 = k_* - 1$) that

Lemma 2.6. *(See Lemma 4.5, [13].) We have* $\log^+_p(F, T) \sim \log^-_p(F, T) \sim (\log_p(1+T))^{\frac{k_*-1}{2}}$.

Let us recall that K is the completion of K_f at our chosen prime over p, that K_ϵ is the field generated by the values of ϵ over K, and that $\mathcal{O}_\epsilon$ is the ring of integers of K_ϵ. The main result of this paper is the following:

Theorem 2.7. *Let f be a Hilbert cuspidal newform (over F with strict class number one satisfying the Leopoldt conjecture) of weight $k = (k_1, \dots, k_d)$ and character ω whose conductor divides a fixed integral ideal $\mathfrak{a}$ prime to an odd p. Let R_0 be a nonempty subset of $S = \{\mathfrak{p} \in S_p\colon\ \alpha'(\mathfrak{p}) = -\alpha(\mathfrak{p})\}$ such that $(-1)^{\sum_{\mathfrak{p}_i \in R_0} e_i} = -1$. Assume $h = h_\alpha = \frac{k_* - 1}{2}$ (note that $h_\alpha = h_{\alpha'_R} = h_{\alpha'_{R_0 \cup R}}$). Then for any subset $R \subset S$ which is disjoint from R_0, we have*

$$L_p\bigl(f, \alpha'_R, \epsilon, T\bigr) = L_p^+(f, R, R_0, \epsilon, T) \cdot \log_p^+(F, T) + \prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p}) \cdot L_p^-(f, R, R_0, \epsilon, T) \cdot \log_p^-(F, T)$$

where $L_p^{\pm}(f, R, R_0, \epsilon, T) \in \mathcal{O}_\epsilon[\![T]\!] \otimes K_\epsilon$. Let $\widetilde{R}_0$ be another nonempty subset of S satisfying $(-1)^{\sum_{\mathfrak{p}_i \in \widetilde{R}_0} e_i} = -1$ and let $\widetilde{R}$ be any subset of S disjoint from $\widetilde{R}_0$. Then $L_p^{\pm}(f, R, R_0, \epsilon, T) = L_p^{\pm}(f, \widetilde{R}, \widetilde{R}_0, \epsilon, T)$ if and only if $L_p(f, \alpha'_R, \epsilon, T) = L_p(f, \alpha'_{\widetilde{R}}, \epsilon, T)$.

Proof. We can write

$$L_p\bigl(f, \alpha'_R, \epsilon, T\bigr) = G_\epsilon^+(R, R_0, T) + \prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p}) \cdot G_\epsilon^-(R, R_0, T).$$

The interpolation property of Theorem 2.3 forces that

$$G_\epsilon^+\bigl(R, R_0, \bigl(1 + p^e\bigr)^m \zeta_{p^n} - 1\bigr) = 0,$$

for $m_* \leqslant m \leqslant m^*$ and $n \geqslant 1$ such that $e + n$ is odd, and also that

$$G_\epsilon^-\bigl(R, R_0, \bigl(1 + p^e\bigr)^m \zeta_{p^n} - 1\bigr) = 0,$$

for $m_* \leqslant m \leqslant m^*$ and $n \geqslant 1$ such that $e + n$ is even. Since all the zeros of $\log_p^+(F, T)$ (respectively $\log_p^-(F, T)$) are also zeros of $G_\epsilon^+(R, R_0, T)$ (respectively $G_\epsilon^-(R, R_0, T)$), we have (by (4.8) in [10]) that

$$\log_p^+(F, T) \text{ divides } G_\epsilon^+(R, R_0, T) \quad \text{and} \quad \log_p^-(F, T) \text{ divides } G_\epsilon^-(R, R_0, T)$$

in $K_\epsilon[\![T]\!]$. Let

$$L_p^+(f, R, R_0, \epsilon, T) := \frac{G_\epsilon^+(R, R_0, T)}{\log_p^+(F, T)} \quad \text{and} \quad L_p^-(f, R, R_0, \epsilon, T) := \frac{G_\epsilon^-(R, R_0, T)}{\log_p^-(F, T)}.$$

By Theorem 2.3 and the assumption $h = \frac{k_* - 1}{2}$, we get $G_\epsilon^{\pm}(R, R_0, T) \sim \log_p(1 + T)^{\frac{k_* - 1}{2}}$. Lemma 2.6 says that $\log_p^+(F, T) \sim \log_p^-(F, T) \sim (\log_p(1 + T))^{\frac{k_* - 1}{2}}$. Therefore both $L_p^+(f, R, R_0, \epsilon, T)$ and $L_p^-(f, R, R_0, \epsilon, T)$ are $O(1)$ (i.e. bounded). Finally Lemma 5.2 in [13] guarantees that

$$L_p^{\pm}(f, R, R_0, \epsilon, T) \in \mathcal{O}_\epsilon[\![T]\!] \otimes K_\epsilon.$$

The second statement follows easily from the definition of $L_p^{\pm}(f, R, R_0, \epsilon, T)$ by considering its interpolation properties. □

Remark 2.8. 1. The case of elliptic modular form in [13] corresponds to the case $R_0 = \{p\}$ and $R = \emptyset$.

2. Though there are many choices of R_0 and R, there are essentially unique plus/minus p-adic L-functions. More precisely, there are unique plus/minus p-adic L-functions up to ±1, since $L_p(f, \alpha'_R, \epsilon, T) = \pm L_p(f, \alpha'_{\widetilde{R}}, \epsilon, T)$ due to the running assumption $\mathrm{val}_p(\alpha(\mathfrak{p})) \leqslant \mathrm{val}_p(\alpha'(\mathfrak{p}))$.

3. The assumption that F has strict class number one and satisfies the Leopoldt conjecture can be removed without difficulty. But $h_\alpha = \frac{k_*-1}{2}$ is a crucial condition for getting the p-adic boundedness for the plus/minus p-adic L-functions.

2.6. Example: CM theta series

In this section we provide the examples of Hilbert modular forms which have the plus/minus p-adic L-functions. Let K be a totally imaginary quadratic extension of F. Let $\mathbb{A}_K$ be the group of adeles. Let $\theta : \mathbb{A}_K^\times / K^\times \to \mathbb{C}_p^*$ denote a Hecke character whose infinite component is $\theta_\infty(x_1, \ldots, x_d) = \prod_{i=1}^d x_i^{k_i-1} \bar{x}_i^{-k_i+2}$. By the Weil–Jacquet–Langlands theorem (see [8, p. 44]) there exists a cuspidal Hilbert modular form f_θ of weight $(k_1, \ldots, k_d)$ such that

$$L(f_\theta, s) = L(K, \theta, s),$$

where $L(K, \theta, s) = \sum_{\mathfrak{A} \subset K} \frac{\theta(\mathfrak{A})}{N(\mathfrak{A})^s}$ ($\mathfrak{A}$ varies over nonzero integral ideals of K). Moreover, the explicit form of the roots $\alpha(\mathfrak{p}) = \alpha(\mathfrak{p}, f_\theta)$, $\alpha'(\mathfrak{p}) = \alpha(\mathfrak{p}, f_\theta)$ are given by the following: if $\mathfrak{p} \subset F$ remains prime $\mathfrak{P}$ in the CM field K, then $\alpha(\mathfrak{p}) = \theta(\mathfrak{P})^{\frac{1}{2}}$ and $\alpha'(\mathfrak{p}) = -\theta(\mathfrak{P})^{\frac{1}{2}}$. But if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}\widetilde{\mathfrak{P}}$ splits in K, then $\alpha(\mathfrak{p}) = \theta(\mathfrak{P})$ and $\alpha'(\mathfrak{p}) = \theta(\widetilde{\mathfrak{P}})$. Therefore $S := \{\mathfrak{p} \in S_p\colon\ \alpha'(\mathfrak{p}) = -\alpha(\mathfrak{p})\} = \{\mathfrak{p} \in S_p\colon\ \mathfrak{p} \text{ is inert in } K\}$. Let $\mathfrak{c}(f_\theta)$ be the level of f_θ and let ω_{f_θ} be the nebentypus character of f_θ. Note that $\alpha(\mathfrak{p}) \cdot \alpha'(\mathfrak{p}) = \omega_{f_\theta}(\mathfrak{p}) N\mathfrak{p}^{k^*-1}$.

Fix a finite order character $\epsilon \in \mathrm{Hom}_{cts}(T, \mathbb{C}_p^\times)$ whose conductor is $\mathfrak{c}(\epsilon) = \mathfrak{c}(f_\theta) \prod_j \mathfrak{p}_j^{r_j}$, where $r_j \geqslant 0$ for $j = 1, 2, \ldots, \kappa$. Let R_0 be a subset of S such that $(-1)^{\sum_{\mathfrak{p}_i \in R_0} e_i} = -1$. If $h_\alpha := \max_i \{\mathrm{val}_p(\alpha(\mathfrak{p}(\sigma_i))) - \frac{k^*-k_i}{2}\}$, where $J_F = \{\sigma_1, \sigma_2, \ldots, \sigma_d\}$, is equal to $\frac{k_*-1}{2}$, then for any subset $R \subset S$ which is disjoint from R_0 we can construct the plus/minus p-adic L-functions $L_p^{\pm}(f_\theta, R, R_0, \epsilon, T)$. For example, the condition $h_\alpha = \frac{k_*-1}{2}$ is satisfied when $k_1 = \cdots = k_d$, p splits completely in F and $S \neq \emptyset$.

3. Elliptic curves over totally real fields

In [5], Iovita and Pollack attached the plus/minus p-Selmer group to an elliptic curve E/F with certain condition following Kobayashi's work for $E/\mathbb{Q}$. If E/F is modular, then we can define the plus/minus p-adic L-functions to E/F from what we did in the previous sections. Therefore it is natural to formulate the plus/minus Iwasawa main conjecture between these two objects.

3.1. p-Adic L-function of elliptic curves

Let F be a totally real field. Let E be an elliptic curve over F with conductor $\mathfrak{c}$ prime to p. If there is a modularity result, then we can apply our construction to E/F. If E is a semistable elliptic curve over F with some technical condition (for example, see Theorem 7.6 of Skinner and Wiles in [3]), then one can associate a Hilbert newform f_E of parallel weight 2 to E. Recently, Kisin proved more stronger modularity theorems over totally real fields (see [6]) and [1] (and the references therein) is a good place to read for the recent progresses on modularity of elliptic curves over totally real fields (more generally Galois representations of the absolute Galois groups of totally real fields). Now we assume that $S := \{\mathfrak{p} \in S_p\colon\ \alpha'(\mathfrak{p}, f_E) = -\alpha(\mathfrak{p}, f_E)\}$ is not empty for the plus/minus theory of p-adic L-functions and the Selmer groups of E/F. For example, if E/F comes from an elliptic curve $E/\mathbb{Q}$ with supersingular reduction at a prime $p > 3$, then $a_p(E) := 1 + p - \widetilde{E}(\mathbb{F}_p)$ (where $\widetilde{E}$ is the reduction of $E/\mathbb{Q}$ mod p) is 0 and so f_E satisfies that $S \neq \emptyset$. Note that the condition $h_\alpha := \max_i \{\mathrm{val}_p(\alpha(\mathfrak{p}(\sigma_i))) - \frac{k^*-k_i}{2}\} = \frac{k_*-1}{2}$ in Theorem 2.7 translates into $h_\alpha = \frac{1}{2}$.

Proposition 3.1. *The condition $h_\alpha = \frac{1}{2}$ holds if p splits completely in F and $S \neq \emptyset$.*

Proof. Since every prime $\mathfrak{p} \in S$ has residue degree 1, we have $N(\mathfrak{p}) = p$. Then it follows that $h_\alpha := \max_{\mathfrak{p} \in S}\{\mathrm{val}_p(\alpha(\mathfrak{p}))\} = \frac{1}{2}$ from that $\alpha(\mathfrak{p})\alpha'(\mathfrak{p}) = N(\mathfrak{p}) = p$ for every $\mathfrak{p} \in S_p$ and the assumption $\mathrm{val}_p(\alpha(\mathfrak{p})) \leqslant \mathrm{val}_p(\alpha'(\mathfrak{p}))$ by noting that $S \neq \emptyset$. □

By the above proposition we can construct the plus/minus p-adic L-functions of a modular elliptic curve E/F when p splits completely in F. Now we assume this, i.e. $p\mathcal{O}_F = \prod_{i=1}^{d} \mathfrak{p}_i$. We choose a nonzero subset $R_0 \subset S$ such that $\sum_{\mathfrak{p}_i \in R_0} 1 = \#R_0$ is odd and $R \subset S$ disjoint from R_0.

Definition 3.2. We define

$$L_p(E/F, T) := L_p\big(f_E, \alpha'_\emptyset, 1, T\big) \quad \text{and} \quad L_p^\pm(E/F, T) := L_p^\pm(f_E, \emptyset, R_0, 1, T).$$

The interpolation property (2.4) gives

$$L_p\big(f_E, \alpha'_R, 1, \zeta_{p^n} - 1\big) = \frac{c_n}{(-1)^{\sum_{\mathfrak{p}_i \in R} e+n} \prod_j \alpha(\mathfrak{p}_j)^{e+n}}$$

for $n \geqslant 1$. From above we see that

$$L_p\big(f_E, \alpha'_\emptyset, 1, T\big) = \pm L_p\big(f_E, \alpha'_R, 1, T\big) \quad \text{and} \quad L_p^\pm(f_E, \emptyset, R_0, 1, T) = \pm L_p^\pm(f_E, R, R_0, 1, T),$$

where the sign depends on the parity of $\#R$; the sign is 1 if the parity is even, and the sign is -1 if the parity is odd. Therefore $L_p(E/F, T) = \pm L_p(f_E, \alpha'_R, 1, T)$ and it is independent of R up to ± 1. Note that $L_p^\pm(f_E, \emptyset, R_0, 1, T)$ does not depend on R_0 which justifies why we omitted R_0 from the notation $L_p^\pm(E/F, T)$.

Then Theorem 2.7 gives the following corollary:

Corollary 3.3. *Let F be a totally real field with strict class number one satisfying the Leopoldt conjecture, in which p splits completely. Let E be an elliptic curve over F with conductor prime to p. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p} \in S_p$ and let $\mathcal{O}_{F_\mathfrak{p}}$ be its ring of integers. We have*

$$L_p(E/F, T) = L_p^+(E/F, T) \cdot \log_p^+(F, T) + \prod_{\mathfrak{p} \in S_p} \alpha(\mathfrak{p}) \cdot L_p^-(E/F, T) \cdot \log_p^-(F, T)$$

with $L_p^\pm(E/F, T) \in \mathcal{O}_{F_\mathfrak{p}}[\![T]\!] \otimes F_\mathfrak{p}$.

3.2. Plus/minus Selmer groups

In this section we briefly review the definition of the algebraic plus/minus Selmer group following [5] and [7]. Kobayashi defined the plus/minus Selmer groups for elliptic curves over $\mathbb{Q}$ and Iovita and Pollack defined them for elliptic curves over general number fields in which p splits completely. For such a plus/minus theory we will need to assume $S := \{\mathfrak{p} \in S_p\colon \alpha'(\mathfrak{p}, f_E) = -\alpha(\mathfrak{p}, f_E)\} = S_p$. Let $F_{cyc} \subset F_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of F and F_n, for $n \geqslant 0$, be the unique subextension of F_{cyc} such that $\mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$. We assume that p splits completely in F, say $S_p = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d\}$, and that each $\mathfrak{p}_i$ is totally ramified in F_{cyc} which is the key condition in [5] in order to study the plus/minus Selmer groups. Recall that we fixed an isomorphism $\Lambda := \mathbb{Z}_p[\![\mathrm{Gal}(F_{cyc}/F)]\!] \simeq \mathbb{Z}_p[\![T]\!]$.

Let $v = v_i$ and $v(n) = v_i(n)$ be the unique primes of F_{cyc} and F_n respectively over the prime $\mathfrak{p} = \mathfrak{p}_i$ of F $(i = 1, \ldots, d)$ such that $v | v(n+1) | v(n)$ for all $n \geqslant 0$. Let $F_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of F, and let $F_{n,v}$ be the $v(n)$-adic completion of F_n. Denote by $F_{cyc,v}$ the union of all $F_{n,v}$ (for $n \geqslant 0$). We have local Kummer maps

$$\kappa_v : E(F_{cyc,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1\big(F_{cyc,v}, E\big[p^\infty\big]\big),$$

where $E[p^\infty] = E[p^\infty](\bar{F}_{\mathfrak{p}})$. The p-primary Selmer group of E over F_{cyc} is defined by

$$Sel_p(E/F_{cyc}) := \ker\left(H^1\big(F_{cyc}, E\big[p^\infty\big]\big) \to \prod_w \frac{H^1(F_{cyc,w}, E[p^\infty])}{\kappa_w(E(F_{cyc,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)}\right)$$

where w varies over all prime ideals of F_{cyc}. One can define $Sel_p(E/F_n)$ in the same manner and clearly we have $Sel_p(E/F_{cyc}) = \lim_{n\to\infty} Sel_p(E/F_n)$.

Since Λ naturally acts on $H^1(F_{cyc}, E[p^\infty])$ and the Λ-action preserves $Sel_p(E/F_{cyc})$, it follows that $Sel_p(E/F_{cyc})$ is a Λ-module. Then $Sel_p(E/F_{cyc})$ is known to be co-finitely generated over Λ for any prime p, with no restriction on the reduction type of E. The theorem of Kato and Rohrlich says that $Sel_p(E/F_{cyc})$ is a co-torsion Λ-module if E is defined over $\mathbb{Q}$, E has good, ordinary reduction or multiplicative reduction at p and $F/\mathbb{Q}$ is abelian. It is conjectured that $Sel_p(E/F_{cyc})$ is co-torsion over Λ if E has good, ordinary reduction at every $\mathfrak{p} \in S_p$. But if there is a prime $\mathfrak{p} \in S_p$ which is supersingular prime for E, then $Sel_p(E/F_{cyc})$ is not any more co-torsion over Λ. In this case, it is not clear how to define the characteristic ideal for $Sel_p(E/F_{cyc})$. Kobayashi and Iovita–Pollack's work gives a recipe to naturally define two Selmer groups, called *the plus/minus Selmer groups*, which are co-finitely generated co-torsion over Λ, if $S = S_p$ and a certain condition holds (which always holds conjecturally, see Conjecture 3.6). When $F = \mathbb{Q}$ this certain condition is true and so the plus/minus Selmer groups are Λ-co-torsion.

We define the plus/minus subgroups

$$E^+(F_{cyc,v_i}) := \lim_{n\to\infty}\big\{x \in E(F_{n,v_i})\colon \mathrm{Tr}_{n/m}(x) \in E(F_{m-1,v}) \text{ for } 0 < m \leqslant n,\ m\text{: odd}\big\},$$

$$E^-(F_{cyc,v_i}) := \lim_{n\to\infty}\big\{x \in E(F_{n,v_i})\colon \mathrm{Tr}_{n/m}(x) \in E(F_{m-1,v}) \text{ for } 0 < m \leqslant n,\ m\text{: even}\big\},$$

for $i = 1, \dots, d$

Definition 3.4 *(Kobayashi and Iovita–Pollack).* We assume that $S = S_p$, i.e. $a_{\mathfrak{p}} = 0$ for each prime $\mathfrak{p}|p$. Then we define

$$Sel_p^{\pm}(E/F_{cyc}) := \ker\left(Sel(E/F_{cyc}) \to \prod_{i=1}^{d} \frac{H^1(F_{cyc,v_i}, E[p^\infty])}{\kappa_{v_i}(E^{\pm}(F_{cyc,v_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)}\right).$$

The following theorem of Iovita and Pollack (Corollary 7.7 in [5]) gives a criterion when $Sel_p^{\pm}(E/F_{cyc})$ is co-torsion over Λ.

Theorem 3.5 *(Iovita–Pollack). The plus/minus Selmer groups $Sel_p^+(E/F_{cyc})$ and $Sel_p^-(E/F_{cyc})$ are co-torsion Λ-modules if and only if the $\mathbb{Z}_p$-corank of $Sel_p(E/F_n)$ is bounded as $n \to \infty$.*

The above theorem is also valid for arbitrary $\mathbb{Z}_p$-extensions of F (not necessarily for the cyclotomic $\mathbb{Z}_p$-extension).

Conjecture 3.6. *The $\mathbb{Z}_p$-corank of $Sel_p(E/F_n)$ is bounded as $n \to \infty$.*

See Conjecture 1.8 of [4] for more details regarding this conjecture. Therefore conjecturally we have

$$\mathrm{Hom}_{cts}\big(Sel_p^{\pm}(E/F_{cyc}), \mathbb{Q}_p/\mathbb{Z}_p\big) \text{ is pseudo-isomorphic to } \Lambda/\big(\mathbf{f}_E^{\pm}\big).$$

for some $\mathbf{f}_E^{\pm} \in \Lambda$. We define the algebraic plus/minus p-adic L-functions:

$$L_p^{\pm,alg}(E/F,T) = \mathbf{f}_E^{\pm},$$

which are well defined up to units in Λ. Now we state the plus/minus Iwasawa main conjecture for E/F.

Conjecture 3.7 *(Plus/minus Iwasawa main conjecture). Let F be a totally real field with strictly class number one in which p splits completely. Let E/F be a modular elliptic curve defined over F whose conductor is prime to p. Assume that $S = S_p$ and the $\mathbb{Z}_p$-corank of $Sel_p(E/F_n)$ is bounded. Then*

$$\big(L_p^{\pm,alg}(E/F,T)\big) = \big(L_p^{\pm}(E/F,T)\big)$$

as ideals in $\mathcal{O}_{F_\mathfrak{p}}[\![T]\!] \otimes F_\mathfrak{p}$.

When $F = \mathbb{Q}$, then one divisibility of this conjecture, namely $L_p^{\pm,alg}(E/F,T)$ divides $L_p^{\pm}(E/F,T)$, was proven by Kobayashi in [7] using Kato's Euler system. The other divisibility is not known. If $F \neq \mathbb{Q}$, then neither divisibility of this conjecture is known. If $F = \mathbb{Q}$ and $E/\mathbb{Q}$ has complex multiplication, then the above conjecture was proven in [14].

3.3. Elliptic curves with complex multiplication

In Section 2.6, we explained how to construct the plus/minus p-adic L-functions for the CM theta series. Here we give more details in the special case of CM elliptic curves over F. If E/F has CM, one knows how to construct explicitly a Hilbert modular newform of parallel weight 2. Let E be an elliptic curve over F with complex multiplication by the maximal order of an imaginary quadratic field K_0, i.e. $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}_{K_0}$. We consider the composite field K of K_0 and F, which is a CM field, i.e. a totally imaginary quadratic extension of F. We assume that the conductor $\mathrm{Cond}(E/F)$ is prime to $p\mathcal{O}_F$, so that E/F has good reduction at every prime of F above p. We also keep all the assumptions about F we made so far (e.g. $d = [F:\mathbb{Q}]$, $p\mathcal{O}_F = \prod_{i=1}^d \mathfrak{p}_i$, F has strict class number one, and the Leopoldt conjecture holds for F).

By the main theorem of complex multiplication (cf. Theorem 10.5(b), Chapter II of [12]), there is an algebraic Hecke character $\Psi = \Psi_{E_K} : \mathbb{A}_K^\times/K^\times \to K_0^\times$ of K such that

$$L(E/F,s) = L(K,\Psi,s). \tag{3.1}$$

Then the infinite part of Ψ satisfies $\Psi_\infty(x_1,\ldots,x_d) = \prod_{j=1}^d x_j$. By the Weil–Jacquet–Langlands theorem there exists a CM Hilbert newform f_Ψ of parallel weight 2 such that

$$L(K,\Psi,s) = L(f_\Psi,s). \tag{3.2}$$

Now suppose $\mathfrak{p}|p$ is a prime of F. If $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}\widetilde{\mathfrak{P}}$ splits in K, then $\alpha(\mathfrak{p}, f_\Psi) = \Psi(\mathfrak{P})$ and $\alpha'(\mathfrak{p}, f_\Psi) = \Psi(\widetilde{\mathfrak{P}})$, assuming $\mathrm{val}_p(\Psi(\mathfrak{P})) \leqslant \mathrm{val}_p(\Psi(\widetilde{\mathfrak{P}}))$. And if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}$ is inert in K, then $\alpha(\mathfrak{p}, f_\Psi) = \Psi(\mathfrak{P})^{\frac{1}{2}}$ and $\alpha'(\mathfrak{p}, f_\Psi) = -\Psi(\mathfrak{P})^{\frac{1}{2}}$. In fact, local Euler factor at $\mathfrak{p}$ of the L-series of E/F is given by the following (Exercise 2.32, Chapter II of [12]):

$$L_{\mathfrak{p}}(E/F,T)=\begin{cases}(1-\Psi(\mathfrak{P})T)(1-\Psi(\widetilde{\mathfrak{P}})T) & \text{if } \mathfrak{p}\mathcal{O}_K=\mathfrak{P}\widetilde{\mathfrak{P}},\\ 1-\Psi(\mathfrak{P})T & \text{if } \mathfrak{p}\mathcal{O}_K=\mathfrak{P},\\ 1 & \text{if } \mathfrak{p}\mathcal{O}_K=\mathfrak{P}^2.\end{cases}$$

As we saw in Section 2.6 on the CM theta series, $S=\{\mathfrak{p}\subset\mathcal{O}_F\colon\ \mathfrak{p}$ divides p and is inert in $K\}$. If $S\neq\emptyset$, p splits completely in F (which implies $p\nmid D_F$), and there exists $R_0\subset S$ such that the cardinality of R_0 is odd, then we can define $L_p(E/F,T)$ and $L_p^{\pm}(E/F,T)$ as in Definition 3.2. Depending on the factorization of the rational prime p in the field K_0, we have two possibilities: Either p splits or it is inert in K_0 (note that the condition $\mathfrak{c}=\mathrm{Cond}(E/F)$ being prime to $p\mathcal{O}_F$ rules out the ramified case). If p splits in K_0, then all the primes $\mathfrak{p}_i|p$ of F should split in K, i.e. for $i=1,\dots,d$, one has $\mathfrak{p}_i\mathcal{O}_K=\mathfrak{P}_i\widetilde{\mathfrak{P}_i}$ where $\mathfrak{P}_i,\widetilde{\mathfrak{P}_i}$ are two distinct prime ideals of K above $\mathfrak{p}_i$. If p is inert in K_0, then all the primes $\mathfrak{p}_i|p$ of F should be inert K, i.e. for $i=1,\dots,d$, one has $\mathfrak{p}_i\mathcal{O}_K=\mathfrak{P}_i$ where $\mathfrak{P}_i$ is a prime of K.

If we let $a_{\mathfrak{p}}=N_{F/Q}(\mathfrak{p})+1-\#\widetilde{E}(\mathbb{F}_{\mathfrak{p}})$ where $\mathbb{F}_{\mathfrak{p}}$ is the residue field of F at $\mathfrak{p}$ and $\widetilde{E}$ is the reduction of E modulo $\mathfrak{p}$ (we are assuming that $\mathfrak{p}$ is a good prime for E/F), then $\alpha(\mathfrak{p})+\alpha'(\mathfrak{p})=a_{\mathfrak{p}}$. One can show that the former case (split case) corresponds to the *p-ordinary* situation in the sense that $\widetilde{E}$ for each $\mathfrak{p}|p$ is ordinary and the latter one (inert case) matches with the *most p-supersingular* situation in the sense that $\widetilde{E}$ for each $\mathfrak{p}|p$ is supersingular and $a_{\mathfrak{p}}=0$ (see the Exercises 2.30 and 2.31, [12] for details).

If we are in the p-ordinary situation, then a theorem of Manin [8] (see also Dabrowski [2] whose result was quoted above) says that the p-adic L-function $L_p(f_\Psi,\alpha,\epsilon,T)$ is already p-adically bounded, where $\alpha=\{\alpha(\mathfrak{p}_i)\mid i=1,\dots,d\}$ (see (1) and (3) of Theorem 2.3 for its existence and p-adic boundedness respectively). Therefore our main interest in this paper is to construct, using the results of the preceding sections, plus/minus p-adic L-functions for E/F at the most p-supersingular case which are p-adically bounded. For that matter we assume that *p is inert in* K_0. Then $h_\alpha=\frac{1}{2}$ by Proposition 3.1 and hence the plus/minus p-adic L-functions $L_p^{\pm}(E/F,T)$ exist.

Acknowledgments

Both authors are very grateful to CRM-ISM and CICMA at Montreal for their support during the preparation of the manuscript.

References

[1] K. Buzzard, Potential modularity — a survey, arXiv:1101.0097v1 [math.NT].

[2] A. Dabrowski, p-Adic L-functions of Hilbert modular forms, Ann. Inst. Fourier (Grenoble) 44 (4) (1994) 1025–1041.

[3] H. Darmon, Rational Points on Modular Elliptic Curves, CBMS Reg. Conf. Ser. Math., vol. 101, Amer. Math. Soc., Providence, RI, 2004, xii+129 pp., published for the Conference Board of the Mathematical Sciences, Washington, DC.

[4] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, in: Arithmetic Algebraic Geometry, Park City, UT, 1999, in: IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464.

[5] A. Iovita, R. Pollack, Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields, J. Reine Angew. Math. 598 (2006) 71–103.

[6] M. Kisin, Modularity for Some Geometric Galois Representations, L-functions and Galois Representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, with an appendix by Ofer Gabber, pp. 438–470.

[7] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (1) (2003) 1–36.

[8] Ju.I. Manin, Non-Archimedean integration and p-adic Jacquet–Langlands L-functions, Uspekhi Mat. Nauk 31 (1) (1976) 5–54 (in Russian).

[9] B. Mazur, P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. Math. 25 (1974) 1–61.

[10] M. Lazard, Les zéros des fonctions analytiques d'une variable sur un corps valué complet, Inst. Hautes Études Sci. Publ. Math. 14 (1962) 47–75 (in French).

[11] G. Shimura, The special values of zeta functions associated with Hilbert modular forms, Duke Math. J. 45 (1978) 637–679.

[12] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 151, Springer-Verlag, New York, 1994, xiv+525 pp.

[13] R. Pollack, On the p-adic L-functions of a modular form at a supersingular prime, Duke Math. J. 118 (3) (2003) 523–558.

[14] R. Pollack, K. Rubin, The main conjecture for CM elliptic curves at supersingular primes, Ann. of Math. (2) 159 (1) (2004) 447–464.

[15] M.M. Višik, Non-Archimedean measures connected with Dirichlet series, Math. USSR Sbornik 28 (2) (1976).

[16] L. Washington, Introduction to Cyclotomic Fields, 2nd edition, Grad. Texts in Math., vol. 83, Springer, 1997.

[17] H. Yoshida, On the zeta functions of Shimura varieties and periods of Hilbert modular forms, Duke Math. J. 75 (1) (1994) 121–191.