Glasgow Math. J. **54** (2012) 241–259. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000553.

IWASAWA THEORY FOR THE SYMMETRIC SQUARE OF A CM MODULAR FORM AT INERT PRIMES

ANTONIO LEI

School of Mathematical Sciences, Monash University, Clayton, VIC 3800, Australia
e-mail: antonio.lei@monash.edu

(Received 3 February 2011; accepted 15 August 2011; first published online 12 December 2011)

Abstract. Let f be a modular form with complex multiplication (CM) and p an odd prime that is inert in the CM field. We construct two p-adic L-functions for the symmetric square of f, one of which has the same interpolating properties as the one constructed by Delbourgo and Dabrowski (A. Dabrowski and D. Delbourgo, S-adic L-functions attached to the symmetric square of a newform, *Proc. Lond. Math. Soc.* 74(3) (1997), 559–611), whereas the other one has a similar interpolating properties but corresponds to a different eigenvalue of the Frobenius. The symmetry between these two p-adic L-functions allows us to define the plus and minus p-adic L-functions à la Pollack (R. Pollack, on the p-adic L-function of a modular form at a supersingular prime, Duke Math. J. 118(3) (2003), 523–558). We also define the plus and minus p-Selmer groups analogous to the ones defined by Kobayashi (S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152(1) (2003), 1–36). We explain how to relate these two sets of objects via a main conjecture.

2000 *Mathematics Subject Classification.* 11R23, 11F80.

1. Introduction. Let f be a normalised eigen-newform of weight k, level N and character ϵ. Fix a prime $p \neq 2$ such that $p \nmid N$. In **[3]** (also in **[1]** under some additional conditions), even distributions on $\mathbb{Z}_p^\times$ are constructed to interpolate the L-values of the symmetric square of f. More precisely, if the Euler factor of $L(f, s)$ at p is given by $(1 - \alpha_1(p)p^{-s})(1 - \alpha_2(p)p^{-s})$, then there exists an admissible distribution $\mu_{\alpha_i(p)^2}$ for $i = 1, 2$ such that

$$\int_{\mathbb{Z}_p^\times} \theta \, d\mu_{\alpha_i(p)^2} = \frac{p^{3n(k-1)}}{\alpha_i(p)^{2n}\tau(\theta^{-1})} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(\text{period})} \tag{1}$$

for any non-trivial even Dirichlet character θ of conductor p^n, where $\tau(\theta^{-1})$ denotes the Gauss sum of θ^{-1}.

Since the Euler factor of $L(\mathrm{Sym}^2 f, s)$ at p is $(1 - \alpha_1(p)^2p^{-s})(1 - \alpha_2(p)^2p^{-s})(1 - \epsilon(p)p^{k-1-s})$, we expect that there should be a distribution $\mu_{\epsilon(p)p^{k-1}}$ satisfying interpolating properties similar to (1), but with $\alpha_i(p)^2$ replaced by $\epsilon(p)p^{k-1}$. In this paper, we construct such a distribution for the case when f is a modular form with complex multiplication (CM) that is non-ordinary at p. In other words, when the L-function of f coincides with that of a Grossencharacter ϕ defined over K and p inerts in K. More precisely, we prove the following theorem in Section 3 (Theorem 3.20).

The author is supported by an ARC DP1092496 grant.

THEOREM 1.1. *If f is as above, then there exist even admissible distributions $\mu_{\pm\epsilon(p)p^{k-1}}$ such that*

$$\int_{\mathbb{Z}_p^\times} \theta d\mu_{\pm\epsilon(p)p^{k-1}} = \frac{p^{3n(k-1)}}{(\pm\epsilon(p)p^{k-1})^n\tau(\theta^{-1})} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(\text{period})}.$$

Note that we have $\alpha_1(p)^2 = \alpha_2(p)^2 = -\epsilon(p)p^{k-1}$ in this case, methods in [**3**] only produce one distribution, which agrees with $\mu_{-\epsilon(p)p^{k-1}}$ as given by Theorem 1.1.

The idea of the construction is rather simple. Let V_f be the p-adic representation of $G_{\mathbb{Q}}$ associated to f as constructed by Deligne in [**4**]. In order to prove Theorem 1.1, we make use of the following observation. As $G_{\mathbb{Q}}$-representations, we have

$$\mathrm{Sym}^2(V_f) \cong V_1 \oplus V_2,$$

where V_1 is an one-dimensional representation associated to some Dirichlet character η twisted by a power of the cyclotomic character and V_2 is a two-dimensional representation associated to the Grossencharacter ϕ^2. This implies that the L-function of f factorises into

$$L(\mathrm{Sym}^2 f, s) = L(\phi^2, s)L(\eta, s-k+1).$$

We can therefore make use of the Euler system constructed from elliptic units to interpolate the L-values of ϕ^2 and multiply the resulting distributions with an appropriate twist of the Kubota–Leopoldt p-adic L-function associated to η, which interpolates the L-values of η.

Because of the symmetry between the two distributions, we show that some plus and minus logarithms $\log^\pm$ of the Pollack divide $\mu_{+\epsilon(p)p^{k-1}} \pm \mu_{-\epsilon(p)p^{k-1}}$. This allows us to obtain two bounded measures:

THEOREM 1.2. (Theorem 3.25). *Let θ be an even Dirichlet character of conductor p^n. There exist bounded p-adic measures $\mu^\pm(\mathrm{Sym}^2(V_f))$ such that the followings hold.*
(a) *If n is even, then*

$$\int_{\mathbb{Z}_p^\times} \theta \mu^+(\mathrm{Sym}^2(V_f)) = \frac{(2k-3)!(k-1)!p^{2n(k-1)}}{\theta(\log^+)\tau(\theta^{-1})^2\epsilon(p)^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(\text{period})}.$$

(b) *If n is odd, then*

$$\int_{\mathbb{Z}_p^\times} \theta \mu^-(\mathrm{Sym}^2(V_f)) = \frac{(2k-3)!(k-1)!p^{2n(k-1)}}{\theta(\log^-)\tau(\theta^{-1})^2\epsilon(p)^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(\text{period})}.$$

Moreover, $\mu^\pm(\mathrm{Sym}^2(V_f))$ are uniquely determined by (a) *and* (b)*, respectively.*

In Section 4, we make use of some of the ideas in [**6**] to show that these measures can be obtained from some appropriate Coleman maps and define the corresponding plus and minus p-Selmer groups $\mathrm{Sel}_p^\pm(\mathrm{Sym}^2(V_f))$. On identifying the measures as elements in some Iwasawa algebra $\Lambda \otimes \mathbb{Q}$, we show that the following holds under some appropriate conditions (see Theorem 4.8 for a precise statement).

THEOREM 1.3. *The Selmer groups $\mathrm{Sel}_p^\pm(\mathrm{Sym}^2(V_f))$ are Λ-cotorsion and*

$$\mathrm{Char}_{\Lambda\otimes\mathbb{Q}}\big(\mathrm{Sel}_p^\pm(\mathrm{Sym}^2(V_f))^\vee\big) = (\mu^\pm(\mathrm{Sym}^2(V_f))).$$

Finally, in the Appendix, we explain how some of the linear algebra results that we use to prove the main theorems can be easily generalised to general symmetric powers $\mathrm{Sym}^m f$ where $m \geq 2$ is an integer.

2. Notation.

2.1. Extensions by p power roots of unity. 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, χ the p-cyclotomic character on G_K and $\mathcal{O}_K$ the ring of integers of K. We write ι for the complex conjugation in $G_{\mathbb{Q}}$.

For an integer $n \geq 0$, we write K_n for the extension $K(\mu_{p^n})$, where μ_{p^n} is the set of p^nth roots of unity and K_∞ denotes $\bigcup_{n\geq 1} K_n$. When $K = \mathbb{Q}$, we write $k_n = \mathbb{Q}(\mu_{p^n})$ instead. In particular, we write $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$. Let G_n denotes the Galois group $\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$ for $0 \leq n \leq \infty$. Then, $G_\infty \cong \Delta \times \Gamma$, where $\Delta = G_1$ is a finite group of order $p-1$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_{p,1}) \cong \mathbb{Z}_p$. We fix a topological generator γ of Γ.

2.2. Iwasawa algebras and power series. Given a finite extension K of $\mathbb{Q}_p$, $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_{\mathcal{O}_K}(\Gamma)$) denotes the Iwasawa algebra of G_∞ (respectively Γ) over $\mathcal{O}_K$. We write $\Lambda_K(G_\infty) = \Lambda_{\mathcal{O}_K}(G_\infty) \otimes K$ and $\Lambda_K(\Gamma) = \Lambda_{\mathcal{O}_K}(\Gamma) \otimes K$. If M is a finitely generated $\Lambda_{\mathcal{O}_K}(\Gamma)$-torsion (respectively $\Lambda_K(\Gamma)$-torsion) module, we write $\mathrm{Char}_{\Lambda_{\mathcal{O}_K}(\Gamma)}(M)$ (respectively $\mathrm{Char}_{\Lambda_K(\Gamma)}(M)$) for its characteristic ideal.

Given a module M over $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_K(G_\infty)$) and a character $\delta : \Delta \to \mathbb{Z}_p^\times$, M^δ denotes the δ-isotypical component of M. For any $m \in M$, we write m^δ for the projection of m into M^δ. The Pontryagin dual of M is written as $M^\vee$.

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

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

where $|\cdot|_p$ is the p-adic norm on $\mathbb{C}_p$ such that $|p|_p = p^{-1}$. We write $\mathcal{H}_\infty = \cup_{r\geq 0}\mathcal{H}_r$ and $\mathcal{H}_r(G_\infty) = \{f(\gamma - 1) : f \in \mathcal{H}_r\}$ for $r \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. In other words, the elements of $\mathcal{H}_r$ (respectively $\mathcal{H}_r(G_\infty)$) are the power series in X (respectively $\gamma - 1$) over $\mathbb{C}_p[\Delta]$ with growth rate $O(\log_p^r)$. If $F, G \in \mathcal{H}_\infty$ or $\mathcal{H}_\infty(G_\infty)$ are such that $F = O(G)$ and $G = O(F)$, we write $F \sim G$.

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

Let $n \in \mathbb{Z}$. We define the K-linear map Tw_n from $\mathcal{H}_{r,K}(G_\infty)$ to itself to be the map that sends σ to $\chi(\sigma)^n\sigma$ for all $\sigma \in G_\infty$. It is clearly bijective (with inverse Tw_{-n}).

2.3. Crystalline representations. We write $\mathbb{B}_{\mathrm{cris}}$ and $\mathbb{B}_{\mathrm{dR}}$ for the rings of Fontaine and φ for the Frobenius acting on these rings. Recall that there exists an element $t \in \mathbb{B}_{\mathrm{dR}}$ such that $\varphi(t) = pt$ and $g \cdot t = \chi(g)t$ for $g \in G_{\mathbb{Q}_p}$.

Let V be a p-adic representation of $G_{\mathbb{Q}_p}$. We denote the Dieudonné module by $\mathbb{D}_{\mathrm{cris}}(V) = (\mathbb{B}_{\mathrm{cris}} \otimes V)^{G_{\mathbb{Q}_p}}$. We say that V is crystalline if V has the same $\mathbb{Q}_p$-dimension as $\mathbb{D}_{\text{cris}}(V)$. Fix such a V. If $j \in \mathbb{Z}$, $\text{Fil}^j\mathbb{D}_{\text{cris}}(V)$ denotes the jth de Rham filtration of $\mathbb{D}_{\text{cris}}(V)$.

Let T be a lattice of V, which is stable under $G_{\mathbb{Q}_p}$. Let $\mathbb{H}^1_{\text{Iw}}(T)$ denote the inverse limit $\varprojlim H^1(\mathbb{Q}_{p,n}, T)$ with respect to the corestriction and $\mathbb{H}^1_{\text{Iw}}(V) = \mathbb{Q} \otimes \mathbb{H}^1_{\text{Iw}}(T)$. Moreover, if V arises from the restriction of a p-adic representation of $G_{\mathbb{Q}}$ and T is a lattice stable under $G_{\mathbb{Q}}$, we write

$$\mathbb{H}^1(T) = \varprojlim_n H^1(\mathbb{Z}[\mu_{p^n}, 1/p], T) \quad \text{and} \quad \mathbb{H}^1(V) = \mathbb{Q} \otimes \mathbb{H}^1(T).$$

We have localisation maps

$$\text{loc} : \mathbb{H}^1(T) \to \mathbb{H}^1_{\text{Iw}}(T) \quad \text{and} \quad \text{loc} : \mathbb{H}^1(V) \to \mathbb{H}^1_{\text{Iw}}(V).$$

If F is a number field, we define the p-Selmer group of T over F to be

$$\text{Sel}_p(T/F) = \ker\left(H^1(F, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_v \frac{H^1(F_v, T \otimes \mathbb{Q}_p/\mathbb{Z}_p)}{H^1_f(F_v, T \otimes \mathbb{Q}_p/\mathbb{Z}_p)}\right),$$

where v runs through the places of F.

Let $V(j)$ denote the jth Tate twist of V, i.e. $V(j) = V \otimes \mathbb{Q}_p e_j$ where $G_{\mathbb{Q}_p}$ acts on e_j via χ^j. We have

$$\mathbb{D}_{\text{cris}}(V(j)) = t^{-j}\mathbb{D}_{\text{cris}}(V) \otimes e_j.$$

For any $v \in \mathbb{D}_{\text{cris}}(V)$, $v_j = v \otimes t^{-j}e_j$ denotes its image in $\mathbb{D}_{\text{cris}}(V(j))$. We write $\text{Tw}_j : \mathbb{H}^1_{\text{Iw}}(V) \to \mathbb{H}^1_{\text{Iw}}(V(j))$ for the isomorphism defined in Section A.4 in **[9]**, which depends on a choice of primitive p-power roots of unity.

Finally, we write

$$\exp : \mathbb{Q}_{p,n} \otimes \mathbb{D}_{\text{cris}}(V) \to H^1(\mathbb{Q}_{p,n}, V) \quad \text{and} \quad \exp^* : H^1(\mathbb{Q}_{p,n}, V) \to \mathbb{Q}_{p,n} \otimes \text{Fil}^0\mathbb{D}_{\text{cris}}(V)$$

for Bloch–Kato's exponential and dual exponential, respectively.

2.4. Imaginary quadratic fields. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and idele class group C_K. We write ε_K for the quadratic character associated to K, i.e. the character on $G_{\mathbb{Q}}$, which sends σ to 1 if $\sigma \in G_K$ and to -1 otherwise.

A Grossencharacter of K is simply a continuous homomorphism $\phi : C_K \to \mathbb{C}^\times$ with 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. Let $\mathfrak{f}$ be the conductor of ϕ. We say that η is of type (m, n) where $m, n \in \mathbb{Z}$ if the restriction of η to the Archimedean part $\mathbb{C}^\times$ of C_K is of the form $z \mapsto z^m\bar{z}^n$.

We write $\mathcal{K} = \cup K(p^n\mathfrak{f})$, where $K(\mathfrak{a})$ denotes the ray class field of K modulo $\mathfrak{a}$ if $\mathfrak{a}$ is an ideal of $\mathcal{O}$.

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

If T is a $\mathbb{Z}_p$-representation of G_K, we write

$$\mathbb{H}^1_{p^\infty \mathfrak{f}}(T) = \varprojlim_{K'} H^1(\mathcal{O}_{K'}[1/p], T) \quad \text{and} \quad \mathbb{H}^1_{p^\infty \mathfrak{f}}(\mathbb{Q} \otimes_{\mathbb{Z}} T) = \mathbb{H}^1_{p^\infty \mathfrak{f}}(T) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where K' ranges over all finite extensions of K contained in $K(p^\infty \mathfrak{f})$.

2.5. Modular forms. Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geq 2$, level N and character ϵ. We assume that f is a CM modular form, i.e. $L(f, s) = L(\phi, s)$ for some Grossencharacter ϕ of an imaginary quadratic field K with conductor $\mathfrak{f}$. Then, ϕ is of type $(-k+1, 0)$. Moreover, p inerts in K if and only if f is non-ordinary at p. In this case, a_p is always 0. Throughout, we fix such a p with $p \neq 2$.

The coefficient field F_f of f is contained in the field of definition of ϕ. We write E for the completion of this field at a fixed prime above p.

We write V_f for the two-dimensional E-linear representation of $G_{\mathbb{Q}}$ associated to f from **[4]**, so we have a homomorphism

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}(V_f).$$

Throughout the paper, we assume that the following hypothesis holds.

HYPOTHESIS 2.1. *If ϵ and K are as above, then $\varepsilon_K \neq \epsilon$.*

3. p-adic L-functions.

3.1. Grossencharacters over K. We first review some results on Grossencharacters. Let η be a Grossencharacter on G_K of conductor $\mathfrak{f}$. We fix a finite extension E of $\mathbb{Q}_p$ such that E contains the image of η. We write $V(\eta)$ for the one-dimensional E-linear representation of G_K associated to η. It is a representation that factors through $\mathrm{Gal}(\mathcal{K}/K)$. For an ideal $\mathfrak{a}$ of $\mathcal{O}$, which is prime to $p\mathfrak{f}$, the Artin symbol $(\mathfrak{a}, \mathcal{K}/K) \in \mathrm{Gal}(\mathcal{K}/K)$ acts on $V(\eta)$ as the multiplication by $\eta(\mathfrak{a})^{-1}$. We write $\tilde{\eta} : G_K \to E^\times$ for the corresponding character.

We write $\tilde{V}_\eta = \mathrm{Ind}_K^{\mathbb{Q}}(V(\eta))$. The canonical homomorphism $K \otimes \mathbb{Q}(\zeta_{p^\infty}) \to K(p^\infty \mathfrak{f})$ induces a map

$$\mathrm{Ind} : \mathbb{H}^1_{p^\infty \mathfrak{f}}(V(\eta)) \to \mathbb{H}^1(\tilde{V}_\eta).$$

Let γ be a non-zero element of $V(\eta)$. By Section 15.5 in **[5]**, a system of norm compatible elliptic units in $K(p^n \mathfrak{f})$ defines an element $z_{p^\infty \mathfrak{f}} \in \mathbb{H}^1_{p^\infty \mathfrak{f}}(\mathbb{Z}_p(1))$. We write the image of $z_{p^\infty \mathfrak{f}}$ under the composition

$$\mathbb{H}^1_{p^\infty \mathfrak{f}}(\mathbb{Z}_p(1)) \xrightarrow{\gamma} \mathbb{H}^1_{p^\infty \mathfrak{f}}(V(\eta)(1)) \xrightarrow{\mathrm{Ind}} \mathbb{H}^1(\tilde{V}_\eta(1)) \xrightarrow{\mathrm{loc}} \mathbb{H}^1_{\mathrm{Iw}}(\tilde{V}_\eta(1)) \xrightarrow{\mathrm{Tw}_{-1}} \mathbb{H}^1_{\mathrm{Iw}}(\tilde{V}_\eta)$$

as $z_\gamma(\eta) = z(\eta)$ and its projection into $H^1(\mathbb{Q}_{p,n}, \tilde{V}_\eta(j))$ is denoted by $z_{j,n}(\eta)$.

Note that the eigenvalues of ι on $\tilde{V}_\eta$ are ± 1, each with multiplicity 1. If $v \in \tilde{V}_\eta$, we write $v^\pm$ for the projection of v into the ± 1 eigenspace.

Proposition 3.1. *Let η be a Grossencharacter over K of type $(-r, 0)$ with $r \geq 1$. Let θ be a character on G_n and write*

$$\kappa_\theta : \mathbb{Q}_{p,n} \otimes \mathrm{Fil}^0\mathbb{D}_{\mathrm{cris}}(\tilde{V}_\eta(1)) \to \mathbb{C} \otimes \tilde{V}_\eta(1),$$
$$x \otimes y \mapsto \sum_{\sigma \in G_n} \theta(\sigma)\sigma(x)\mathrm{per}(y),$$

where per *is the period map associated to η as defined in* Section 15.8 in [**5**]. *Then, we have*

$$\kappa_\theta \circ \exp^*(z_{1,n}(\eta)) = L_{\{p\}}(\bar{\eta}\theta, r) \cdot (\gamma')^{\pm},$$

where $\pm = \theta(-1)$ and γ' denotes the image of γ in $\tilde{V}_\eta$.

Proof. Section 15.12 in [**5**]. □

3.2. The symmetric square of a CM modular form. Let f be a modular form as in Section 2.5. By comparing the eigenvalues of Frobenii, we see that the representation V_f is isomorphic to $\tilde{V}_\phi = \mathrm{Ind}_K^{\mathbb{Q}} V(\phi)$. Therefore, V_f admits a basis x, y such that for $\sigma \in G_{\mathbb{Q}}$, the matrix of $\rho_f(\sigma)$ with respect to this basis is given by

$$\rho_f(\sigma) = \begin{pmatrix} \tilde{\phi}(\sigma) & 0 \\ 0 & \tilde{\phi}(\iota\sigma\iota) \end{pmatrix} \tag{2}$$

if $\sigma \in G_K$. Otherwise,

$$\rho_f(\sigma) = \begin{pmatrix} 0 & \tilde{\phi}(\iota\sigma'\iota) \\ \tilde{\phi}(\sigma') & 0 \end{pmatrix}, \tag{3}$$

where $\sigma = \iota\sigma'$ with $\sigma' \in G_K$.

Lemma 3.2. *The determinant of ρ_f is given by*

$$\det(\rho_f)(\sigma) = \begin{cases} \tilde{\phi}(\sigma)\tilde{\phi}(\iota\sigma\iota) & \text{if } \sigma \in G_K \\ -\tilde{\phi}(\sigma')\tilde{\phi}(\iota\sigma'\iota) & \text{if } \sigma = \iota\sigma' \text{ where } \sigma' \in G_K. \end{cases}$$

Proof. This is immediate from (2) and (3). □

Proposition 3.3. *As a $G_{\mathbb{Q}}$-representation,* $\mathrm{Sym}^2(V_f)$ *decomposes into*

$$\mathrm{Sym}^2(V_f) \cong V_1 \oplus V_2,$$

where $\rho_i : G_{\mathbb{Q}} \to GL(V_i)$ is an i-dimensional representation of $G_{\mathbb{Q}}$ for $i = 1, 2$. Moreover,

$$\rho_1 \cong \varepsilon_K \cdot \det(\rho_f) = \varepsilon_K \cdot \epsilon \cdot \chi^{k-1}, \tag{4}$$
$$\rho_2 \cong \tilde{V}_{\phi^2}. \tag{5}$$

Proof. It is clear that $x \otimes x$, $y \otimes y$, $x \otimes y + y \otimes x$ form a basis of $\mathrm{Sym}^2(V_f)$. By formulae (2) and (3), $\sigma \cdot (x \otimes y + y \otimes x)$ is a multiple of $x \otimes y + y \otimes x$ for any $\sigma \in G_{\mathbb{Q}}$.

Hence, it gives a one-dimensional sub-representation V_1 of $\mathrm{Sym}^2(V_f)$. More explicitly, we have

$$\sigma\cdot(x\otimes y+y\otimes x)=\begin{cases}\tilde{\phi}(\sigma)\tilde{\phi}(\iota\sigma\iota)(x\otimes y+y\otimes x) & \text{if } \sigma\in G_K\\ \tilde{\phi}(\sigma')\tilde{\phi}(\iota\sigma'\iota)(x\otimes y+y\otimes x) & \text{if } \sigma=\iota\sigma' \text{ where } \sigma'\in G_K.\end{cases}$$

Therefore, we deduce (4) from Lemma 3.2.

It is also clear that $x\otimes x$, $y\otimes y$ form a basis of a two-dimensional representation $\rho_2: G_{\mathbb{Q}}\to \mathrm{GL}(V_2)$. With respect to this basis,

$$\rho_2(\sigma)=\begin{pmatrix}\tilde{\phi}^2(\sigma) & 0\\ 0 & \tilde{\phi}^2(\iota\sigma\iota)\end{pmatrix}$$

if $\sigma\in G_K$. Otherwise if $\sigma=\iota\sigma'$, where $\sigma'\in G_K$, then

$$\rho_2(\sigma)=\begin{pmatrix}0 & \tilde{\phi}^2(\iota\sigma'\iota)\\ \tilde{\phi}^2(\sigma') & 0\end{pmatrix}.$$

Therefore, $V_2\cong \mathrm{Ind}_K^{\mathbb{Q}} V(\phi^2)$ as required. □

COROLLARY 3.4. *The complex L function admits a factorisation*

$$L(\mathrm{Sym}^2 f,s)=L(\phi^2,s)L(\varepsilon_K\cdot\epsilon,s-k+1).$$

Proof. The L-function of $\mathrm{Sym}^2 f$ only have non-trivial Euler factors at $q\nmid N$. The Euler factors on the two sides of the equation at q agree by Proposition 3.3, so we are done. □

3.3. The symmetric square as a $G_{\mathbb{Q}_p}$-representation.

We study the representation $\mathrm{Sym}^2(V_f)$ restricted to $G_{\mathbb{Q}_p}$. More specifically, we study $\mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2 V_f)$.

LEMMA 3.5. *As $G_{\mathbb{Q}_p}$-representations, both V_1 and V_2 are crystalline.*

Proof. The functor $\mathbb{D}_{\mathrm{cris}}$ is compatible with taking direct sums, so we can identify $\mathbb{D}_{\mathrm{cris}}(V_i)$ as a filtered sub-φ-module of $\mathbb{D}_{\mathrm{cris}}(V_f)$ for $i=1,2$. That is,

$$\mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2(V_f))\cong \mathbb{D}_{\mathrm{cris}}(V_1)\oplus\mathbb{D}_{\mathrm{cris}}(V_2). \tag{6}$$

Since $\mathrm{Sym}^2(V_f)$ is crystalline, $\mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2(V_f))$ is of dimension 3 over E. Hence, $\mathbb{D}_{\mathrm{cris}}(V_i)$ must have dimension i and V_i is crystalline for $i=1,2$. □

We now give explicit descriptions of $\mathbb{D}_{\mathrm{cris}}(V_1)$ and $\mathbb{D}_{\mathrm{cris}}(V_2)$.

Recall that $\mathbb{D}_{\mathrm{cris}}(V_f)$ is a two-dimensional E-vector space with Hodge–Tate weights 0 and $1-k$. Moreover, the de Rham filtration is given by

$$\mathrm{Fil}^i\mathbb{D}_{\mathrm{cris}}(V_f)=\begin{cases}E\omega\oplus E\varphi(\omega) & \text{if } i\le 0\\ E\omega & \text{if } 1\le i\le k-1\\ 0 & \text{if } i\ge k\end{cases} \tag{7}$$

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

for some $\omega \neq 0$. The action of φ on $\mathbb{D}_{\mathrm{cris}}(V_f)$ satisfies $\varphi^2 = -\epsilon(p)p^{k-1}$. Therefore,

$$\mathrm{Fil}^i\mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2(V_f)) = \begin{cases} \mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2(V_f)) & \text{if } i \leq 0 \\ E(\omega\otimes\omega) \oplus E(\varphi(\omega)\otimes\omega + \omega\otimes\varphi(\omega)) & \text{if } 1 \leq i \leq k-1 \\ E(\omega\otimes\omega) & \text{if } k \leq i \leq 2k-2 \\ 0 & \text{if } i \geq 2k-1 \end{cases}. \tag{8}$$

Since $\varphi^2(\omega) = -\epsilon(p)p^{k-1}\omega$, we have

$$\varphi(\omega\otimes\varphi(\omega) + \varphi(\omega)\otimes\omega) = -\epsilon(p)p^{k-1}(\omega\otimes\varphi(\omega) + \varphi(\omega)\otimes\omega).$$

In particular, $\omega\otimes\varphi(\omega) + \varphi(\omega)\otimes\omega$ is an eigenvector of φ. Therefore, we have a decomposition of filtered φ-modules

$$\mathbb{D}_{\mathrm{cris}}(\mathrm{Sym}^2(V_f)) = (E(\omega\otimes\omega)\oplus E(\varphi(\omega)\otimes\varphi(\omega)))\oplus(E(\omega\otimes\varphi(\omega)+\varphi(\omega)\otimes\omega)).$$

PROPOSITION 3.6. *As filtered φ-modules, we have*

$$\mathbb{D}_{\mathrm{cris}}(V_1) = E(\varphi(\omega)\otimes\omega + \omega\otimes\varphi(\omega)),$$
$$\mathbb{D}_{\mathrm{cris}}(V_2) = E(\omega\otimes\omega)\oplus E(\varphi(\omega)\otimes\varphi(\omega)).$$

Proof. By (4), $\rho_1 = \varepsilon_K \cdot \epsilon \cdot \chi^{k-1}$. Since p is inert in K, $\varepsilon_K(p) = -1$. The Hodge–Tate weight of V_1 is therefore $1-k$ and φ acts on $\mathbb{D}_{\mathrm{cris}}(V_1)$ as multiplication by $-\epsilon(p)p^{k-1}$. This proves the first equality. The second equality is then automatic by (6). □

REMARK 3.7. Such a decomposition of $G_{\mathbb{Q}_p}$-representations is in fact possible for f without CM (see Section 2.2 in [**10**]).

COROLLARY 3.8. *The eigenvalues of φ on $\mathbb{D}_{\mathrm{cris}}(V_2)$ are $\pm\epsilon(p)p^{k-1}$.*

Proof. By Proposition 3.6, the matrix of φ with respect to the basis $\omega\otimes\omega$, $\varphi(\omega)\otimes\varphi(\omega)$ is

$$\begin{pmatrix} 0 & \epsilon(p)^2p^{2k-2} \\ 1 & 0 \end{pmatrix},$$

hence the result. □

COROLLARY 3.9. *The Hodge–Tate weights of V_2 are* 0 *and* $2-2k$.

Proof. This follows from (8) and Proposition 3.6. □

3.4. The Perrin–Riou pairing. By Corollary 3.8, the slope of φ on $\mathbb{D}_{\mathrm{cris}}(V_2)$ is $k-1$. Hence, by Corollary 3.9, given any $v \in \mathbb{D}_{\mathrm{cris}}(V_2)$, we have the Perrin–Riou pairing

$$\mathcal{L}_v : \mathbb{H}^1_{\mathrm{Iw}}(V_2^*) \to \mathcal{H}_{k-1,E}(G_\infty),$$

which satisfies the following properties.

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

PROPOSITION 3.10. *For an integer $r \geq 0$, we have*

$$\chi^r(\mathcal{L}_v(\mathbf{z})) = r!\left[\left(1 - \frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(v_{r+1}), \exp^*(z_{-r,0})\right]_0 .$$

Let θ be a character of G_n which does not factor through G_{n-1} with $n \geq 1$, then

$$\chi^r\theta(\mathcal{L}_v(\mathbf{z})) = \frac{r!}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)\left[\varphi^{-n}(v_{r+1}), \exp^*(z^{\sigma}_{-r,n})\right]_n ,$$

where $[,]_n$ is the pairing

$$[,]_n : H^1(\mathbb{Q}_{p,n}, V_2(r+1)) \times H^1(\mathbb{Q}_{p,n}, V_2^*(-r)) \to H^2(\mathbb{Q}_{p,n}, E(1)) \cong E,$$

$z_{-r,n}$ denotes the projection of $\mathrm{Tw}_{-r}(z)$ *into $H^1(\mathbb{Q}_{p,n}, V_2^*(-r))$ and $\tau(\theta^{-1})$ denotes the Gauss sum of θ^{-1}.*

Proof. See Section 3.2 in [**6**]. □

REMARK 3.11. The assumption on the eigenvalues of φ made in [**6**] are not necessary for our purposes here because the Perrin–Riou pairings can be defined by applying $1-\varphi$ to the (φ, G_∞)-module of V_2^* (see [**7**] and Section 16.4 in [**5**]).

We fix a non-zero element $\bar{\omega} \in \mathrm{Fil}^{-1}\mathbb{D}_{\mathrm{cris}}(V_2^*(1))$ and write

$$\mathrm{per}(\bar{\omega}) = \Omega_+(\gamma')^+ + \Omega_-(\gamma')^-,$$

where $\Omega_\pm \in \mathbb{C}^\times$ and γ' is as given in the statement of Proposition 3.1 for some fixed γ.

DEFINITION 3.12. Under the choices made above, we define $v^\pm \in \mathbb{D}_{\mathrm{cris}}(V_2)$ by

$$v^\pm = \frac{1}{[\varphi(\omega)\otimes\varphi(\omega), \bar{\omega}]}(\pm\epsilon(p)p^{k-1}\omega\otimes\omega + \varphi(\omega)\otimes\varphi(\omega)).$$

LEMMA 3.13. *The elements $v^\pm$ satisfy*:

(a) *Both $v^\pm$ are eigenvalues of φ with $\varphi(v^\pm) = \pm\epsilon(p)p^{k-1}v^\pm$.*

(b) *For any $x \in \mathrm{Fil}^0\mathbb{D}_{\mathrm{cris}}(V_2^*(-r))$ and an integer r such that $0 \leq r \leq 2k-3$, we have*

$$[v^+_{r+1}, x] = [v^-_{r+1}, x],$$

where $[,]$ denotes the pairing

$$[,] : \mathbb{D}_{\mathrm{cris}}(V_2(r+1)) \times \mathbb{D}_{\mathrm{cris}}(V_2^*(-r)) \to \mathbb{D}_{\mathrm{cris}}(E(1)) = E\cdot t^{-1}e_1.$$

Proof. (a) is easy to check using the matrix given in the proof of Corollary 3.8 (or by direct calculations).

By Corollary 3.9, the Hodge–Tate weights of V_2^* are 0 and $2k-2$. Hence, $\mathrm{Fil}^0\mathbb{D}_{\mathrm{cris}}(V_2^*(-r))$ is one-dimensional with basis $\bar{\omega}_{-r-1}$ for $0 \leq r \leq 2k-3$. Since $(\omega\otimes\omega)_{r+1} \in \mathrm{Fil}^0\mathbb{D}_{\mathrm{cris}}(V_2(r+1))$, we have $[(\omega\otimes\omega)_{r+1}, \bar{\omega}_{-r-1}] = 0$. Hence,

$$[v^+_{r+1}, \bar{\omega}_{-r-1}] = [v^-_{r+1}, \bar{\omega}_{-r-1}] = 1,$$

which implies (b). □

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

Note that $V_2^* \cong \tilde{V}_{\bar{\phi}^2}(2k-2)$. This enables us to make the following definition of p-adic L-functions associated to ϕ^2.

DEFINITION 3.14. On taking $\eta = \bar{\phi}^2$ in Section 3.1, we define

$$L_{\pm\epsilon(p)p^{k-1}}(\phi^2) = \mathcal{L}_{v^\pm}(\mathrm{Tw}_{2k-2}(z(\bar{\phi}^2))) \in \mathcal{H}_{k-1,E}(G_\infty).$$

LEMMA 3.15. *Let θ be a character of G_n which does not factor through G_{n-1} with $n \geq 1$ and write $\delta = \theta(-1)$, then*

$$\chi^{2k-3}\theta(L_\alpha(\phi^2)) = \frac{(2k-3)!p^{(2k-2)n}}{\tau(\theta^{-1})\alpha^n} \times \frac{L(\phi^2\theta^{-1}, 2k-2)}{\Omega_\delta},$$

where $\alpha = \pm\epsilon(p)p^{k-1}$.

Proof. We have

$$\begin{aligned}
&\chi^{2k-3}\theta(L_{\pm\epsilon(p)p^{k-1}}(\phi^2))\\
&\quad= \chi^{2k-3}\theta(\mathcal{L}_{v^\pm}(\mathrm{Tw}_{2k-2}(z(\bar{\phi}^2))))\\
&\quad= \frac{(2k-3)!}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)[\varphi^{-n}(v_{2k-2}^\pm), \exp^*(z_{1,n}(\bar{\phi}^2)^\sigma)]_n\\
&\quad= \frac{(2k-3)!}{\tau(\theta^{-1})}\left[(\pm\epsilon(p)p^{k-1}\times p^{-2k+2})^{-n}v_{2k-2}^\pm, \sum_{\sigma\in G_n}\theta^{-1}(\sigma)\exp^*(z_{1,n}(\bar{\phi}^2)^\sigma)\right]_n\\
&\quad= \frac{(2k-3)!p^{(2k-2)n}}{\tau(\theta^{-1})(\pm\epsilon(p)p^{k-1})^n} \times \frac{L(\phi^2\theta^{-1}, 2k-2)}{\Omega_\delta},
\end{aligned}$$

where the second equality follows from Proposition 3.10, the third follows from Lemma 3.13(a) and the last equality is a consequence of Proposition 3.1 and the fact that p divides the conductor of θ. □

LEMMA 3.16. *We have*

$$\chi^{2k-3}(L_{\pm\epsilon(p)p^{k-1}}(\phi^2)) = (1 - p^{-1} + (1-\epsilon(p)^{-2}p^{2k-3})(\pm\epsilon(p)p^{1-k})) \times \frac{L(\phi^2, 2k-2)}{\Omega_+}.$$

Proof. Since $\varphi^2 = \epsilon(p)^2p^{2-2k}$ on $\mathbb{D}_{\mathrm{cris}}(V_2(2k-2))$, we have

$$\begin{aligned}
&\left(1 - \frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}\\
&\quad= (1 - \epsilon(p)^{-2}p^{2k-3}\varphi)\frac{1+\varphi}{1-\epsilon(p)^2p^{2-2k}}\\
&\quad= \frac{1 - p^{-1} + (1-\epsilon(p)^{-2}p^{2k-3})\varphi}{1-\epsilon(p)^2p^{2-2k}}.
\end{aligned}$$

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

Therefore, similar to the proof of Lemma 3.15, we have

$$\begin{aligned}
&\chi^{2k-3}(L_{\pm\epsilon(p)p^{k-1}}(\phi^2))\\
&= \chi^{2k-3}(\mathcal{L}_{v^{\pm}}(\mathrm{Tw}_{2k-2}(z(\bar{\phi}^2))))\\
&= (2k-3)!\left[\frac{1-p^{-1}+(1-\epsilon(p)^{-2}p^{2k-3})\varphi}{1-\epsilon(p)^2p^{2-2k}}(v^{\pm}_{2k-2}), \exp^*(z_{1,0}(\bar{\phi}^2))\right]_0\\
&= (2k-3)!\left[\frac{1-p^{-1}+(1-\epsilon(p)^{-2}p^{2k-3})(\pm\epsilon(p)p^{1-k})}{1-\epsilon(p)^2p^{2-2k}}\cdot v^{\pm}_{2k-2}, \exp^*(z_{1,0}(\bar{\phi}^2))\right]_0\\
&= \frac{1-p^{-1}+(1-\epsilon(p)^{-2}p^{2k-3})(\pm\epsilon(p)p^{1-k})}{1-\epsilon(p)^2p^{2-2k}}\times\frac{L_{\{p\}}(\phi^2, 2k-2)}{\Omega_+}\\
&= (1-p^{-1}+(1-\epsilon(p)^{-2}p^{2k-3})(\pm\epsilon(p)p^{1-k}))\times\frac{L(\phi^2, 2k-2)}{\Omega_+}.
\end{aligned}$$

□

REMARK 3.17. Consider the p-adic L-function $L_{+\epsilon(p)p^{k-1}}(\phi^2)$. The first factor on the right-hand side of the equation in the statement of Lemma 3.16 vanishes if and only if $k=2$ and $\epsilon(p)=1$ (e.g. when f corresponds to an elliptic curve over $\mathbb{Q}$). This recovers the trivial zero result in [**10**].

3.5. p-adic L-functions of the symmetric square.

Let us first recall the following result of Kubota and Leopoldt.

THEOREM 3.18. *If η is a non-trivial Dirichlet character of conductor prime to p, there exists a bounded p-adic measure $L_p(\eta)\in\mathcal{H}_{0,E}(G_\infty)$, where E is some finite extension of $\mathbb{Q}_p$ which contains the image of η such that*

$$\chi^r\theta(L_p(\eta)) = \frac{(r+1)!p^{n(r+1)}}{(2\pi i)^{r+1}\tau(\theta^{-1})}\times L(\eta\theta^{-1}, r+1);$$
$$\chi^r(L_p(\eta)) = \frac{(r+1)!}{(2\pi i)^{r+1}}L(\eta, r+1)$$

for any integer $r\geq 0$ and the Dirichlet character θ of conductor p^n such that $\chi^{r+1}\theta(-1)=\eta(-1)$.

Since we assume that Hypothesis 2.1 holds, we may take $\eta=\varepsilon_K\cdot\epsilon$ in Theorem 3.18. This enables us to give the following definition.

DEFINITION 3.19. For $\alpha=\pm\epsilon(p)p^{k-1}$ we define

$$L_\alpha(\mathrm{Sym}^2(V_f)) = L_\alpha(\phi^2)\times\mathrm{Tw}_{-k+1}(L_p(\varepsilon_K\cdot\epsilon)).$$

For the rest of this section, unless otherwise stated, θ denotes an even character on G_n, which does not factor through G_{n-1} with $n\geq 1$.

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

Theorem 3.20. *Both* $L_{\pm\epsilon(p)p^{k-1}}\left(\mathrm{Sym}^2(V_f)\right)$ *lie inside* $\mathcal{H}_{k-1,E}(G_\infty)$ *and admit the following interpolating properties:*

$$\chi^{2k-3}\theta(L_\alpha(\mathrm{Sym}^2(V_f))) = \frac{(2k-3)!(k-1)!p^{3n(k-1)}}{\tau(\theta^{-1})^2\alpha^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(2\pi i)^{k-1}\Omega_+};$$

$$\chi^{2k-3}(L_\alpha(\mathrm{Sym}^2(V_f))) = (2k-3)!(k-1)!\left(1-\frac{1}{p}+\alpha\left(p^{-2k+2}-\frac{1}{p\epsilon(p)^2}\right)\right) \times \frac{L(\mathrm{Sym}^2 f, 2k-2)}{(2\pi i)^{k-1}\Omega_+},$$

where $\alpha = \pm\epsilon(p)p^{k-1}$.

Proof. By definition, $L_\alpha(\phi^2) \in \mathcal{H}_{k-1,E}(G_\infty)$ and $L_p(\varepsilon_K \cdot \epsilon) \in \mathcal{H}_{0,E}(G_\infty)$, which implies the first part of the theorem.

Since $\det(V_f) = \epsilon\chi^{k-1}$ and ρ_f is odd, we have $\epsilon\chi^{k-1}(-1) = -1$. But $\varepsilon_K(-1) = -1$ and $\theta(-1) = 1$, so $\chi^{k-1}\theta(-1) = \varepsilon_K\epsilon(-1)$ and we can apply Theorem 3.18 and Lemma 3.15 as follows:

$$\begin{aligned}
&\chi^{2k-3}\theta(L_\alpha(\mathrm{Sym}^2(V_f)))\\
&= \chi^{2k-3}\theta(L_\alpha(\phi^2)) \times \chi^{k-2}\theta(L_p(\varepsilon_K\cdot\epsilon))\\
&= \frac{(2k-3)!p^{(2k-2)n}}{\tau(\theta^{-1})\alpha^n} \times \frac{L(\phi^2\theta, 2k-2)}{\Omega_+} \times \frac{(k-1)!p^{n(k-1)}}{(2\pi i)^{k-1}\tau(\theta^{-1})} \times L(\varepsilon_k\cdot\epsilon\cdot\theta^{-1}, k-1)\\
&= \frac{(2k-3)!(k-1)!p^{3n(k-1)}}{\tau(\theta^{-1})^2\alpha^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(2\pi i)^{k-1}\Omega_+},
\end{aligned}$$

where the last equality follows from Corollary 3.4. This gives the first interpolating formula and the second one can be deduced in the same way. □

Lemma 3.21. *Let* η *be an even character on* Δ, *then* $L^\eta_{\pm\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)) \neq 0$.

Proof. We have $L(\mathrm{Sym}^2(V_f), \eta, 2k-2) \neq 0$ because the critical strip of $\mathrm{Sym}^2(V_f)$ is $k-1 < \mathrm{Re}(s) < k$. Therefore, we are done by the interpolating properties given by Theorem 3.20. □

3.6. Pollack's plus and minus splittings.

As in [**11**], we define

$$\log^+(\gamma) = \prod_{r=0}^{2k-3}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(\chi(\gamma)^{-r}\gamma)}{p},$$

$$\log^-(\gamma) = \prod_{r=0}^{2k-3}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(\chi(\gamma)^{-r}\gamma)}{p},$$

where Φ_m denotes the p^mth cyclotomic polynomial. Then, $\log^\pm(\gamma) \sim \log^{k-1}$.

Lemma 3.22. *For an integer* r *such that* $0 \leq r \leq 2k-3$ *and a character* θ *of* G_n *which does not factor through* G_{n-1} *with* $n \geq 1$,

$$\chi^r\theta(L_{+\epsilon(p)p^{k-1}}(\phi^2)) = (-1)^n\chi^r\theta(L_{-\epsilon(p)p^{k-1}}(\phi^2)).$$

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

Proof. This follows from the same calculations as in the proof of Lemma 3.15, thanks to Lemma 3.13(b). □

COROLLARY 3.23. *We have divisibilities*

$$\log^+(\gamma) \mid L_{+\epsilon(p)p^{k-1}}(\phi^2) + L_{-\epsilon(p)p^{k-1}}(\phi^2);$$
$$\log^-(\gamma) \mid L_{+\epsilon(p)p^{k-1}}(\phi^2) - L_{-\epsilon(p)p^{k-1}}(\phi^2).$$

Similarly,

$$\log^+(\gamma) \mid L_{+\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)) + L_{-\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f));$$
$$\log^-(\gamma) \mid L_{+\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)) - L_{-\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)).$$

Proof. The first set of divisibilities follows from Lemma 3.22. The second set is then immediate by definition. □

This allows us to define the following.

DEFINITION 3.24. We define the plus and minus p-adic L-functions for $\mathrm{Sym}^2(V_f)$ by

$$L_p^+(\mathrm{Sym}^2(V_f)) = (L_{+\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)) + L_{-\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)))/2\log^+(\gamma);$$
$$L_p^-(\mathrm{Sym}^2(V_f)) = (L_{+\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)) - L_{-\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f)))/2\log^-(\gamma).$$

Similarly, we define the plus and minus p-adic L-functions for V_2 by

$$L_p^+(\phi^2) = (L_{+\epsilon(p)p^{k-1}}(\phi^2) + L_{-\epsilon(p)p^{k-1}}(\phi^2))/2\log^+(\gamma);$$
$$L_p^-(\phi^2) = (L_{+\epsilon(p)p^{k-1}}(\phi^2) - L_{-\epsilon(p)p^{k-1}}(\phi^2))/2\log^-(\gamma).$$

It is immediate that

$$L_p^\pm(\mathrm{Sym}^2(V_f)) = L_p^\pm(\phi^2) \times \mathrm{Tw}_{-k+1}(L_p(\varepsilon_K \cdot \epsilon)). \tag{9}$$

THEOREM 3.25. *Both* $L_p^\pm(\mathrm{Sym}^2(V_f))$ *are elements of* $\Lambda_E(G_\infty)$ *and admit the following interpolating properties*:

(a) *If n is even, then*

$$\chi^{2k-3}\theta(L_p^+(\mathrm{Sym}^2(V_f))) = \frac{(2k-3)!(k-1)!p^{2n(k-1)}}{\log^+(\chi^{2k-3}\theta(\gamma))\tau(\theta^{-1})^2\epsilon(p)^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(2\pi i)^{k-1}\Omega_+},$$
$$\chi^{2k-3}(L_p^+(\mathrm{Sym}^2(V_f))) = \frac{(2k-3)!(k-1)!(1-p^{-1})}{\log^+(\chi^{2k-3}(\gamma))} \times \frac{L(\mathrm{Sym}^2 f, 2k-2)}{(2\pi i)^{k-1}\Omega_+}.$$

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

(b) *If n is odd, then*

$$\chi^{2k-3}\theta(L_p^-(\mathrm{Sym}^2(V_f))) = \frac{(2k-3)!(k-1)!p^{2n(k-1)}}{\log^-(\chi^{2k-3}\theta(\gamma))\tau(\theta^{-1})^2\epsilon(p)^n} \times \frac{L(\mathrm{Sym}^2 f, \theta^{-1}, 2k-2)}{(2\pi i)^{k-1}\Omega_+},$$

$$\chi^{2k-3}(L_p^-(\mathrm{Sym}^2(V_f))) = \frac{(2k-3)!(k-1)!(\epsilon(p)p^{-k+1} - \epsilon(p)^{-1}p^{k-2})}{\log^-(\chi^{2k-3}(\gamma))} \times \frac{L(\mathrm{Sym}^2 f, 2k-2)}{(2\pi i)^{k-1}\Omega_+}.$$

Moreover, $L_p^\pm(\mathrm{Sym}^2(V_f))$ *are uniquely determined by* (a) *and* (b)*, respectively.*

Proof. By the first part of Theorem 3.20, $L_{\pm\epsilon(p)p^{k-1}}(\mathrm{Sym}^2(V_f))$ are both elements of $\mathcal{H}_{k-1,E}(G_\infty)$. But $\log^\pm(\gamma) \sim \log^{k-1}$, so the quotients above are in $\mathcal{H}_{0,E}(G_\infty) = \Lambda_E(G_\infty)$. The interpolating formulae in (a) and (b) follow from those given in Theorem 3.20.

Finally, since $L_p^\pm(\mathrm{Sym}^2(V_f)) \in \Lambda_E(G_\infty)$, they are uniquely determined by their values at an infinite number of characters, hence the last part of the theorem. □

LEMMA 3.26. *Let* η *be an even character on* Δ*, then* $L_p^{\pm,\eta}(\mathrm{Sym}^2(V_f)) \neq 0$.

Proof. The same as the proof of Lemma 3.21. □

REMARK 3.27. Analogues of Theorem 3.25 and Lemma 3.26 for $L_p^\pm(\phi^2)$ can be deduced in the same way.

REMARK 3.28. A conjectural generalisation of Pollack's plus and minus splittings of p-adic L-functions for motives has been formulated in [**2**]. Theorem 3.25 gives an affirmative answer to Conjecture 2 (op. cit.) for the special case when the motive corresponds to the symmetric square of a CM modular form.

4. Selmer groups. In this section, we define the plus and minus p-Selmer groups for $\mathrm{Sym}^2(V_f)$ and relate these to the p-adic L-functions $L_p^\pm\left(\mathrm{Sym}^2(V_f)\right)$ defined above. By the decomposition given by Proposition 3.3, we only need to define their counterparts for $V_2 = \tilde{V}_{\phi^2}$ because the Selmer group of V_1 is relatively well understood. The $G_\mathbb{Q}$-representation V_2 behaves in exactly the same way as $V_{f'}$, where f' is some CM modular form of weight $2k-1$, so many of the results on V_2 below can be proved using the arguments given in [**6**]. Therefore, we only outline the proofs without giving all the details here.

4.1. Coleman maps and Selmer groups. As in [**6, 7**], we define plus and minus Selmer groups using the kernels of some Coleman maps.

PROPOSITION 4.1. *If* $z \in \mathbb{H}^1_{\mathrm{Iw}}(V_2^*)$*, then*

$$\log^+(\gamma) \mid \mathcal{L}_{\varphi(\omega)\otimes\varphi(\omega)}(z),$$
$$\log^-(\gamma) \mid \mathcal{L}_{\omega\otimes\omega}(z).$$

Proof. As in Proposition 3.14 in [**6**], this can be proved using Proposition 3.10. □

Therefore, as in [**6**], we may define $\Lambda_E(G_\infty)$ homomorphisms

$$\begin{aligned}\mathrm{Col}^+ : \mathbb{H}^1_{\mathrm{Iw}}(V_2^*) &\to \Lambda_E(G_\infty)\\ z &\mapsto \frac{1}{2[\varphi(\omega)\otimes\varphi(\omega),\bar{\omega}]\log^+(\gamma)}\mathcal{L}_{\varphi(\omega)\otimes\varphi(\omega)}(z);\\ \mathrm{Col}^- : \mathbb{H}^1_{\mathrm{Iw}}(V_2^*) &\to \Lambda_E(G_\infty)\\ z &\mapsto \frac{1}{2[\varphi(\omega)\otimes\varphi(\omega),\bar{\omega}]\log^-(\gamma)}\mathcal{L}_{\omega\otimes\omega}(z).\end{aligned}$$

Then, it is clear by definition that $\mathrm{Col}^\pm\left(\mathrm{Tw}_{2k-2}\left(z(\bar{\phi}^2)\right)\right) = L_p^\pm(\phi^2)$.

We now fix an $\mathcal{O}_E$-lattice T of $V(\phi)$, which is stable under $G_\mathbb{Q}$, it then gives rise to natural $\mathcal{O}_E$-lattices $T_f = \mathrm{Ind}_K^\mathbb{Q}(T)$ and $\mathrm{Sym}^2 T_f$ in $V_f = \tilde{V}_\phi$ and $\mathrm{Sym}^2(V_f)$, respectively, both of which are again stable under $G_\mathbb{Q}$. As $p \neq 2$, we have

$$\mathrm{Sym}^2 T_f \cong T_1 \oplus T_2 \quad\text{and}\quad \mathrm{Sym}^2 V_f/T_f \cong V_1/T_1 \oplus V_2/T_2$$

for some $\mathcal{O}_E$-lattice T_i inside V_i for $i = 1, 2$.

Write $H^1_\pm(\mathbb{Q}_{p,n}, T_2^*)$ for the projection of $\ker(\mathrm{Col}^\pm)$ into $H^1(\mathbb{Q}_{p,n}, T_2^*)$ and define $H^1(\mathbb{Q}_{p,n}, V_2/T_2(1))^\pm$ to be the exact annihilator of $H^1_\pm(\mathbb{Q}_{p,n}, T_2^*)$ under the Pontryagin duality

$$H^1(\mathbb{Q}_{p,n}, T_2^*) \times H^1(\mathbb{Q}_{p,n}, V_2/T_2(1)) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Let F be a number field. Then the p-Selmer group of $\mathrm{Sym}^2 T_f(1)$ decomposes into those of $T_1(1)$ and $T_2(1)$:

$$\mathrm{Sel}_p(\mathrm{Sym}^2 T_f(1)/F) = \mathrm{Sel}_p(T_1(1)/F) \oplus \mathrm{Sel}_p(T_2(1)/F).$$

We define the plus/minus Selmer groups over $k_n = \mathbb{Q}(\mu_{p^n})$ by

$$\begin{aligned}\mathrm{Sel}_p^\pm(T_2(1)/k_n) &= \ker\left(\mathrm{Sel}_p(T_2(1)/k_n) \to \frac{H^1(\mathbb{Q}_{p,n}, V_2/T_2(1))}{H^1_f(\mathbb{Q}_{p,n}, V_2/T_2(1))^\pm}\right),\\ \mathrm{Sel}_p^\pm(\mathrm{Sym}^2 T_f(1)/k_n) &= \mathrm{Sel}_p(T_1(1)/k_n) \oplus \mathrm{Sel}_p^\pm(T_2(1)/k_n),\end{aligned}$$

and let

$$\begin{aligned}\mathrm{Sel}_p^\pm(T_2(1)/k_\infty) = \lim_{\rightarrow}\mathrm{Sel}_p^\pm(T_2(1)/k_n) \quad\text{and}\quad &\mathrm{Sel}_p^\pm(\mathrm{Sym}^2 T_f(1)/k_\infty)\\ &= \lim_{\rightarrow}\mathrm{Sel}_p^\pm(\mathrm{Sym}^2 T_f(1)/k_n).\end{aligned}$$

4.2. Description of the kernels. In this section we give a more explicit description of the groups $H^1_f(\mathbb{Q}_{p,n}, V_2/T_2(1))^\pm$ under the following additional assumption.

HYPOTHESIS 4.2. *Either* $p-1 \nmid k-1$ *or* $\epsilon \neq 1$.

In Section in [**6**], one of the key ingredients to give an explicit description of $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^\pm$ is the fact that $(V_f/T_f(j))^{G_{\mathbb{Q}_{p,n}}} = 0$ under some appropriate assumptions. We show below that we get an analogue of such description under Hypothesis 4.2.

https://doi.org/10.1017/S0017089511000553 Published online by Cambridge University Press

LEMMA 4.3. *If Hypothesis 4.2 holds, then* $(V_2/T_2(j))^{G_{\mathbb{Q}_{p,n}}} = 0$ *for all* $j \in \mathbb{Z}$ *and* $n \in \mathbb{Z}_{\geq 0}$.

Proof. Let $q \nmid N$ be a prime which is inert in K. Then, by the second half of the proof of Proposition 3.3, we see that the eigenvalues of the q-Frobenius on $V_2(j)$ are $\pm\epsilon(q)\chi^j(q)q^{k-1}$. Therefore, as in proof of Lemma 4.4 in [**6**], it is enough to show that there exists some q such that

$$\pm\epsilon(q)\chi^j(q)q^{k-1} \not\equiv 1 \mod p.$$

If either $p-1 \nmid k-1$ or $\epsilon(q) \neq 1$, we can find such a q by Dirichlet's theorem, so we are done. □

COROLLARY 4.4. *If Hypothesis 4.2 holds, then the restriction map* $H^1(\mathbb{Q}_{p,m}, T_2(1)) \to H^1(\mathbb{Q}_{p,n}, T_2(1))$ *is injective for any integers* $n \geq m \geq 0$. *On identifying the former as a subgroup of the latter, we have*

$$H^1_f(\mathbb{Q}_{p,n}, V_2/T_2(1))^{\pm} = H^1_f(\mathbb{Q}_{p,n}, T_2(1))^{\pm} \otimes E/\mathcal{O}_E.$$

Here

$$H^1_f(\mathbb{Q}_{p,n}, T_2(1))^{\pm} = \left\{x \in H^1_f(\mathbb{Q}_{p,n}, T_2(1)) : \mathrm{cor}_{n/m+1}(x) \in H^1_f(\mathbb{Q}_{p,m}, T_2(1)) \forall m \in S_n^{\pm}\right\},$$

where cor *denotes the corestriction map and*

$$S_n^+ = \{m \in [0, m-1] : m \text{ even}\},$$
$$S_n^- = \{m \in [0, m-1] : m \text{ odd}\}.$$

Proof. These can be proved in exactly the same way as their counterparts in Section 4 in [**6**] using Lemma 4.3. □

4.3. Main conjectures.

THEOREM 4.5. *Let* θ *be a character on* Δ *and* $r \geq 0$ *an integer such that* $\chi^{r+1}\theta(-1) = \eta(-1)$. *Then* $\mathrm{Sel}_p(\mathbb{Z}_p(\eta)(r+1))^{\theta}$ *is* $\Lambda_E(\Gamma)$*-cotorsion and*

$$\mathrm{Char}_{\Lambda_E(\Gamma)}(\mathrm{Sel}_p(\mathbb{Z}_p(\eta)(r+1))^{\vee,\theta}) = \left(\mathrm{Tw}_{-r}L_p^{\theta}(\eta)\right).$$

Proof. For any $\Lambda_E(G_\infty)$-module, $M^{\vee}(r) = M(-r)^{\vee}$. If M is a $\Lambda_E(\Gamma)$ torsion module, we have $\mathrm{Char}(M(r)) = \mathrm{Tw}_r(\mathrm{Char}(M))$. Therefore, the result is just a rewrite of the Iwasawa main conjecture, as proved by Mazur and Wiles [**8**]. □

COROLLARY 4.6. *Let* η *be an even character on* Δ. *Then*

$$\mathrm{Char}_{\Lambda_E(\Gamma)}(\mathrm{Sel}_p(T_1(1)/k_\infty)^{\vee,\eta}) = (\mathrm{Tw}_{-k+1}L_p^{\eta}(\varepsilon_K \cdot \epsilon)).$$

Proof. We may apply Theorem 4.5 to $\varepsilon_K \cdot \epsilon$ with $r = k-1$. □

PROPOSITION 4.7. *Let* $\delta = \pm$ *and let* η *be a character on* Δ *such that* $\eta = 1$ *if* $\delta = -$. *Then,* $\mathrm{Sel}_p^{\delta}(T_2(1)/k_\infty)^{\theta}$ *is* $\Lambda_E(\Gamma)$ *cotorsion and*

$$\mathrm{Char}_{\Lambda_E(\Gamma)}\left(\mathrm{Sel}_p^{\delta}(T_2(1)/k_\infty)^{\vee,\eta}\right) = \left(L_p^{\delta,\eta}(\phi^2)\right).$$

Proof. This follows from the same argument as in **[12]**, which has been generalised for CM modular forms in Section 7 in **[6]**. It relies on the main conjecture for K as proved in **[13]**. □

THEOREM 4.8. *Let η be a character on Δ as in the statement of Proposition 4.7. Then $\mathrm{Sel}_p^{\pm}(\mathrm{Sym}^2(V_f)/k_\infty)^\eta$ is $\Lambda_E(\Gamma)$ cotorsion and*

$$\mathrm{Char}_{\Lambda_E(\Gamma)}\big(\mathrm{Sel}_p^{\pm}(\mathrm{Sym}^2(V_f)/k_\infty)^{\vee,\eta}\big) = \big(L_p^{\pm,\eta}(\mathrm{Sym}^2(V_f))\big).$$

Proof. Recall that

$$\mathrm{Sel}_p^{\pm}(\mathrm{Sym}^2 T_f(1)/k_\infty) = \mathrm{Sel}_p(T_1(1)/k_\infty) \oplus \mathrm{Sel}_p^{\pm}(T_2(1)/k_\infty)$$

by definition, so

$$\mathrm{Sel}_p^{\pm}(\mathrm{Sym}^2 T_f(1)/k_\infty)^{\vee,\eta} = \mathrm{Sel}_p(T_1(1)/k_\infty)^{\vee,\eta} \oplus \mathrm{Sel}_p^{\pm}(T_2(1)/k_\infty)^{\vee,\eta}.$$

But we have

$$L_p^{\pm,\eta}(\mathrm{Sym}^2(V_f)) = L_p^{\pm,\eta}(\phi^2) \times \mathrm{Tw}_{-k+1}\big(L_p^{\eta}(\varepsilon_K \cdot \epsilon)\big)$$

by (9). Therefore, the theorem follows from Corollary 4.6 and Proposition 4.7 because

$$\mathrm{Char}(M_1 \oplus M_2) = \mathrm{Char}(M_1)\mathrm{Char}(M_2)$$

for any torsion modules M_1 and M_2. □

5. Appendix. In this section, we fix an integer $m \geq 2$. We prove an analogue of Proposition 3.3.

PROPOSITION 5.1. *If m is even, we have a decomposition of $G_{\mathbb{Q}}$-representations*

$$\mathrm{Sym}^m V_f \cong \bigoplus_{i=0}^{m/2-1} \big(\tilde{V}_{\phi^{m-2i}} \otimes \big(\varepsilon_K \det \rho_f\big)^i\big) \oplus \big(\varepsilon_K \det \rho_f\big)^{m/2}.$$

If m is odd, then

$$\mathrm{Sym}^m V_f \cong \bigoplus_{i=0}^{(m-1)/2} \big(\tilde{V}_{\phi^{m-2i}} \otimes \big(\varepsilon_K \det \rho_f\big)^i\big).$$

Proof. We only give the proof for the case when m is even, since the other case can be proved in a similar way. Let x, y be the basis of V_f given as in Section 3.2. For an integer r such that $0 \leq r \leq m$, we write x_r for the element in $V_f^{\otimes m}$ given by

$$\sum a_1 \otimes a_2 \otimes \cdots \otimes a_m,$$

where the sum runs over $a_i \in \{x, y\}$ with $\#\{i : a_i = x\} = r$. Then, $x_0, \ldots, x_m$ give a basis of $\mathrm{Sym}^m V_f$.

If $\sigma \in G_K$, we have

$$\sigma(x_r) = \tilde{\phi}^r(\sigma)\tilde{\phi}^{m-r}(\iota\sigma\iota)x_r$$

by (2). If $\sigma = \iota\sigma'$ with $\sigma' \in G_K$, then

$$\sigma(x_r) = \tilde{\phi}^r(\sigma')\tilde{\phi}^{m-r}(\iota\sigma'\iota)x_{m-r}$$

by (3). Therefore, x_r and x_{m-r} generate a sub-representation of $\mathrm{Sym}^m V_f$, which we denote by $\rho_r : G_{\mathbb{Q}} \to \mathrm{GL}(V_r)$, where $0 \le r \le m/2$. Note that V_r is two-dimensional if $r < m/2$ and $V_{m/2}$ is one-dimensional. We have a decomposition

$$\mathrm{Sym}^m V_f \cong \oplus_{r=0}^{m/2} V_r.$$

For $r < m/2$, the matrix of $\sigma \in G_K$ with respect to the basis x_{m-r}, x_r is

$$\begin{pmatrix} \tilde{\phi}^{m-r}(\sigma)\tilde{\phi}^r(\iota\sigma\iota) & 0 \\ 0 & \tilde{\phi}^r(\sigma)\tilde{\phi}^{m-r}(\iota\sigma\iota) \end{pmatrix} = \tilde{\phi}^r(\sigma\iota\sigma\iota) \begin{pmatrix} \tilde{\phi}^{m-2r}(\sigma) & 0 \\ 0 & \tilde{\phi}^{m-2r}(\iota\sigma\iota) \end{pmatrix},$$

whereas that of $\sigma = \iota\sigma'$ with $\sigma' \in G_K$ is given by

$$\begin{pmatrix} 0 & \tilde{\phi}^r(\sigma')\tilde{\phi}^{m-r}(\iota\sigma'\iota) \\ \tilde{\phi}^{m-r}(\sigma')\tilde{\phi}^r(\iota\sigma'\iota) & 0 \end{pmatrix} = \tilde{\phi}^r(\sigma'\iota\sigma'\iota) \begin{pmatrix} 0 & \tilde{\phi}^{m-2r}(\iota\sigma'\iota) \\ \tilde{\phi}^{m-2r}(\sigma') & 0 \end{pmatrix}.$$

Therefore, we see that $\rho_r \cong \mathrm{Ind}_K^{\mathbb{Q}}(V(\phi^{m-2r})) \cdot (\varepsilon_K \det \rho_f)^r$ by Lemma 3.2.

Finally, for $r = m/2$, we have

$$\sigma(x_{m/2}) = \begin{cases} \tilde{\phi}^{m/2}(\sigma\iota\sigma\iota)x_{m/2} & \text{if } \sigma \in G_K \\ \tilde{\phi}^{m/2}(\sigma'\iota\sigma'\iota)x_{m/2} & \text{if } \sigma = \iota\sigma' \text{ where } \sigma' \in G_K. \end{cases}$$

Hence, $V_{m/2} = (\varepsilon_K \det \rho_f)^{m/2}$ again by Lemma 3.2. This finishes the proof. □

COROLLARY 5.2. *The complex L-function admits a factorisation*

$$L(\mathrm{Sym}^m f, s) = \begin{cases} \left(\prod_{i=0}^{m/2-1} L(\phi^{m-2i}, (\varepsilon_K\epsilon)^i, s - i(k-1))\right) L((\varepsilon_K\epsilon)^{m/2}, s - m/2(k-1)) & \text{if } m \text{ is even,} \\ \prod_{i=0}^{(m-1)/2} L(\phi^{m-2i}, (\varepsilon_K\epsilon)^i, s - i(k-1)) & \text{otherwise.} \end{cases}$$

Proof. This can be proved in the same way as Corollary 3.4. □

REMARK 5.3. For $0 \le i \le \lfloor (m-1)/2 \rfloor$, we may obtain a p-adic L-function that interpolates the L-values of ϕ^{m-2i} at $(m-2i)(k-1)$ using Proposition 3.1. However, when $m > 2$, their product does not interpolate the L-values of $\mathrm{Sym}^m f$. We would need p-adic L-functions that interpolate the L-values of ϕ^{m-2i} at $(m-i)(k-1)$ instead.

ACKNOWLEDGEMENT. The author is extremely grateful for very helpful discussions with Daniel Delbourgo during the writing of this paper. He is indebted to Alex Bartel and Robert Harron for their useful comments on earlier versions of this paper. He is also indebted to an anonymous referee for many suggestions, which helped to improve the paper.

REFERENCES

1. J. Coates and C.-G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve, *J. Reine Angew. Math.* **375/376** (1987), 104–156.

2. A. Dabrowski, Bounded p-adic L-functions of motives at supersingular primes, *C. R. Math. Acad. Sci. Paris* **349**(7–8) (2011), 365–368.

3. A. Dabrowski and D. Delbourgo, S-adic L-functions attached to the symmetric square of a new form, *Proc. Lond. Math. Soc.* **74**(3) (1997), 559–611.

4. P. Deligne, Formes modulaires et représentations l-adiques, *Séminaire Bourbaki* 21, Exp. No. 355 (1968–1969), 139–172.

5. K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, *Astérisque* (295) (2004), ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

6. A. Lei, Iwasawa theory for modular forms at supersingular primes, *Compos. Math.* **147**(3) (2011), 803–838.

7. A. Lei, D. Loeffler and S. L. Zerbes, Wach modules and Iwasawa theory for modular forms, *Asian J. Math.* **14**(4) (2010), 475–528.

8. B. Mazur and A. Wiles, Class fields of Abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76**(2) (1984), 179–330.

9. B. Perrin-Riou, Fonctions L p-adiques d'une courbe elliptique et points rationnels, *Ann. Inst. Fourier (Grenoble)* **43**(4) (1993), 945–995.

10. B. Perrin-Riou, Zéros triviaux des fonctions L p-adiques, un cas particulier, *Compos. Math.* **114**(1) (1998), 37–76.

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

12. R. Pollack and K. Rubin, The main conjecture for CM elliptic curves at supersingular primes, *Ann. Math.* (2) **159**(1) (2004), 447–464.

13. K. Rubin, The "main conjecture" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103**(1) (1991), 25–68.