THE MÖBIUS-WALL CONGRUENCES FOR p-ADIC L-FUNCTIONS OF CM ELLIPTIC CURVES

THANASIS BOUGANIS

In this work we prove, under a technical assumption, the so-called "Möbius-Wall" congruences between abelian p-adic L-functions of CM elliptic curves. These congruences are the analogue of those shown by Ritter and Weiss for the Tate motive, and offer strong evidences in favor of the existence of non-abelian p-adic L-functions for CM elliptic curves.

1. Introduction

In [3, 4] a vast generalization of the Main Conjecture of the classical (abelian) Iwasawa theory to a non-abelian setting was proposed. As in the classical theory, the non-abelian Main Conjecture predicts a deep relation between an analytic object (a non-abelian p-adic L-function) and an algebraic object (a Selmer group or complex over a non-abelian p-adic Lie extension). However, the evidences for this non-abelian Main Conjecture are still very modest. One of the central difficulties of the theory seems to be the construction of non-abelian p-adic L-functions. Actually, the known results in this direction are mainly restricted to the Tate motive, initially for particular totally real p-adic Lie extensions (see [5, 7, 9, 10]) and later for a large family of totally real p-adic Lie extension as it is shown by Kakde [8] and in the joint work of Ritter and Weiss [10, 11].

For other motives besides the Tate motive our knowledge is more restricted. We refer to [1, 2] for an account of what is known. The main aim of this work is to tackle the question of the existence of non-abelian p-adic L-functions for "motives" associated to particular Grössencharacters of CM fields (including those associated to elliptic curves with CM). In particular we prove the so-called "Möbius-Wall" congruences, which we define below, for these motives. Without going into details, we simply mention here that these results plus the vanishing of the analytic μ-invariant of the abelian p-adic L-functions allow one to conclude the existence of a non-abelian p-adic L-function in $K_1(\widehat{\Lambda(G)_S})$ for our motives, see for example [12]. The stronger result, that the non-abelian p-adic L-function actually lies in $K_1(\Lambda(G)_S)$, as it is conjectured in [3], is a deeper fact. In the case of the Tate motive, this is known thanks to the work of Kakde, Ritter-Weiss. However the fact that the abelian Main Conjectures for all intermediate fields are known is essential for their arguments.

The "Möbius-Wall" congruences for motives: The setting is the one described in the paper of Ritter and Weiss [11]. Let p be an odd prime number. We write F for a totally real field and F' for a totally real finite Galois extension of p-power degree and we denote the associated Galois group with $\Gamma := Gal(F'/F)$. We assume that the extension is unramified outside p. Let F_i be an intermediate field of F'/F, we write $G_{F_i} := Gal(F_i(p^\infty)/F_i)$, where $F_i(p^\infty)$ is the maximal abelian extension of F_i unramified outside p (may be ramified at infinity). Our assumption on the ramification of F'/F implies that for extensions $F \subseteq F_i \subseteq F_j \subseteq F'$ there exists a transfer map $ver : G_{F_i} \to G_{F_j}$, which induces also a map $ver_{F_i}^{F_j} : \mathcal{J}[[G_{F_i}]] \to \mathcal{J}[[G_{F_j}]]$ between the Iwasawa algebras of G_{F_i} and G_{F_j}, both of them taken with coefficients in $\mathcal{J} := \widehat{\mathbb{Z}_p^{nr}}$. Here we define

$$ver_{F_i}^{F_j}|_{\mathcal{J}} := \Phi_{[F_j:F_i]},$$

where $\Phi_{[F_j:F_i]} := \phi^e$ for $p^e = [F_j : F_i]$ and $\phi \in Gal(\mathcal{J}/\mathbb{Z}_p)$ the Frobenius element.

Let us now consider a motive M/F (by which we really mean the usual realizations of it and their compatibilities) defined over F such that its p-adic realization has coefficients in $\mathcal{R}$, a subring of $\mathcal{J}$. Then under some assumptions on the critical values of M and some ordinarity assumptions at p (to be made more specific later) it is conjectured that there exists an element $\lambda_F \in \mathcal{R}[[G_F]]$ that interpolates the critical values of M/F twisted by characters of G_F. Similarly we write λ_{F_i} for the element in $\mathcal{R}[[G_{F_i}]]$ associated to M/F_i, the base change of M/F to F_i, for F_i an intermediate field of F'/F. We now introduce the Möbius function $\mu := \mu_\Gamma$ for the finite group Γ. It is defined by

$$\mu(1) = 1, \;\; \mu(\Gamma') = -\sum_{\{1\} \leq \Gamma'' < \Gamma'} \mu(\Gamma''), \;\; for \;\; \{1\} \neq \Gamma' \leq \Gamma.$$

We also write $\Gamma_i := Gal(F'/F_i)$. Then the so-called "Möbius-Wall" congruences are:

$$\sum_{F \subseteq F_i \subseteq F'} \mu(\Gamma_i) ver_{F_i}^{F'}(\lambda_{F_i}) \in T,$$

where T is the trace ideal in $\mathcal{R}[[G_{F'}]]^\Sigma$ generated by the elements $\sum_{\sigma \in \Gamma} \alpha^\sigma$ with $\alpha \in \mathcal{R}[[G_{F'}]]$, where the action of Γ on $\mathcal{R}[[G_{F'}]]$ is the extension of the action of Γ on $G_{F'}$ (by conjugation). A slight generalization of Proposition 4 in [11] gives the following equivalence.

Proposition 1.1. *The Möbius-Wall congruences*

$$\sum_{F \subseteq F_i \subseteq F'} \mu(\Gamma_i) ver_{F_i}^{F'}(\lambda_{F_i}) \in T,$$

are equivalent to the congruences:

$$\sum_{F \subseteq F_i \subseteq F'} \mu(\Gamma_i) \left(\int_{G_{F_i}} \epsilon_{F'} \circ ver_{F_i}^{F'}(x) d\lambda_{F_i}(x) \right)^{\Phi_{[F':F_i]}} \equiv 0 \mod |St_\Gamma(\epsilon_{F'})|\mathcal{R},$$

for all locally constant $\mathbb{Z}_p$-valued functions $\epsilon_{F'}$ on $G_{F'}$.

Here, following Ritter and Weiss [11], we denote by $St_\Gamma(\epsilon_{F'})$ the stabilizer of $\epsilon_{F'}$ with respect to the action of Γ given by $(\gamma \cdot \epsilon_{F'})(x) := \epsilon_{F'}(x^{\gamma^{-1}})$.

The Möbius-Wall congruences have been proved by Ritter and Weiss [11] for M/F the Tate motive. We should also remark here that Kakde showed in [8], in his proof of the non-commutative Main Conjecture for the Tate motive, a different family of congruences that, as the Möbius-Wall congruences, they also imply the existence of the non-abelian p-adic L-function for the Tate motive. In order to explain the result of our work we need to introduce some more notation. We do this next.

The general setting of this work: We keep the notations already introduced above. We now write K for a totally imaginary quadratic extension of F, that is K is a CM field. On our prime number p we put the following ordinary assumption: all primes above p in F are split in K. As before we consider a totally real finite Galois extension F' of F of p-power degree that is ramified only at p. For an intermediate field extension F_i of F'/F we define $K_i := F_iK$ and $K' := F'K$, CM fields with $K_i^+ = F_i$ and $K'^+ = F'$ respectively. We will write $\mathfrak{g}_i$ for the ring of integers of F_i and $\mathfrak{r}_i$ for the ring of integers of K_i. Now we fix, once and for all, the embeddings $incl_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $incl_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. Next we fix, with respect to the fixed embeddings $(incl_\infty, incl_p)$ an ordinary CM type Σ of K and denote this pair by (Σ, K). We recall that Σ is called ordinary when the following condition is satisfied: "whenever $\sigma \in \Sigma$ and $\lambda \in \Sigma^\rho$ (ρ is the complex conjugation), the p-adic valuations induced from the p-adic embeddings $incl_p \circ \sigma$ and $incl_p \circ \lambda$ are inequivalent". We note that the splitting condition on p implies the existence of such an ordinary CM type. We consider the induced types Σ_i of Σ to K_i. That is, we fix a CM type for K_i such that for every $\sigma \in \Sigma_i$ we have that its restriction $\sigma_{|K}$ to K lies in Σ. We write (Σ_i, K_i) for this CM type, and we remark that this is also an ordinary CM type. Similarly we define the ordinary CM pair (Σ', K'). In addition to the splitting condition we also impose the condition that the reflex field E of (K, Σ) (and hence of all pairs (K_i, Σ_i) since it is the same) has the property that $E_w = \mathbb{Q}_p$, where w's are the places of E corresponding to the embeddings $E \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. For example this is the case if p does not ramify in F or if the type (K, Σ) is the lift of a type (K_0, Σ_0) where K_0 is a quadratic imaginary field, such that K/K_0 is a Galois extension and p splits in K_0.

Now we are ready to define the motives M/F that appear in this work. Let ψ be a Hecke character of K and assume that its infinite type is $k\Sigma$ for some integer $k \geq 1$. Moreover we assume that the p-adic realization of ψ takes values in $\mathbb{Z}_p^\times$. We write $M(\psi)/F$ for the motive over F that is obtained by "Weil Restriction" to F from the rank one motive over K associated to ψ. In particular we have that $L(M(\psi)/F, s) = L(\psi, s)$ or more generally for a finite character χ of G_F we have

$$L(M(\psi) \otimes \chi, s) = L(\psi\tilde{\chi}, s),$$

where $\tilde{\chi} = \chi \circ N_{K/F}$, the base change of χ to $G(K(p^\infty)/K)$. We note that this family of motives inlcudes the case of an elliptic curve over F with complex multiplication (then $k = 1$).

Now we consider the character $\psi_i := \psi \circ N_{K_i/K}$, the base change of ψ from K to K_i. It is a Hecke character of infinite type $k\Sigma_i$. Moreover we have that $M(\psi_i)/F'$ is the base change of $M(\psi)/F$ to F_i. We now make the following technical assumption:

Assumption: The q-expansion principle in its p-adic integral form holds for all the groups $U(1,1)/F_i$ with $F \subseteq F_i \subseteq F'$.

Then in this work we prove that for $M/F := M(\psi)/F$ we have the congruences

$$\sum_{F\subseteq F_i\subseteq F'} \mu(\Gamma_i)\left(\int_{G_{F_i}} \epsilon_{F'}\circ ver^{F'}_{F_i}(x)d\lambda_{F_i}(x)\right)(\Omega_p(K_i,\Sigma_i))^{\Phi_{[F':F_i]}} \equiv 0 \mod |St_{\Gamma}(\epsilon_{F'})|\mathcal{J},$$

for all locally constant $\mathbb{Z}_p$-valued functions $\epsilon_{F'}$ on $G_{F'}$. Here we recall that $\Omega_p(K_i,\Sigma_i) = \Omega(K,\Sigma)^{[F_i:F]}$, where $\Omega(K,\Sigma)\in\mathcal{J}^{\times}$ the p-adic periods attached to the CM pair (K,Σ) (see [1, 2]). In particular if we set $\lambda^*_{F_i} := \Omega_p(K_i,\Sigma_i)\cdot\lambda_{F_i} \in \mathcal{J}[[G_{F_i}]]$, then these congruences and Proposition 1.1 give the following theorem.

Theorem 1.2. *For the motive $M(\psi)/F$ and the extension F'/F the Möbius-Wall congruences hold for the "modified" abelian p-adic L-functions $\lambda^*_{F_i}$. That is we have,*

$$\sum_{F\subseteq F_i\subseteq F'} \mu(\Gamma_i) ver^{F'}_{F_i}(\lambda^*_{F_i}) \in T.$$

Let now G be a compact p-adic Lie group and F_∞/F a totally real extension of F with $G\cong Gal(F_\infty/F)$. We assume that G contains a closed normal subgroup H such that $G/H\cong\mathbb{Z}_p$. We assume moreover that the analytic μ invariant of all abelian p-adic L functions λ_{F_i} is zero. Here λ_{F_i} are the abelian p-adic L-functions which appear in the congruences. Then our theorem in combination with the works of Kakde, Ritter and Weiss (see [12]) implies the existence of an element $\mathcal{L}_{M(\psi)}\in K_1(B)$, where $B := \widehat{\Lambda_{\mathcal{J}}(G)_S}$ is the $Jac(\Lambda_{\mathcal{J}}(H))$-adic complection of $\Lambda_{\mathcal{J}}(G)_S$, with the property that for any Artin representation ρ of G we have

$$\mathcal{L}_M(\rho) = \Omega_p(K,\Sigma)^{dim(\rho)}L^*(M(\psi),\rho,1),$$

where

$$L^*(M(\psi),\rho,1) := \frac{L_{\mathcal{S}\cup\{\mathfrak{p}|p\}}(M(\psi),\rho,1)}{\Omega(K,\Sigma)^{dim(\rho)}}\prod_{\mathfrak{p}}\left(e_{\mathfrak{p}}(M(\psi),\rho)\mathcal{L}_{\mathfrak{p}}(M(\psi),\rho)\right),$$

with $e_{\mathfrak{p}}(M(\psi),\rho)$, $\mathcal{L}_{\mathfrak{p}}(M(\psi),\rho)$ local epsilon and L-factors and $L_{\mathcal{S}\cup\{\mathfrak{p}|p\}}(M(\psi),\rho,s)$ the L function of $M(\psi)\times\rho$ with the Euler factors above p and in a finite set $\mathcal{S}$, depending on G, removed (see [3] and [4] for all these). For the element $\Omega_p := \Omega_p(K,\Sigma)\cdot 1_G \in \Lambda_{\mathcal{J}}(G)^{\times}\subset K_1(B)$ we have $\Omega_p(\rho) = \Omega_p(K,\Sigma)^{dim(\rho)}$. Hence if we consider $\mathcal{L}^*_M := \Omega_p^{-1}\mathcal{L}_M\in K_1(B)$, then this element has the interpolation property,

$$\mathcal{L}^*_M(\rho) = L^*(M(\psi),\rho,1).$$

This element has the conjectured interpolation properties but we had to consider the Iwasawa algebra $\Lambda_{\mathcal{J}}(G)$, that is with coefficients in $\mathcal{J}$. However as it is explained by Ritter and Weiss [11] such an element implies the Möbius-Wall congruences for the "untwisted" abelian p-adic L-functions. That is we have the Möbius-Wall congruences

$$\sum_{F\subseteq F_i\subseteq F'} \mu(\Gamma_i) ver^{F'}_{F_i}(\lambda_{F_i}) \in T \subseteq \mathbb{Z}_p[[G_{F'}]]^{\Gamma}.$$

Again by the general theory of Kakde, Ritter and Weiss, these congruences now in turn imply the existence of an element $\mathcal{L}^{**}\in K_1(\widehat{\Lambda(G)_S})$ with the conjectured interpolation properties and with the right coefficients (i.e. $\mathbb{Z}_p$) for the Iwasawa algebra.

2. Congruences between p-adic L-functions

For any set X with an action of Γ we write $St_\Gamma(x) \leq \Gamma$ for the stabilizer of an $x \in X$. Moreover for any CM field K we will write $S(K)$ for the hermitian matrices with entries in K.

2.1. **Congruences between Siegel-type Eisenstein series:** Let ϵ be a locally constant $\mathbb{Z}_p$-valued function on $G_{K'}(p^\infty)$. We define $\psi_i := \psi \circ N_{K_i/K}$ and $\epsilon_i := \epsilon \circ ver_{K_i}^{K'}$. And we also write ψ' for the character $\psi \circ N_{K'/K}$. In [6] (see also [2, pages 23-24]) a Siegel-type Eisenstein series of the unitary group $U(1,1)/F_i$ is associated to these data. Following the notation of [2, 6] we write

$$E_{K_i} := E_{K_i}(z, m(A), \epsilon_i\psi_i),$$

where $A \in GL_n(\mathbb{A}_K^{(p)}) \times GL_n(\mathfrak{r} \otimes \mathbb{Z}_p)$, for $\mathfrak{r}$ the ring of integers of K. Our assumptions on the CM types (K_i, Σ_i) allow us to define the diagonal embedding $\Delta_i : \mathbb{H}_K \hookrightarrow \mathbb{H}_{K_i}$, where here $\mathbb{H}_{K_i}$ (resp. $\mathbb{H}_K$) is the symmetric space associated to the group $U(1,1))/F_i$ (resp. $U(1,1)/F$). Using this map we can define by pull back a map of hermitian modular forms of $U(1,1)/F_i$ to hermitian modular forms of $U(1,1)/F$. We write $res_K^{K_i}$ for this map. We then define the Eisestein series of $U(1,1)/F$

$$E_i := Frob_{[K':K_i]} res_K^{K_i} E_{K_i} \ \ and \ \ E_0 := Frob_{[K':K]} E_K.$$

Here $Frob_{p^m}$ is the standard Frobenius action on hermitian modular forms. In particular for a q-expansion $f(q) = \sum_\beta a(f,\beta)q^\beta$ we have $Frob_{p^m} f(q) = \sum_\beta a(f,\beta)q^{p^m\beta}$. The next proposition is stated for Siegel-type Eisenstein series of $U(1,1)$. However we believe that it is true in a more general setting, namely for Eisenstein series of $U(n,n)$. As we will explain later the proof of the general case demands the investigation of some Siegel series that appear in the theory of Eisenstein series. These phenomena are simplified in the case $n = 1$. Finally we remark that our proof is based on ideas of Ritter and Weiss [11].

Proposition 2.1. (*Congruences of Eisenstein series of* $U(1,1)$) *We have the congruences of Eisenstein series:*

$$\mathcal{E} := \sum_{K \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_i \equiv 0 \mod |St_\Gamma(\epsilon)|\mathbb{Z}_p$$

Proof. We start the proof in the general setting of Eisenstein series of $U(n,n)$. Later in the proof we will take $n = 1$. If we write the q-expansion

$$E_{K_i}(z, m(A), \epsilon_i\psi_i) = \sum_{\beta_i \in S(K_i)} E_{\beta_i}(m(A), \epsilon_i\psi_i) q^{\beta_i},$$

where $S(K_i) = \{x \in GL_n(K_i) | {}^t x^\rho = x\}$, with $1 \neq \rho \in Gal(K_i/F_i)$, then we have that

$$res_K^{K_i} E_{K_i} = \sum_{\beta \in S(K)} \left(\sum_{Tr_{K_i/K}(\beta_i) = \beta} E_{\beta_i}(m(A), \epsilon_i\psi_i) \right) q^\beta,$$

and hence

$$E_i := Frob_{[K':K_i]} res_K^{K_i} E_{K_i} = \sum_{\beta \in S(K)} \left(\sum_{Tr_{K_i/K}(\beta_i)=\beta} E_{\beta_i}(m(A), \epsilon_i \psi_i) \right) q^{[K':K_i]\beta}.$$

For a hermitian matrix $\beta \in S(K)$ we define the following sets of pairs of matrices and integral ideals

$$[\beta]_i := \{(\beta_i, \mathfrak{a}_i) | \beta_i \in S(K_i),\ det({}^t\bar{A}\beta_i A) \in \mathfrak{a}_i,\ Tr_{K_i/K}(\beta_i) = \frac{1}{[K':K_i]}\beta\},$$

and

$$[\beta] := \{(\beta', \mathfrak{a}') |\ \beta' \in S(K'),\ det({}^t\bar{A}\beta' A) \in \mathfrak{a}',\ Tr_{K'/K}(\beta') = \beta\}.$$

By [6] (see also [2, page 24]) we have that the coefficients $E_{\beta_i}(m(A), \epsilon_i\psi_i)$ are of the form

$$E_{\beta_i}(m(A), \epsilon_i\psi_i) = \sum_{det({}^t\bar{A}\beta_i A) \in \mathfrak{a}_i \subseteq \mathfrak{g}_i} n_{\mathfrak{a}_i}(\beta_i, A) f_i(\beta_i, \mathfrak{a}_i) \psi_i(\mathfrak{a}_i) N_{F_i/F}(\mathfrak{a}_i)^{k-n},$$

for some function f_i on the hermitian matrices and on the fractional ideals of F_i with the property that we have $f_i = f \circ ver_{F_i}^{F'}$, where the function f, as a function on the hermitian matrices and on the fractional ideals of F', is invariant under the operation of Γ. In particular for a hermitian matrix β with entries in K_i and a fractional ideal $\mathfrak{a}$ of F_i we have $f_j(\beta, \mathfrak{a}\mathfrak{g}_j) = f_i(\beta, \mathfrak{a})$.

Then the β^{th} Fourier-coefficient of $\mathcal{E}$ is given by

$$\sum_{K \subseteq K_i \subseteq K'} \mu(\Sigma_i) \sum_{Tr_{K_i/K}(\beta_i) = \frac{1}{[K':K_i]}\beta} E_{\beta_i}(m(A), \epsilon_i\psi_i) =$$

$$\sum_{K \subseteq K_i \subseteq K'} \mu(\Sigma_i) \sum_{(\beta_i, \mathfrak{a}_i) \in [\beta]_i} n_{\mathfrak{a}_i}(\beta_i, A) f_i(\beta_i, \mathfrak{a}_i) \psi_i(\mathfrak{a}_i) N_{F_i/F}(\mathfrak{a}_i)^{k-n}$$

We note that the set $[\beta]_i$ is empty when $[K' : K_i]$ does not divide the matrix β, since all the β_i coefficients are p-integral (see [6, page 63]. We have the obvious embedding $\imath_{K_i} : [\beta]_i \hookrightarrow [\beta]$ induced by the embedding $K_i \hookrightarrow K'$. Indeed for a pair $(\beta_i, \mathfrak{a}_i) \in [\beta]_i$ we have that

$$Tr_{K'/K}(\beta_i) = [K' : K_i] Tr_{K_i/K}(\beta_i) = [K' : K_i] \frac{1}{[K' : K_i]}\beta = \beta.$$

The map on the ideals is given by $\mathfrak{a}_i \mapsto \mathfrak{a}_i\mathfrak{g}'$ and has obviously the needed properties. Or more general for $K_i \hookrightarrow K_j$ we have $\imath_{ij} : [\beta]_i \hookrightarrow [\beta]_j$ since

$$Tr_{K_j/K}(\beta_i) = [K_j : K_i] Tr_{K_i/K}(\beta_i) = [K_j : K_i] \frac{1}{[K' : K_i]}\beta = \frac{1}{[K' : K_j]}\beta.$$

The group Γ acts on $[\beta]$ and we have that $[\beta]_i = [\beta]^{\Gamma_i}$. In particular the β^{th} coefficient of $\mathcal{E}$ may be rewritten as

$$\sum_{K \subseteq K_i \subseteq K'} \mu(\Sigma_i) \sum_{(\beta_i, \mathfrak{a}_i) \in [\beta]^{\Gamma_i}} n_{\mathfrak{a}_i}(\beta_i, A) f_i(\beta_i, \mathfrak{a}_i) \psi_i(\mathfrak{a}_i) N_{F_i/F}(\mathfrak{a}_i)^{k-n} \quad (*).$$

From the sum above we pick now the part that corresponds to a fixed pair $(\beta', \mathfrak{a}') \in [\beta]$. It is given by

$$\sum_{K_i \ so \ \Gamma_i \leq St_\Gamma((\beta',\mathfrak{a}'))} \mu(\Gamma_i) n_{\mathfrak{a}_i}(\beta_i, A) f_i(\beta_i, \mathfrak{a}_i)\psi_i(\mathfrak{a}_i) N_{F_i/F}(\mathfrak{a}_i)^{k-n},$$

where for each i we write $\beta_i = \beta' \in S(K_i)$ and $\mathfrak{a}_i \subset F_i$ such that $\mathfrak{a}_i\mathfrak{g}' = \mathfrak{a}'$. By the properties of the functions f_i the above sum can also written as

$$\sum_{K_i \ so \ \Gamma_i \leq St_\Gamma((\beta',\mathfrak{a}'))} \mu(\Gamma_i) n_{\mathfrak{a}_i}(\beta_i, A) f(\beta', \mathfrak{a}')\psi'(\mathfrak{a}')^{\frac{1}{[K':K_i]}} N_{F'/F}(\mathfrak{a}')^{\frac{k-n}{[K':K_i]}}.$$

Now we restrict ourselves to the case $n = 1$. In this case we have that $n_{\mathfrak{a}_i}(\beta_i, A) = 1$ (see [6, page 53]). In particular the above sum is now written as

$$\sum_{K_i \ so \ \Gamma_i \leq St_\Gamma((\beta',\mathfrak{a}'))} \mu(\Gamma_i) f(\beta', \mathfrak{a}')\psi'(\mathfrak{a}')^{\frac{1}{[K':K_i]}} N_{F'/F}(\mathfrak{a}')^{\frac{k-1}{[K':K_i]}},$$

For an element $\gamma \in \Gamma$ we have that the part of the summation in $(*)$ corresponding to $(\beta'^{\gamma}, \mathfrak{a}'^{\gamma})$ is given by

$$\sum_{K_i \ so \ \Gamma_i \leq St_\Gamma(\beta'^{\gamma},\mathfrak{a}'^{\gamma})} \mu(\Gamma_i) f(\beta'^{\gamma}, \mathfrak{a}'^{\gamma})\psi'(\mathfrak{a}'^{\gamma})^{\frac{1}{[K':K_i]}} N_{F'/F}(\mathfrak{a}'^{\gamma})^{\frac{k-1}{[K':K_i]}} =$$

$$\sum_{K_i \ so \ \Gamma_i \leq St_\Gamma(\beta'^{\gamma},\mathfrak{a}'^{\gamma})} \mu(\Gamma_i) f(\beta', \mathfrak{a}')\psi'(\mathfrak{a}')^{\frac{1}{[K':K_i]}} N_{F'/F}(\mathfrak{a}')^{\frac{k-1}{[K':K_i]}}$$

since f is invariant with respect to the operation of Γ. Considering the $St_\Gamma(\epsilon)$ orbit of all these partial sums we obtain the sum

$$\sum_{\gamma \in (St_\Gamma(\epsilon) \cap St_\Gamma(\beta',\mathfrak{a}') \backslash St_\Gamma(\epsilon))} f(\beta', \mathfrak{a}') \sum_{K_i, \ so \ \Gamma_i \leq St_\Gamma(\beta'^{\gamma},\mathfrak{a}'^{\gamma})} \mu(\Gamma_i)\psi'(\mathfrak{a}')^{\frac{1}{|\Gamma_i|}} N_{F'/F}(\mathfrak{a}')^{\frac{k-1}{|\Gamma_i|}}.$$

As in [11] in order to conclude the congruences we have to show that

$$\sum_{K_i, \ so \ \Gamma_i \leq St_\Gamma(\beta'^{\gamma},\mathfrak{a}'^{\gamma})} \mu(\Gamma_i)\psi'(\mathfrak{a}')^{\frac{1}{|\Gamma_i|}} N_{F'/F}(\mathfrak{a}')^{\frac{k-1}{|\Gamma_i|}} \equiv 0 \mod |St_\Gamma(\epsilon) \cap St_\Gamma(\beta', \mathfrak{a}')|\mathbb{Z}_p,$$

We set $r := \psi'(\mathfrak{a}')^{\frac{1}{|St_\Gamma(\beta',\mathfrak{a}')|}} N_{F'/F}(\mathfrak{a}')^{\frac{k-1}{|St_\Gamma(\beta',\mathfrak{a}')|}} \in \mathbb{Z}_p^\times$. If we set $P := |St_\Gamma(\beta', \mathfrak{a}')|$ then the needed congruences follow from the following "CLAIM" of [11, page 9].

Lemma 2.2. *Let P be a finite p-group and r be in $\mathbb{Z}_p^\times$. Then*

$$\sum_{1 \leq P' \leq P} \mu(P') r^{[P:P']} \equiv 0 \mod |P|\mathbb{Z}_p.$$

Remark: In [11] the congruences of the "CLAIM" are in $\mathbb{Z}_{(p)}$ but it is easy to see that the exact same proof gives also the congruences above.

With this lemma we can now conclude the proof of the proposition.

□

Remark on the case $n > 1$: If we consider the more general case, that is n larger than one, then the coefficients $n_{\mathfrak{a}_i}(\beta, A)$ above are not trivial. Then we need to understand the relation between these coefficients for various i's (that is of different fields K_i). For example we may ask whether we have an equality of the form $n_{\mathfrak{a}_i}(\beta_i, A_i) = n_{\mathfrak{a}_j}(\beta_j, A_j)$ for $\mathfrak{a}_j, \beta_j$ and A_j the images of $\mathfrak{a}_i, \beta_i$ and A_i with respect to the natural embedding $K_i \hookrightarrow K_j$.

2.2. **Congruences between special values.** For a locally constant function $\epsilon_{F'}$ of $G_{F'}$, we write $\epsilon := \epsilon_{F'} \circ N_{K'/F'}$, that is the base-change of $\epsilon_{F'}$ to K'. We are going to use Proposition 2.1 to prove our main theorem under the assumption that for $K_i \hookrightarrow K_j$ we have $CM(K_i) = CM(K_j)^{Gal(K_j/K_i)}$. As it is explained in [2, Proposition 6.3] this can be achieved under some mild assumptions on the conductor of ψ. Here by $CM(K_i)$ we denote the set of CM points (plus arithmetic information) of $U(1,1)/F_i$ such that

$$\Omega_p(K_i, \Sigma_i) L^*(M(\psi_i)/F_i, \epsilon_{F'} \circ ver^{F'}_{F_i}) := \Omega_p(K_i, \Sigma_i) \int_{G_{F_i}} \epsilon_{F'} \circ ver^{F'}_{F_i}(x) d\lambda_{F_i}(x)$$

$$= \sum_{P \in CM(K_i)} E_{K_i}(P),$$

where in the definition of E_{K_i} the matrix $m(A)$ is determined from the CM point P and the locally constant functions are those obtained from ϵ. Here P is just the notation for the tuple (A, j) where A is an abelian variety with CM by a particular CM algebra and j is a p^∞-aritmetic stracture. For the details of all these we refer to [2] and especially to the proof of Theorem 4.1 in [2]. We remark here again that we have the following relation between the p-adic periods $\Omega_p(K_i, \Sigma_i)$:

$$\Omega_p(K_i, \Sigma_i) = \Omega_p(K, \Sigma)^{[K_i:K]}$$

We now prove the following theorem.

Theorem 2.3. *For $M/F := M(\psi)/F$ we have the congruences*

$$\sum_{F \subseteq F_i \subseteq F'} \mu(\Gamma_i) L^*(M/F_i, \epsilon_{F'} \circ ver^{F'}_{F_i}) (\Omega_p(K_i, \Sigma_i))^{\Phi_{[K':K_i]}} \equiv 0 \mod |St_\Gamma(\epsilon_{F'})| \mathcal{J},$$

for all locally constant $\mathbb{Z}_p$-valued functions $\epsilon_{F'}$ on $G_{F'}$.

Proof. We start by considering the sum,

$$\sum_{P \in CM(K)} \mathcal{E}(P) = \sum_{P \in CM(K)} \sum_{K \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_i(P) =$$

$$\sum_{P \in CM(K)} \mu(\Gamma) E_0(P) + \sum_{P \in CM(K)} \sum_{K \subset K_i \subseteq K'} \mu(\Gamma_i) E_i(P) =$$

$$\mu(\Gamma) \left(L^*(M/F, \epsilon_{F'} \circ ver^{F'}_{F}) \Omega_p(K, \Sigma) \right)^{\Phi_{[K':K]}} + \sum_{P \in CM(K)} \sum_{K \subset K_i \subseteq K'} \mu(\Gamma_i) E_i(P) =$$

$$\mu(\Gamma) L^*(M/F, \epsilon_{F'} \circ ver^{F'}_{F}) \Omega_p(K, \Sigma)^{\Phi_{[K':K]}} + \sum_{P \in CM(K)} \sum_{K \subset K_i \subseteq K'} \mu(\Gamma_i) E_i(P),$$

since $L^*(M/F,\epsilon_{F'}\circ ver_F^{F'})\in\mathbb{Z}_p$ because of our assumptions on the coefficients of the p-adic realization of $M(\psi)$ and the fact that $\epsilon_{F'}$ is $\mathbb{Z}_p$ valued. We also note that the third equality follows from the reciprocity law on CM points [2, Proposition 6.2]. By Proposition 2.1 we have that this sum is congruent to zero modulo $|St_\Gamma(\epsilon)|$. That is,

$$\mu(\Gamma)L^*(M/F,\epsilon_{F'}\circ ver_F^{F'})\Omega_p(K,\Sigma)^{\Phi_{[K':K]}}+\sum_{P\in CM(K)}\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)E_i(P)\equiv 0 \mod |St_\Gamma(\epsilon)|\mathcal{J}.$$

In order to conclude the theorem we need to show that

$$\sum_{P\in CM(K)}\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)E_i(P)\equiv$$

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)L^*(M/F_i,\epsilon_{F'}\circ ver_{F_i}^{F'})(\Omega_p(K_i,\Sigma_i))^{\Phi_{[K':K_i]}} \mod |St_\Gamma(\epsilon)|\mathcal{J}.$$

So, it suffices to prove,

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)\sum_{P\in CM(K)}E_i(P)\equiv$$

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)L^*(M/F_i,\epsilon_{F'}\circ ver_{F_i}^{F'})(\Omega_p(K_i,\Sigma_i))^{\Phi_{[K':K_i]}} \mod |St_\Gamma(\epsilon)|\mathcal{J}.$$

But we know that

$$L^*(M/F_i,\epsilon_{F'}\circ ver_{F_i}^{F'})(\Omega_p(K_i,\Sigma_i))^{\Phi_{[K':K_i]}}=L^*(M/F_i,\epsilon_{F'}\circ ver_{F_i}^{F'})^{\Phi_{[K':K_i]}}(\Omega_p(K_i,\Sigma_i))^{\Phi_{[K':K_i]}}$$

$$=\left(\sum_{P\in CM(K_i)}E_{K_i}(P)\right)^{\Phi_{[K':K_i]}}=\sum_{P\in CM(K)}Frob_{[K':K_i]}res_K^{K_i}E_{K_i}(P)$$

$$+\sum_{P\in CM(K_i)\backslash CM(K)}Frob_{[K':K_i]}E_{K_i}(P),$$

where the second sum runs over the CM points $CM(K_i)$ excluding all those "coming" from the embedding $K\hookrightarrow K_i$. In particular we have that

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)L^*(M/F_i,\epsilon_{F'}\circ ver_{F_i}^{F'})(\Omega_p(K_i,\Sigma_i))^{\Phi_{[K':K_i]}}=$$

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)\left(\sum_{P\in CM(K)}E_i(P)+\sum_{P\in CM(K_i)\backslash CM(K)}Frob_{[K':K_i]}E_{K_i}(P)\right)$$

Hence, in order to prove the theorem, we need to show that

$$\sum_{K\subset K_i\subseteq K'}\mu(\Gamma_i)\sum_{P\in CM(K_i)\backslash CM(K)}Frob_{[K':K_i]}E_{K_i}(P)\equiv 0 \mod |St_\Gamma(\epsilon)|.$$

We now note that for $K_i\subset K_j$ we have $CM(K_i)=CM(K_j)^{Gal(K_j/K_i)}$. In particular the above equation is equivalent to

$$\sum_{P\in CM(K')\backslash CM(K)}\sum_{K_P\subseteq K_i\subseteq K'}\mu(\Gamma_i)E_{i,K_P}(P)\equiv 0 \mod |St_\Gamma(\epsilon)|,$$

where for a point $P \in CM(K')$ we write $K_P \subseteq K'$ for its (smallest) field of definition and $E_{i,K_P} := Frob_{[K':K_i]} res^{K_i}_{K_P} E_{K_i}$. We already know by Proposition 2.1 (by taking K_P as K there) that

$$\sum_{K_P \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_{i,K_P} \equiv 0 \mod |St_{\Gamma_{K_P}}(\epsilon)|$$

and hence after evaluating at the CM point P we have

$$\sum_{K_P \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_{i,K_P}(P) \equiv 0 \mod |St_{\Gamma_{K_P}}(\epsilon)|.$$

We also know that in the set $CM(K')$ the orbit of the point P is of size $|\Gamma|/|\Gamma_{K_P}|$. In particular, if we write $[P]$ for the orbit of a point P, then we have the equation

$$\sum_{P \in CM(K') \setminus CM(K)} \sum_{K_P \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_{i,K_P}(P) =$$

$$\sum_{[P] \in CM(K') \setminus CM(K)} \frac{|\Gamma|}{|\Gamma_{K_P}|} \sum_{K_P \subseteq K_i \subseteq K'} \mu(\Gamma_i) E_{i,K_P}(P),$$

since we have $E_{i,K_P}(P_1) = E_{i,K_P}(P_2)$ for all $P_1, P_2 \in [P]$ (see [2, Proposition 7.9 and Corollary 7.10]). But we have that $|St_\Gamma(\epsilon)|$ divides $|St_{\Gamma_{K_P}}(\epsilon)| \times \frac{|\Gamma|}{|\Gamma_{K_P}|}$, which allows us to conclude the congruences. The last statement follows by observing first that $St_{\Gamma_{K_P}}(\epsilon) = St_\Gamma(\epsilon) \cap \Gamma_{K_P}$ and

$$|St_{\Gamma_{K_P}}(\epsilon)| \times \frac{|\Gamma|}{|\Gamma_{K_P}|} = \frac{|St_\Gamma(\epsilon)| \times |\Gamma_{K_P}|}{|St_\Gamma(\epsilon)\Gamma_{K_P}|} \times \frac{|\Gamma|}{|\Gamma_{K_P}|} = \frac{|St_\Gamma(\epsilon)| \times |\Gamma|}{|St_\Gamma(\epsilon)\Gamma_{K_P}|}.$$

But $|St_\Gamma(\epsilon)\Gamma_{K_P}|$ divides $|\Gamma|$. Indeed $|St_\Gamma(\epsilon)\Gamma_{K_P}|$ is a power of p since Γ is a p-group and $|St_\Gamma(\epsilon)\Gamma_{K_P}|$ divides $|St_\Gamma(\epsilon)| \times |\Gamma_{K_P}|$. But we have that $St_\Gamma(\epsilon)\Gamma_{K_P} \subseteq \Gamma$. $\square$

Acknowledgments: The author acknowledges support by the ERC.

References

[1] Th. Bouganis, Non-abelian congruences between special values of L-fucntions of elliptic curves; the CM case, *International Journal of Number Theory, Vol. 7, No. 7 (2011)*, pp 1883-1934.

[2] Th Bouganis, Non abelian p-adic L-functions and Eisenstein series of unitary groups; the CM-method. arXiv:1107,1377v2[math.NT] (submitted)

[3] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, The GL_2-main conjecture for elliptic curves without complex multiplication, Publ. Math. IHES. 101 (2005), no. 1, 163-208

[4] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory, Proceedings of the St. Petersburg Mathematical Society, vol XII (Providence RI), Amer. Math. Soc. Transl. Ser. 2 vol 219, 2006

[5] T. Hara, Iwasawa theory of totally real fields for certain non-commutative p-extensions, J. Number Theory 130 (4), 1068-1097 (2010)

[6] M. Harris, J.-S. Li, and C. Skinner, p-adic L-functions for unitary Shimura varieties, I: Construction of the Eisenstein measure, *Documenta Math.*, Extra Volume: John H.Coates' Sixtieth Birthday 393-464 (2006)

[7] M. Kakde, Proof of the main conjecture of non-commutative Iwasawa theory of totally real number fields in certain cases, J. Algebr. Geom. 20. 631-683 (2011)

[8] M. Kakde, Proof of the main conjecture of non-commutative Iwasawa theory of totally real number fields, Inventiones mathematicae, DOI 10.1007/s00222-012-0436-x, (2012)

[9] K. Kato, Iwasawa theory of totally real fields for Galois extensions of Heisenberg type, preprint.

[10] J. Ritter and A. Weiss, Congruences between abelian pseudomeasures, *Math. Res. Lett.* 15 (2008) 715-725

[11] J. Ritter and A. Weiss, Congruences between abelian pseudomeasures II, arXiv:1001.2091v1[math.NT].

[12] O. Venjakob, On the work of Ritter and Weiss in Comparison with Kakde's Approach, in Non-commutative Iwasawa Main Conjectures over Totally Real Fields, ed. J. Coates et al. Springer Proceedings in Mathematics and Statistics, vol 29, Springer (2013)

Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany.

E-mail address: bouganis@mathi.uni-heidelberg.de