Congruences between abelian p-adic zeta functions

Mahesh Kakde

This article is a reproduction of lectures in the workshop based on section 6 of [Kak10] with a slight change in the notation to make it consistent with previous articles in the volume. Let p be an odd prime. Let F be a totally real number field. Let F_∞ be an admissible p-adic Lie extension of F satisfying the Iwasawa conjecture (see [Coa11]). To prove the main conjecture (theorem 5.1 [Coa11]) we need to prove it (by virtue of the reductions [Suj11]; more precisely theorems 3.3, 3.8, 3.15 and 3.17 in [Suj11]) only for admissible p-adic Lie extension F_∞/F satisfying the Iwasawa conjecture such that $Gal(F_\infty/F) = \Delta \times \mathscr{G}$, where $\mathscr{G}$ is a pro-p p-adic Lie group of dimension one and Δ is a finite cyclic group of order prime to p.

1 Notations

For a pro-finite group P and a ring O, we let

$$\Lambda_O(P) := \varprojlim_U O[P/U],$$

where U runs through open normal subgroups of P. We denote $\Lambda_{\mathbb{Z}_p[\Delta]}(P)$ simply by $\Lambda(P)$. Note that $\Lambda(P) = \Lambda_{\mathbb{Z}_p}(\Delta \times P)$ (**Warning:** this notation is inconsistent with [Coa11]). We use results and notations from [Sch11]. The results in $loc.\ cit.$ are proven for $\Lambda_O(\mathscr{G})$, where O is the ring of integers in a finite unramified extension of $\mathbb{Q}_p$. It is easy to see that the statements and the proofs in $loc.\ cit.$ extend easily to $\Lambda(\mathscr{G}) = \Lambda_{\mathbb{Z}_p[\Delta]}(\mathscr{G})$ because the ring $\mathbb{Z}_p[\Delta]$ decomposes into direct sum of rings of integers in finite unramified extensions of $\mathbb{Q}_p$. Let $H := Gal(F_\infty/F^{cyc})$ and $\Gamma := Gal(F^{cyc}/F)$. Then

---

Mahesh Kakde
King's College London, Strand, London, e-mail: mkakde@kcl.ac.uk

$$S := \{f \in \Lambda(\mathscr{G}) : \Lambda(\mathscr{G})/\Lambda(\mathscr{G})f \text{ is a f.g. } \Lambda_{\mathbb{Z}_p}(H) - \text{module}\}$$

Then according to [Coa05] S is an Ore set in $\Lambda(\mathscr{G})$ consisting of regular elements. Hence we form the localisation $A(\mathscr{G}) := \Lambda(\mathscr{G})_S$ as well as its $Jac(\Lambda_{\mathbb{Z}_p}(H))$-adic completion

$$B(\mathscr{G}) = \widehat{A(\mathscr{G})}.$$

We fix an open central pro-cyclic subgroup Z of $\mathscr{G}$. Let $S(\mathscr{G},Z)$ be the set of all subgroups U of $\mathscr{G}$ such that $Z \subset U$ and let $C(\mathscr{G},Z)$ be the set of all $U \in S(\mathscr{G},Z)$ such that U/Z is cyclic. For $U \in C(\mathscr{G},Z)$ put

$$P_c(U) = \{W \in C(\mathscr{G},Z) : [W : U] = p\}.$$

We have a maps

$$\theta : K_1'(\Lambda(\mathscr{G})) \to \prod_{U \in S(\mathscr{G},Z)} \Lambda(U^{ab})^\times$$

$$\theta_A : K_1'(A(\mathscr{G})) \to \prod_{U \in S(\mathscr{G},Z)} A(U^{ab})^\times$$

and

$$\theta_B : K_1'(B(\mathscr{G})) \to \prod_{U \in S(\mathscr{G},Z)} B(U^{ab})^\times$$

defined in [Sch11]. Recall also the subgroups

$$\Phi := \Phi_Z^{\mathscr{G}} \subset \prod_{U \in S(\mathscr{G},Z)} \Lambda(U^{ab})^\times,$$

$$\Phi_A := (\Phi_Z^{\mathscr{G}})_A \subset \prod_{U \in S(\mathscr{G},Z)} A(U^{ab})^\times$$

and

$$\Phi_B := (\Phi_Z^{\mathscr{G}})_B \subset \prod_{U \in S(\mathscr{G},Z)} B(U^{ab})^\times$$

defined by conditions M1-M4 in *loc. cit.*.

We denote the field $F_\infty^{\Delta \times U}$ by F_U and denote the field $F_\infty^{[U,U]}$ by K_U. Then K_U/F_U is an abelian extension with $Gal(K_U/F_U) = \Delta \times U^{ab}$. Note that $F_{N_{\mathscr{G}}U} \subset F_U$ and $Gal(F_U/F_{N_{\mathscr{G}}U}) \cong N_{\mathscr{G}}U/U =: W_{\mathscr{G}}U$. We denote the Deligne-Ribet, Cassou-Nogues, Barsky p-adic zeta function for the abelian extension K_U/F_U by ζ_U. It is an element in $A(U^{ab})^\times$. Let ζ_0 be the p-adic zeta function of the extension $F_\infty/F_\infty^{\Delta \times Z^p}$. Recall that we have fixed a finite set Σ of finite primes of F containing all primes which ramify in F_∞. Let Σ_U denote the set of primes of F_U lying above Σ. Let $r_U := [F_U : \mathbb{Q}]$ and $d_U = [F_U : F]$. If a group P acts on a set X, then we denote the stabiliser of $x \in X$ by P_x.

Let $U \subset V \subset \mathscr{G}$ be two subgroups such that U is normal in V. Then we have the map

$$\sigma_U^V : B(U^{ab}) \to B(U^{ab}),$$

given by $f \mapsto \sum_{g \in V/U} gfg^{-1}$. The map $\sigma_U^{N_{\mathscr{G}}U}$ will simply be denoted by σ_U. Put

$$T_U^V = \mathrm{im}(\sigma_U^V|_{\Lambda(U^{ab})}),$$

$$T_{U,S}^V = \mathrm{im}(\sigma_U^V|_{A(U^{ab})}),$$

and

$$\widehat{T_U^V} = \mathrm{im}(\sigma_U^V).$$

Put T_U, $T_{U,S}$ and $\widehat{T_U}$ for $T_U^{N_{\mathscr{G}}U}$, $T_{U,S}^{N_{\mathscr{G}}U}$ and $\widehat{T_U^{N_{\mathscr{G}}U}}$ respectively.

For any $U \in C(\mathscr{G}, Z)$, we choose and fix ω_U to be a character of U of order p. For any $U \subset V \subset \mathscr{G}$ subgroups, we denote by ver_U^V the transfer homomorphism $V^{ab} \to U^{ab}$. The induced maps

$$\Lambda(V^{ab}) \to \Lambda(U^{ab}),$$

$$A(V^{ab}) \to A(U^{ab})$$

and

$$B(V^{ab}) \to B(U^{ab})$$

are also denoted by ver_U^V.

2 The strategy of Burns and Kato

Lemma 2.1 *Let ρ be an irreducible Artin representation of $\mathscr{G}$. Then there is a one dimensional representation χ of $\mathscr{G}$ inflated from Γ such that $\rho \otimes \chi$ is trivial on Z.*

Proof: We use induction on the order of $\mathscr{G}/Z$. By proposition 24 in [Ser77] either a) ρ restricted to Z is isotypic (i.e. direct sum of isomorphic irreducible representations) OR
b) ρ is induced from an irreducible representation of a proper subgroup A of $\mathscr{G}$ containing Z.

In case a) let $\rho|_\Gamma = \oplus_i \chi_i$ Define $\chi = \chi_i^{-1}$ for any i (note that $\chi_i|_Z = \chi_j|_Z$ for any i, j). Then $\rho \otimes \chi$ is trivial on Z.

In case b) Say $\rho = Ind_A^{\mathscr{G}}(\eta)$. Let r be such that image of A in Γ is Γ^{p^r}. By induction hypothesis we can find a χ inflated from Γ^{p^r} such that $\eta \otimes \chi$ is trivial on Z. We may extend χ to $\tilde{\chi}$ on Γ. Then

$$Ind_A^{\mathscr{G}}(\eta \otimes \chi) = Ind_A^{\mathscr{G}}(\eta) \otimes \tilde{\chi} = \rho \otimes \tilde{\chi}.$$

Since $\eta \otimes \chi|_Z$ is trivial and Z is central, $Ind_A^{\mathscr{G}}(\eta \otimes \chi)|_Z = (\rho \otimes \tilde{\chi})|_Z$ is trivial. $\square$

Proposition 2.2 *With the notations as above, the main conjecture is true for F_∞/F if and only if $(\zeta_U)_U \in \Phi_A$.*

Proof: Let $f \in K_1'(A(\mathscr{G}))$ be any element such that

$$\partial(f) = -[C(F_\infty/F)].$$

Let $\theta_A(f) = (f_U)_U$ in $\prod_{U\in S(\mathscr{G},Z)} A(U^{ab})^\times$. Then $(f_U)_U \in \Phi_A$ by theorem 6.1 (i) [Sch11]. Let $u_U = \zeta_U f_U^{-1}$. As $\partial(f_U) = \partial(\zeta_U) = -[C(K_U/F_U)]$ (since the abelian main conjecture is true, [Suj11] theorem 3.10) , we have $u_U \in \Lambda(U^{ab})^\times$. Moreover, if $(\zeta_U)_U \in \Phi_A$, then $(u_U)_U \in \Phi$. Then by theorem 4.1 [Sch11] there is a unique $u \in K_1'(\Lambda(\mathscr{G}))$ such that $\theta(u) = (u_U)_U$. Define $\zeta = \zeta(F_\infty/F) = uf$. We claim that ζ is the p-adic zeta function satisfying the main conjecture for F_∞/F. It is clear that $\partial(\zeta) = -[C(F_\infty/F)]$. We now show the interpolation property. Let ρ be an irreducible Artin representation of $\mathscr{G}$. Let σ be a one dimensional representation of $\mathscr{G}$ given by the previous lemma i.e. such that $\rho\otimes\sigma$ is trivial on Z. Then $\rho\otimes\sigma = Ind_U^{\mathscr{G}}(\eta)$ for some $U \in S(\mathscr{G},Z)$ and a one dimensional Artin character η of U (by [Ser77] theorem 16). We denote the restriction of σ to U by the same letter σ. Hence $\rho = Ind_U^{\mathscr{G}}(\eta)\otimes\sigma^{-1} = Ind_U^{\mathscr{G}}(\eta\otimes(\sigma^{-1}))$. Then for any character χ of Δ and any positive integer r divisible by $[F(\mu_p):F]$, we have

$$\begin{aligned}\zeta(\chi\rho\kappa_F^r) &= \zeta_U(\chi\eta\sigma^{-1}\kappa_{F_U}^r)\\ &= L_{\Sigma_U}(\chi\eta\sigma^{-1}, 1-r)\\ &= L_\Sigma(\chi\rho, 1-r)\end{aligned}$$

Hence ζ satisfies the required interpolation property. □

Hence we need to show the following

Theorem 2.3. *The tuple $(\zeta_U)_{U\in S(\mathscr{G},Z)}$ in the set $\prod_{U\in S(\mathscr{G},Z)} A(U^{ab})^\times$ actually lies in Φ_A i.e. it satisfies for all $U\subset V$ in $S(\mathscr{G},Z)$, the conditions*
M1. $\nu_U^V(\zeta_V) = \pi_U^V(\zeta_U)$ *if* $[V,V]\subset U$.
M2. $\zeta_{gUg^{-1}} = g\zeta_U g^{-1}$ *for any* $g\in\mathscr{G}$.
M3. $ver_U^V(\zeta_V) - \zeta_U \in T_{U,S}^V$ *if* $[V:U] = p$.
M4. $\alpha_U(\zeta_U) - \prod_{W\in P_c(U)}\varphi(\alpha_W(\zeta_W)) \in pT_{U,S}$ *if* $U\in C(\mathscr{G},Z)$.

Proposition 2.4 *The tuple $(\zeta_U)_U$ in the theorem satisfies M1. and M2.*

Proof Let $U\subset V$ in $S(\mathscr{G},Z)$ be such that $[V,V]\le U$. Then we must show that

$$\nu_U^V(\zeta_V) = \pi_U^V(\zeta_U)$$

in $A(U/[V,V])$. Let ρ be an irreducible Artin representation of $U/[V,V]$ and let r be any positive integer divisible by $[F(\mu_p):F]$. Then for any character χ of Δ, we have

$$\begin{aligned}\nu_U^V(\zeta_V)(\chi\rho\kappa_{F_U}^r) &= \zeta_V(\chi Ind_U^V(\rho)\kappa_{F_V}^r)\\ &= L_{\Sigma_V}(\chi Ind_U^V(\rho), 1-r)\\ &= L_{\Sigma_U}(\chi\rho, 1-r).\end{aligned}$$

On the other hand,

$$\begin{aligned}\pi_U^V(\zeta_U)(\chi\rho\kappa_{F_U}^r) &= \zeta_U(\chi\rho\kappa_{F_U}^r)\\ &= L_{\Sigma_U}(\chi\rho, 1-r).\end{aligned}$$

Since both $\nu_U^V(\zeta_U)$ and $\pi_U^V(\zeta_U)$ interpolate the same values on a dense subset of representations of $\Delta \times U/[V,V]$, they must be equal. This shows that the tuple $(\zeta_U)_U$ satisfies M1.

Next we show that the tuple $(\zeta_U)_U$ satisfies M2 i.e. for all $g \in \mathscr{G}$

$$g(\zeta_U)g^{-1} = \zeta_{gUg^{-1}}$$

in $gA(U^{ab})g^{-1} = A(gU^{ab}g^{-1})$. We let ρ be any one dimensional Artin representation of gUg^{-1} and r be any positive integer divisible by $[F(\mu_p):F]$. Then for any character χ of Δ, we have

$$\begin{aligned}g(\zeta_U)g^{-1}(\chi\rho\kappa_{F_{gUg^{-1}}}^r) &= \zeta_U(\chi g\rho g^{-1}\kappa_{F_U}^r)\\ &= L_{\Sigma_U}(\chi g\rho g^{-1}, 1-r)\\ &= L_{\Sigma}(\chi Ind_U^{\mathscr{G}}(g\rho g^{-1}), 1-r).\end{aligned}$$

On the other hand,

$$\begin{aligned}\zeta_{gUg^{-1}}(\chi\rho\kappa_{F_{gUg^{-1}}}^r) &= L_{\Sigma_U}(\chi\rho, 1-r)\\ &= L_{\Sigma}(\chi Ind_{gUg^{-1}}^{\mathscr{G}}(\rho), 1-r).\end{aligned}$$

But $Ind_U^{\mathscr{G}}(g\rho g^{-1}) = Ind_{gUg^{-1}}^{\mathscr{G}}(\rho)$. Hence $g(\zeta_U)g^{-1}$ and $\zeta_{gUg^{-1}}$ interpolate the same values on a dense subset of representations of $\Delta \times gU^{ab}g^{-1}$ and so must be equal. This proves that the tuple $(\zeta_U)_U$ satisfies M2. $\square$

The rest of the paper is devoted to proving that $(\zeta_U)_U$ satisfies M3 and M4.

3 Basic congruences

The congruence M4 is multiplicative and does not yield directly to the method of Deligne-Ribet. In this section we state certain additive congruences which yield to the Deligne-Ribet method as we show in the following sections. These congruences are then used in the last section to prove M4.

Let $\mathfrak{p}$ be the maximal ideal of $\mathbb{Z}_p[\mu_p]$.

Proposition 3.1 *For every $U \subset V$ in $S(\mathscr{G}, Z)$ such that $[V:U] = p$, we have*

$$ver_U^V(\zeta_V) - \zeta_U \in T_{U,S}^V. \tag{1}$$

Proposition 3.2 *For every $U \in C(\mathscr{G}, Z)$ such that $P_c(U)$ is empty*

$$\zeta_U - \omega_U^k(\zeta_U) \in \mathfrak{p}T_{U,S} \tag{2}$$

for all $0 \le k \le p-1$.

Proposition 3.3 *If* $U \in C(\mathscr{G}, Z)$ *is such that* $P_c(U)$ *is non-empty, we have*

$$\zeta_U - \sum_{V \in P_c(U)} \varphi_V(\zeta_V) \in T_{U,S}. \tag{3}$$

Proposition 3.4 *If* $U \in C(\mathscr{G}, Z)$ *and* $V \in P_c(U)$*, then*

$$\zeta_U - \varphi_V(\zeta_V) \in T_{U,S}^{N_{\mathscr{G}}V}. \tag{4}$$

$$\zeta_0 - \varphi_Z(\zeta_Z) \in pT_{Z,S}. \tag{5}$$

The congruence (1) is of course M3. Other congruences will be put together in section 14 to prove M4. We prove the above propositions in section (13).

4 *L*-values

Let $j \ge 0$. Let $x \in \Delta \times U^{ab}/Z^{p^j}$. Then we define $\delta^{(x)} : \Delta \times U^{ab} \to \mathbb{C}$ to be the characteristic function of the coset x of Z^{p^j} in $\Delta \times U^{ab}$. Define the partial zeta function by

$$\zeta(\delta^{(x)}, s) = \sum_{\mathfrak{a}} \frac{\delta^{(x)}(g_{\mathfrak{a}})}{N(\mathfrak{a})^s}, \qquad \text{for } Re(s) > 1,$$

where the sum is over all ideals $\mathfrak{a}$ of O_{F_U} which are prime to Σ_U, the Artin symbol of $\mathfrak{a}$ in $\Delta \times U^{ab}$ is denoted by $g_{\mathfrak{a}}$ and the absolute norm of the ideal $\mathfrak{a}$ is denoted by $N(\mathfrak{a})$. A well known theorem of [Kli62] and [Sei70] says that the function $\zeta(\delta^{(x)}, s)$ has analytic continuation to the whole complex place except for a simple pole at $s = 1$, and that $\zeta(\delta^{(x)}, 1-k)$ is rational for any even positive integer k.

If ε is a locally constant function on $\Delta \times U^{ab}$ with values in a $\mathbb{Q}$-vector space V, say for a large enough j

$$\varepsilon \equiv \sum_{x \in \Delta \times U^{ab}/Z^{p^j}} \varepsilon(x)\delta^{(x)}.$$

Then the special value $L_{\Sigma_U}(\varepsilon, 1-k)$ can be canonically defined as

$$L_{\Sigma_U}(\varepsilon, 1-k) = \sum_{x \in \Delta \times U^{ab}/Z^{p^j}} \varepsilon(x)\zeta(\delta^{(x)}, 1-k) \in V. \tag{6}$$

If ε is an Artin character of degree 1, then $L_{\Sigma_U}(\varepsilon, 1-k)$ is of course the value at $1-k$ of the complex L-function associated to ε with Euler factors at primes in Σ_U

removed. If ε is a locally constant $\mathbb{Q}_p$-values function on $\Delta \times U^{ab}$, then for any positive integer k divisible by $[F(\mu_p):F]$ and any $u \in U^{ab}$, we define

$$\Delta_U^u(\varepsilon, 1-k) = L_{\Sigma_U}(\varepsilon, 1-k) - \kappa(u)^k L_{\Sigma_U}(\varepsilon_u, 1-k), \tag{7}$$

where ε_u is a locally constant function defined by $\varepsilon_u(g) = \varepsilon(ug)$, for all $g \in \Delta \times U^{ab}$.

5 Approximation to p-adic zeta functions

We get a sequence of elements in certain group rings which essentially approximate the abelian p-adic zeta functions ζ_U. These group rings are obtained as follows. Recall that κ is the p-adic cyclotomic character of F. Let f be a positive integer such that $\kappa^{p-1}(Z) = 1 + p^f\mathbb{Z}_p$.

Definition 5.1 *Let $U \subset V$ be in $S(\mathscr{G}, Z)$ such that U is normal in V. Define the map*

$$\sigma_{U,j}^V : \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}) \to \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}),$$

given by

$$x \mapsto \sum_{g \in V/U} gxg^{-1}.$$

Put $T_{U,j}^V = im(\sigma_{U,j}^V)$ and denote $T_{U,j}^{N_{\mathscr{G}}U}$ simply by $T_{U,j}$.

Lemma 5.2 *For any $U \in S(\mathscr{G}, Z)$, we have an isomorphism*

$$\Lambda(U^{ab}) \xrightarrow{\sim} \varprojlim_{j \geq 0} \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}).$$

If $U \subset V$ in $S(\mathscr{G}, Z)$ are such that U is normal in V, then under this isomorphism T_U^V maps isomorphically to $\varprojlim_j T_{U,j}^V$.

Proof: We prove the surjectivity first. Given any

$$(x_j)_j \in \varprojlim_{j \geq 0} \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}),$$

we construct a canonical $\tilde{x}_j \in \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]$ as follows: for every $t \geq j$, let $\bar{x}_t$ be the image of $x_t \in \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^t}]/(p^{f+t})$ in $\mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+t})$. Then $(\bar{x}_t)_{t \geq j}$ forms an inverse system. We define $\tilde{x}_j$ to be the limit of $\bar{x}_t$ in $\mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]$. The tuple $(\tilde{x}_j)_{j \geq 0}$ forms an inverse system. We define x to be their limit in $\Lambda(U^{ab})$. This is an inverse image of $(x_j)_{j \geq 0}$ in $\Lambda(U^{ab})$. This construction also proves the injectivity of the map.

To prove the second assertion we use the following exact sequence

$$0 \to \mathrm{Ker}(\sigma_{U,j}^{V}) \to \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}) \to T_{U,j}^{V} \to 0.$$

Passing to the inverse limit over j gives

$$0 \to \varprojlim_{j} \mathrm{Ker}(\sigma_{U,j}^{V}) \to \Lambda(U^{ab}) \to \varprojlim_{j} T_{U,j}^{V} \to 0.$$

Exactness on the right is because all the abelian groups involved are finite. Hence $T_U^V \cong \varprojlim_{j} T_{U,j}^V$. $\square$

Proposition 5.3 *(Ritter-Weiss) For any $j \geq 0$, any positive integer k divisible by $[F(\mu_p):F]$ and any $U \in S(\mathscr{G}, Z)$, the natural surjection of $\Lambda(U^{ab})$ onto $\mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j})$, maps $(1-u)\zeta_U \in \Lambda(U^{ab})$ to*

$$\sum_{x \in U^{ab}/Z^{p^j}} \Delta_U^u(\delta^{(x)}, 1-k)\kappa(x)^{-k}x \quad (mod\ p^{f+j}).$$

In particular, we claim that the inverse limit is independent of the choice of k. Also note that since x is a coset of Z^{f+j} in $\Delta \times U^{ab}$, the value $\kappa(x)^k$ is well defined only modulo p^{f+j}.

Proof: Since ζ_U is a pseudomeasure, $(1-u)\zeta_U$ lies in $\Lambda(U^{ab})$. We prove the proposition in 3 steps: first we show that the sums form an inverse system. Second we show that the inverse limit is independent of the choice of k. And thirdly we show that it interpolates the same values as $(1-u)\zeta_U$.

Step1: Let $j \geq 0$ be an integer. Let

$$\pi : \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^{j+1}}]/(p^{f+j+1}) \to \mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j}),$$

denote the natural projection. Then

$$\begin{aligned}
&\pi\Big(\sum_{x \in \Delta \times U^{ab}/Z^{p^{j+1}}} \Delta_U^u(\delta^{(x)}, 1-k)\kappa(x)^{-k}x\Big) \\
&= \sum_{y \in \Delta \times U^{ab}/Z^{p^j}} \Big(\sum_{x \in yZ^{p^j}/Z^{p^{j+1}}} \Delta_U^u(\delta^{(x)}, 1-k)\kappa(x)^{-k}\pi(x)\Big) (\mathrm{mod}\ p^{f+j}) \\
&= \sum_{y \in \Delta \times U^{ab}/Z^{p^j}} \Big(\kappa(y)^{-k}y \sum_{x \in Z^{p^j}/Z^{p^{j+1}}} \Delta_U^u(\delta^{(x)}, 1-k)\Big) (\mathrm{mod}\ p^{f+j}) \\
&= \sum_{y \in \Delta \times U^{ab}/Z^{p^j}} \Delta_U^u(\delta^{(y)}, 1-k)\kappa(y)^{-k}y (\mathrm{mod}\ p^{f+j}).
\end{aligned}$$

Here the second equality is because for any $x \in \Delta \times U^{ab}/Z^{p^{j+1}}$ we have $\kappa(x)^k \equiv \kappa(y)^k (\mathrm{mod}\ p^{f+j})$ if $\pi(x) = y$. This shows that the sums form an inverse system.

Step2: The inverse limit would be independent of the choice of k if we show that for any two positive integers k and k' divisible by $[F(\mu_p):F]$, we have

$$\sum_{x\in\frac{\Delta\times U^{ab}}{Z^{p^j}}} \Delta_U^u(\delta^{(x)},1-k)\kappa(x)^{-k}x \equiv \sum_{x\in\frac{\Delta\times U^{ab}}{Z^{p^j}}} \Delta_U^u(\delta^{(x)},1-k')\kappa(x)^{-k'}x (\mathrm{mod}\ p^{f+j}).$$

Or equivalently that,

$$\Delta_U^u(\delta^{(x)},1-k)\kappa(x)^{-k} \equiv \Delta_U^u(\delta^{(x)},1-k')\kappa(x)^{-k'} (\mathrm{mod}\ p^{f+j}), \tag{8}$$

for all $x\in\Delta\times U^{ab}/Z^{p^j}$. Choose a locally constant function $\eta:\Delta\times U^{ab}\to\mathbb{Z}_p^\times$ such that $\eta^{[F(\mu_p):F]}\equiv\kappa^{[F(\mu_p):F]}(\mathrm{mod}\ p^{f+j})$. Define the functions ε_k and $\varepsilon_{k'}$ from $\Delta\times U^{ab}$ to $\mathbb{Q}_p$ by

$$\varepsilon_k = \frac{1}{p^{f+j}}\eta(x)^{-k}\delta^{(x)},$$

and

$$\varepsilon_{k'} = \frac{1}{p^{f+j}}\eta(x)^{-k'}\delta^{(x)}.$$

Then the function $(\varepsilon_k\kappa^{k-1}-\varepsilon_{k'}\kappa^{k'-1})$ takes values in $\mathbb{Z}_p$. Hence the congruence (8) is satisfied by [Del80], theorem 0.4.

Step3: Let

$$\zeta_u = \varprojlim_{j\geq 0}\left(\sum_{x\in\Delta\times U^{ab}/Z^{p^j}} \Delta_U^u(\delta^{(x)},1-k)\kappa(x)^{-k}x(\mathrm{mod}\ p^{f+j})\right)\in\Lambda(U^{ab}).$$

Let ε be a locally constant function on $\Delta\times U^{ab}$ factoring through $\Delta\times U^{ab}/Z^{p^j}$ for some $j\geq 0$. Note that for every $i\geq j$

$$\begin{aligned}
&\sum_{x\in\Delta\times U^{ab}/Z^{p^i}} \Delta_U^u(\delta^{(x)},1-k)\varepsilon(x)\\
&= \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} L_{\Sigma_U}(\delta^{(x)},1-k)\varepsilon(x) - \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} \kappa(u)^k L_{\Sigma_U}(\delta_u^{(x)},1-k)\varepsilon(x)\\
&= \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} L_{\Sigma_U}(\delta^{(x)},1-k)\varepsilon(x) - \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} \kappa(u)^k L_{\Sigma_U}(\delta^{(u^{-1}x)},1-k)\varepsilon(x)\\
&= \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} L_{\Sigma_U}(\delta^{(x)},1-k)\varepsilon(x) - \sum_{x\in\Delta\times U^{ab}/Z^{p^i}} \kappa(u)^k L_{\Sigma_U}(\delta^{(x)},1-k)\varepsilon(ux)\\
&= L_{\Sigma_U}(\varepsilon,1-k)-\kappa(u)^k L_{\Sigma_U}(\varepsilon_u,1-k)\\
&= \Delta_U^u(\varepsilon,1-k).
\end{aligned}$$

Then by definition of ζ_u, for any $i\geq j$, we have

$$\begin{aligned}
\zeta_u(\kappa^k\varepsilon) &\equiv \sum_{x\in\Delta\times U^{ab}/Z^{p^j}} \Delta_U^u(\delta^{(x)},1-k)\varepsilon(x)(\mathrm{mod}\ p^{f+i})\\
&\equiv \Delta_U^u(\varepsilon,1-k)(\mathrm{mod}\ p^{f+i}).
\end{aligned}$$

On the other hand, by definition of the p-adic zeta function or the construction of Deligne-Ribet (see discussion after theorem 0.5 in [Del80]) we have

$$(1-u)\zeta_U(\kappa^k\varepsilon) = \Delta_U^u(\varepsilon, 1-k).$$

Hence $(1-u)\zeta_U = \zeta_u$ because they interpolate the same values on all cyclotomic twists of locally constant functions. This finishes the proof. $\square$

6 A sufficient condition to prove the basic congruences

Lemma 6.1 *Let y be a coset of Z^{p^j} in $\Delta \times U^{ab}$. Then for any $u \in Z$ and for any $g \in \mathscr{G}$, we have*

$$\Delta_U^u(\delta^{(y)}, 1-k) = \Delta_{gUg^{-1}}^u(\delta^{(gyg^{-1})}, 1-k).$$

Proof: It is sufficient to show that $\zeta(\delta^{(y)}, 1-k) = \zeta(\delta^{(gyg^{-1})}, 1-k)$ because of the following:

$$\Delta_U^u(\delta^{(y)}, 1-k) = \zeta(\delta^{(y)}, 1-k) - \kappa^k(u)\zeta(\delta_u^{(y)}, 1-k),$$

$$\Delta_{gUg^{-1}}^u(\delta^{(gyg^{-1})}, 1-k) = \zeta(\delta^{(gyg^{-1})}, 1-k) - \kappa^k(u)\zeta(\delta_u^{(gyg^{-1})}, 1-k).$$

But

$$\delta_u^{(y)} = \delta^{(u^{-1}y)} \qquad \text{and} \qquad \delta_u^{(gyg^{-1})} = \delta^{(u^{-1}gyg^{-1})} = \delta^{(gu^{-1}yg^{-1})}.$$

Now to show that $\zeta(\delta^{(y)}, 1-k) = \zeta(\delta^{(gyg^{-1})}, 1-k)$, note that for $Re(s) > 1$

$$\begin{aligned}\zeta(\delta^{(gyg^{-1})}, s) &= \sum_{\mathfrak{a}} \frac{\delta^{(gyg^{-1})}(g_{\mathfrak{a}})}{N(\mathfrak{a})^s} \\ &= \sum_{\mathfrak{a}} \frac{\delta^{(y)}(g_{\mathfrak{a}^g})}{N(\mathfrak{a}^g)^s} \\ &= \zeta(\delta^{(y)}, s).\end{aligned}$$

Since $\zeta(\delta^{(gyg^{-1})}, s)$ and $\zeta(\delta^{(y)}, s)$ are meromorphic functions agreeing on the right half plane, we deduce $\zeta(\delta^{(gyg^{-1})}, 1-k) = \zeta(\delta^{(y)}, 1-k)$, as required. $\square$

Proposition 6.2 *To prove the congruence (1) in proposition (3.1) it is sufficient to prove the following: for any $j \geq 1$ and any coset y of Z^{p^j} in $\Delta \times U^{ab}$ fixed by V and any $u \in Z$*

$$\Delta_U^{u^p}(\delta^{(y)}, 1-k) \equiv \Delta_V^u(\delta^{(y)} \circ ver_U^V, 1-pk) (mod\ p\mathbb{Z}_p) \tag{9}$$

for all positive integers k divisible by $[F(\mu_p) : F]$.

Proof: By lemma 5.3 the image of $(1-u^p)\zeta_U$ in $\mathbb{Z}_p[\Delta \times U^{ab}/Z^{p^j}]/(p^{f+j-1})$ is

$$\sum_{y\in\Delta\times U^{ab}/Z^{p^j}} \Delta_U^{u^p}(\delta^{(y)},1-k)\kappa(y)^{-k}y(\bmod\ p^{f+j-1}). \tag{10}$$

And the image of $(1-u)\zeta_V$ in $\mathbb{Z}_p[\Delta\times V^{ab}/Z^{p^{j-1}}]/(p^{f+j-1})$ is

$$\sum_{x\in\Delta\times V^{ab}/Z^{p^{j-1}}} \Delta_V^{u}(\delta^{(x)},1-pk)\kappa(x)^{-pk}x(\bmod\ p^{f+j-1}).$$

Let V' be the kernel of the homomorphism $ver_U^V : V^{ab}\to U^{ab}$. Then $V'\cap Z=\{1\}$ which implies that the map

$$\Delta\times V^{ab}/V'Z^{p^{j-1}} \to \Delta\times U^{ab}/Z^{p^j}$$

induced by ver_U^V is injective. Moreover $\kappa^k(V')=\{1\}$. Hence the image of $ver_U^V((1-u)\zeta_V)=(1-u^p)ver_U^V(\zeta_V)$ in $\mathbb{Z}_p[\Delta\times U^{ab}/Z^{p^j}]/(p^{f+j-1})$ is

$$\sum_{x\in\Delta\times V^{ab}/V'Z^{p^{j-1}}} \Delta_V^{u}(\delta^{(x)},1-pk)\kappa(x)^{-pk}ver_U^V(x)(\bmod\ p^{f+j-1}),$$

which can be written as

$$\sum_{y\in\Delta\times U^{ab}/Z^{p^j}} \Delta_V^{u}(\delta^{(y)}\circ ver_U^V,1-pk)\kappa(y)^{-k}y(\bmod\ p^{f+j-1}) \tag{11}$$

because if $y\notin Im(ver_U^V)$, then $\delta^{(y)}\circ ver_U^V\equiv 0$ and if $y=ver_U^V(x)$, then $\kappa(y)^k=\kappa(x)^{pk}$. Subtracting (11) from (10) gives

$$\sum_{y\in\Delta\times U^{ab}/Z^{p^j}} \Big(\Delta_U^{u^p}(\delta^{(y)},1-k)-\Delta_V^{u}(\delta^{(y)}\circ ver_U^V,1-pk)\Big)\kappa(y)^{-k}y(\bmod\ p^{f+j-1}). \tag{12}$$

If y is fixed by V then $\Big(\Delta_U^{u^p}(\delta^{(y)},1-k)-\Delta_V^{u}(\delta^{(y)}\circ ver_U^V,1-pk)\Big)\kappa(y)^{-k}y\equiv py\equiv 0(\bmod\ T_{U,j}^V)$ under equation (9). On the other hand if y is not fixed by V, then the full orbit of y under the action of V in the above sum is

$$\begin{aligned}&\sum_{g\in V/U}(\Delta_U^{u^p}(\delta^{(gyg^{-1})},1-k)-\Delta_V^{u}(\delta^{(gyg^{-1})}\circ ver_U^V,1-pk))\kappa(gyg^{-1})^{-k}gyg^{-1}\\ =&\Big(\Delta_U^{u^p}(\delta^{(y)},1-k)-\Delta_V^{u}(\delta^{(y)}\circ ver_U^V,1-pk)\Big)\kappa(y)^{-k}\sum_{g\in V/U}gyg^{-1}\\ \in&T_{U,j}^V.\end{aligned}$$

The equality is by lemma 6.1. Hence the sum in (12) lies in $T_{U,j}^V(\bmod\ p^{f+j-1})$. By lemma 5.2 $(1-u^p)(\zeta_U-ver_U^V(\zeta_V))\in T_U^V$. As u is a central element congruence (1) holds. □

Remark 6.3 *Proofs of following three propositions are very similar to the above proof.*

Proposition 6.4 *To prove congruence (2) in proposition (3.2) it is sufficient to show the following: for any $j \geq 0$ and any coset y of Z^{p^j} in $\Delta \times U$ whose image in U/Z is a generator of U/Z, and any $u \in Z$*

$$\Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) \equiv 0 (mod\ |(W_{\mathscr{G}}U)_y|\mathbb{Z}_p), \tag{13}$$

for all positive integers k divisible by $[F(\mu_p):F]$.

Proof: Let $v = u^{d_U}$. Then by lemma 5.3 the image of $(1-v)\zeta_U - \omega_U^k((1-v)\zeta_U)$ in $\mathbb{Z}_p[\Delta \times U/Z^{p^j}]/(p^{f+j})$ is

$$\sum_{y \in \Delta \times U/Z^{p^j}} \Delta_U^v(\delta^{(y)}, 1-k)\kappa(y)^{-k}(y - \omega_U^k(y)) (\text{mod } p^{f+j}). \tag{14}$$

If the image of y in U/Z is not a generator of U/Z, then $y - \omega_U^k(y) = 0$. For y whose image in U/Z is a generator of U/Z, we look at the $P := W_{\mathscr{G}}U$ orbit of y in expression (14). It is

$$\begin{aligned}&\sum_{g \in P/P_y} \Delta_U^v(\delta^{(gyg^{-1})}, 1-k)\kappa(gyg^{-1})^{-k}(gyg^{-1} - \omega_U^k(gyg^{-1}))(\text{mod } p^{f+j})\\ =&\Delta_U^v(\delta^{(y)}, 1-k)\kappa(y)^{-k} \sum_{g \in P/P_y} (gyg^{-1} - \omega_U^k(gyg^{-1}))\end{aligned}$$

which lies in $\mathfrak{p}T_{U,j}$ under equation (13) and then the sum in expression (14) lies in $\mathfrak{p}T_{U,j}$. Then by lemma 5.2 $(1-v)(\zeta_U - \omega_U^k(\zeta_U)) \in \mathfrak{p}T_U$. As v is a central element congruence (2) holds. □

Proposition 6.5 *To prove congruence (3) in proposition (3.3) it is sufficient to prove the following: for any $j \geq 0$ and any coset y of Z^{p^j} in $\Delta \times U$, and any $u \in Z$*

$$\Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) \equiv \sum_{V \in P_c(U)} \Delta_V^{u^{d_U/p}}(\delta^{(y)} \circ \varphi_V, 1-pk)(mod\ |(W_{\mathscr{G}}U)_y|\mathbb{Z}_p), \tag{15}$$

for all positive integers k divisible by $[F(\mu_p):F]$.

Proof: Let $v = u^{d_U/p}$. By lemma 5.3 the image of $(1-v^p)\zeta_U$ in $\frac{\mathbb{Z}_p[\Delta \times U/Z^{p^j}]}{(p^{f+j-1})}$ is

$$\sum_{y \in \Delta \times U/Z^{p^j}} \Delta_U^{v^p}(\delta^{(y)}, 1-k)\kappa(y)^{-k} y (\text{mod } p^{f+j-1}). \tag{16}$$

And the image of $(1-v)\zeta_V$ in $\mathbb{Z}_p[\Delta \times V/Z^{p^{j-1}}]/(p^{f+j-1})$ is

$$\sum_{x \in \Delta \times V/Z^{p^{j-1}}} \Delta_V^v(\delta^{(x)}, 1-pk)\kappa(x)^{-pk} x (\text{mod } p^{f+j-1}).$$

Let V' be the kernel of the homomorphism $\varphi : V \to U$. Then $V' \cap Z = \{1\}$ which implies that the map

$$\Delta \times V/V'Z^{p^{j-1}} \to \Delta \times U/Z^{p^j}$$

induced by φ_V is injective. Moreover, $\kappa^k(V') = \{1\}$. Hence the image of

$$\sum_{V \in P_c(U)} \varphi_V((1-v)\zeta_V) = (1-v^p) \sum_{V \in P_c(U)} \varphi_V(\zeta_V)$$

in $\mathbb{Z}_p[\Delta \times U/Z^{p^j}]/(p^{f+j-1})$ is

$$\sum_{V \in P_c(U)} \sum_{x \in \Delta \times V/V'Z^{p^{j-1}}} \Delta_V^v(\delta^{(x)}, 1-pk)\kappa(x)^{-pk}\varphi_V(x)(\mathrm{mod}\ p^{f+j-1}),$$

which can be written as

$$\sum_{y \in \Delta \times U/Z^{p^j}} \sum_{V \in P_c(U)} \Delta_V^v(\delta^{(y)} \circ \varphi_V, 1-pk)\kappa(y)^{-k} y(\mathrm{mod}\ p^{f+j-1}) \tag{17}$$

because if $y \notin Im(\varphi_V)$, then $\delta^{(y)} \circ \varphi_V \equiv 0$ and if $y = \varphi_V(x)$, then $\kappa(y)^k = \kappa(x)^{pk}$. Subtracting (17) from (16) gives

$$\sum_{y \in \Delta \times U/Z^{p^j}} \Big(\Delta_U^{v^p}(\delta^{(y)}, 1-k) - \sum_{V \in P_c(V)} \Delta_V^v(\delta^{(y)} \circ \varphi_V, 1-pk)\Big)\kappa(y)^{-k} y(\mathrm{mod}\ p^{f+j-1}) \tag{18}$$

Now we take the orbit of y in the sum in (18) under the action of $P = W_{\mathscr{G}}U$. It is

$$\Big(\Delta_U^{v^p}(\delta^{(y)}, 1-k) - \sum_{V \in P_c(U)} \Delta_V^v(\delta^{(y)} \circ \varphi_V, 1-pk)\Big)\kappa(y)^{-k} \sum_{g \in P/P_y} gyg^{-1}$$

which lies in $T_{U,j}(\mathrm{mod}\ p^{f+j-1})$ under equation (15) and then the sum in expression (18) lies in $T_{U,j}(\mathrm{mod}\ p^{f+j-1})$. Then by lemma (5.2) $(1-v^p)(\zeta_U - \sum_{V \in P_c(V)} \varphi_V(\zeta_V))$ lies in T_U. As v is a central element congruence (3) holds. □

Proposition 6.6 *To prove congruence (4) in proposition (3.4) it is sufficient to prove the following: for any $j \geq 0$, any coset y of Z^{p^j} in $\Delta \times U$ and any u in Z*

$$\Delta_U^{u^{pd_V}}(\delta^{(y)}, 1-k) \equiv \Delta_V^{u^{d_V}}(\delta^{(y)} \circ \varphi_V, 1-pk)(mod\ |(N_{\mathscr{G}}V/U)_y|\mathbb{Z}_p), \tag{19}$$

for all positive integers k divisible by $[F(\mu_p) : F]$.

To prove the congruence (5) in proposition (3.4) it is sufficient to show the following: for any $j \geq 1$, any coset y of Z^{p^j} in $\Delta \times Z^p$ and any u in Z^p

$$\Delta_0^{u^{p|\mathscr{G}/Z|}}(\delta^{(y)}, 1-k) \equiv \Delta_Z^{u^{|\mathscr{G}/Z|}}(\delta^{(y)} \circ \varphi_Z, 1-pk)(mod\ p|\mathscr{G}/Z|\mathbb{Z}_p), \tag{20}$$

for any positive integer k divisible by $[F(\mu_p) : F]$.

Proof: We will only prove the first assertion. Proof of the second one exactly the same. Let $v = u^{d_V}$. By lemma 5.3 the image of $(1-v^p)\zeta_U$ in $\frac{\mathbb{Z}_p[\Delta\times U/Z^{p^j}]}{(p^{f+j-1})}$ is

$$\sum_{y\in\Delta\times U/Z^{p^j}} \Delta_U^{v^p}(\delta^{(y)},1-k)\kappa(y)^{-k}y(\text{mod } p^{f+j-1}). \tag{21}$$

And the image of $(1-v)\zeta_V$ in $\mathbb{Z}_p[\Delta\times V/Z^{p^{j-1}}]/(p^{f+j-1})$ is

$$\sum_{x\in\Delta\times V/Z^{p^{j-1}}} \Delta_V^{v}(\delta^{(x)},1-pk)\kappa(x)^{-pk}x(\text{mod } p^{f+j-1}).$$

Let V' be the kernel of the homomorphism $\varphi_V : V\to U$. Then $V'\cap Z=\{1\}$ which implies that the map

$$\Delta\times V/V'Z^{p^{j-1}} \to \Delta\times U/Z^{p^j}$$

induced by φ_V is injective. Moreover $\kappa^k(V')=\{1\}$. Hence the image of

$$\varphi_V((1-v)\zeta_V) = (1-v^p)\varphi_V(\zeta_V)$$

in $\mathbb{Z}_p[\Delta\times U/Z^{p^j}]/(p^{f+j-1})$ is

$$\sum_{x\in\Delta\times V/V'Z^{p^{j-1}}} \Delta_V^{v}(\delta^{(x)},1-pk)\kappa(x)^{-pk}\varphi_V(x)(\text{mod } p^{f+j-1}),$$

which can be written as

$$\sum_{y\in\Delta\times U/Z^{p^j}} \Delta_V^{v}(\delta^{(y)}\circ\varphi_V,1-pk)\kappa(y)^{-k}y(\text{mod } p^{f+j-1}) \tag{22}$$

because if $y\notin Im(\varphi_V)$, then $\delta^{(y)}\circ\varphi_V\equiv 0$ and if $y=\varphi_V(x)$, then $\kappa(y)^k=\kappa(x)^{pk}$. Subtracting (22) from (21) we get

$$\sum_{y\in\Delta\times U/Z^{p^j}} \Big(\Delta_U^{v^p}(\delta^{(y)},1-k) - \Delta_V^{v}(\delta^{(y)}\circ\varphi_V,1-pk)\Big)\kappa(y)^{-k}y(\text{mod } p^{f+j-1}). \tag{23}$$

Now for a fixed $y\in\Delta\times U/Z^{p^j}$ we take the orbit of y in this sum under the action of $P=N_{\mathscr{G}}V/U$. It is

$$\Big(\Delta_U^{v^p}(\delta^{(y)},1-k) - \Delta_V^{v}(\delta^{(y)}\circ\varphi_V,1-pk)\Big)\kappa(y)^{-k}\sum_{g\in P/P_y} gyg^{-1}$$

which lies in $T_{U,j}^{N_{\mathscr{G}}V}(\text{mod } p^{f+j-1})$ under equation (19) and then the sum in (23) lies in $T_{U,j}^{N_{\mathscr{G}}V}(\text{mod } p^{f+j-1})$. Then by lemma (5.2) $(1-v^p)(\zeta_U-\varphi(\zeta_V))\in T_U^{N_{\mathscr{G}}V}$. As v is a central element congruence (4) holds. $\square$

7 Hilbert modular forms

In this section we briefly recall the basic notions in the theory of Hilbert modular forms. Let L be an arbitrary totally real number field of degree r over $\mathbb{Q}$. Let $\mathfrak{H}_L$ be the Hilbert upper half plane of L. Let Σ be a finite set of finite primes of L containing all primes above p. Let κ be the p-adic cyclotomic character of L. Let $\mathfrak{f}$ be an integral ideal of L with all its prime factors in Σ. We put $GL_2^+(L\otimes\mathbb{R})$ for the group of all 2×2 matrices with totally positive determinant. For any even positive integer k, the group $GL_2^+(L\otimes\mathbb{R})$ acts on functions $f:\mathfrak{H}_L\to\mathbb{C}$ by

$$f|k\begin{pmatrix} a & b\\ c & d\end{pmatrix}(\tau)=\mathscr{N}(ad-bc)^{k/2}\mathscr{N}(c\tau+d)^{-k}f(\frac{a\tau+d}{c\tau+d}),$$

where $\mathscr{N}:L\otimes\mathbb{C}\to\mathbb{C}$ is the norm map. Set

$$\Gamma_{00}(\mathfrak{f})=\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(L): a,d\in 1+\mathfrak{f}, b\in\mathfrak{D}^{-1}, c\in\mathfrak{f}\mathfrak{D}\},$$

where $\mathfrak{D}$ is the different of $L/\mathbb{Q}$. A *Hilbert modular form* f of weight k on $\Gamma_{00}(\mathfrak{f})$ is a holomorphic function $f:\mathfrak{H}_L\to\mathbb{C}$ (which we assume to be holomorphic at ∞ if $L=\mathbb{Q}$) satisfying

$$f|_k M=f \qquad \text{for all } M\in\Gamma_{00}(\mathfrak{f}).$$

The space of all Hilbert modular forms of weight k on $\Gamma_{00}(\mathfrak{f})$ is denoted by $M_k(\Gamma_{00}(\mathfrak{f}),\mathbb{C})$. Since f is invariant under the translation $\tau\mapsto\tau+b$ (for $b\in\mathfrak{D}^{-1}$), we may expand f as a Fourier series to get the standard q-expansion

$$f(\tau)=c(0,f)+\sum_{\mu}c(\mu,f)q_L^{\mu},$$

where μ runs through all totally positive elements in O_L and $q_L^{\mu}=e^{2\pi i tr_{L/\mathbb{Q}}(\mu\tau)}$.

8 Restrictions along diagonal

Let L' be another totally real number field containing L. Let r' be the degree of L' over L. The inclusion of L in L' induces maps $\mathfrak{H}_L\xrightarrow{*}\mathfrak{H}_{L'}$ and $SL_2(L\otimes\mathbb{R})\xrightarrow{*}SL_2(L'\otimes\mathbb{R})$. For a holomorphic function $f:\mathfrak{H}_{L'}\to\mathbb{C}$, we define the "restriction along diagonal" $R_{L'/L}f:\mathfrak{H}_L\to\mathbb{C}$ by $R_{L'/L}f(\tau)=f(\tau^*)$. We then have

$$(R_{L'/L}f)|_{r'k}M=R_{L'/L}(f|_k M^*),$$

for any $M\in SL_2(L\otimes\mathbb{R})$. Let $\mathfrak{f}$ be an integral ideal of L, then $R_{L'/L}$ induces a map

$$R_{L'/L}:M_k(\Gamma_{00}(\mathfrak{f}O_{L'}),\mathbb{C})\to M_{r'k}(\Gamma_{00}(\mathfrak{f}),\mathbb{C}).$$

If the standard q-expansion of f is

$$c(0,f)+\sum_{\nu\in O_{L'}^{+}} c(\nu,f)q_{L'}^{\nu},$$

then the standard q-expansion of $R_{L'/L}f$ is

$$c(0,f)+\sum_{\mu\in O_{L}^{+}}\Big(\sum_{\nu:tr_{L'/L}(\nu)=\mu} c(\nu,f)\Big)q_{L}^{\mu}.$$

Here O_L^+ and $O_{L'}^+$ denotes totally positive elements of O_L and $O_{L'}$ respectively.

9 Cusps

Let $\mathbb{A}_L$ be the ring of finite adeles of L. Then by strong approximation

$$SL_2(\mathbb{A}_L)=\widehat{\Gamma_{00}(\mathfrak{f})}\cdot SL_2(L).$$

Any $M\in SL_2(\mathbb{A}_L)$ can be written as M_1M_2 with $M_1\in\widehat{\Gamma_{00}(\mathfrak{f})}$ and $M_2\in SL_2(L)$. We define $f|_kM$ to be $f|_kM_2$. Any α in $\mathbb{A}_L^\times$ determines a *cusp*. We let

$$f|_\alpha=f|_k\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}.$$

The q-expansion of f at the cusp determined by α is defined to the standard q-expansion of $f|_\alpha$. We write it as

$$c(0,\alpha,f)+\sum_{\mu} c(\mu,\alpha,f)q_L^{\mu},$$

where the sum is restricted to all totally positive elements of L which lie in the square of the ideal "generated" by α.

Lemma 9.1 *Let $\mathfrak{f}$ be an integral ideal in L. Let $f\in M_k(\Gamma_{00}(\mathfrak{f}O_{L'}),\mathbb{C})$. Then the constant term of the q-expansion of $R_{L'/L}f$ at the cusp determined by $\alpha\in\mathbb{A}_L^\times$ is equal to the constant term of the q-expansion of f at the cusp determined by $\alpha^*\in\mathbb{A}_{L'}^\times$ i.e.*

$$c(0,\alpha,R_{L'/L}f)=c(0,\alpha^*,f).$$

Proof: The q-expansion of f at the cusp determined by α^* is the standard q-expansion of $f|_{\alpha^*}$. Similarly, the q-expansion of $R_{L'/L}f$ at the cusp determined by α is the standard q-expansion of $(R_{L'/L}f)|_\alpha$. But $(R_{L'/L}f)|_\alpha=R_{L'/L}(f|_{\alpha^*})$. □

10 A Hecke operator

Lemma 10.1 *Let $\beta \in O_L$ be a totally positive element. Assume that $\mathfrak{f} \subset \beta O_L$. Then there is a Hecke operator U_β on $M_k(\Gamma_{00}(\mathfrak{f}), \mathbb{C})$ so that for $f \in M_k(\Gamma_{00}(\mathfrak{f}), \mathbb{C})$ the standard q-expansion of $f|_k U_\beta$ is*

$$c(0,f) + \sum_\mu c(\mu\beta, f) q_L^\mu.$$

Proof: The claimed operator U_β is the one defined by $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$\Gamma_{00}(\mathfrak{f}) \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \Gamma_{00}(\mathfrak{f}) = \cup_b \Gamma_{00}(\mathfrak{f}) \begin{pmatrix} 1 & b \\ 0 & \beta \end{pmatrix}.$$

where b ranges over all coset representatives of $\beta\mathfrak{D}$ in $\mathfrak{D}$ and the union is a disjoint union. Define

$$f|_k U_\beta(\tau) = \mathscr{N}(\beta)^{k/2-1} \sum_b f|_k \begin{pmatrix} 1 & b \\ 0 & \beta \end{pmatrix} (\tau),$$

where b runs through the set of coset representatives of $\beta\mathfrak{D}$ in $\mathfrak{D}$. Then

$$\begin{aligned} f|_k U_\beta(\tau) &= \mathscr{N}(\beta)^{k/2-1} \sum_b f|_k \begin{pmatrix} 1 & b \\ 0 & \beta \end{pmatrix} (\tau) \\ &= \mathscr{N}(\beta)^{k/2-1} \mathscr{N}(\beta)^{k/2} \mathscr{N}(\beta)^{-k} \sum_b f(\frac{\tau+b}{\beta}) \\ &= \mathscr{N}(\beta)^{-1} \sum_b \left(c(0,f) + \sum_\mu c(\mu,f) e^{2\pi i tr_{L/\mathbb{Q}}(\mu(\beta^{-1}\tau + \beta^{-1}b))} \right) \\ &= c(0,f) + \mathscr{N}(\beta)^{-1} \sum_\mu c(\mu,f) e^{2\pi i tr_{L/\mathbb{Q}}(\mu\tau/\beta)} (\sum_b e^{2\pi i tr_{L/\mathbb{Q}}(\mu b/\beta)}) \end{aligned}$$

The sum $\sum_b e^{2\pi i tr_{L/\mathbb{Q}}(\mu b/\beta)} = 0$ unless $\mu \in \beta O_L$. On the other hand, if $\mu \in \beta O_L$, then $\sum_b e^{2\pi i tr_{L/\mathbb{Q}}(\mu b/\beta)} = \mathscr{N}(\beta)$. Hence we get

$$f|_k U_\beta(\tau) = c(0,f) + \sum_\mu c(\mu\beta, f) q_L^\mu.$$

□

11 Eisenstein series

The following proposition is proven by Deligne-Ribet ([Del80], proposition 6.1).

Proposition 11.1 *Let L_Σ be the maximal abelian totally real extension of L unramified outside Σ. Let ε be a locally constant $\mathbb{C}$-valued function on $Gal(L_\Sigma/L)$. Then for every even positive integer k*
(i) There is an integral ideal $\mathfrak{f}$ of L with all its prime factors in Σ, and a Hilbert modular form $G_{k,\varepsilon}$ in $M_k(\Gamma_{00}(\mathfrak{f}),\mathbb{C})$ with standard q-expansion

$$2^{-r}L(\varepsilon,1-k)+\sum_{\mu}\Big(\sum_{\mathfrak{a}}\varepsilon(g_{\mathfrak{a}})N(\mathfrak{a})^{k-1}\Big)q_L^{\mu},$$

where the first sum ranges over all totally positive $\mu \in O_L$, and the second sum ranges over all integral ideals $\mathfrak{a}$ of L containing μ and prime to Σ. Here $g_{\mathfrak{a}}$ is the image of $\mathfrak{a}$ under the Artin symbol map. $N(\mathfrak{a})$ denotes norm of the ideal $\mathfrak{a}$.
(ii) Let q-expansion of $G_{k,\varepsilon}$ at the cusp determined by any $\alpha \in \mathbb{A}_L^\times$ has constant term

$$N^k((\alpha))2^{-r}L(\varepsilon_g,1-k),$$

where (α) is the ideal of L generated by α and $N((\alpha))$ is its norm. The element g is the image of (α) under the Artin symbol map (see for instance 2.22 in Deligne-Ribet [Del80]). The locally constant function ε_g is given by

$$\varepsilon_g(h)=\varepsilon(gh) \qquad \text{for all } h \in Gal(L_\Sigma/L).$$

12 The q-expansion principle

Let $f \in M_k(\Gamma_{00}(\mathfrak{f}),\mathbb{Q}))$ i.e. $c(\mu,\alpha,f) \in \mathbb{Q}$ for all $\mu \in O_L^+ \cup \{0\}$ and all $\alpha \in \mathbb{A}_L^\times$. Suppose the standard q-expansion of f has all non-constant coefficients in $\mathbb{Z}_{(p)}$ and let $\alpha \in \mathbb{A}_L^\times$ be a finite adele. Then

$$c(0,f)-N(\alpha_p)^{-k}c(0,\alpha,f) \in \mathbb{Z}_p.$$

Here $\alpha_p \in L\otimes_{\mathbb{Q}}\mathbb{Q}_p$ is the pth component of α and $N : L\otimes_{\mathbb{Q}}\mathbb{Q}_p \to \mathbb{Q}_p$ is the norm map. This is the q-expansion principle of Deligne-Ribet (see [Del80] 0.3 and 5.13-5.15).

Remark 12.1 *Hence if u is the image in $Gal(L_\Sigma/L)$ of an idèle α under the Artin symbol map, then using the equation $N((\alpha))^kN(\alpha_p)^{-k}=\kappa(u)^k$, we get*

$$c(0,G_{k,\varepsilon})-N(\alpha_p)^{-k}c(0,\alpha,G_{k,\varepsilon})=2^{-r}\Delta^u(\varepsilon,1-k),$$

for any positive even integer k.

13 Proof of the sufficient conditions in section 6

Proposition 13.1 *The sufficient condition in proposition (6.2) for proving proposition (3.1) holds. Hence M3 holds.*

Proof: We must show that for any $U \subset V$ in $S(\mathscr{G}, Z)$ such that $[V:U] = p$ and any $j \geq 0$, any coset y of Z^{p^j} in $\Delta \times U^{ab}$ fixed by V and any u in Z, we have the congruence

$$\Delta_U^{u^p}(\delta^{(y)}, 1-k) \equiv \Delta_V^u(\delta^{(y)} \circ ver_U^V, 1-pk) (\mathrm{mod}\ p\mathbb{Z}_p),$$

for all positive integers k divisible by $[F(\mu_p):F]$. Choose an integral ideal $\mathfrak{f}$ of F_V such that the Hilbert Eisenstein series $G_{k,\delta^{(y)}}$ and $G_{pk,\delta^{(y)}\circ ver_U^V}$, given by proposition (11.1), on $\mathfrak{H}_{F_U}$ and $\mathfrak{H}_{F_V}$ respectively are defined over $\Gamma_{00}(\mathfrak{f}O_{F_U})$ and $\Gamma_{00}(\mathfrak{f})$ respectively. Moreover, we may assume that all prime ideals dividing $\mathfrak{f}$ lie in Σ_{F_V} and $\mathfrak{f} \subset pO_{F_V}$. Define E by

$$E = R_{F_U/F_V}(G_{k,\delta^{(y)}})|_{pk}U_p - G_{pk,\delta^{(y)}\circ ver_U^V}.$$

Let $\alpha \in \mathbb{A}_{F_V}^{\times}$ whose image in $\Delta \times V^{ab}$ under the Artin symbol map coincides with u. Then by lemma 9.1 and remark 12.1

$$\begin{aligned} &c(0,E) - N(\alpha_p)^{-pk}c(0,\alpha,E) \\ &= 2^{-r_U}\Delta_U^{u^p}(\delta^{(y)}, 1-k) - 2^{-r_V}\Delta_V^u(\delta^{(y)} \circ ver_P^{P'}, 1-pk). \end{aligned}$$

Note that the image of α^* in $\Delta \times U^{ab}$ under the Artin symbol map is u^p. Since $2^{-r_U} \equiv 2^{-r_V} (\mathrm{mod}\ p)$ it is enough to prove, using the q-expansion principle, that the non-constant terms of the standard q-expansion of E all lie in $p\mathbb{Z}_{(p)}$ i.e. for all $\mu \in O_{F_V}^+$

$$\begin{aligned} &c(\mu, E) = c(p\mu, R_{F_U/F_V}(G_{k.\delta^{(y)}})) - c(\mu, G_{pk,\delta^{(y)}\circ ver_U^V}) \\ &= \sum_{(\mathfrak{b},\eta)} \delta^{(y)}(g_{\mathfrak{b}})N(\mathfrak{b})^{k-1} - \sum_{\mathfrak{a}} \delta^{(y)}(g_{\mathfrak{a}O_{F_U}})N(\mathfrak{a})^{pk-1} \in p\mathbb{Z}_{(p)} \end{aligned}$$

Here the pairs $(\mathfrak{b}, \eta)$ runs through all integral ideals $\mathfrak{b}$ of F_U which are prime to Σ_{F_U} and contains the totally positive element $\eta \in O_{F_U}$ and $tr_{F_U/F_V}(\eta) = p\mu$. The ideal $\mathfrak{a}$ runs through all integral ideals of F_V prime to Σ_{F_V} and contains μ. The group V/U acts trivially on the pair $(\mathfrak{b}, \eta)$ if and only if there is an ideal $\mathfrak{a}$ such that $\mathfrak{a}O_{F_U} = \mathfrak{b}$ and $\eta \in O_{F_V}$. In this case

$$\begin{aligned} &\delta^{(y)}(g_{\mathfrak{b}})N(\mathfrak{b})^{k-1} - \delta^{(y)}(g_{\mathfrak{a}O_{F_p}})N(\mathfrak{a})^{pk-1} \\ =&\delta^{(y)}(g_{\mathfrak{b}})(N(\mathfrak{a})^{p(k-1)} - N(\mathfrak{a})^{pk-1}) \\ \in& p\mathbb{Z}_{(p)}. \end{aligned}$$

On the other hand, if V/U does not act trivially on the $(\mathfrak{b},\eta)$, then the orbit of $(\mathfrak{b},\eta)$ under the action of V/U in the above sum is

$$\begin{aligned}&\sum_{g\in V/U}\left(\delta^{(y)}(gg_{\mathfrak{b}}g^{-1})N(\mathfrak{b}^g)^{k-1}\right)\\ =&|V/U|\delta^{(y)}(g_{\mathfrak{b}})N(\mathfrak{b})^{k-1}\\ \in& p\mathbb{Z}_{(p)}.\end{aligned}$$

Here we use $\delta^{(y)}(gg_{\mathfrak{b}}g^{-1}) = \delta^{(y)}(g_{\mathfrak{b}})$ because y is fixed under the action of V. This proves the proposition. $\square$

Lemma 13.2 *Let $U \in C(\mathscr{G},Z)$ be such that $P_c(U)$ is empty. Let N be a subgroup of $N_{\mathscr{G}}U$ containing U but different from U. Then the image of the transfer homomorphism*

$$ver : N^{ab} \to U$$

is a proper subgroup of U.

Proof: Recall the definition of transfer map. Let $g \in N$. Let $\{x_1,\dots,x_n\}$ be the double coset representatives of $\langle g\rangle\backslash N/U$. Let m be the smallest integer such that $g^m \in U$. Then a set of left coset representatives of U in N is

$$\{1,g,\dots,g^{m-1},x_1,gx_1,\dots,g^{m-1}x_1,\dots,x_n,gx_n,\dots,g^{m-1}x_n\}.$$

for all $0 \le i \le m-1$ and $1 \le j \le n$, we define $h_{ij}(g) \in U$ by

$$g(g^i x_j) = g^{i'} x_{j'} h_{ij}(g).$$

for a unique $0 \le i' \le m-1$ and $1 \le j' \le n$. Then

$$h_{ij}(g) = \begin{cases} 1 & \text{if } i \le m-2 \\ x_j^{-1} g^m x_j & \text{if } i = m-1 \end{cases}$$

Hence $ver(g) = \prod_{j=1}^{n} x_j^{-1} g^m x_j$. If $g \notin U$ then g^m is not a generator of U/Z because $P_c(U)$ is empty. Hence $ver(g)$ is not a generator of U/Z and the image of ver is a proper subgroup of U. On the other hand if $g \in U$ then

$$ver(g) = \prod_{x\in N/U} x^{-1} g x.$$

Since Z is central and both U/Z and N/Z are p-groups, the action of N/Z on the subgroup of order p of U/Z is trivial. If p^r is the order of g in U/Z, then N acts trivially on $g^{p^{r-1}} (\text{mod } Z)$. Hence

$$ver(g)^{p^{r-1}} = \prod_{x\in N/U} x^{-1} g^{p^{r-1}} x = \prod_{x\in N/U} g^{p^{r-1}} \in Z.$$

Hence $ver(g)$ is not a generator of U/Z and hence the image of ver is a proper subgroup of U. $\square$

Proposition 13.3 *The sufficient condition in proposition (6.4) for proving proposition (3.2) holds.*

Proof: We must show that for any $U \in C(\mathscr{G}, Z)$ such that $P_c(U)$ is empty and any $j \geq 0$, any coset y of Z^{p^j} in $\Delta \times U$ whose image in U/Z is a generator of U/Z and any u in Z we have

$$\Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) \equiv 0(\text{mod } |(W_{\mathscr{G}}U)_y|\mathbb{Z}_p),$$

for any positive integer k divisible by $[F(\mu_p):F]$. Choose an integral ideal $\mathfrak{f}$ of $O_{F_{N_{\mathscr{G}}U}}$ such that the Hilbert Eisenstein series $G_{k,\delta^{(y)}}$ over $\mathfrak{H}_{F_U}$, given by proposition (11.1), is defined on $\Gamma_{00}(\mathfrak{f}O_{F_U})$. Define

$$E = R_{F_U/F_{N_{\mathscr{G}}U}}(G_{k,\delta^{(y)}}).$$

Then E is a Hilbert modular form of weight $d_U k$ on $\Gamma_{00}(\mathfrak{f})$. Let α be a finite idèle of $F_{N_{\mathscr{G}}U}$ whose image under the Artin symbol map coincides with u. Then by lemma 9.1 and remark 12.1, we have

$$c(0,E) - N(\alpha_p)^{-d_U k} c(0,\alpha,E) = 2^{-r_U} \Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k).$$

Hence, using the q-expansion principle, it is enough to prove that the non-constant terms of the standard q-expansion of E all lie in $|(W_{\mathscr{G}}U)_y|\mathbb{Z}_{(p)}$ i.e. for any $\mu \in O^+_{F_{N_{\mathscr{G}}U}}$,

$$c(\mu,E) = \sum_{(\mathfrak{b},\nu)} \delta^{(y)}(g_{\mathfrak{b}}) N(\mathfrak{b})^{k-1} \in |(W_{\mathscr{G}}U)_y|\mathbb{Z}_{(p)},$$

where $(\mathfrak{b},\nu)$ runs through all integral ideals $\mathfrak{b}$ of F_U which are prime to Σ_{F_U} and $\nu \in \mathfrak{b}$ is totally positive with $tr_{F_U/F_{N_{\mathscr{G}}U}}(\nu) = d_U \mu$. The group $(W_{\mathscr{G}}U)_y$ acts on the pairs $(\mathfrak{b},\nu)$. Let V be the stabiliser of $(\mathfrak{b},\nu)$. Then there is an integral ideal $\mathfrak{c}$ of $F_V := F_U^V$ and a totally positive element η of O_{F_V} such that $\mathfrak{c}O_{F_U} = \mathfrak{b}$ and $\nu = \eta$. If V is a nontrivial group then $\delta^{(y)}(g_{\mathfrak{b}}) = 0$ by lemma (13.2). On the other hand, if V is trivial, then the $(W_{\mathscr{G}}U)_y$ orbit of $(\mathfrak{b},\nu)$ in the above sum is

$$\begin{aligned}
&\sum_{g \in (W_{\mathscr{G}}U)_y} \delta^{(y)}(g g_{\mathfrak{b}} g^{-1}) N(\mathfrak{b}^g)^{k-1} \\
=&|(W_{\mathscr{G}}U)_y| \delta^{(y)}(g_{\mathfrak{b}}) N(\mathfrak{b})^{k-1} \\
\in&|(W_{\mathscr{G}}U)_y|\mathbb{Z}_{(p)}.
\end{aligned}$$

Here we use $\delta^{(y)}(g g_{\mathfrak{b}} g^{-1}) = \delta^{(y)}(g_{\mathfrak{b}})$ for any $g \in (W_{\mathscr{G}}U)_y$. This proves the proposition. $\square$

Proposition 13.4 *The sufficient condition in proposition (6.5) for proving proposition (3.3) holds.*

Proof: We have to show that for any $U \in C(\mathscr{G}, U)$ such that $P_c(U)$ is non-empty, any $j \geq 0$, any coset y of Z^{p^j} in $\Delta \times U$ and any u in Z, we have

$$\Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) \equiv \sum_{V \in P_c(U)} \Delta_V^{u^{d_U/p}}(\delta^{(y)} \circ \varphi_V, 1-pk) (\bmod\ |(W_{\mathscr{G}}U)_y|\mathbb{Z}_p),$$

for any positive integer k divisible by $[F(\mu_p):F]$.

Choose an integral ideal $\mathfrak{f}$ of $F_{N_{\mathscr{G}}U}$ such that the Hilbert Eisenstein series $G_{k,\delta^{(y)}}$ and $G_{pk,\delta^{(y)}\circ\varphi_V}$, given by proposition (11.1), on $\mathfrak{H}_{F_U}$ and $\mathfrak{H}_{F_V}$ respectively are defined over $\Gamma_{00}(\mathfrak{f}O_{F_U})$ and $\Gamma_{00}(\mathfrak{f}O_{F_V})$ respectively for every $V \in P_c(U)$. We may assume that all prime factors of $\mathfrak{f}$ are in $\Sigma_{F_{N_{\mathscr{G}}U}}$ and $\mathfrak{f} \subset d_U O_{F_{N_{\mathscr{G}}U}}$. Define

$$E = R_{F_U/F_{N_{\mathscr{G}}U}}(G_{k,\delta^{(y)}})|_{d_U k} U_{d_U} - \sum_{V \in P_c(U)} R_{F_V/F_{N_{\mathscr{G}}U}}(G_{pk,\delta^{(y)}\circ\varphi_V})|_{d_U k} U_{d_U/p}.$$

Then $E \in M_{d_U k}(\Gamma_{00}(\mathfrak{f}), \mathbb{C})$. Let α be a finite idèle of $F_{N_{\mathscr{G}}U}$ whose image under the Artin symbol map coincides with u. Then by lemma 9.1 and remark 12.1

$$\begin{aligned} &c(0,E) - N(\alpha_p)^{-d_U k} c(0,\alpha,E) \\ &= 2^{-r_U} \Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) - \sum_{V \in P_c(U)} 2^{-r_U/p} \Delta_V^{u^{d_U/p}}(\delta^{(y)} \circ \varphi_V, 1-pk). \end{aligned}$$

As $2^{-r_U} \equiv 2^{-r_U/p} (\bmod\ r_U)$ and $r_U \geq |(W_{\mathscr{G}}U)_y|$,

$$\begin{aligned} &2^{-r_U} \Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) - \sum_{V \in P_c(U)} 2^{-r_U/p} \Delta_V^{u^{d_U/p}}(\delta^{(y)} \circ \varphi_V, 1-pk) \\ \equiv &2^{-r_U} \Big(\Delta_U^{u^{d_U}}(\delta^{(y)}, 1-k) - \sum_{V} \Delta_V^{u^{d_U/p}}(\delta^{(y)} \circ \varphi_V, 1-pk) \Big) (\bmod\ |(W_{\mathscr{G}}U)_y|\mathbb{Z}_p). \end{aligned}$$

Hence using the q-expansion principle it is enough to prove that the non-constant terms of the standard q-expansion of E all lie in $|(W_{\mathscr{G}}U)_y|\mathbb{Z}_{(p)}$ i.e. for all totally positive μ in $O_{F_{N_{\mathscr{G}}U}}$, we have

$$\begin{aligned} c(\mu,E) &= c(d_U\mu, R_{F_U/F_{N_{\mathscr{G}}U}}(G_{k,\delta^{(y)}})) - \sum_{V \in P_c(U)} c(d_U\mu/p, R_{F_V/F_{N_{\mathscr{G}}U}}(G_{pk,\delta^{(y)}\circ\varphi_V})) \\ &= \sum_{(\mathfrak{b},\eta)} \delta^{(y)}(g_{\mathfrak{b}}) N(\mathfrak{b})^{k-1} - \sum_{V \in P_c(U)} \sum_{(\mathfrak{a},\nu)} \delta^{(y)}(g_{\mathfrak{a}O_{F_U}}) N(\mathfrak{a})^{pk-1} \in |(W_{\mathscr{G}}U)_y|\mathbb{Z}_{(p)}. \end{aligned}$$

Here the pair $(\mathfrak{b},\eta)$ runs through all integral ideals $\mathfrak{b}$ of F_U which are prime to Σ_{F_U} and $\eta \in \mathfrak{b}$ is a totally positive element with $tr_{F_U/F_{N_{\mathscr{G}}U}}(\eta) = d_U\mu$. The pair $(\mathfrak{a},\nu)$ runs through all integral ideals $\mathfrak{a}$ of F_V which are prime to Σ_{F_V} and $\nu \in \mathfrak{a}$ is a totally positive element with $tr_{F_V/F_{N_{\mathscr{G}}U}}(\nu) = d_U\mu/p$. The group $P := (W_{\mathscr{G}}U)_y$ acts on the pairs $(\mathfrak{b},\eta)$ and $(\mathfrak{a},\nu)$. Let $W \subset P$ be the stabiliser of $(\mathfrak{b},\eta)$. Then there is an integral ideal $\mathfrak{c}$ of $F_W := F_U^W$ and a totally positive element γ in O_{F_W} such that $\mathfrak{c}O_{F_U} = \mathfrak{b}$ and $\eta = \gamma$. Then the P orbit of $(\mathfrak{b},\eta)$ in the above sum is

$$\begin{aligned}
&\sum_{g \in P/W} \Big(\delta^{(y)}(g g_{\mathfrak{b}} g^{-1}) N(\mathfrak{b}^g)^{k-1} - \sum_{W \supset V \in P_c(U)} \delta^{(y)}(g g_{\mathfrak{b}} g^{-1}) N(\mathfrak{b}^g)^{pk-1} \Big) \\
=&|P/W| \delta^{(y)}(g_{\mathfrak{b}}) \Big(N(\mathfrak{b})^{k-1} - N(\mathfrak{b})^{pk-1} \Big) \\
=&|P/W| \delta^{(y)}(g_{\mathfrak{b}}) \Big(N(\mathfrak{c})^{|W|(k-1)} - N(\mathfrak{c})^{|W|(pk-1)/p} \Big) \\
\in&|P|\mathbb{Z}_{(p)}.
\end{aligned}$$

The second sum is 0 if W is trivial and in that case inclusion in the last line is trivial. The first equality uses $\delta^{(y)}(g g_{\mathfrak{b}} g^{-1}) = \delta^{(y)}(g_{\mathfrak{b}})$ as $g \in P$. The last inclusion is because $N(\mathfrak{c})^{|W|} \equiv N(\mathfrak{c})^{|W|/p} (\mathrm{mod}\ |W|)$. This proves the proposition. $\square$

Proposition 13.5 *The sufficient conditions in proposition (6.6) for proving proposition (3.4) hold.*

Proof: We just prove the sufficient condition for congruence (4). Proof of the other sufficient condition in proposition (6.6) is similar. We must show that for any $U \in C(\mathscr{G},Z)$ and $V \in P_c(U)$, for any $j \geq 0$, any coset y of Z^{p^j} in $\Delta \times U$ and any u in Z

$$\Delta_U^{u^{pd_V}}(\delta^{(y)}, 1-k) \equiv \Delta_V^{u^{d_V}}(\delta^{(y)} \circ \varphi_V, 1-pk) (\mathrm{mod}\ |(N_{\mathscr{G}}V/U)_y|\mathbb{Z}_p),$$

for any positive integer k divisible by $[F(\mu_p):F]$.

Choose an integral ideal $\mathfrak{f}$ of $F_{N_{\mathscr{G}}V}$ such that the Hilbert Eisenstein series $G_{k,\delta^{(y)}}$ and $G_{pk,\delta^{(y)}\circ\varphi_V}$, given by proposition (11.1), on $\mathfrak{H}_{F_U}$ and $\mathfrak{H}_{F_V}$ respectively are defined over $\Gamma_{00}(\mathfrak{f}O_{F_U})$ and $\Gamma_{00}(\mathfrak{f}O_{F_V})$ respectively. Moreover, we may assume that all prime factors of $\mathfrak{f}$ are in $\Sigma_{F_{N_{\mathscr{G}}V}}$ and $\mathfrak{f} \subset pd_V O_{F_{N_{\mathscr{G}}V}}$. Define

$$E = R_{F_U/F_{N_{\mathscr{G}}V}}(G_{k,\delta^{(y)}})|_{pd_V k} U_{pd_V} - R_{F_V/F_{N_{\mathscr{G}}V}}(G_{pk,\delta^{(y)}\circ\varphi_V})|_{pd_V k} U_{d_V}.$$

Then $E \in M_{pd_V k}(\Gamma_{00}(\mathfrak{f}),\mathbb{C})$. Let α be a finite idèle of $F_{N_{\mathscr{G}}V}$ whose image under the Artin symbol map coincides with u. Then by lemma 9.1 and remark 12.1

$$c(0,E) - N(\alpha_p)^{-pd_V} c(0,\alpha,E) = 2^{-r_U} \Delta_U^{u^{pd_V}}(\delta^{(y)}, 1-k) - 2^{-r_V} \Delta_V^{u^{d_V}}(\delta^{(y)} \circ \varphi_V, 1-pk).$$

As $2^{-r_U} \equiv 2^{-r_V} (\mathrm{mod}\ r_U)$ and $r_U \geq |(N_{\mathscr{G}}V/U)_y|$,

$$\begin{aligned}
&2^{-r_U} \Delta_U^{u^{pd_V}}(\delta^{(y)}, 1-k) - 2^{-r_V} \Delta_V^{u^{d_V}}(\delta^{(y)} \circ \varphi_V, 1-pk) \\
\equiv&2^{-r_U} \Big(\Delta_U^{u^{pd_V}}(\delta^{(y)}, 1-k) - \Delta_V^{u^{d_V}}(\delta^{(y)} \circ \varphi_V, 1-pk) \Big) (\mathrm{mod}\ |(N_{\mathscr{G}}V/U)_y|\mathbb{Z}_p).
\end{aligned}$$

Hence using the q-expansion principle it is enough to prove that the non-constant terms of the standard q-expansion of E all lie in $|(N_{\mathscr{G}}V/U)_y|\mathbb{Z}_{(p)}$ i.e. for all totally positive μ in $O_{F_{N_{\mathscr{G}}V}}$ we have

$$\begin{aligned}c(\mu,E) &= c(pd_V\mu, R_{F_U/F_{N_{\mathscr{G}}V}}(G_{k,\delta^{(y)}})) - c(d_V\mu, R_{F_V/F_{N_{\mathscr{G}}V}}(G_{pk,\delta^{(y)}\circ\varphi_V}))\\ &= \sum_{(\mathfrak{b},\eta)} \delta^{(y)}(g_{\mathfrak{b}})N(\mathfrak{b})^{k-1} - \sum_{(\mathfrak{a},\nu)} \delta^{(y)}(g_{\mathfrak{a}O_{F_U}})N(\mathfrak{a})^{pk-1} \in |(N_{\mathscr{G}}V/U)_y|\mathbb{Z}_{(p)}.\end{aligned}$$

Here the pairs $(\mathfrak{b},\eta)$ run through all integral ideals $\mathfrak{b}$ of F_U which are prime to Σ_{F_U} and $\eta \in \mathfrak{b}$ is a totally positive element with $tr_{F_U/F_{N_{\mathscr{G}}V}}(\eta) = pd_V\mu$. The pairs $(\mathfrak{a},\nu)$ run through all integral ideals $\mathfrak{a}$ of F_V which are prime to Σ_{F_V} and $\nu \in \mathfrak{a}$ is a totally positive element with $tr_{F_V/F_{N_{\mathscr{G}}V}}(\nu) = d_V\mu$. The group $P := (N_{\mathscr{G}}V/U)_y$ acts on the pairs $(\mathfrak{b},\eta)$ and $(\mathfrak{a},\nu)$. Let $W \subset P$ be the stabiliser of $(\mathfrak{b},\eta)$. Then there is an integral ideal $\mathfrak{c}$ of $F_W := F_U^W$ and a totally positive element γ of O_{F_W} such that $\mathfrak{c}O_{F_U} = \mathfrak{b}$ and $\eta = \gamma$. First assume that W is a non-trivial group. Then the P orbit of $(\mathfrak{b},\eta)$ in the above sum is

$$\begin{aligned}&\sum_{g\in P/W}\Big(\delta^{(y)}(gg_{\mathfrak{b}}g^{-1})N(\mathfrak{b}^g)^{k-1} - \delta^{(y)}(gg_{\mathfrak{b}}g^{-1})N(\mathfrak{b}^g)^{pk-1}\Big)\\ =&|P/W|\delta^{(y)}(g_{\mathfrak{b}})\Big(N(\mathfrak{b})^{k-1} - N(\mathfrak{b})^{pk-1}\Big)\\ =&|P/W|\delta^{(y)}(g_{\mathfrak{b}})\Big(N(\mathfrak{c})^{|V|(k-1)} - N(\mathfrak{c})^{|V|(pk-1)/p}\Big)\\ \in&|P/W|\mathbb{Z}_{(p)}.\end{aligned}$$

On the other hand if W is a trivial group then the P orbit of the pair $(\mathfrak{b},\eta)$ in the above sum is

$$\sum_{g\in P}\delta^{(y)}(gg_{\mathfrak{b}}g^{-1})N(\mathfrak{b}^g)^{k-1} = |P|\delta^{(y)}(g_{\mathfrak{b}})N(\mathfrak{b})^{k-1}.$$

In both cases the first equality uses $\delta^{(y)}(gg_{\mathfrak{b}}g^{-1}) = \delta^{(y)}(g_{\mathfrak{b}})$ for $g \in P$. In the first case we also use the fact that $N(\mathfrak{c})^{|W|} \equiv N(\mathfrak{c})^{|W|/p} (\mathrm{mod}\ |W|)$. This proves the proposition. □

14 Proof of M4. from the basic congruences

We have proved the basic congruences in previous subsections. We want to deduce M4 from these congruences. However, we cannot do it directly for the extension F_∞/F. We use the following trick: we extend our field slightly to $\tilde{F}_\infty \supset F_\infty$ such that $\tilde{F}_\infty/F$ is an admissible p-adic Lie extension satisfying the Iwasawa conjecture and $Gal(\tilde{F}_\infty/F) = \Delta \times \tilde{\mathscr{G}}$ with $\tilde{\mathscr{G}} \cong \tilde{H} \times \mathscr{G}$, where $\tilde{H}$ is a cyclic group of order $|\mathscr{G}/Z|$. We know the basic congruences for $\tilde{F}_\infty/F$ which we use to deduce the M4 for $\tilde{F}_\infty/F$. This proves the main conjecture for $\tilde{F}_\infty/F$ and hence implies the main conjecture for F_∞/F.

14.1 The field $\tilde{F}_\infty$

Choose a prime l large enough such that $l \equiv 1 (\text{mod } |\mathscr{G}/Z|)$ and $\mathbb{Q}(\mu_l) \cap F_\infty = \mathbb{Q}$. Let K be the extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_l)$ such that $[K : \mathbb{Q}] = |\mathscr{G}/Z|$. Define $\tilde{F} = KF$ and $\tilde{F}_\infty = \tilde{F}F_\infty$. Then

$$Gal(\tilde{F}_\infty/F) = Gal(\tilde{F}/F) \times Gal(F_\infty/F) =: \tilde{H} \times \Delta \times \mathscr{G} =: \Delta \times \tilde{\mathscr{G}}.$$

14.2 A key lemma

We extend the field F_∞ to $\tilde{F}_\infty$ as we need the following key lemma. For any $U \in C(\tilde{\mathscr{G}}, Z)$, define the integer i_U by

$$i_U = max_{V \in C(\tilde{\mathscr{G}},Z)}\{[V : U] | U \subset V\}$$

Lemma 14.1 *Let $U \in C(\tilde{\mathscr{G}}, Z)$. If $U \neq Z$, then*

$$T_U \subset p i_U^2 \Lambda(U).$$

And

$$T_Z = |\tilde{\mathscr{G}}/Z| \Lambda(Z).$$

Similar statements hold for $T_{U,S}$ and $\widehat{T_U}$.

Proof: Case 1: $U/Z \subset \tilde{H}$. Then $i_U = [\tilde{H} : (U/Z)]$ and $N_{\tilde{\mathscr{G}}}U = \tilde{\mathscr{G}}$ acts trivially on $\Lambda(U)$. Hence

$$T_U = [\tilde{\mathscr{G}} : U]\Lambda(U) = |\mathscr{G}/Z|[\tilde{H} : (U/Z)]]\Lambda(U).$$

If $U \neq Z$, then $|\mathscr{G}/Z| \geq p i_U$. Hence the claim.
Case 2: $U/Z \not\subseteq \tilde{H}$. Let U/Z be generated by $(\tilde{h}, h)$, with $\tilde{h} \in \tilde{H}$ and $h \in \mathscr{G}/Z$. By assumption $h \neq 1$. Let $V \in C(\tilde{\mathscr{G}}, Z)$ such that $[V : U] = i_U$. Let $(\tilde{h}_0, h_0)$ be a generator of V/Z such that $\tilde{h}_0^{i_U} = \tilde{h}$ and $h_0^{i_U} = h$. Now note that

$$\tilde{H} \times \langle h_0 \rangle \subset N_{\tilde{\mathscr{G}}/Z}(U/Z)$$

acts trivially on $\Lambda(U)$. As $U/Z \subset \tilde{H} \times \langle h_0 \rangle$ this implies that

$$\begin{aligned} T_U &\subset \frac{|\tilde{H} \times \langle h_0 \rangle|}{|U/Z|} \Lambda(U) \\ &= \frac{|\tilde{H}||\langle h_0 \rangle|}{|U/Z|} \Lambda(U) \\ &= |\tilde{H}| i_U \Lambda(U) \\ &\subset p i_U^2 \Lambda(U). \end{aligned}$$

The last containment holds because $|\tilde{H}| \geq p i_U$. The assertion about T_Z is clear. $\square$

14.3 Completion of the proof

Lemma 14.2 *For any $U \in C(\tilde{\mathscr{G}}, Z)$ and any $0 \leq k \leq p-1$, we have*

$$\zeta_U - \omega_U^k(\zeta_U) \in \mathfrak{p} \frac{T_{U,S}}{i_U}.$$

Hence $\zeta_U^p / \prod_{k=0}^{p-1} \omega_U^k(\zeta_U) \in 1 + pT_{U,S}/i_U$.

Proof: We use reverse induction on $|U/Z|$. When U/Z is a maximal cyclic subgroup $i_U = 1$ and the required congruence is proven in proposition 3.2. In general we use the congruence in proposition 3.3 so that

$$\zeta_U - \omega_U^k(\zeta_U) \equiv \sum_{V \in P_c(U)} \Big(\varphi_V(\zeta_V) - \omega_U^k(\varphi_V(\zeta_V)) \Big) \tag{24}$$

$$= \sum_{V \in P_c(U)} \varphi_V(\zeta_V - \omega_V^k(\zeta_V)) (\mathrm{mod}\ \mathfrak{p} T_{U,S}), \tag{25}$$

for appropriately chosen ω_U and ω_V. But by induction hypothesis

$$\zeta_V - \omega_V^k(\zeta_V) \in \mathfrak{p} \frac{T_{V,S}}{i_V}.$$

Now for any $V \in P_c(U)$, note that

$$\varphi_V(\sum_{x \in N_{\tilde{\mathscr{G}}} U / N_{\tilde{\mathscr{G}}} V} x T_{V,S} x^{-1}) \subset \frac{T_{U,S}}{p}.$$

This finishes the proof of the first assertion noting that $i_U = p i_V$. Hence

$$\zeta_U^p / \big(\prod_{k=0}^{p-1} \omega_U^k(\zeta_U) \big) \in 1 + \mathfrak{p} T_{U,S} / i_U.$$

But since it is invariant under action of the group $Gal(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$, we get

$$\zeta_U^p/\Big(\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)\Big)\in 1+pT_{U,S}/i_U.$$

□

Using the above lemma

$$log(\frac{\omega_U^k(\zeta_U)}{\zeta_U})\equiv 1-\frac{\omega_U^k(\zeta_U)}{\zeta_U}\mathrm{mod}\ (\mathfrak{p}\widehat{T_U}/i_U)^2,$$

which implies

$$log\Big(\frac{\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}{\zeta_U^p}\Big)\equiv\frac{p\zeta_U-\sum_{k=0}^{p-1}\omega_U^k(\zeta_U)}{\zeta_U}(\mathrm{mod}\ (p\widehat{T_U}/i_U)^2).$$

Then

$$\begin{aligned}
&log\Big(\frac{\prod_{V\in P_c(U)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_U^p/\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}\Big)\\
&\equiv\sum_{V\in P_c(U)}\Big(\frac{p\varphi_V(\zeta_V)-\sum_{k=0}^{p-1}\omega_U^k(\varphi_V(\zeta_V))}{\varphi_V(\zeta_V)}\Big)-\Big(\frac{p\zeta_U-\sum_{k=0}^{p-1}\omega_U^k(\zeta_U)}{\zeta_U}\Big)\\
&\equiv\sum_{V\in P_c(U)}\Big(\frac{p\varphi_V(\zeta_V)-\sum_{k=0}^{p-1}\omega_U^k(\varphi_V(\zeta_V))}{\varphi_V(\zeta_V)}\Big)-\sum_V\Big(\frac{p\varphi_V(\zeta_V)-\sum_{k=0}^{p-1}\omega_U^k(\zeta_V)}{\zeta_U}\Big)\\
&\equiv\sum_{V\in P_c(U)}\frac{(p\varphi(\zeta_V)-\sum_{k-0}^{p-1}\omega_U^k(\varphi_V(\zeta_V)))(\zeta_U-\varphi_V(\zeta_V))}{\zeta_U\varphi_V(\zeta_V)}(\mathrm{mod}\ p\widehat{T_U}).
\end{aligned}$$

Here we use $(p\widehat{T_U}/i_U)^2\subset p\widehat{T_U}$ as implied by lemma 14.1. The second congruence above uses congruence 25. Now note that

$$p\varphi_V(\zeta_V)-\sum_{k=0}^{p-1}\omega_U^k(\varphi_V(\zeta_V))\in p\varphi_V(T_{V,S}/i_V)\qquad\text{(by lemma 14.2)}$$

and

$$\zeta_U-\varphi_V(\zeta_V)\in T_{U,S}^{N_{\mathscr{G}}V}\qquad\text{(by congruence (4) and (5)).}$$

Hence

$$\begin{aligned}
&\big(p\varphi_V(\zeta_V)-\sum_{k=0}^{p-1}\omega_U^k(\varphi_V(\zeta_V))\big)\big(\zeta_U-\varphi_V(\zeta_V)\big)\\
&\in p\varphi_V(T_{V,S})/i_V)\cdot T_{U,S}^{N_{\mathscr{G}}V}\subset pT_{U,S}^{N_{\mathscr{G}}V}.
\end{aligned}$$

Which in turn implies that

$$\sum_{V\in P_c(U)}\Big((p\varphi_V(\zeta_V)-\sum_{k-0}^{p-1}\omega_U^k(\varphi(\zeta_V)))(\zeta_U-\varphi_V(\zeta_V))\Big)\in pT_{U,S}.$$

Hence

$$log\Big(\frac{\prod_{V\in P_c(U)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_U^p/\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}\Big)\in p\widehat{T_U}.$$

As log induces an isomorphism between $1+p\widehat{T_U}$ and $p\widehat{T_U}$, we have

$$\frac{\prod_{V\in P_c(U)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_U^p/\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}\in 1+p\widehat{T_U}.$$

But by lemma 14.2 $\frac{\prod_{V\in P_c(U)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_U^p/\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}\in 1+pT_{U,S}/i_U$ and

$$1+p\widehat{T}_U\cap 1+pT_{U,S}/i_U=1+pT_{U,S}.$$

Hence

$$\frac{\prod_V\varphi_V(\alpha_V(\zeta_V))}{\zeta_U^p/\prod_{k=0}^{p-1}\omega_U^k(\zeta_U)}\in 1+pT_{U,S}.$$

When $U\neq Z$, this is the required congruence M4. When $U=Z$, note that

$$\prod_{k=0}^{p-1}\omega_Z^k(\zeta_Z)=\zeta_0.$$

This can be seen either by interpolation properties of $\prod_{k=0}^{p-1}\omega_Z^k(\zeta_Z)$ and ζ_0. Hence we get

$$\frac{\prod_{V\in P_c(Z)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_Z^p/\zeta_0}\in 1+pT_{Z,S}.$$

Now use the basic congruence (5) which says $\zeta_0\equiv\varphi_Z(\zeta_Z)(\text{mod }p|\tilde{\mathscr{G}}/Z|)$. Note that $T_{Z,S}=|\tilde{\mathscr{G}}/Z|\Lambda(Z)_S$. Hence

$$\frac{\prod_{V\in P_c(Z)}\varphi_V(\alpha_V(\zeta_V))}{\zeta_Z^p/\varphi_Z(\zeta_Z)}\in 1+pT_{Z,S}.$$

This is M4 for $U=Z$. This finishes proof of the main conjecture.

References

[Coa05] Coates, J. and Fukaya, T. and Kato, K. and R. Sujatha and Venjakob, O., *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES (2005), 163–208.

[Coa11] Coates, J. and Kim, D., *Introduction to the work of M. Kakde on the non-commutative*

main conjectures for totally real fields, This volume, 2011.
[Del80] Deligne, P and Ribet, Kenneth A., *Values of abelian L-functions at negative integers over totally real fields.*, Inventiones Math. **59** (1980), 227–286.
[Kak10] Kakde, M., K_1 *of some noncommutative p-adic group rings*, Preprint, March 2010.
[Kli62] Klingen, H., *Über die werte der Dedekindschen Zetafunktionen*, Math. Ann. (1962), 265–272.
[Sch11] Schneider, Peter and Venjakob, Otmar, K_1 *of certain Iwasawa algebras, after Kakde*, This volume, 2011.
[Sei70] Seigel, C., *Über die Fourierschen Koeffizienten von Modulformen*, Göttingen Nachr. **3** (1970), 15–56.
[Ser77] Serre, J-P, *Linear representation of finite groups*, Springer-Verlag, 1977.
[Suj11] Sujatha, R., *Reductions of the main conjecture*, This volume, 2011.