

On the transfer congruence between p -adic Hecke L -functions

DOHYEONG KIM

We prove the transfer congruence between p -adic Hecke L -functions for CM fields over cyclotomic extensions, which is a non-abelian generalization of the Kummer's congruence. The ingredients of the proof include the comparison between Hilbert modular varieties, the q -expansion principle, and some modification of Hsieh's Whittaker model for Katz' Eisenstein series. As a first application, we prove explicit congruence between special values of Hasse-Weil L -function of a CM elliptic curve twisted by Artin representations. As a second application, we prove the existence of a non-commutative p -adic L -function in the algebraic K_1 -group of the completed localized Iwasawa algebra.

1	Introduction	356
2	Hilbert modular forms and q-expansion principle	359
2.1	Hilbert modular forms	359
2.2	q -expansion of Hilbert modular forms	361
2.3	Λ -adic Hilbert modular forms	362
2.4	CM points	364
2.5	Restriction along the diagonal	369
3	Toric Eisenstein series and p-adic L-functions	373
3.1	Normalization of epsilon factors	375
3.2	Fourier coefficients of Eisenstein series	376
3.3	The local Whittaker integrals	380
3.4	Normalized Eisenstein series	381
3.5	Measures and Iwasawa algebra	385

3.6	<i>p</i> -adic interpolation of Fourier coefficients	385
3.7	A modification factor	388
3.8	<i>p</i> -adic <i>L</i> -function	391
3.9	Remarks on Iwasawa main conjecture and μ -invariants	393
4	Transfer congruence	394
4.1	The normalized diagonal embedding	395
4.2	Properties of Katz' <i>p</i> -adic modular forms	397
4.3	A map between <i>p</i> -adic modular forms	399
4.4	Proof of the main theorem	400
4.5	Verifying the conditions (P'), (I) and (C)	415
5	Applications to the false Tate curve extensions	419
5.1	Algebraic preliminaries	420
5.2	Specialization to the false Tate curve extensions	422
5.3	Congruence between special values of <i>L</i> -functions	426
5.4	The interpolation formula for $\mathcal{L}(G)$	432
	Acknowledgement	436
	References	436

1. Introduction

One of the major themes of number theory is the relationship between the critical values of *L*-functions of motives and the arithmetic of these motives. Iwasawa theory asserts, among many other things, that there is a precise relationship between the two, provided we vary both in suitable *p*-adic families. A rigorous formulation of such an equality is usually called a main conjecture of Iwasawa theory.

In traditional Iwasawa theory one works with an odd prime *p* which is ordinary for the given motive, and an abelian *p*-adic Lie extension H_∞ of a number field *H*. Let \mathcal{G} be the Galois group $\text{Gal}(H_\infty/H)$. Given a motivic *L*-function, the suitably normalized critical values of its twist by characters of \mathcal{G} are expected to admit a *p*-adic analytic interpolation, and a *p*-adic *L*-function

is a p -adic analytic function defined on a certain domain that achieves this desired interpolation. The Iwasawa main conjecture in this situation is then the assertion that such a p -adic L -function is equal to a suitably defined characteristic element of the Selmer group of the motive over H_∞ . Of course, the Selmer group encodes the arithmetic of the motive over H_∞ .

Non-commutative Iwasawa theory proposed by [3, 7] generalizes traditional Iwasawa theory in order to enable one to work with a possibly non-commutative p -adic Lie Galois group \mathcal{G} . In this case, a characteristic element of the Selmer group of the motive over H_∞ lies in the algebraic K_1 group of a suitably localized version of the Iwasawa algebra of \mathcal{G} . Hence we expect the p -adic L -function to be inside the same K_1 -group, and, at the same time, to interpolate suitably normalized L -values. We call such p -adic L -function commutative (resp. non-commutative) if \mathcal{G} is commutative (resp. non-commutative). Although we have plenty of examples of commutative p -adic L -functions, no non-commutative examples have yet been proven to exist for motives other than the Tate motive. For the Tate motive and a totally real H_∞ , Kakde and Ritter-Weiss independently established the existence of the non-commutative p -adic L -function and proved the associated main conjecture, assuming the vanishing of certain μ -invariants. Their result is unconditional when the base field H is abelian over \mathbb{Q} , since the theorem of Ferrero-Washington proves the vanishing of μ -invariants for such fields.

One of the key aspects of the work of Kakde and Ritter-Weiss is to formulate and prove non-commutative generalizations of the Kummer congruence, following an idea of Kato [16]. Specifically, they list a set of congruences between commutative p -adic L -functions implied by the existence of a non-commutative p -adic L -function, and show that in certain cases those congruence in turn imply the existence of a non-commutative p -adic L -function. These predicted congruences between commutative p -adic L -functions are what we shall call non-commutative congruences.

The principal result of the present paper is Theorem 4.4.11, where we prove the transfer congruence between commutative p -adic Hecke L -functions, which is one of the most important non-commutative congruences. By a p -adic Hecke L -function, we shall mean the p -adic L -function interpolating Hecke L -values of p -ordinary CM fields which was first constructed by Katz [15], and later studied by Hida-Tilouine [11] and Hsieh [12]. Our method heavily depends on the work of Hsieh, in which the relevant Eisenstein series are constructed using Whittaker models. This is the key difference between Hsieh's approach and the earlier work. The theory of Whittaker models reduces the computation of Fourier expansion to purely local problems, and our proof crucially depends on this aspect of Hsieh's work.

Furthermore, this is not only a reconstruction of the same Eisenstein series, but the resulting p -adic L -functions in fact differ by certain factor which is not always a p -adic unit. This difference is crucial for us as this factor has a large p -adic valuation for the cases that are studied in the current paper, while it is a p -adic unit in the earlier work [13] of Hsieh.

We stress that our modification of the earlier definition of p -adic Hecke L -functions is vital even for commutative Iwasawa theory. Indeed, the abelian p -adic L -functions constructed by Katz, Hida-Tilouine and Hsieh definitely do not satisfy the main conjecture when the base field contains non-trivial p -power roots of unity. To the best of our knowledge, this fact seems to have been ignored in the earlier literature. We believe, although we cannot prove it, that our modified p -adic Hecke L -functions do indeed satisfy the main conjecture. We also think that it is highly probable that our modified p -adic Hecke L -functions will always have μ -invariant equal to zero, and it seems an interesting challenge to prove this assertion. See Subsection 3.9 and [17] for more details.

As a consequence of the transfer congruence, we will prove some results on the existence of non-commutative p -adic L -functions for some p -adic Galois groups \mathcal{G} , assuming certain μ -invariants vanish. The argument is almost identical to [14], but our result is conditional since we do not know the validity of the assumption on the vanishing of μ -invariants. Such a group \mathcal{G} shall be of the form

$$(1.0.1) \quad \mathcal{G} = \lim_{\leftarrow r} \text{Gal}(\mathcal{M}(\mu_{p^r}, m^{1/p^r})/\mathcal{M})$$

where \mathcal{M} is an imaginary quadratic field in which p splits, μ_{p^r} is the group of p^r -th roots of unity, and m is an integer. To avoid the trivial cases in which \mathcal{G} becomes abelian, we will always assume that m is a p -th power free integer, and m is neither 0, 1, or -1 . This type of extension is often called a false Tate curve extension. Unfortunately, even with the hypothesis on the vanishing of μ -invariants, we need to consider the completion of the localized Iwasawa algebra and take its K_1 -group, in order to produce a non-commutative p -adic L -function in it. If we assume the commutative main conjectures in addition, then our method will produce the non-commutative p -adic L -function which satisfies the main conjecture. For the details, see Section 5.

We now briefly outline the contents of the paper. In Section 2, we review the theory of Hilbert modular Shimura varieties and Hilbert modular forms. It is important to choose a good diagonal embedding between Hilbert modular Shimura varieties, so that we have controls over the CM points and the

cusps. In Section 3, we review the work of Hsieh [12]. Although it is clear from Hsieh’s computation, it was not explicitly pointed out in his papers that in certain cases it is possible to improve the p -integrality of p -adic L -function constructed by Katz and Hida-Tilouine. We explain how to modify Hsieh’s construction to obtain a p -integrally optimal measure. Also, we reformulate the work of Hsieh in the language of Λ -adic forms. Although we do not use any deep result about Λ -adic forms, the approach using Λ -adic forms is more convenient when we prove the transfer congruence. Section 4 contains the proof of the transfer congruences under the hypotheses (P’), (I) and (C), and the proof of these hypotheses for the p -ordinary CM fields of the form $\mathbb{Q}(\sqrt{-D}, \mu_{p^r})$ with $r \geq 1, D < 0$. In fact, as it will become clear in Subsection 4.5, the hypotheses (P’), (I), and (C) are formulated in order to axiomatize the properties of the cyclotomic \mathbb{Z}_p -extension that we use in the proofs. In Section 5, we explain the consequences on the existence of non-commutative p -adic L -functions and the associated non-commutative Iwasawa main conjecture, as well as the congruence between special values of L -functions in concrete terms.

2. Hilbert modular forms and q -expansion principle

In this section, we review Hilbert modular forms, Λ -adic forms, and the q -expansion principle. Also, we specify CM points on the Hilbert Shimura variety following [12], and study the behavior of those CM points under the diagonal embedding.

2.1. Hilbert modular forms

Let \mathbb{Q} be the field of rational numbers with a fixed algebraic closure $\overline{\mathbb{Q}}$. By a number field, we mean a subfield of $\overline{\mathbb{Q}}$ which is a finite extension of \mathbb{Q} . We write the ring of adeles associated to a number field H by \mathbb{A}_H , and use the convention that if \bullet is a set of places of H , a place of H , or a product of these two, then \mathbb{A}_H^\bullet denotes the ring of adeles whose component at the place dividing \bullet equals 1. For example, \mathbb{A}_H^∞ denotes the ring of finite adeles. Also, if g is an element of $\mathrm{GL}_2(\mathbb{A}_H)$ then we use similar convention for g^\bullet , and g_\bullet denotes the product of all v -component of g for v dividing \bullet .

Let \mathcal{F} be a totally real field, and we consider the algebraic group $\mathrm{GL}_2/\mathcal{F}$. Let I be the set of embedding of \mathcal{F} into the field of real numbers \mathbb{R} . Let \mathfrak{H} be the complex upper half plane, and let

$$(2.1.1) \quad X_+ = \mathfrak{H}^I = \{(\tau_\sigma)_{\sigma \in I} \mid \tau_\sigma \in \mathfrak{H}\}.$$

Let $\mathrm{GL}_2(\mathbb{R})_+$ be the subgroup of $\mathrm{GL}_2(\mathbb{R})$ whose elements have positive determinant. Then $\mathrm{GL}_2(\mathbb{R})_+$ acts on \mathfrak{H} by the linear fractional transformation

$$(2.1.2) \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})_+, \tau \in \mathfrak{H}.$$

Using the identification $\mathcal{F} \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^I$, we identify $\mathrm{GL}_2(\mathcal{F} \otimes_{\mathbb{Q}} \mathbb{R}) = \mathrm{GL}_2(\mathbb{R})^I$, and define $\mathrm{GL}_2(\mathcal{F} \otimes_{\mathbb{Q}} \mathbb{R})_+ = \mathrm{GL}_2(\mathbb{R})^I_+$. In particular, $\mathrm{GL}_2(\mathbb{R})^I_+$ acts on X_+ by componentwise linear fractional transformation. Let $\mathbb{Z}[I]$ be the free abelian group generated by I . A typical element $m \in \mathbb{Z}[I]$ is written as $\sum_{\sigma \in I} m_{\sigma} \sigma$. We often write $I = \sum_{\sigma \in I} \sigma$. For $g \in \mathrm{GL}_2(\mathbb{R})$ and $\tau \in \mathfrak{H}$, we put

$$(2.1.3) \quad J(g, \tau) = c\tau + d. \quad g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R}), \tau \in \mathfrak{H},$$

and for $g_{\infty} \in \mathrm{GL}_2(\mathbb{R})^I$ and $\tau \in X_+$, then we put

$$(2.1.4) \quad J(g_{\infty}, \tau)^m = \prod_{\sigma \in I} J(g_{\sigma}, \tau_{\sigma})^{m_{\sigma}}.$$

Now we define the space of Hilbert modular forms. Let k be an integer and K be an open compact subgroup of $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$. Let \mathbb{C} denote the field of complex numbers. Let $\mathrm{GL}_2(\mathcal{F})_+$ be the subgroup of $\mathrm{GL}_2(\mathcal{F})$ which consists of the elements with totally positive determinant. Then $\mathrm{GL}_2(\mathcal{F})_+$ acts on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$ from the left, $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$ acts on it from the right, and the two actions commute. Precisely speaking, for $\alpha \in \mathrm{GL}_2(\mathcal{F})_+$, $u \in \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$, and $(z, g^{\infty}) \in X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$, we define the action to be $\alpha(z, g^{\infty})u = (\alpha z, \alpha^{\infty} g^{\infty} u)$.

Definition 2.1.5. Define $M_k(K, \mathbb{C})$ to be the space of functions $f: X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty}) \rightarrow \mathbb{C}$ such that

1. for each $g^{\infty} \in \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$, $f(\cdot, g^{\infty}): X_+ \rightarrow \mathbb{C}$ is holomorphic,
2. for each $\alpha \in \mathrm{GL}_2(\mathcal{F})_+$ and $u \in K$, f satisfies

$$(2.1.6) \quad f(\alpha(z, g^{\infty})u) = J(\alpha, z)^{kI} f(z, g^{\infty}).$$

When $\mathcal{F} = \mathbb{Q}$, we add a growth condition at cusps in the definition of $M_k(K, \mathbb{C})$. The growth condition is automatically satisfied if $\mathcal{F} \neq \mathbb{Q}$ by the Koecher principle, which is our main interest in the current article.

2.2. q -expansion of Hilbert modular forms

We first introduce some notation. For a number field H , let \mathcal{O}_H be the ring of integers of H , and \mathfrak{d}_H the absolute different of H . For our fixed totally real field \mathcal{F} , we simply write $\mathcal{O} = \mathcal{O}_{\mathcal{F}}$ and $\mathfrak{d} = \mathfrak{d}_{\mathcal{F}}$. For a nonzero fractional ideal \mathfrak{a} of \mathcal{F} , we write $\mathfrak{a}^* = \mathfrak{a}^{-1}\mathfrak{d}^{-1}$. We consider the algebraic group $\mathrm{GL}_2/\mathcal{F}$, and for any \mathcal{F} -algebra R we denote by $\mathrm{GL}_2(R)$ the group of invertible 2×2 matrices over R . Let $V = \mathcal{F} \oplus \mathcal{F}$ be the two dimensional vector space over \mathcal{F} , which we regard as the space of row vectors of length two. For an \mathcal{F} -algebra R , we let $V_R = V \otimes_{\mathcal{F}} R$, on which $\mathrm{GL}_2(R)$ acts by multiplication from the right. We also define an action of $\mathrm{GL}_2(R)$ on V_R from the left by

$$(2.2.1) \quad g * x = x \cdot g^{-1} \det(g)$$

for $g \in \mathrm{GL}_2(R)$ and $x \in V_R$. The reason for defining the above left action in this way originates from Subsection 2.4. of [12], where the moduli problem for the Shimura variety is described using this left action.

Let $e_1 = (1, 0)$ and $e_2 = (0, 1)$ be vectors in V so that $V = \mathcal{F}e_1 \oplus \mathcal{F}e_2$. We denote by L the canonical lattice $\mathcal{O}e_1 \oplus \mathcal{O}^*e_2$ of V . For a positive integer N , we define

$$(2.2.2) \quad U(N) := \{g^\infty \in \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty) \mid g^\infty L \subset L, g \equiv 1 \pmod{N \cdot L}\}.$$

Let K be an open compact subgroup of $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$ which is of the form

$$(2.2.3) \quad K = \prod_{v < \infty} K_v$$

where v runs over the set of finite places of \mathcal{F} and K_v is an open compact subgroup of $\mathrm{GL}_2(\mathcal{F}_v)$. Define

$$(2.2.4) \quad K_p = \prod_{v|p} K_v$$

to be the product of K_v with $v|p$. We will always assume that $K \supset U(N)$ for some N , and that K_p is equal to K_p^0 which we define as

$$(2.2.5) \quad K_p^0 := \{g_p \in \mathrm{GL}_2(\mathcal{F}_p) \mid g_p * (L \otimes_{\mathcal{O}} \mathcal{O}_p) = L \otimes_{\mathcal{O}} \mathcal{O}_p\}.$$

For such an open compact subgroup $K \subset \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$ we define

$$(2.2.6) \quad K_1^n = \{g^\infty \in K \mid g_p \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{p^n}\}.$$

Let \mathfrak{c} be a non-zero fractional ideal of \mathcal{F} prime to pN . For each place v of \mathcal{F} prime to pN , choose $\mathfrak{c}_v \in \mathcal{F}_v$ such that $\mathfrak{c}_v \mathcal{O}_v = \mathfrak{c}_v$. For $v \mid pN$, let $\mathfrak{c}_v = 1$. Write $\mathfrak{c} = \prod_v \mathfrak{c}_v \in \mathbb{A}_{\mathcal{F}}^{\infty}$. For a fractional ideal \mathfrak{a} of \mathcal{F} , denote by \mathfrak{a}_+ the subset of \mathfrak{a} consisting of totally positive elements. For any ring R and a finitely generated semigroup $L \subset \mathcal{F}$, we write $R[[q^L]]$ for the set of formal power series

$$(2.2.7) \quad \sum_{\beta \in L_{\geq 0}} a_{\beta} q^{\beta}$$

where $L_{\geq 0} = \{0\} \cup (L \cap \mathcal{F}_+)$. We view $R[[q^L]]$ as a ring of formal power series, where the rule of associative and distributive multiplication is characterized by $q^{\beta_1} \cdot q^{\beta_2} = q^{\beta_1 + \beta_2}$ for $\beta_1, \beta_2 \in \mathcal{F}_+$. However, there is an exception to this, where we interpret q^{β} as a function. Given a holomorphic Hilbert modular form $f \in M_k(K, \mathbb{C})$, we consider the restriction of f to the component $X_+ \times [{}^1_0 \mathfrak{c}^{-1}]$, written as $f|_{(\mathcal{O}, \mathfrak{c}^{-1})}$. Then $f|_{(\mathcal{O}, \mathfrak{c}^{-1})}$ has Fourier expansion

$$(2.2.8) \quad f|_{(\mathcal{O}, \mathfrak{c}^{-1})}(q) = \sum_{\beta \in (N\mathfrak{c})_{\geq 0}^{-1}} a_{\beta}(f, \mathfrak{c}) q^{\beta}$$

where we interpret q^{β} as a function on X_+ defined by

$$(2.2.9) \quad q^{\beta}: \tau \mapsto \exp\left(\sum_{\sigma \in I} \sigma(\beta) \tau_{\sigma} 2\pi\sqrt{-1}\right).$$

The coefficients $a_{\beta}(f, \mathfrak{c})$ is independent of the choices for \mathfrak{c}_v , and (2.2.8) is called q -expansion of f at the cusp $(\mathcal{O}, \mathfrak{c}^{-1})$.

By the q -expansion principle, for a subring R of \mathbb{C} , we may define

$$(2.2.10) \quad M_k(\mathfrak{c}, K, R) := \{f \in M_k(K, \mathbb{C}) \mid f|_{(\mathcal{O}, \mathfrak{c}^{-1})} \in R[[q^{(N\mathfrak{c})^{-1}}]]\}.$$

Although this interpretation of q^{β} 's as variables in the Fourier expansion is important for our later computation, we keep viewing $R[[q^L]]$ as a ring of formal power series because such an interpretation is not available when we consider $R[[q^L]]$ for a ring R that is not contained in \mathbb{C} .

2.3. Λ -adic Hilbert modular forms

We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of \mathbb{Q}_p and let \mathbb{C}_p be the completion of $\overline{\mathbb{Q}}_p$. Let \mathcal{I} be the ring of Witt vectors of an algebraic closure of the finite field

of p element, and we fix an embedding of \mathcal{I} into \mathbb{C}_p . We will always regard \mathcal{I} as a subring of \mathbb{C}_p . Also, we fix embeddings $i_\infty: \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $i_p: \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

We say that a ring R is a p -adic ring if the natural map $R \rightarrow \lim R/p^n R$ is an isomorphism, where the inverse limit is taken over the set of all positive integers n . Of course, a p -adic ring R is a \mathbb{Z}_p -algebra. For a fractional ideal \mathfrak{c} of \mathcal{F} prime to pN , we would like to define the space of R -adic Hilbert modular forms which we will denote by $V(\mathfrak{c}, K; R)$. Consider a formal power series

$$(2.3.1) \quad f = \sum_{\beta \in (N\mathfrak{c})_{\geq 0}^{-1}} a_\beta(f) q^\beta \in R[[q^{(N\mathfrak{c})^{-1}}]].$$

For any \mathbb{Z}_p -algebra homomorphism

$$(2.3.2) \quad \alpha: R \rightarrow \mathbb{C}_p$$

define

$$(2.3.3) \quad \alpha(f) = \sum_{\beta \in (N\mathfrak{c})_{\geq 0}^{-1}} \alpha(a_\beta(f)) q^\beta \in \mathbb{C}_p[[q^{(N\mathfrak{c})^{-1}}]].$$

We say a family Y consisting of \mathbb{Z}_p -algebra homomorphisms $\alpha: R \rightarrow \mathbb{C}_p$ is Zariski dense if an element $\mathcal{M} \in R$ is determined by $\alpha(\mathcal{M})$ for $\alpha \in Y$.

Definition 2.3.4. We say f is an R -adic Hilbert modular form, or simply an R -adic modular form, if there is a Zariski dense set Y for R such that for every $\alpha \in Y$ we have

$$(2.3.5) \quad \alpha(f) = \sum_{\beta \in (N\mathfrak{c})_{\geq 0}^{-1}} i_p(a_\beta(g_\alpha)) q^\beta$$

for some element g_α of $M_k(\mathfrak{c}, K_1^n, \overline{\mathbb{Q}})$, where K_1^n is an open compact subgroup of $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$ defined in (2.2.6). Here k and n may vary with α . The space of R -adic modular forms is denoted by $V_0(\mathfrak{c}, K; R)$.

Remark 2.3.6. When we refer to a p -adic modular form, we mean an R -adic modular form with an unspecified p -adic ring R . Since we will not use the symbol p to denote a ring, it does not cause any confusion. The definition for a p -adic modular form in the style of Definition 2.3.4 is due to Hida. This definition is sufficient for our purpose for a while, but we will need a stronger notion of a p -adic modular form in Section 4.4, which is due to Katz. See Subsection 4.2 for the comparison of two notions.

The main example of such an R for us is certain Iwasawa algebra which we now explain. Let \mathcal{M} be a quadratic totally imaginary field extension of \mathcal{F} . We will always assume that every place of \mathcal{F} lying over p splits in \mathcal{M} . Such number field \mathcal{M} is called p -ordinary. We choose an integral ideal \mathfrak{C} of \mathcal{M} which is prime to p , and consider the ray class field $\mathcal{M}(p^n\mathfrak{C})$ of \mathcal{M} modulo $p^n\mathfrak{C}$ for all $n \geq 0$. We define

$$(2.3.7) \quad Z = Z(\mathfrak{C}) = \varprojlim_{\infty \leftarrow n} \text{Gal}(\mathcal{M}(p^n\mathfrak{C})/\mathcal{M}),$$

and consider the Iwasawa algebra

$$(2.3.8) \quad \Lambda = \Lambda(Z) = \varprojlim_{\leftarrow} \mathcal{I}[Z/Y]$$

where the inverse limit is taken over the set of all open normal subgroups Y of Z . We will be considering Λ -adic Eisenstein series lying in $V_0(\mathfrak{c}, K; \Lambda)$, where Λ is given by (2.3.8).

2.4. CM points

In this subsection, we will introduce the notion of CM points in $\text{GL}_2(\mathbb{A}_{\mathcal{F}})$ and the level structure on them, where \mathcal{F} is a totally real field and $\mathbb{A}_{\mathcal{F}}$ is the ring of adèles of \mathcal{F} . Instead of delving into the most general definition of a CM point, we will specify the CM points which will be used later. Roughly speaking, choosing a CM point amounts to choosing a suitable totally imaginary quadratic extension \mathcal{M} of \mathcal{F} and an element $\delta \in \mathcal{M}$ satisfying certain conditions which is listed below, and choosing a level structure amounts to making some explicit choice of a base for each place of \mathcal{F} . When we specify the CM points and their level structure, we will follow the convention of [12] closely. However, we note, in contrast to the previous works on p -adic Hecke L -functions, including [12], that the proof of our main result will rely on some particular choices of δ .

We begin specifying the CM points. Fix an odd prime p . Let \mathcal{M} be a totally imaginary quadratic extension of \mathcal{F} . We say that \mathcal{M} is p -ordinary if every place of \mathcal{F} dividing p splits in \mathcal{M} . Let c be the complex conjugation, which also defines a canonical nontrivial involution $\text{Gal}(\mathcal{M}/\mathcal{F})$. A CM type of \mathcal{M} is a set of embeddings $\sigma: \mathcal{M} \rightarrow \mathbb{C}$ such that the restricting σ to \mathcal{F} induces a bijection $\Sigma \cong I$, where we recall that I was defined to be the set of embedding of \mathcal{F} into \mathbb{R} . We define the p -adic CM type Σ_p associated to Σ to be the set of places induced by $i_p \circ i_{\infty}^{-1} \circ \sigma$ for $\sigma \in \Sigma$. From the definition of p -ordinary CM fields, it follows that the restriction induces a

bijection between Σ_p and the set of places of \mathcal{F} lying above p . Let \mathcal{R} be the ring of integers of \mathcal{M} , and let \mathfrak{d} be the absolute different of \mathcal{F} . We choose an element $\delta_{\mathcal{M}} \in \mathcal{M}$ which is often written as δ when a reference to \mathcal{M} is unimportant, satisfying the following three conditions:-

- (pol-1) For each $\sigma \in \Sigma$, we have $\text{Im}(\sigma(\delta)) > 0$.
- (pol-2) For each $\sigma \in \Sigma$, we have $\delta^c = -\delta$.
- (pol-3) Let $\text{Tr}_{\mathcal{M}/\mathcal{F}}: \mathcal{M} \rightarrow \mathcal{F}$ be the trace map. Then the alternating pairing

$$(x, y) \mapsto \text{Tr}_{\mathcal{M}/\mathcal{F}} \left(\frac{xy^c}{2\delta} \right)$$

defines an isomorphism $\mathcal{R} \wedge_{\mathcal{O}} \mathcal{R} \xrightarrow{\sim} (\mathfrak{c}\mathfrak{d})^{-1}$ for an integral ideal $\mathfrak{c} \subset \mathcal{O}$ that is prime to p .

The above three conditions are called polarization conditions, as suggested by the labels. For such δ , we let $D = -\delta^2$ which is a totally positive element in \mathcal{F} . Of course, D depends on the choice of δ , but we often suppress it from the notation.

We remark that in the literature the choice of δ is often referred to as the choice of polarization and the resulting \mathfrak{c} is called the polarization ideal. We note that having a polarization ideal which is prime to p is crucial for establishing the q -expansion principle for p -adic modular forms on which the proof of our main theorem is based on. On the other hand, it will be clear from the computations that we will carry out why we need to impose the first two conditions on δ . See the paragraph after (P) in Subsection 2.5 for the choice of δ we make relative to a smaller CM field \mathcal{M}' of \mathcal{M} .

From now, we explain what we call the level structure. Let V be the two dimensional vector space $\mathcal{F} \oplus \mathcal{F}$ over \mathcal{F} , viewed as the set of row vectors of length two with entries in \mathcal{F} . In particular, an element x in V is written as a row vector (a, b) with $a, b \in \mathcal{F}$. Given δ , an element $y \in \mathcal{M}$ can be written uniquely in the form $a\delta + b$, and we introduce an isomorphism $q_{\delta}: \mathcal{M} \xrightarrow{\sim} V$ defined by

$$(2.4.1) \quad q_{\delta}: a\delta + b \mapsto (a, b).$$

Of course, it would suffice to choose any δ in $\mathcal{M} - \mathcal{F}$ in order to conclude that q_{δ} is an isomorphism, and the above sophisticated conditions on δ are not used here. In any case, for our later purpose, we record the dependence of the isomorphism q_{δ} on the choice of δ in the following lemma.

Lemma 2.4.2. *Let u be an element in \mathcal{F} and $\tilde{\delta}$ be an element in $\mathcal{M} - \mathcal{F}$. We have*

$$(2.4.3) \quad q_{u\tilde{\delta}}(a\tilde{\delta} + b) \cdot \begin{bmatrix} u & 0 \\ 0 & 1 \end{bmatrix} = q_{\tilde{\delta}}(a\tilde{\delta} + b).$$

Proof. The proof is a straightforward calculation. We have

$$(2.4.4) \quad q_{u\tilde{\delta}}(a\tilde{\delta} + b) = q_{u\tilde{\delta}}(au^{-1}u\tilde{\delta} + b)$$

$$(2.4.5) \quad = au^{-1}(1, 0) + b(0, 1).$$

Multiplying $\begin{bmatrix} u & 0 \\ 0 & 1 \end{bmatrix}$ on the both sides from the right yields

$$(2.4.6) \quad q_{u\tilde{\delta}}(a\tilde{\delta} + b) \cdot \begin{bmatrix} u & 0 \\ 0 & 1 \end{bmatrix} = a(1, 0) + b(0, 1),$$

whose right hand side equals $q_{\tilde{\delta}}(a\tilde{\delta} + b)$ by the definition of $q_{\tilde{\delta}}$. The proof of the lemma is complete. \square

Let $M(2, \mathcal{F})$ be the algebra of 2×2 matrices and denote by ϱ the embedding

$$(2.4.7) \quad \varrho: \mathcal{M} \hookrightarrow M(2, \mathcal{F}), \quad \varrho: a\delta + b \mapsto \begin{bmatrix} b & -Da \\ a & b \end{bmatrix}.$$

When we need to emphasize the dependence of ϱ on the choice of δ , we will write ϱ_δ instead of ϱ . Clearly, the first two conditions imposed on δ are indispensable in order to have ϱ , while the third condition is irrelevant here.

Let \mathfrak{C} be an integral ideal of \mathcal{R} which is prime to p . For an ideal \mathfrak{A} of \mathcal{M} , denote by \mathfrak{A}^c the complex conjugate of \mathfrak{A} . We decompose

$$(2.4.8) \quad \mathfrak{C} = \mathfrak{F}\mathfrak{F}_c\mathfrak{I}$$

for ideals \mathfrak{F} , \mathfrak{F}_c , and \mathfrak{I} of \mathcal{M} so that \mathfrak{F} is a product of prime ideals split over \mathcal{F} , $\mathfrak{F}^c \subset \mathfrak{F}_c$, and \mathfrak{I} is a product of prime ideals ramified or inert over \mathcal{F} . Such a decomposition is unique. Also, we write

$$(2.4.9) \quad \mathfrak{C}^+ := \mathfrak{F}\mathfrak{F}_c$$

and

$$(2.4.10) \quad \mathfrak{D} := p\mathfrak{C}D_{\mathcal{M}/\mathcal{F}}$$

where $D_{\mathcal{M}/\mathcal{F}}$ is the relative discriminant for \mathcal{M}/\mathcal{F} . For a finite place v of \mathcal{F} , we define

$$(2.4.11) \quad \mathcal{R}_v = \mathcal{R} \otimes_{\mathcal{O}} \mathcal{O}_v.$$

We are going to choose certain \mathcal{O}_v -basis for \mathcal{R}_v , which will be used to define the level structure. We divide it into several cases.

First, let v be a place of \mathcal{F} which divides $p\mathfrak{f}\mathfrak{f}_c$. Then, v decomposes in \mathcal{M} into two places in \mathcal{M} . We define w to be the one of the two such that $w \in \Sigma_p$ or $w|\mathfrak{f}$, recalling that Σ_p was defined in the beginning of this subsection to be the set of places above p corresponding to Σ . We define \bar{w} to be the unique place of \mathcal{M} which is different from w and lies over v . In particular, \mathcal{R}_v is canonically isomorphic to $\mathcal{R}_w \oplus \mathcal{R}_{\bar{w}}$, which we view as an identification without further indication. Let e_w (resp. $e_{\bar{w}}$) be the idempotent in $\mathcal{R}_w \oplus \mathcal{R}_{\bar{w}}$ corresponding to w (resp. \bar{w}). Then $\{e_w, e_{\bar{w}}\}$ is an \mathcal{O}_v -basis for \mathcal{R}_v .

Let v be a place of \mathcal{F} which does not divide $p\mathfrak{C}$ and split in \mathcal{M} . As in the previous case, v splits into two places w and \bar{w} in \mathcal{M} . The difference is that we do not have a preferred choice for w . We identify \mathcal{R}_v with $\mathcal{R}_w \oplus \mathcal{R}_{\bar{w}}$, and define e_w and $e_{\bar{w}}$ as idempotents, as in the previous case.

Next we consider a place v of \mathcal{F} which is either inert or ramified in \mathcal{M} . In any case, there is a unique place w of \mathcal{M} which lies above v , and \mathcal{R}_v is canonically identified with \mathcal{R}_w . We explain how we choose a basis $\{1, \theta_v\}$ for \mathcal{R}_v as an \mathcal{O}_v -module. When v is ramified in \mathcal{M} , we take $\{1, \theta_v\}$ to be an \mathcal{O}_v -basis of \mathcal{R}_w with θ_v being a uniformizer in \mathcal{R}_w . We always require θ_v to satisfy $\theta_v^c = -\theta_v$ if $v \nmid 2$. If we put $t_v = \theta_v + \theta_v^c$, then by our choice $t_v = 0$ for $v \nmid 2$ but possibly non-zero if $v|2$. If v is inert in \mathcal{R} and does not divide 2, then we take $\{1, \theta_v\}$ to be an \mathcal{O}_v -basis of \mathcal{R}_v such that $\theta_v^c = -\theta_v$. If v is inert in \mathcal{R} and v divides 2, then we relax the condition $\theta_v^c = -\theta_v$.

We need to make one more choice before we choose the level structure. Write $\widehat{\mathbb{Z}}$ for the profinite completion of \mathbb{Z} and write $\widehat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. We fix a finite idele $d = d_{\mathcal{F}} = (d_{\mathcal{F}_v})_v \in \mathbb{A}_{\mathcal{F}}^{\infty, \times}$ such that

$$(2.4.12) \quad d\widehat{\mathcal{O}} \cap \mathcal{F} = \mathfrak{d},$$

where \mathfrak{d} is the absolute different of \mathcal{F} . We further assume that

$$(2.4.13) \quad d_{\mathcal{F}_v} = -2\delta_w$$

if v divides $\mathfrak{f}\Sigma_p$. Note that (pol-3) ensures that (2.4.13) does not conflict with the condition (2.4.12) we imposed on d .

We will now choose an \mathcal{O}_v -basis $\{e_{1,v}, e_{2,v}\}$ for \mathcal{R}_v for each finite place v of \mathcal{F} which we call the level structure. Recall that for an ideal $\mathfrak{a} \subset \mathcal{O}$, we write $\mathfrak{a}^* = \mathfrak{a}^{-1}\mathfrak{d}^{-1}$. For a finite place v of \mathcal{F} such that $v \nmid p\mathfrak{C}\mathfrak{C}^c$, we want to choose $\{e_{1,v}, e_{2,v}\}$ so that $\mathcal{R}_v = \mathcal{O}_v e_{1,v} \oplus \mathcal{O}_v^* e_{2,v}$. In order to achieve this, we define

$$(2.4.14) \quad e_{1,v} = \begin{cases} e_{\overline{w}} & \text{if } v \text{ splits in } \mathcal{M} \\ \theta_v & \text{if } v \text{ is inert or ramified in } \mathcal{M} \end{cases}$$

and

$$(2.4.15) \quad e_{2,v} = \begin{cases} d_{\mathcal{F}_v} \cdot e_w & \text{if } v \text{ splits in } \mathcal{M} \\ d_{\mathcal{F}_v} \cdot 1 & \text{if } v \text{ is inert or ramified in } \mathcal{M}. \end{cases}$$

Having fixed the level structure, we give the definition of the CM points in the rest of this subsection. Recall that we defined V to be the space of row vectors of length two over \mathcal{F} , and we define $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Also recall that the choice of δ gives rise to an isomorphism q_δ from \mathcal{M} to V . For any place v of \mathcal{F} , let $q_{\delta,v}$ be the isomorphism $\mathcal{M}_v \xrightarrow{\sim} V \otimes_{\mathcal{O}} \mathcal{O}_v$ extending q_δ . Recall that we defined in (2.2.1) the left action of $\mathrm{GL}_2(R)$ on the row vectors, written as $*$. If v is a finite place, then we denote by ς_v the element in $\mathrm{GL}_2(\mathcal{F}_v)$ which is characterized by

$$(2.4.16) \quad \varsigma_v * e_i = q_{\delta,v}(e_{i,v}), \quad i = 1, 2.$$

Unfolding the definitions, for $v \mid \mathfrak{D}$, ς_v is simply

$$(2.4.17) \quad \varsigma_v = \begin{cases} \begin{bmatrix} d_{\mathcal{F}_v} & \frac{-t_v}{2} \\ 0 & d_{\mathcal{F}_v}^{-1} \end{bmatrix} & \text{if } v \mid D_{\mathcal{M}/\mathcal{F}}\mathfrak{C}^- \\ \begin{bmatrix} -\delta_w & -\frac{1}{2} \\ 1 & \frac{-1}{2\delta_w} \end{bmatrix} & \text{if } v \mid p\mathfrak{C}^+ \text{ and } w \mid \Sigma_p\mathfrak{F}. \end{cases}$$

Remark 2.4.18. Suppose that \mathcal{M} contains an imaginary quadratic field \mathcal{M}_0 . Let D_0 be the positive squarefree integer such that $\mathcal{M}_0 = \mathbb{Q}(\sqrt{-D_0})$. If 2 is split in \mathcal{M}_0 , then all t_v can be chosen to be zero. If D_0 is congruent to 1 modulo 4, then we choose

$$(2.4.19) \quad \theta_v = \frac{1 + \sqrt{D_0}}{2}$$

for each place v of \mathcal{F} dividing 2. In particular, we have $t_v = 1$ for those v . If 2 divides D_0 , then we choose $\theta_v = \sqrt{-D_0}$, in which case $t_v = 0$.

Remark 2.4.20. Suppose that we are given a degree p extension of \mathcal{M}/\mathcal{M} CM fields, and let v' be a place of \mathcal{F}' . For each place v of \mathcal{F} lying over v' , we can choose θ_v to be the image of $\theta_{v'}$.

For an infinite place v of \mathcal{F} , let $\sigma \in \Sigma$ be the unique element in Σ extending v and define ς_v to be

$$(2.4.21) \quad \varsigma_v = \begin{bmatrix} \text{Im}(\sigma(\delta)) & 0 \\ 0 & 1 \end{bmatrix}.$$

We define

$$(2.4.22) \quad \varsigma = \prod_v \varsigma_v \in \text{GL}_2(\mathbb{A}_{\mathcal{F}}), \text{ and } \varsigma_f = \prod_{v < \infty} \varsigma_v \in \text{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty}).$$

Recall that \mathfrak{H} denotes the upper half plane and that we defined X_+ to be \mathfrak{H}^I in (2.1.1). We can naturally identify $\mathcal{M} \otimes_{\mathbb{Q}} \mathbb{R}$ with \mathbb{C}^{Σ} , and further identify X_+ as the subset of \mathbb{C}^{Σ} which consists of Σ -tuple of complex numbers $(\tau_{\sigma})_{\sigma \in \Sigma}$ such that for every σ the imaginary part of τ_{σ} is positive. In particular, if we denote by δ_{Σ} the Σ -tuple $(\sigma(\delta))_{\sigma \in \Sigma}$, then δ_{Σ} is viewed as an element of X_+ . We finally define the CM point associated to a finite idele $a \in \mathbb{A}_{\mathcal{F}}^{(pN), \times}$ to be

$$(2.4.23) \quad x(a) = (\delta_{\Sigma}, \varrho(a)\varsigma_f) \in X_+ \times \text{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty}).$$

2.5. Restriction along the diagonal

The purpose of this subsection is to define a map which we call the diagonal map, associated to a degree p extension \mathcal{F}/\mathcal{F}' of totally real fields, and to study the effect of this diagonal map on the level structure which we defined in the previous subsection. As before, I denotes the set of embeddings of \mathcal{F} into \mathbb{R} , and similarly define I' to be the set of embeddings of \mathcal{F}' into \mathbb{R} . We similarly denote by X'_+ the I' -tuple of complex upper half plane, which is again identified as a subset of $\mathbb{C}^{I'}$ as in the previous subsection. Then embedding $\mathcal{F}' \rightarrow \mathcal{F}$ induces an embedding $X'_+ \rightarrow X_+$. This is called as the diagonal map in [14], but let us call it a naive diagonal map in order to avoid the conflict with our terminology. In [14], using the naive diagonal map, Kakde proved various non-commutative Kummer congruences for p -adic Dedekind L -function associated to totally real fields. However, we need

to modify the naive diagonal map for our purposes because of the two reasons. Firstly, we are working with adèles instead of just upper half planes, so if we were to use the naive diagonal embedding, we need to make a non-canonical identification between adelic automorphic forms and classical automorphic forms on upper half planes. It would be technically undesirable if our computation relies on adelic techniques and we have to keep track of the non-canonical identifications that we have made. The second reason is due to the role of level structure in our work, which was irrelevant in [14]; what we need is not only some sort of diagonal map, but also the compatibility between the diagonal map and the level structure we choose.

We now explain the diagonal map in our sense. Let \mathcal{F}/\mathcal{F}' be a degree p extension of totally real fields and let $\mathcal{M}'/\mathcal{F}'$ be a quadratic CM extension such that every prime of \mathcal{F}' lying over p splits in \mathcal{M}' . Let \mathcal{M} be the compositum of \mathcal{M}' and \mathcal{F} . For a CM type Σ' of \mathcal{M}' , we denote by Σ the CM type on \mathcal{M} induce by Σ' . It is defined to be

$$(2.5.1) \quad \Sigma := \{\sigma | \sigma: \mathcal{M} \hookrightarrow \mathbb{C}, \sigma|_{\mathcal{M}'} \in \Sigma'\}.$$

We introduce a condition:-

- (P) The relative different $\mathfrak{d}_{\mathcal{F}/\mathcal{F}'}$ can be generated by an element $d_{\mathcal{F}/\mathcal{F}'} \in \mathcal{F}$, which is totally positive.

Suppose (P) holds, and let $\tilde{d}_{\mathcal{F}/\mathcal{F}'}$ be a generator of $\mathfrak{d}_{\mathcal{F}/\mathcal{F}'}$ which is totally positive. For a given level structure associated to $\delta' \in \mathcal{M}'$, we define δ to be $d_{\mathcal{F}/\mathcal{F}'}\delta'$. Then δ induces a level structure for \mathcal{M} , and we want to compare the two level structures in terms of the diagonal embedding $\tilde{\Delta}$, which we now define. Let I' be the set of embeddings of \mathcal{F}' into \mathbb{R} and let X'_+ be the product of I' copies of complex upper half planes. Then we define the diagonal map, denoted by $\tilde{\Delta}_{\mathcal{F}'}$, as

$$(2.5.2) \quad \tilde{\Delta}_{\mathcal{F}'}^{\mathcal{F}}: X'_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^{\infty}) \rightarrow X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$$

$$(2.5.3) \quad (z', h'^{\infty}) \mapsto \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot (z', h'^{\infty}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'}^{\infty} \end{bmatrix}^{-1}.$$

Precisely speaking, our map $\tilde{\Delta}_{\mathcal{F}'}$ depends on $d_{\mathcal{F}/\mathcal{F}'}$, but we suppress $d_{\mathcal{F}/\mathcal{F}'}$ in order to ease the notation. When it is clear what \mathcal{F} and \mathcal{F}' are, we often write $\tilde{\Delta}$ instead of $\tilde{\Delta}_{\mathcal{F}'}$.

Denote by \mathcal{O}' (resp. \mathcal{R}') the ring of integers of \mathcal{F}' (resp. \mathcal{M}'). Let \mathfrak{d}' be the absolute different ideal of \mathcal{F}' . Suppose that we are given $\delta' \in \mathcal{M}'$ such

that

$$(2.5.4) \quad (x', y') \mapsto \mathrm{Tr}_{\mathcal{M}'/\mathcal{F}'} \left(\frac{x'y'^c}{2\delta'} \right)$$

induces an isomorphism $\mathcal{R}' \wedge_{\mathcal{O}'} \mathcal{R}' \xrightarrow{\sim} (\mathfrak{c}'\mathfrak{d}')^{-1}$ for an integral ideal $\mathfrak{c}' \subset \mathcal{O}'$ prime to p . Define $\delta = \delta' d_{\mathcal{F}/\mathcal{F}'}$ and $\mathfrak{c} = (\mathfrak{c}'\mathcal{O}) \cdot \mathfrak{d}_{\mathcal{F}/\mathcal{F}'}$. Then

$$(2.5.5) \quad (x, y) \mapsto \mathrm{Tr}_{\mathcal{M}/\mathcal{F}} \left(\frac{xy^c}{2\delta} \right)$$

induces an isomorphism $\mathcal{R} \wedge_{\mathcal{O}} \mathcal{R} \xrightarrow{\sim} (\mathfrak{c}\mathfrak{d})^{-1}$. We fix a finite idele $d_{\mathcal{F}'} \in \mathbb{A}_{\mathcal{F}'}^\infty$ with $d_{\mathcal{F}'} \widehat{\mathcal{O}}' \cap \mathcal{F}' = \mathfrak{d}'$, and define $d_{\mathcal{F}} = d_{\mathcal{F}'} d_{\mathcal{F}/\mathcal{F}'}$. Then we have $d_{\mathcal{F}} \widehat{\mathcal{O}} \cap \mathcal{F} = \mathfrak{d}$. Using the choice of δ' , we fix $\mathcal{O}'_{v'}$ -basis $(e_{1,v'}, e_{2,v'})$ for $\mathcal{R}'_{v'}$, for each finite place v' of \mathcal{F}' , satisfying the conditions (2.4.14) and (2.4.15). Viewing $\mathcal{R}' \subset \mathcal{R}$ via the embedding induced by $\mathcal{M}' \subset \mathcal{M}$, we put

$$(2.5.6) \quad e_{1,v} = e_{1,v'} \text{ and } e_{2,v} = d_{\mathcal{F}/\mathcal{F}'} e_{2,v'}.$$

Then $(e_{1,v}, e_{2,v})$ satisfies the conditions described in the previous subsection for \mathcal{M}/\mathcal{F} . After all, we have two embeddings

$$(2.5.7) \quad \varrho: \mathbb{A}_{\mathcal{M}}^{\infty pN, \times} \longrightarrow \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$$

$$(2.5.8) \quad \varrho': \mathbb{A}_{\mathcal{M}'}^{\infty pN, \times} \longrightarrow \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty).$$

Proposition 2.5.9. *Assume (P) and we make the choices as above. We have*

$$(2.5.10) \quad x(1) = \widetilde{\Delta}_{\mathcal{F}'}^{\mathcal{F}}(x'(1)),$$

where $x(1)$ (resp. $x'(1)$) is the CM point on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$ (resp. on $X'_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty)$) given by (2.4.23) with respect to our choice of δ and ς (resp. δ' and ς').

Proof. The proposition can be written as

$$(2.5.11) \quad \widetilde{\Delta}_{\mathcal{F}'}^{\mathcal{F}}(\delta'^{\Sigma'}, \varsigma'^{\infty}) = (\delta^{\Sigma}, \varsigma^{\infty}).$$

By the definition (2.5.2) of $\widetilde{\Delta}_{\mathcal{F}'}^{\mathcal{F}}$, the left hand side equals

$$(2.5.12) \quad \widetilde{\Delta}_{\mathcal{F}'}^{\mathcal{F}}(\delta'^{\Sigma'}, \varsigma'^{\infty}) = \left((d_{\mathcal{F}/\mathcal{F}'} \delta')^{\Sigma}, \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot \varsigma'^{\infty} \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'}^{\infty} \end{bmatrix}^{-1} \right)$$

As we defined $\delta = d_{\mathcal{F}/\mathcal{F}'}\delta'$, the equality in the first component of (2.5.11) holds. Now we verify the equality in the second component of (2.5.11). Denote by ξ the second component of the right hand side of (2.5.12), and by ξ_v the v -component of ξ for a finite place v of \mathcal{F} . Let v' be the restriction of v to \mathcal{F}' . Although we often identify $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'})$ as a subset of $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}})$, let us denote the natural embedding by $j: \mathrm{GL}_2(\mathcal{F}'_v) \hookrightarrow \mathrm{GL}_2(\mathcal{F}_v)$, in order to emphasize the ambient set. Similarly, we slightly abuse notation by writing $j: V' \hookrightarrow V$. In particular, $j(e'_i) = e_i$. By the defining property (2.4.16) of ς , it suffices to prove that for each finite place v of \mathcal{F} ,

$$(2.5.13) \quad \xi_v * e_i = q_{\delta,v}(e_{i,v}), \quad i = 1, 2.$$

For $i = 1$,

$$(2.5.14) \quad \xi_v * e_1 = \left(\begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot j(\varsigma'_{v'}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'} \end{bmatrix}^{-1} \right) * e_1$$

$$(2.5.15) \quad = \left(\begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot j(\varsigma'_{v'}) \right) * (d_{\mathcal{F}/\mathcal{F}'})^{-1} e_1$$

$$(2.5.16) \quad = \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} * (d_{\mathcal{F}/\mathcal{F}'})^{-1} j(q_{\delta',v'}(e_{1,v'}))$$

$$(2.5.17) \quad = \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} * (d_{\mathcal{F}/\mathcal{F}'})^{-1} q_{\delta',d_{\mathcal{F}/\mathcal{F}'},v}(e_{1,v}) \cdot \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix}$$

$$(2.5.18) \quad = \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} * (d_{\mathcal{F}/\mathcal{F}'})^{-1} q_{\delta,v}(e_{1,v}) \cdot \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix}$$

$$(2.5.19) \quad = (d_{\mathcal{F}/\mathcal{F}'})^{-1} q_{\delta,v}(e_{1,v}) \cdot \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'} \end{bmatrix}$$

$$(2.5.20) \quad = q_{\delta,v}(e_{1,v}).$$

From (2.5.16) to (2.5.17), we used Lemma 2.4.2 and $j(e_{1,v'}) = e_{1,v}$. For $i = 2$,

$$(2.5.21) \quad \xi_v * e_2 = \left(\begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot j(\varsigma'_{v'}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'} \end{bmatrix}^{-1} \right) * e_2$$

$$(2.5.22) \quad = \left(\begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot j(\varsigma'_{v'}) \right) * e_2$$

$$(2.5.23) \quad = \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} * j(q_{\delta',v'}(e_{2,v'}))$$

$$(2.5.24) \quad = \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} * q_{\delta,v}(j(e_{2,v'})) \cdot \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix}$$

$$(2.5.25) \quad = q_{\delta,v}(j(e_{2,v'})) \cdot \begin{bmatrix} d_{\mathcal{F}/\mathcal{F}'} & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & d_{\mathcal{F}/\mathcal{F}'} \end{bmatrix}$$

$$(2.5.26) \quad = d_{\mathcal{F}/\mathcal{F}'} q_{\delta,v}(j(e_{2,v'}))$$

$$(2.5.27) \quad = q_{\delta,v}(e_{2,v}).$$

From (2.5.23) to (2.5.24), we used Lemma 2.4.2, and from (2.5.26) to (2.5.27) we used (2.5.6), the definition of $e_{2,v}$. The proof of the proposition is complete. \square

3. Toric Eisenstein series and p -adic L -functions

In this section, we define the Whittaker model of certain adelic Eisenstein series, the associated p -adic Eisenstein measure, and the construction of the p -adic L -function. In the construction of the Whittaker model, we rather closely follow [12, 13] except the two minor deviations we make. Firstly, we allow imprimitive characters. That is, we fix an ideal \mathfrak{C} of a CM field \mathcal{M} , and we will consider an algebraic Hecke character χ of \mathcal{M} such that the prime-to- p part of the conductor of χ merely divides \mathfrak{C} , instead of being equal. In [12, 13], \mathfrak{C} was assumed to be of exact conductor of χ , or the primitive characters are used. It forces us to slightly change the choice of local sections for inert or ramified places. It also makes some formulae to appear in this subsection look different from theirs. Secondly, our notation is occasionally different from that used in [12, 13]. When it comes to the construction of the p -adic measure, we will adopt the language of p -adic modular forms with coefficients in certain Iwasawa algebra, while Hsieh used the language of p -adic measures. Of course, the correspondence between Iwasawa algebra and the space of p -adic measures will identify two languages with little difficulty, but the author believes that our later discussions become simpler in terms of Iwasawa algebras.

As in the previous sections, we consider a p -ordinary CM field \mathcal{M} with maximal real subfield \mathcal{F} and a CM type Σ and associated p -adic CM type Σ_p . Let χ be a continuous group homomorphism

$$(3.0.28) \quad \chi: \mathbb{A}_{\mathcal{M}}^{\times} \rightarrow \mathbb{C}^{\times}$$

such that the kernel χ contains \mathcal{M} embedded diagonally in $\mathbb{A}_{\mathcal{M}}^{\times}$. Let $\mathbb{Z}[\Sigma \cup \mathcal{C}\Sigma]$ be the free abelian group generated by $\Sigma \cup \mathcal{C}\Sigma$, and let $\mathbb{Z}[\Sigma]$ be the free abelian group generated by Σ .

Definition 3.0.29. The continuous group homomorphism χ as above is called an algebraic Hecke character if there exists an integer k and $m \in \mathbb{Z}[\Sigma]$ with the following properties. For every $z_\infty = (z_\sigma)_{\sigma \in \Sigma} \in (\mathbb{C}^\times)^\Sigma$,

$$(3.0.30) \quad \chi(z_\infty) = \prod_{\sigma \in \Sigma} z_\sigma^k \left(\frac{z_\sigma}{z_\sigma^c} \right)^{m_\sigma}$$

holds, where m is understood as $\sum_{\sigma} m_\sigma \sigma$ and m_σ is an integer. We call

$$(3.0.31) \quad k\Sigma + (1 - c)m \in \mathbb{Z}[\Sigma \cup c\Sigma]$$

the infinity type of χ .

For an algebraic Hecke character χ of \mathcal{M} , we define

$$(3.0.32) \quad \chi_+ = \chi|_{\mathbb{A}_{\mathcal{F}}^\times},$$

to be the restriction of χ to $\mathbb{A}_{\mathcal{F}}^\times$.

We identify $\mathrm{GL}_2(\mathcal{F}_\infty)$ with $\prod_{\sigma \in \Sigma} \mathrm{GL}_2(\mathbb{R})$ by sending $\begin{bmatrix} a \otimes a' & b \otimes b' \\ c \otimes c' & d \otimes d' \end{bmatrix}$ to $\left(\begin{bmatrix} \sigma(a)a' & \sigma(b)b' \\ \sigma(c)c' & \sigma(d)d' \end{bmatrix} \right)_{\sigma \in \Sigma}$, and define the subgroup $U_\infty \subset \mathrm{GL}_2(\mathcal{F}_\infty)$ to be the maximal compact subgroup corresponding to $\prod_{\sigma \in \Sigma} \mathrm{SO}_2(\mathbb{R})$. We denote by B the subgroup of GL_2 consisting of upper triangular matrices. Recall that a function $\phi: \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}) \rightarrow \mathbb{C}$ is called U_∞ -finite if the \mathbb{C} -linear span of $\{u_\infty \phi | u_\infty \in U_\infty\}$ in the space of the continuous functions from $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}})$ to \mathbb{C} is finite dimensional.

For $s \in \mathbb{C}$, we define $I(s, \chi_+)$ to be the space consisting of smooth U_∞ -finite functions $\phi: \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}) \rightarrow \mathbb{C}$ satisfying

$$(3.0.33) \quad \phi \left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} g \right) = \chi_+^{-1}(d) \left| \frac{a}{d} \right|_{\mathbb{A}_{\mathcal{F}}}^s \phi(g)$$

for every $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in B(\mathbb{A}_{\mathcal{F}})$ and every $g \in \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}})$. We call the functions in $I(s, \chi_+)$ as sections. For each section $\phi \in I(s, \chi_+)$, we define the adelic Eisenstein series associated to ϕ by

$$(3.0.34) \quad E_{\mathbb{A}}(g, \phi) = \sum_{\gamma \in B(\mathcal{F}) \backslash \mathrm{GL}_2(\mathcal{F})} \phi(\gamma g),$$

whenever the series is absolutely convergent. It is well known that $E_{\mathbb{A}}(g, \phi)$ is absolutely convergent when the real part of s is sufficiently large, and it has meromorphic continuation to the entire complex plane.

3.1. Normalization of epsilon factors

We make explicit the normalization of epsilon factors, which we use throughout the paper. Let $\psi_{\mathbb{Q}}$ be the additive character

$$(3.1.1) \quad \psi_{\mathbb{Q}}: \mathbb{A}/\mathbb{Q} \rightarrow \mathbb{C}^{\times}$$

such that $\psi_{\mathbb{Q}} = \prod_v \psi_{\mathbb{Q}_v}$ with each $\psi_{\mathbb{Q}_v}$ specified by the following rules. For $v = \infty$, we put

$$(3.1.2) \quad \psi_{\mathbb{R}}(x_{\infty}) = \exp(-2\pi i x_{\infty}).$$

For a finite place $v = \ell$, let $(\mathbb{Q}/\mathbb{Z})[\ell^{\infty}]$ be the ℓ -primary subgroup of \mathbb{Q}/\mathbb{Z} . Denote by $\langle x_{\ell} \rangle$ the image of x_{ℓ} under the canonical homomorphism

$$(3.1.3) \quad \mathbb{Q}_{\ell} \rightarrow \mathbb{Q}_{\ell}/\mathbb{Z}_{\ell} \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})[\ell^{\infty}] \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

We may view $\langle x_{\ell} \rangle$ as the fractional part of x_{ℓ} . Then, we define

$$(3.1.4) \quad \psi_{\mathbb{Q}_{\ell}}(x_{\ell}) = \exp(2\pi i \langle x_{\ell} \rangle).$$

For a finite extension K of \mathbb{Q}_v , where v may be infinite or finite, we define

$$(3.1.5) \quad \psi_K = \psi_{\mathbb{Q}_v} \circ \text{Tr}_{K/\mathbb{Q}_v}$$

where $\text{Tr}_{K/\mathbb{Q}_v}$ denotes the trace map $K \rightarrow \mathbb{Q}_v$. For a number field H , define

$$(3.1.6) \quad \psi_H = \psi_{\mathbb{Q}} \circ \text{Tr}_{H/\mathbb{Q}}$$

where $\text{Tr}_{H/\mathbb{Q}}$ denotes the trace map $\mathbb{A}_H \rightarrow \mathbb{A}_{\mathbb{Q}}$. In other words, if v is a place of H , then ψ_H can be written as

$$(3.1.7) \quad \psi_H = \prod_v \psi_{H_v}$$

where v runs over the set of all places of H . When it is clear what H is, we simply write ψ and ψ_v instead of ψ_H and ψ_{H_v} , respectively. For a non-archimedean local field K with valuation ring \mathcal{O}_K , we write \mathfrak{d}_K for the absolute different, and choose a generator d_K for \mathfrak{d}_K . For a continuous character $\chi_K: K^{\times} \rightarrow \mathbb{C}^{\times}$, let $e_K(\chi_K)$ denote the exponent of the conductor of χ_K . In other words, $e_K(\chi_K) = 0$ if χ_K is trivial on \mathcal{O}_K^{\times} , and otherwise it is the smallest integer n for which χ_K is trivial on $1 + \mathfrak{m}_K^n$, where \mathfrak{m}_K is the maximal ideal of \mathcal{O}_K . We define the epsilon factor as

$$(3.1.8) \quad \epsilon(s, \chi_K, \psi_K) = |c|_K^s \int_{c^{-1}\mathcal{O}_K} \chi_K^{-1}(x) \psi_K(s) d_K x$$

where $c = d_K \varpi_K^{e_K(\chi_K)}$, and $d_K x$ is the Haar measure on K which is self-dual with respect to ψ_K . According to our normalization of ψ_K

$$(3.1.9) \quad \text{Vol}(\mathcal{O}_K, d_K x) = |\mathcal{O}_K/\mathfrak{d}_K|^{-\frac{1}{2}}$$

where $|\mathcal{O}_K/\mathfrak{d}_K|$ is the number of elements in $\mathcal{O}_K/\mathfrak{d}_K$. The local root number $W(\chi_K)$ is defined as

$$(3.1.10) \quad W(\chi_K) = \epsilon\left(\frac{1}{2}, \chi_K, \psi_K\right).$$

We refer the reader to [19] for general facts about epsilon factors. It is well known that

$$(3.1.11) \quad |W(\chi_K)|_{\mathbb{C}} = 1$$

if χ_K is unitary.

Remark 3.1.12. Note that the self-dual Haar measure $d_K x$ is different from the Haar measure we use for the period integral of Eisenstein series which is normalized so that the volume of \mathcal{O}_K is always one.

3.2. Fourier coefficients of Eisenstein series

In this subsection, we review the computation of Fourier coefficients of an Eisenstein series. We keep the notation introduced in the beginning of the current section. Let \mathbf{w} be the matrix $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. For a place v of \mathcal{F} , we define $I_v(s, \chi_+)$, the space of local sections, to be the space consisting of the Bruhat-Schwartz functions $\phi_v: \text{GL}_2(\mathcal{F}_v) \rightarrow \mathbb{C}$ satisfying

$$(3.2.1) \quad \phi_v \left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} g \right) = \chi_{+,v}^{-1}(d) \left| \frac{a}{d} \right|_v^s \phi_v(g)$$

for every $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in B(\mathcal{F}_v)$ and $g \in \text{GL}(2, \mathcal{F}_v)$. For a non-archimedean place v , a function $\phi_v: \text{GL}_2(\mathcal{F}_v)$ is called Bruhat-Schwartz if it is locally constant and compactly supported. For an archimedean place v , such ϕ_v is called Bruhat-Schwartz if it is smooth and of moderate growth. Since our arguments in the current paper will not involve the analytical issues arising from the growth condition of archimedean sections, we refer the readers to Section 2.8 of [1] for the precise definition and general analytic theory of archimedean local

sections. For a place v of \mathcal{F} , let dx_v be the Haar measure on \mathcal{F}_v which is normalized by

$$(3.2.2) \quad \text{Vol}(\mathcal{O}_{\mathcal{F}_v}, dx_v) = 1.$$

For each $\phi_v \in I_v(s, \chi_+)$, $g_v \in \text{GL}_2(\mathcal{F}_v)$, and $\beta \in \mathcal{F}_v$, we define the β -th local Whittaker integral $W_\beta(\phi_v, g_v)$ by

$$(3.2.3) \quad W_\beta(\phi_v, g_v) = \int_{\mathcal{F}_v} \phi_v \left(\mathbf{w} \begin{bmatrix} 1 & x_v \\ 0 & 1 \end{bmatrix} g_v \right) \psi(-\beta x_v) dx_v,$$

and the intertwining operator $M_{\mathbf{w}}$ by

$$(3.2.4) \quad (M_{\mathbf{w}}\phi_v)(g_v) = \int_{\mathcal{F}_v} \phi_v \left(\mathbf{w} \begin{bmatrix} 1 & x_v \\ 0 & 1 \end{bmatrix} g_v \right) dx_v.$$

By definition, $(M_{\mathbf{w}}\phi_v)(g_v)$ is equal to the 0-th local Whittaker integral. It is well known that local Whittaker integrals converge absolutely if the real part of s is sufficiently large, and have meromorphic continuation to all $s \in \mathbb{C}$. We say that a section $\phi \in I(s, \chi_+)$, which is defined in (3.0.33) is a decomposable section if we can write ϕ in the form $\phi = \bigotimes_v \phi_v$ for a family of local sections $\phi_v \in I_v(s, \chi_+)$. In that case, $E_{\mathbb{A}}(g, \phi)$ has the following Fourier expansion

$$(3.2.5) \quad E_{\mathbb{A}}(g, \phi) = \phi(g) + M_{\mathbf{w}}\phi(g) + \sum_{\beta \in \mathcal{F}} W_\beta(E_{\mathbb{A}}, g),$$

where

$$(3.2.6) \quad M_{\mathbf{w}}\phi(g) = \frac{1}{\sqrt{|D_{\mathcal{F}}|}} \prod_v M_{\mathbf{w}}\phi_v(g_v)$$

$$(3.2.7) \quad W_\beta(E_{\mathbb{A}}, g) = \frac{1}{\sqrt{|D_{\mathcal{F}}|}} \prod_v W_\beta(\phi_v, g_v).$$

The sum $\phi(g) + M_{\mathbf{w}}\phi(g)$ is called the constant term of $E_{\mathbb{A}}(g, \phi)$. We refer the reader to Section 2.8 of [1] for the general analytic properties of local Whittaker integrals and the constant term.

Now we recall the choice of local sections made in [12, 13]. We first introduce some notation. For a place v of \mathcal{F} , we simplify our notation by putting $K = \mathcal{F}_v$, and we fix a generator d_K for \mathfrak{d}_K , the absolute different of K . If v is a finite place of \mathcal{F} , define $\mathcal{O}_v = \mathcal{O}_K$, and let $\varpi = \varpi_v$ be the

uniformizer of \mathcal{O}_v . For a set Y , denote by \mathbb{I}_Y the characteristic function of Y . Now we describe our choice of local sections, beginning with the archimedean case.

Let v be an infinite place of \mathcal{F} . Then $K = \mathbb{R}$ and there is a unique $\sigma \in \Sigma$ whose restriction to \mathcal{F} is v . For $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2, \mathbb{R})$, we define

$$(3.2.8) \quad J(g, i) = ci + d, \overline{J(g, i)} = -ci + d$$

$$(3.2.9) \quad \nu(g) = |\det(g)| \cdot \left| J(g, i) \overline{J(g, i)} \right|^{-1}.$$

Define the sections $\phi_{k,s,\sigma}^h$ and $\phi_{k,m_\sigma,s,\sigma}^{n,h}$ in $I_v(s, \chi_+)$ by

$$(3.2.10) \quad \phi_{k,s,\sigma}^h(g) = J(g, i)^{-k} \nu(g)^s$$

$$(3.2.11) \quad \phi_{k,m_\sigma,s,\sigma}^{n,h} = J(g, i)^{-k-m_\sigma} \overline{J(g, i)}^{m_\sigma} \nu(g)^s.$$

The action of the intertwining operator $M_{\mathbf{w}}$ on $\phi_{k,s,\sigma}^h$ is given by

$$(3.2.12) \quad \left(M_{\mathbf{w}} \phi_{k,s,\sigma}^h \right) (g) = i^k (2\pi) \frac{\Gamma(k + 2s - 1)}{\Gamma(k + s) \Gamma(s)} \cdot \overline{J(g, i)}^k \det(g)^{-k} \nu(g)^{1-s}.$$

Define

$$(3.2.13) \quad \mathfrak{D} = p\mathfrak{d}_{\mathcal{M}/\mathcal{F}} \mathfrak{C}^c.$$

We will give the definition of the local sections for each place v of \mathcal{F} by dividing them into several cases. We first consider the case when either v divides $p\mathfrak{F}\mathfrak{F}^c$ or v is prime to \mathfrak{D} . Recall that we simply write \mathcal{F}_v as K . Denote by $\mathcal{S}(K)$ (resp. $\mathcal{S}(K \oplus K)$) the space of Bruhat-Schwartz functions on K (resp. $K \oplus K$). We define the Fourier transform $\widehat{\Phi}$ of a function $\Phi \in \mathcal{S}(K)$ as

$$(3.2.14) \quad \widehat{\Phi}(y) = \int_K \Phi(x) \psi_K(yx) dx.$$

For a character $\mu: K^\times \rightarrow \mathbb{C}^\times$, we define a function $\Phi_\mu \in \mathcal{S}(K)$ by

$$(3.2.15) \quad \Phi_\mu(x) = \mathbb{I}_{\mathcal{O}_v^\times}(x) \mu(x).$$

If v divides $p\mathfrak{F}\mathfrak{F}^c$, then v splits in \mathcal{M} , and we choose a place w of \mathcal{M} over v which satisfies either $w \mid \mathfrak{F}$ or $w \in \Sigma_p$. Let \overline{w} be the unique place of \mathcal{M} which is lying over v and different from w . We put

$$(3.2.16) \quad \Phi_w = \Phi_{\chi_w}$$

$$(3.2.17) \quad \Phi_{\bar{w}} = \Phi_{\chi_{\bar{w}}}.$$

To a Bruhat-Schwartz function $\Phi \in \mathcal{S}(K \oplus K)$, we associate a Godement section $f_{\Phi,s} \in I_v(s, \chi_+)$ defined by

$$(3.2.18) \quad f_{\Phi,s}(g) = |\det(g)|^s \int_{K^\times} \Phi((0, x)g) \chi_+(x) |x|_K^{2s} d^\times x,$$

and define the local section $\phi_{\chi,s,v}$ by

$$(3.2.19) \quad \phi_{\chi,s,v} = f_{\Phi_v^0,s},$$

where

$$(3.2.20) \quad \Phi_v^0(x, y) = \begin{cases} \mathbb{I}_{\mathcal{O}_v}(x) \mathbb{I}_{\mathcal{O}_v^*}(y) & \text{if } v \nmid \mathfrak{D} \\ \Phi_v^0(x, y) = \Phi_{\bar{w}}(x) \widehat{\Phi}_w(y) & \text{if } v \mid p \widehat{\mathfrak{F}}^c. \end{cases}$$

For every $u \in \mathcal{O}_v^\times$ with $v \mid p$, let Φ_w^1 and $\Phi_w^{[u]}$ be the Bruhat-Schwartz functions on K defined by

$$(3.2.21) \quad \Phi_w^1(x) = \mathbb{I}_{1+\varpi\mathcal{O}_v}(x) \chi_w^{-1}(x)$$

$$(3.2.22) \quad \Phi_w^{[u]}(x) = \mathbb{I}_{u(1+\varpi\mathcal{O}_v)}(x) \chi_w(x).$$

We define $\Phi_v^{[u]} \in \mathcal{S}(K \oplus K)$ by

$$(3.2.23) \quad \Phi_v^{[u]}(x, y) = \frac{1}{\text{Vol}(1 + \varpi\mathcal{O}_v d^\times x)} \Phi_w^1(x) \widehat{\Phi}_w^{[u]}(y).$$

From our normalization of the measure, we also have

$$(3.2.24) \quad \frac{1}{\text{Vol}(1 + \varpi\mathcal{O}_v d^\times x)} \Phi_w^1(x) \widehat{\Phi}_w^{[u]}(y) = (|\varpi|_K^{-1} - 1) \Phi_w^1(x) \widehat{\Phi}_w^{[u]}(y).$$

Now we consider the case $v \mid \mathfrak{C}^- \cdot D_{M/F}$. Let w be the unique place of \mathcal{M} lying over v . In this case, $\mathcal{M} \otimes_{\mathcal{F}} \mathcal{F}_v$ is naturally isomorphic to \mathcal{M}_w . Recall the embedding ϱ defined in (2.4.7), and let ϱ_v be the embedding $\mathcal{M}_w^\times \rightarrow \text{GL}_2(\mathcal{F}_v)$ which extends ϱ . Then we have $\text{GL}_2(\mathcal{F}_v) = B(\mathcal{F}_v)\varrho_v(\mathcal{M}_w)$, where B consists of upper triangular matrices. We define $\phi_{\chi,s,v}$ to be the unique smooth section in $I_v(s, \chi_+)$ satisfying

$$(3.2.25) \quad \phi_{\chi,s,v} \left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \varrho_v(z) \varsigma_v \right) = \chi_{+,v}^{-1}(d) \left| \frac{a}{d} \right|_v^s \cdot \chi_w^{-1}(z)$$

for every $b \in B(\mathcal{F}_v)$ and $z \in \mathcal{M}_v^\times$. It is easy to check that the right hand side of (3.2.25) is well-defined.

Remark 3.2.26. Note the difference with the choice made in [12], which differs by a factor of $L(s, \chi_v)$, the local Euler factor of χ_v . If we had added a factor of $L(s, \chi_v)$ as in [12], then we could not guarantee the p -integrality of Fourier-Whittaker coefficients of $\phi_{\chi, s, v}$ because we are allowing \mathfrak{C} to be strictly smaller than the conductor of χ .

3.3. The local Whittaker integrals

The purpose of this subsection is to summarize the formulae of the local Whittaker integrals. In this subsection, we assume $k \geq 1$.

Proposition 3.3.1. *The local Whittaker integrals are given as follows. Suppose that $v \mid \infty$. Let σ be the unique element in Σ whose restriction to \mathcal{F} is v , and we use v and σ interchangeably. Then, we have*

$$(3.3.2) \quad W_\beta \left(\phi_{k, s, \sigma}^h, \begin{bmatrix} y & x \\ 0 & 1 \end{bmatrix} \right) \Big|_{s=0} = \frac{(2\pi i)^k}{\Gamma(k)} \sigma(\beta)^{k-1} \exp(2\pi i \sigma(\beta)(x + yi)) \cdot \mathbb{I}_{\mathbb{R}_+}(\sigma(\beta)).$$

If v is finite and $v \nmid \mathfrak{D}$, then

$$(3.3.3) \quad W_\beta \left(\phi_{\chi, s, v}, \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{c}_v^{-1} \end{bmatrix} \right) = \sum_{j=0}^{\text{val}_v(\beta \mathbf{c}_v)} \chi_{+, v}(\varpi_v^j \mathbf{c}_v) |\varpi_v|_v^{-j} \cdot |\mathfrak{d}_{\mathcal{F}}|_v^{-1} \mathbb{I}_{\mathcal{O}_v}(\beta \mathbf{c}_v).$$

Recall that if $v \mid p\mathfrak{F}\mathfrak{F}^c$, then we denote by w the unique place of \mathcal{M} above v such that $w\mathfrak{F}$ or $w \in \Sigma_p$. If $v \mid \mathfrak{D}$, then

$$(3.3.4) \quad W_\beta(\phi_{\chi, s, v}, 1) \Big|_{s=0} = \begin{cases} \chi_w(\beta) \mathbb{I}_{\mathcal{O}_v^\times}(\beta) \cdot |\mathfrak{d}_{\mathcal{F}}|_v^{-1} & \text{if } v \mid p\mathfrak{F}\mathfrak{F}^c \\ C_\beta(\chi_v) \cdot |\mathfrak{d}_{\mathcal{F}}|_v^{-1} \psi_v \left(\frac{t_v}{2d_{\mathcal{F}_v}} \right) & \text{if } v \mid \mathfrak{I}D_{\mathcal{M}/\mathcal{F}}, \end{cases}$$

where

$$(3.3.5) \quad C_\beta(\chi_v) = \int_{\mathcal{F}_v} \chi_v^{-1}(x + 2^{-1}\delta_v) \psi_v \left(\frac{-\beta x}{d_{\mathcal{F}_v}} \right) dx.$$

If $v = w\bar{w}$ with $w \in \Sigma_p$, and $u \in \mathcal{O}_v^\times$, then we have

$$(3.3.6) \quad W_\beta \left(f_{\Phi_v^{[u]}} , 1 \right) \Big|_{s=0} = \chi_{+,v}(\beta) \mathbb{I}_{u(1+\varpi_v, \mathcal{O}_v)}(\beta) \cdot |\mathfrak{d}_{\mathcal{F}}|_v^{-1}.$$

In particular, we have

$$(3.3.7) \quad W_\beta(\phi_{\chi,s,v}, 1) \Big|_{s=0} = \sum_u W_\beta(f_{\Phi_v^{[u]}} , 1) \Big|_{s=0}$$

where u runs over the torsion subgroup of \mathcal{O}_v^\times

Proof. It is proved in Proposition 4.1 of [12] and Section 4.3 of [13]. Note that in [12], the local character χ_v is denoted by λ_v , and the integral $C_\beta(\chi_v)$ is denoted by $A_\beta(\lambda_v)$. As explained in Remark 3.2.26, our local section for a place v dividing $\mathfrak{I}D_{\mathcal{M}/\mathcal{F}}$ differs by a factor from those in [12], so our Fourier-Whittaker coefficient in (3.3.4) differs by the same factor. \square

Remark 3.3.8. As explained in Remark 4.2 of [12], it is clear from the above proposition that the local Whittaker integrals at all finite places are p -integral.

3.4. Normalized Eisenstein series

We introduce some normalized Eisenstein series.

Definition 3.4.1. Let \bullet denote n.h. or h. They are meant to suggest non-holomorphic and holomorphic, respectively. For each Bruhat-Schwartz function Φ on $\mathcal{F}_p \oplus \mathcal{F}_p$ of the form $\Phi_p = \otimes_{v \nmid p} \Phi_v$, we define

$$(3.4.2) \quad \phi_{\chi,s}^\bullet(\Phi_p) = \left(\otimes_{\sigma \in \Sigma} \phi_{k,s,\sigma}^\bullet \right) \otimes \left(\otimes_{v < \infty, v \nmid p} \phi_{\chi,s,v} \right) \otimes \left(\otimes_{v|p} f_{\Phi_v,s} \right),$$

and define the adelic Eisenstein series

$$(3.4.3) \quad E_\chi^\bullet(\Phi_p)(g) = E_\mathbb{A}(g, \phi_{\chi,s}^\bullet(\Phi_p)) \Big|_{s=0}$$

by (3.0.34). Let $D_{\mathcal{F}}$ be the absolute discriminant of \mathcal{F} . We define the holomorphic (resp. nearly holomorphic Eisenstein series) $\mathbb{E}_\chi^h(\Phi_p)$ (resp. $\mathbb{E}_\chi^{\text{n.h.}}(\Phi_p)$) by

$$(3.4.4) \quad \mathbb{E}_\chi^h(\Phi_p)(\tau, g_f) = \frac{\Gamma_\Sigma(k\Sigma)}{\sqrt{|D_{\mathcal{F}}|} (2\pi i)^{k\Sigma}} E_\chi^h(g_\infty, g_f) \cdot \mathbf{J}(g_\infty, \mathbf{i})^{k\Sigma}$$

$$(3.4.5) \quad \begin{aligned} \mathbb{E}_\chi^{\text{n.h.}}(\Phi_p)(\tau, g_f) \\ = \frac{\Gamma_\Sigma(k\Sigma)}{\sqrt{|D_{\mathcal{F}}|} (2\pi i)^{k\Sigma}} E_\chi^{\text{n.h.}}(g_\infty, g_f) \cdot \mathbf{J}(g_\infty, \mathbf{i})^{k\Sigma+2m} (\det(g_\infty))^{-m}, \end{aligned}$$

where $(\tau, g_f) \in X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$, $\mathbf{i} = (i)_{v \in I} \in X_+$, $g_\infty \in \mathrm{GL}_2(\mathcal{F}_\infty)$ with $g_\infty \mathbf{i} = \tau$.

Let $\Phi_p^0 = \otimes_{v|p} \Phi_v^0$ be the Bruhat-Schwartz function on $\mathcal{F}_p \oplus \mathcal{F}_p$ defined in (3.2.20). We define

$$(3.4.6) \quad \mathbb{E}_\chi^h = \mathbb{E}_\chi^h(\Phi_p^0)$$

$$(3.4.7) \quad \mathbb{E}_\chi^{\mathrm{n.h.}} = \mathbb{E}_\chi^{\mathrm{n.h.}}(\Phi_p^0).$$

For every $u = (u_v)_{v|p} \in \prod_{v|p} \mathcal{O}_v^\times = \mathcal{O}_p^\times$, let $\Phi_p^{[u]} = \otimes_{v|p} \Phi_v^{[u_v]}$ be the Bruhat-Schwartz function as defined in (3.2.23) and define

$$(3.4.8) \quad \mathbb{E}_{\chi, u}^h = \mathbb{E}_\chi^h(\Phi_p^{[u]}).$$

We choose an integer N of the form $\mathrm{Norm}_{\mathcal{M}/\mathbb{Q}}(\mathfrak{C}\mathfrak{d}_{\mathcal{M}/\mathcal{F}})^{j_0}$ for a sufficiently large integer j_0 so that $\phi_{\chi, s, v}$ are invariant by $U(N)$ for every $v|N$, and put $K := U(N)$. Then the section $\phi_{\chi, s}(\Phi_p^{[u]})$ is invariant by K_1^n for a sufficiently large n .

Definition 3.4.9. Let $\mathbf{c} = (\mathbf{c}_v)_v$ be an element of $\mathbb{A}_{\mathcal{F}}^{\infty, \times}$ such that $\mathbf{c}_v = 1$ for $v \nmid \mathfrak{D}$, and let $\mathfrak{c} = \mathbf{c} \cdot \mathbb{A}_{\mathcal{F}}^\infty \cap \mathcal{F}$ be the fractional ideal of \mathcal{F} . We call such finite idele \mathbf{c} an idele associated to \mathfrak{c} .

For each $\beta \in \mathcal{F}_+$, the set of all totally positive elements in \mathcal{F} , we define the prime-to- p Fourier coefficient $a_\beta^{(p)}(\chi, \mathfrak{c})$ as

$$(3.4.10) \quad \begin{aligned} & a_\beta^{(p)}(\chi, \mathfrak{c}) \\ &= \frac{1}{|D_{\mathcal{F}}|_{\mathbb{R}}|D_{\mathcal{F}}|_{\mathbb{Q}_p}} \mathrm{Norm}_{\mathcal{F}/\mathbb{Q}}(\beta^{-1}) \prod_{v \nmid p} W_\beta \left(\phi_{\chi, s, v}, \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{c}_v^{-1} \end{bmatrix} \right) \Big|_{s=0} \cdot \mathbb{I}_{\mathcal{O}_p^\times}(\beta). \end{aligned}$$

It is equal to

$$(3.4.11) \quad \begin{aligned} & \beta^{-\Sigma} \prod_{w \nmid \mathfrak{F}} \chi_w(\beta) \mathbb{I}_{\mathcal{O}_w^\times}(\beta) \\ & \cdot \prod_{v \nmid \mathfrak{D}} \left(\sum_{j=0}^{\mathrm{val}_v(\mathbf{c}_v \beta)} \chi_{+, v}(\varpi_v^j) |\varpi_v|^{-j} \right) \prod_{v \nmid \mathfrak{D}_{M/F}} C_\beta(\chi_v) \psi \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \cdot \mathbb{I}_{\mathcal{O}_p^\times}(\beta) \end{aligned}$$

by the formulae of the local Whittaker integrals summarized in Proposition 3.3.1 and the fact that

$$(3.4.12) \quad \prod_v |D_{\mathcal{F}}|_v = 1$$

where the product is taken over the set of all places of \mathcal{F} . It is clear that $a_{\beta}^{(p)}(\chi, \mathfrak{c})$ is p -integral.

We recall the Fourier expansion of Hilbert modular forms. Let \mathfrak{c} be a fractional ideal prime to \mathfrak{D} . Let $f: X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty}) \rightarrow \mathbb{C}$ be either $\mathbb{E}_{\chi,u}^h$ or $\mathbb{E}_{\chi,u}^{n,h}$. Let \mathfrak{c} be the finite idele associated to \mathfrak{c} introduced in Definition 3.4.9. We define $f|_{(\mathcal{O}, \mathfrak{c}^{-1})}$ to be

$$(3.4.13) \quad f|_{(\mathcal{O}, \mathfrak{c}^{-1})}(\tau) = f\left(\tau, \begin{bmatrix} 1 & 0 \\ 0 & \mathfrak{c}^{-1} \end{bmatrix}\right)$$

and it is called the q -expansion of f at the cusp $(\mathcal{O}, \mathfrak{c}^{-1})$. It is well-defined independently of the choice of \mathfrak{c} .

Remark 3.4.14. In the language of geometric modular forms, the q -expansion at the cusp $(\mathcal{O}, \mathfrak{c}^{-1})$ is interpreted as evaluating at the Tate curve associated to the pair $(\mathcal{O}, \mathfrak{c}^{-1})$ of fractional ideals.

Proposition 3.4.15. *The Eisenstein series $\mathbb{E}_{\chi,u}^h$ belongs to $M_k(K_1^n, \mathbb{C})$ for a sufficiently large n . The q -expansion of $\mathbb{E}_{\chi,u}^h$ at the cusp $(\mathcal{O}, \mathfrak{c}^{-1})$*

$$(3.4.16) \quad \mathbb{E}_{\chi,u}^h|_{(\mathcal{O}, \mathfrak{c}^{-1})}(q) = \sum_{\beta \in (N^{-1}\mathfrak{c}^{-1})_+} a_{\beta}(\mathbb{E}_{\chi,u}^h, \mathfrak{c}) q^{\beta} \in \mathbb{C}[[q^{(N^{-1}\mathfrak{c}^{-1})_+}]]$$

has no constant term and the β -th Fourier coefficient of $\mathbb{E}_{\chi,u}^h$ is given by

$$(3.4.17) \quad a_{\beta}(\mathbb{E}_{\chi,u}^h, \mathfrak{c}) = a_{\beta}^{(p)}(\chi, \mathfrak{c}; u) \beta^{k\Sigma} \prod_{v|p} \mathbb{I}_{u_v(1+\varpi_v \mathcal{O}_v)}(\beta) \cdot \prod_{w \in \Sigma_p} \chi_w(\beta).$$

Therefore, $\mathbb{E}_{\chi,u}^h(g; \mathfrak{c})$ belongs to $M_k(\mathfrak{c}, K_1^n, \mathcal{O}_{H,(p)})$, for a number field H contained in \mathbb{C} . Furthermore, we have

$$(3.4.18) \quad \mathbb{E}_{\chi}^h(g; \mathfrak{c}) = \sum_u \mathbb{E}_{\chi,u}^h(g; \mathfrak{c}),$$

where u runs over the elements of the torsion subgroup of \mathcal{O}_p^{\times} .

Proof. See Proposition 4.4 of [12]. □

As explained in Remark (4.11) of [12], an important feature of our Eisenstein series $\mathbb{E}_{\chi,u}^h$ and \mathbb{E}_{χ}^h is that they are toric Eisenstein series of eigencharacter χ . Let us denote by $|[a]$ the right translation action of $\varsigma_f^{-1}\varrho(a)\varsigma_f \in \mathrm{GL}_2(\mathbb{A}_{\mathcal{M}}^{\infty})$ acting on the space of Hilbert modular forms. We define

$$(3.4.19) \quad \mathcal{T} = \prod'_v \mathcal{T}_v \subset \mathbb{A}_{\mathcal{M}}^{\infty,\times},$$

where \prod'_v denotes the restricted product taken over all finite places of \mathcal{F} and

$$(3.4.20) \quad \mathcal{T}_v = \begin{cases} \mathcal{R}_v^{\times} \mathcal{F}_v^{\times} & \text{if } v \text{ is split in } M \\ \mathcal{M}_v^{\times} & \text{if } v \text{ is not split in } M. \end{cases}$$

Note that in Remark 4.5. of [12] Hsieh calls the action of the operator $[a]$ as Hecke action, but we adopt the terminology stabilizer action, as \mathcal{T} stabilizes CM points in the Shimura variety via the action $|[a]$. In the next proposition, we record the action of \mathcal{T} on our Eisenstein series, from which the terminology toric arises.

Proposition 3.4.21 ((4.11) of [12]). *For every $a \in \mathcal{T}$, we have*

$$(3.4.22) \quad \mathbb{E}_{\chi}^h|[a] = \chi^{-1}(a)\mathbb{E}_{\chi}^h$$

$$(3.4.23) \quad \mathbb{E}_{\chi,u}^h|[a] = \chi^{-1}(a)\mathbb{E}_{\chi,u.a^{1-c}}^h.$$

Here ua^{1-c} denotes the element $(u'_v)_{v|p} \in \prod_{v|p} \mathcal{O}_v^{\times}$ with $u'_v = u_v a_w (a_{cw})^{-1}$, w being the element in Σ_p whose restriction to \mathcal{F} is v . In particular, if the p -component of a is trivial, then $ua^{1-c} = u$.

Proof. See the Remark 4.5 of [12]. □

Corollary 3.4.24. *Let v be a root of unity in \mathcal{M} . Using the natural isomorphism $\prod_{v|p} \mathcal{F}_v \cong \prod_{w \in \Sigma_p} \mathcal{M}_w$, we regard v as an element of \mathcal{O}_p^{\times} . Then, we have*

$$(3.4.25) \quad \mathbb{E}_{\chi,u}^h|[v] = \mathbb{E}_{\chi,uv^2}^h.$$

Proof. Let v be a root of unity in \mathcal{M} . We regard v as an idele in $\mathbb{A}_{\mathcal{M}}^{\infty,\times}$ via the diagonal embedding. Since $\chi(v) = 1$, (3.4.23) yields

$$(3.4.26) \quad \mathbb{E}_{\chi,u}^h|[v] = \mathbb{E}_{\chi,u.v^{1-c}}^h.$$

To prove the corollary, it suffices to observe $u.v^{1-c} = uv^2$, since $v^c = v^{-1}$ when v is a root of unity. \square

3.5. Measures and Iwasawa algebra

We review the basic theory of p -adic measures and Iwasawa algebras. In the current subsection, let Z be a profinite group and Λ be the Iwasawa algebra $\Lambda(Z)$. Let R be a p -adic ring. Any continuous function

$$(3.5.1) \quad \phi: Z \rightarrow R$$

extends to a \mathbb{Z}_p -linear map

$$(3.5.2) \quad \phi: \Lambda \rightarrow R$$

which we denote by the same symbol. If we are given an element $\lambda \in \Lambda$ in addition, then we write

$$(3.5.3) \quad \phi(\lambda) = \int_Z \phi d\lambda$$

suggesting that we interpret λ as a measure which we use to integrate the function ϕ .

3.6. p -adic interpolation of Fourier coefficients

In this subsection, we reformulate Proposition [12] in terms of Λ -adic forms so that it becomes easier later for us to prove the necessary congruence between p -adic L -functions. For simplicity, we write $Z(\mathfrak{C}) = Z$ and $\Lambda(Z(\mathfrak{C})) = \Lambda$. In the followings, we will interpret Eisenstein series $\mathbb{E}_{\chi,u}^h(\cdot, [\begin{smallmatrix} 1 & 0 \\ 0 & c^{-1} \end{smallmatrix}])$ as a specialization of a Λ -adic Eisenstein series.

We begin with the definition of domain of interpolation:

Definition 3.6.1. Let \mathfrak{X}_+ be the set of algebraic Hecke characters χ whose infinity type is $k\Sigma$ with $k \geq 1$.

We want to define $A(\beta, v, \mathbf{c}_v) \in \Lambda$ for a totally positive $\beta \in \mathcal{F}$, a finite place v of \mathcal{F} , and $\mathbf{c}_v \in \mathcal{F}_v$, and show that they interpolate Fourier-Whittaker coefficients introduced in Subsection 3.2. We assume that $\mathbf{c}_v = 1$ for $v \nmid p\mathfrak{F}D_{\mathcal{M}/\mathcal{F}}$. Recall that we use the convention that if $v \mid p\mathfrak{F}\mathfrak{F}^c$, then w denotes the place of \mathcal{M} contained in Σ_p or dividing \mathfrak{F} . If v is not split in \mathcal{M} , w denotes the unique place of \mathcal{M} lying above v .

Lemma 3.6.2. *Let v be a place of \mathcal{F} which does not divide $\mathfrak{I}D_{\mathcal{M}/\mathcal{F}}$. Define $A(\beta, v, \mathbf{c}_v) \in \Lambda$ by*

$$(3.6.3) \quad A(\beta, v, \mathbf{c}_v) = \begin{cases} \text{rec}_w(\beta)\mathbb{I}_{\mathcal{O}_v^\times}(\beta) & \text{if } v|\mathfrak{C} \text{ splits in } \mathcal{M}, w|v, w|\mathfrak{F} \\ \sum_{j=0}^{\text{val}_v(\beta\mathbf{c}_v)} \text{rec}_{\mathcal{M},v}(\varpi_v^j\mathbf{c}_v)|\varpi_v|_v^{-j}\mathbb{I}_{\mathcal{O}_v}(\beta\mathbf{c}_v) & \text{if } v < \infty \text{ and } v \nmid p\mathfrak{C}D_{\mathcal{M}/\mathcal{F}} \end{cases}$$

Then, for every χ

$$(3.6.4) \quad \int_{\mathcal{Z}} \widehat{\chi} dA(\beta, v, \mathbf{c}_v) = |\mathfrak{d}|_v \cdot W_\beta \left(\phi_{\chi,s,v}, \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{c}_v^{-1} \end{bmatrix} \right) |_{s=0}$$

holds.

Proof. The assertion of the lemma is a restatement of the formulas given in Proposition 3.3.1. □

We also need an analogue of the previous lemma for places v dividing $\mathfrak{I}D_{\mathcal{M}/\mathcal{F}}$. As usual, w denotes the unique place of \mathcal{M} lying above v . We first analyze the integral

$$(3.6.5) \quad C_\beta(\chi_v) = \int_{\mathcal{F}_v} \chi_v^{-1}(x + 2^{-1}\boldsymbol{\theta}_v)\psi_v \left(\frac{-\beta x}{d_{\mathcal{F}_v}} \right) dx$$

which was defined in (3.3.5). Let \mathfrak{l} be the maximal ideal of \mathcal{O}_v . There exists sufficiently large non-negative integers j_0 and j_1 such that

$$(3.6.6) \quad C_\beta(\chi_v) = \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}} \chi_v^{-1}(x + 2^{-1}\boldsymbol{\theta}_v)\psi_v \left(\frac{-\beta x}{d_{\mathcal{F}_v}} \right)$$

because the conductor of χ_v divides $\mathfrak{C}\mathcal{R}_w$ for all $\chi \in \mathfrak{X}_+$. It is important that we can choose j_0 and j_1 which satisfies (3.6.6) for a given $\beta \in \mathcal{F}$ independently of $\chi \in \mathfrak{X}_+$. Now we can readily formulate the following analogue of Lemma 3.6.2.

Lemma 3.6.7. *Let v be a place of \mathcal{F} which divides $\mathfrak{I}D_{\mathcal{M}/\mathcal{F}}$. Define $A(\beta, v, \mathbf{c}_v) \in \Lambda$ as*

(3.6.8)

$$A(\beta, v, \mathbf{c}_v) = \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{I}^{j_1}, dx) \sum_{x \in \mathfrak{I}^{-j_0}/\mathfrak{I}^{j_1}} \text{rec}_v(x + 2^{-1}\boldsymbol{\theta}_v)^{-1} \psi_v \left(\frac{-\beta x}{d_{\mathcal{F}_v}} \right).$$

Then, for every $\chi \in \mathfrak{X}_+$

$$(3.6.9) \quad \int_Z \widehat{\chi} dA(\beta, v, 1) = |\mathfrak{d}|_v \cdot W_\beta(\phi_{\chi, s, v}, 1) |_{s=0}$$

holds.

Proof. It follows immediately from (3.6.6). □

Definition 3.6.10. We define $A^{(p)}(\beta, \mathbf{c}) \in \Lambda$ as

$$(3.6.11) \quad A^{(p)}(\beta, \mathbf{c}) = \text{rec}_{\mathcal{M}}^\infty(\beta) \text{Norm}_{\mathcal{F}/\mathbb{Q}}(\beta)^{-1} \prod_{v \nmid p} A(\beta, v, \mathbf{c}_v).$$

The superscript (p) in the notation suggests that it is Fourier coefficients away from p .

For every $u \in \mathcal{O}_p^\times$, which is of finite order, we define $A(\beta, \mathbf{c}; u) \in \Lambda$ as

$$(3.6.12) \quad A(\beta, \mathbf{c}; u) = A^{(p)}(\beta, \mathbf{c}) \text{rec}_{\Sigma_p}(\beta) \mathbb{I}_{u(1+\varpi_p \mathcal{O}_p)}(\beta).$$

Proposition 3.6.13. *We have*

$$(3.6.14) \quad \int_Z \widehat{\chi} dA^{(p)}(\beta, \mathbf{c}) = i_p \left(A_\beta^{(p)}(\chi, \mathbf{c}) \right),$$

and

$$(3.6.15) \quad \int_Z \widehat{\chi} dA(\beta, \mathbf{c}; u) = A_\beta(\chi, \mathbf{c}; u)$$

for every $\chi \in \mathfrak{X}_+$.

Proof. By (3.4.11), Lemma 3.6.2, and Lemma 3.6.7, the equality (3.6.14) follows from

$$(3.6.16) \quad \widehat{\chi} (\text{rec}_{\mathcal{M}}^\infty(\beta)) \text{Norm}_{\mathcal{F}/\mathbb{Q}}(\beta)^{-1} = \beta^{(k-1)\Sigma}.$$

Indeed, by the definition of p -adic avatar

$$(3.6.17) \quad \widehat{\chi} (\text{rec}_{\mathcal{M}}^\infty(\beta)) = \chi(\beta^\infty) i_p \left(\beta^{k\Sigma} \right)$$

$$(3.6.18) \quad =i_p \left(\beta^{k\Sigma} \right).$$

Also, $\beta^\Sigma = \text{Norm}_{\mathcal{F}/\mathbb{Q}}(\beta)$ as $\beta \in \mathcal{F}$, whence (3.6.16) follows. On the other hand, (3.6.15) directly follows from Proposition 3.4.15. \square

Let \mathfrak{c} be a fractional ideal of \mathcal{F} prime to $p\mathfrak{C}D_{\mathcal{M}/\mathcal{F}}$. We define $E(\mathfrak{c}; u)$ as a formal q -expansion

$$(3.6.19) \quad E(\mathfrak{c}; u) = \sum_{\beta} A(\beta, \mathfrak{c}; u)q^\beta.$$

For a continuous function $\phi: Z \rightarrow \overline{\mathbb{Q}}_p$, we write $E(\mathfrak{c}; u)(\phi)$ the formal q -series whose β -th coefficient is $\int_Z \phi dA(\beta, \mathfrak{c}; u)$. Then Proposition 3.4.15 implies that for $\chi \in \mathfrak{X}_+$ we have

$$(3.6.20) \quad E(\mathfrak{c}; u)(\widehat{\chi}) = \mathbb{E}_{\chi, u}^h |_{(\mathcal{O}, c^{-1})}.$$

In particular, $E(\mathfrak{c}; u)$ is a Λ -adic modular form in the sense of Definition 2.3.4.

3.7. A modification factor

In this subsection, we will define a modification factor which we denote by \mathcal{C} . It will be used in our definition of p -adic L -function.

Let us begin with the notation for uniformizers in the completions of \mathcal{M} . Let v be a place of \mathcal{F} lying over p , and let w be the unique place in Σ_p lying over v . Let \bar{w} be the complex conjugate of w . Fix a uniformizer ϖ_w of \mathcal{M}_w . The complex conjugation c extends to an isomorphism

$$(3.7.1) \quad \mathcal{M}_w \rightarrow \mathcal{M}_{\bar{w}}$$

and let $\varpi_{\bar{w}}$ be the image is ϖ_w under the above isomorphism. In particular, $\varpi_{\bar{w}}$ is a uniformizer of $\mathcal{M}_{\bar{w}}$.

As before, for any place w of \mathcal{M} , we denote by rec_w the local Artin reciprocity map

$$(3.7.2) \quad \text{rec}_w: \mathcal{M}_w^\times \rightarrow Z$$

and define the modification factor \mathcal{C} to be

$$(3.7.3) \quad \mathcal{C} = \prod_{w \in \Sigma_p} \left(1 - \frac{\text{rec}_w(\varpi_w)}{\text{rec}_{\bar{w}}(\varpi_{\bar{w}})} \right),$$

which is an element of Λ , the Iwasawa algebra of Z . Of course, \mathcal{C} depends on our choice of uniformizer ϖ_w , but we will make it explicit whenever there is a preferred choice.

Remark 3.7.4. One might attempt to explain why a particular choice of ϖ_w is preferred to others using Lubin-Tate theory, but it will not be one of our main concerns since our main example will be the cyclotomic \mathbb{Z}_p -extension.

Let χ_0 be a Hecke character of \mathcal{M}_0 whose infinity type $1\Sigma_0$, and suppose that $\chi_0|_{\mathbb{A}_{\mathbb{Q}}^\times}$ is the product of the quadratic character of \mathcal{M}_0/\mathbb{Q} and the adelic norm on $\mathbb{A}_{\mathbb{Q}}^\times$. Assume that p splits in \mathcal{M}_0 , and p is relatively prime to the conductor of χ_0 . In this case, a CM type Σ_0 of \mathcal{M}_0 is merely choice of an embedding of \mathcal{M}_0 into \mathbb{C} , which we choose to be the restriction of i_∞ to \mathcal{M}_0 . Let w be the unique element in $\Sigma_{0,p}$, the p -adic CM type of \mathcal{M}_0 induced by Σ_0 , and let p_w be the image of p under the natural isomorphism

$$(3.7.5) \quad \mathbb{Q}_p \longrightarrow \mathcal{M}_{0,w}$$

which is of course a uniformizer of $\mathcal{M}_{0,w}$. If we let $p_{\bar{w}}$ be the image of p under the natural isomorphism

$$(3.7.6) \quad \mathbb{Q}_p \longrightarrow \mathcal{M}_{0,\bar{w}}$$

then the isomorphism

$$(3.7.7) \quad \mathcal{M}_{0,w} \longrightarrow \mathcal{M}_{0,\bar{w}}$$

induced by the complex conjugation maps p_w to $p_{\bar{w}}$. Define $\alpha \in \mathbb{C}$ to be

$$(3.7.8) \quad \alpha := \chi_0(p_w)$$

which is in fact an algebraic number. Furthermore, we assume that α is a p -adic unit with respect to our fixed embedding i_p . If not, using the assumption that p splits in \mathcal{M}_0 , we can make α to be a p -adic unit by replacing χ_0 with its complex conjugate.

Suppose that we are given a CM field \mathcal{M} which contains \mathcal{M}_0 , and define

$$(3.7.9) \quad \chi := \chi_0^k \circ \text{Norm}_{\mathcal{M}/\mathcal{M}_0}$$

for any integer k , where $\text{Norm}_{\mathcal{M}/\mathcal{M}_0} : \mathbb{A}_{\mathcal{M}}^\times \rightarrow \mathbb{A}_{\mathcal{M}_0}^\times$ denotes the map between ideles induced by the norm map. If we let κ be the algebraic Hecke character

$$(3.7.10) \quad \kappa : \mathbb{A}_{\mathcal{M}}^{\times} \rightarrow \mathbb{C}^{\times}$$

$$(3.7.11) \quad x \mapsto |x|_{\mathbb{A}_{\mathcal{M}}}$$

then p -adic avatar $\widehat{\kappa}$ of κ is the p -adic cyclotomic character, because we have normalized the reciprocity maps geometrically.

Important examples of such \mathcal{M} are of the form

$$(3.7.12) \quad \mathcal{M}_r = \mathcal{M}_0(\mu_{p^r})$$

for any non-negative integer r . In this case, we choose the uniformizer ϖ_r for the unique element w_r in the p -adic CM type Σ_p of \mathcal{M}_r to be

$$(3.7.13) \quad \varpi_r = 1 - \zeta_{p^r}$$

for a primitive p^r -th root of unity ζ_{p^r} , and furthermore we may choose them so that

$$(3.7.14) \quad \text{Norm}_{\mathcal{M}_{r+1, w_{r+1}}/\mathcal{M}_{r, w_r}}(\varpi_{r+1}) = \varpi_r$$

for any positive integer r , and

$$(3.7.15) \quad \text{Norm}_{\mathcal{M}_{1, w_1}/\mathcal{M}_{0, w_0}}(\varpi_1) = p$$

for $r = 1$ case.

Proposition 3.7.16. *Suppose that \mathcal{M} is of the form $\mathcal{M}_0(\mu_{p^r})$. In particular, we choose $\varpi_w \in \mathcal{M}_w$ for the unique element $w \in \Sigma_p$ such that*

$$(3.7.17) \quad \text{Norm}_{\mathcal{M}_w/\mathbb{Q}_p}(\varpi_w) = p$$

holds. Then

$$(3.7.18) \quad \int_Z \widehat{\chi \kappa^n} d\mathcal{C} = 1 - \frac{\alpha^k p^k}{\bar{\alpha}^k} = 1 - \alpha^{2k} p^{2k}$$

holds for any integers k and n .

Proof. We can achieve (3.7.17) by (3.7.13). Note that according to the geometric normalization of the reciprocity map, $\alpha \bar{\alpha} = p^{-1}$. Also note the fact that $\kappa(\varpi_w) = \kappa(\varpi_{\bar{w}})$. The assertion of the proposition easily follows from the definitions of χ , α , and p -adic avatars of them. □

3.8. p -adic L -function

In this subsection, we define the p -adic L -function and describe its interpolation property which characterizes it. We make some modifications to the p -adic L -function defined in [12], which is crucial for our proof of the main result.

For a number field H denote by $Cl(H)$ the ideal class group of H . The transfer map induces a map $Cl(\mathcal{F}) \rightarrow Cl(\mathcal{M})$ and let $Cl_-(\mathcal{M})$ be its cokernel. We often write Cl_- instead of $Cl_-(\mathcal{M})$ for simplicity. Let \mathcal{D} a set of representatives for Cl_- , chosen from $\mathbb{A}_{\mathcal{M}}^{\mathbb{Q}, \infty, \times}$. As before, we write Z for $Z(\mathfrak{C})$, and Λ denotes the Iwasawa algebra over Z , and let $\mathcal{C} \in \Lambda$ be the modification factor defined in (3.7.3).

Let U be the torsion subgroup of \mathcal{O}_p^\times . Using our CM type, we regard U as a subgroup of $\prod_{w \in \Sigma_p} \mathcal{R}_w^\times$. On the other hand, \mathcal{R}^\times is embedded into $\prod_{w \in \Sigma_p} \mathcal{R}_w$ via Σ_p . We define the subgroup U_{alg} of U as

$$(3.8.1) \quad U_{\text{alg}} := U \cap (\mathcal{R}^\times)^{1-c},$$

which consists of all roots of unity in \mathcal{R} of odd order, embedded into U via Σ_p . Corollary 3.4.24 shows that $E(\mathfrak{c}(a); u)$ only depends on the coset of u in U/U_{alg} .

Definition 3.8.2. We define a measure $\mathcal{L}_{\Sigma, \mathfrak{c}, \delta}$ on Z to be

$$(3.8.3) \quad \mathcal{L}_{\Sigma, \mathfrak{c}, \delta} = \mathcal{C} \cdot \sum_{u \in U/U_{\text{alg}}} \sum_{a \in \mathcal{D}} \text{rec}_{\mathcal{M}}(a) E(\mathfrak{c}(a); u)(x(a)) \in \Lambda,$$

and we often write $\mathcal{L} = \mathcal{L}_{\Sigma, \mathfrak{c}, \delta}$.

We compare our normalization of p -adic L -function with some of those appeared in the literature. In [12], \mathcal{D} is chosen to be a representative set for Cl_- modulo the image of \mathcal{T} in Cl_- under $\text{rec}_{\mathcal{M}}$, and the sum indexed by u is taken over U . The difference in \mathcal{D} is harmless because the image of \mathcal{T} in Cl_- is 2-primary, whence it simply introduce a constant factor which prime to p . However, the difference introduced by U_{alg} is a constant factor, which is not always prime to p . In [12], p is always assumed to be unramified in \mathcal{F} , which implies that the order of U_{alg} is prime to p . On the other hand, when p ramifies in \mathcal{F} , the order of U_{alg} may be divisible by p , and we possibly obtain more optimal \mathcal{L} by considering U/U_{alg} instead of U . Indeed, this factor is what made the p -adic L -function of [15, 11] sometimes differ from the interpolation formula predicted by non-commutative Iwasawa

theory, as observed in [17]. The factor \mathcal{C} which we defined in (3.7.3) did not appear in the previous work of p -adic Hecke L -functions, but it appeared in the interpolation formula for the p -adic Rankin-Selberg L -functions.

For a place w that divides $p\mathfrak{C}^+$, recalling that we have chosen θ_v in Subsection 2.4, let

$$(3.8.4) \quad \text{Eul}_w(\chi_w) = \chi_w(2\delta_w) \frac{L(0, \chi_w)}{\epsilon(0, \chi_w, \psi)L(1, \chi_w^{-1})}$$

and define

$$(3.8.5) \quad \text{Eul}_p(\chi) = \prod_{w \in \Sigma_p} \text{Eul}(\chi_w), \quad \text{Eul}_{\mathfrak{C}^+}(\chi) = \prod_{w|\mathfrak{F}} \text{Eul}(\chi_w).$$

Also we write

$$(3.8.6) \quad \mathcal{C}_\infty(\chi) = i_\infty(i_p^{-1}\mathcal{C}(\widehat{\chi})).$$

Let $L^{p\mathfrak{C}}(\chi, s)$ be the imprimitive complex L -function, obtained by removing Euler factors dividing $p\mathfrak{C}$ from the primitive complex L -function $L(\chi, s)$. We call \mathcal{L} a p -adic L -function because it interpolates special values of complex Hecke L -functions in the following way.

Proposition 3.8.7. *Let χ be algebraic Hecke character of infinity type $k\Sigma + (1 - c)m$ satisfying either*

$$(3.8.8) \quad k \geq 1, \text{ and } m_\sigma \geq 0 \text{ for all } \sigma$$

or

$$(3.8.9) \quad k \leq 1, \text{ and } k + m \geq 0 \text{ for all } \sigma.$$

Let r be the number of distinct prime factors of the relative discriminant $D_{\mathcal{M}/\mathcal{F}}$. Then

$$(3.8.10) \quad \frac{\int_{\mathbb{Z}} \widehat{\chi} d\mathcal{L}}{\Omega_p^{k\Sigma+2m}} = L^{p\mathfrak{C}}(\chi, 0) \cdot \mathcal{C}_\infty(\chi) \text{Eul}_p(\chi) \text{Eul}_{\mathfrak{C}^+}(\chi) \times \frac{2^r \pi^m \Gamma_\Sigma(k\Sigma + m)}{\sqrt{|D_{\mathcal{F}}|_{\mathbb{R}}} (\text{Im}(\delta))^m \Omega_\infty^{k\Sigma+2m}}$$

holds. The equality is understood as the assertion that the both sides are algebraic numbers in \mathbb{C} and $\overline{\mathbb{Q}}_p$ respectively, and they are equal to each other with respect to the embeddings i_∞ and i_p .

Proof. By definition of \mathcal{L} , we have

$$(3.8.11) \quad \int_{\mathbb{Z}} \widehat{\chi} d\mathcal{L} = \mathcal{C}(\widehat{\chi}) \sum_{u \in U/U_{\text{alg}}} \sum_{a \in \mathcal{D}} \widehat{\chi}(a) E(\mathfrak{c}(a), u)(\widehat{\chi})(x(a)).$$

The right hand side is computed in Proposition 4.9 of [12], from which we deduce (3.8.10). \square

3.9. Remarks on Iwasawa main conjecture and μ -invariants

We give two remarks on Iwasawa main conjectures related to \mathcal{L} , and μ -invariants of specializations of \mathcal{L} , respectively. The remarks are logically independent from the rest of the paper, despite of the importance of main conjecture and μ -invariants.

Firstly, we consider the Iwasawa main conjectures related to \mathcal{L} . Let \mathcal{M} be an imaginary quadratic field and let C/\mathcal{M} be an elliptic curve with complex multiplication by \mathcal{M} . Let $p \geq 5$ be a good ordinary prime for C . We let \mathcal{V} the field obtained by the p -power division points of C to \mathcal{M} . Then, by means of elliptic units, one can prove the Iwasawa main conjecture associated to E and the extension \mathcal{V}/\mathcal{M} . In particular, we have a measure \mathcal{L}^u on $\text{Gal}(\mathcal{V}/\mathcal{M})$, which arises from elliptic units, such that \mathcal{L}^u has a suitable interpolation formula, and \mathcal{L}^u generates the characteristic ideal of the Selmer group of C over \mathcal{V} . Therefore, in order for a Katz measure \mathcal{L} to satisfy a main conjecture, \mathcal{L} must be compatible with \mathcal{L}^u .

Let us elaborate on the meaning of \mathcal{L} being compatible with \mathcal{L}^u by considering

$$(3.9.1) \quad \mathcal{M}_1 = \mathcal{M}(\mu_p)$$

where $p \geq 5$ is a prime number which splits in \mathcal{M} . Then \mathcal{M}_1 is contained in \mathcal{V} , and there are $p-1$ characters of $\text{Gal}(\overline{\mathbb{Q}}/\mathcal{M})$ which factor through $\text{Gal}(\mathcal{M}_1/\mathcal{M})$. For such a character χ , and let \mathcal{L}_χ^u be the branch associated to it. On the other hand, we let \mathcal{L} be the Katz measure associated to \mathcal{M}_1 . We may assume that the conductor \mathfrak{C} of \mathcal{L} is sufficiently small so that \mathcal{L} can be restricted to $\text{Gal}(\mathcal{V}/\mathcal{M}_1)$. We denote the restricted measure by $\mathcal{L}(\mathcal{V}/\mathcal{M}_1)$. If the main conjecture were true for \mathcal{L} , then it would imply that

$$(3.9.2) \quad \mathcal{L}(\mathcal{V}/\mathcal{M}_1) \cdot \Lambda = \prod_{\chi} \mathcal{L}_\chi^u \cdot \Lambda$$

where Λ is the Iwasawa algebra of $\text{Gal}(\mathcal{V}/\mathcal{M}_1)$.

However, according to the original construction of \mathcal{L} due to Katz and its generalization due to Hida and Tilouine, one should multiply p to the right hand side of (3.9.2) in order to have the equality. For the detailed analysis of $\mathcal{L}(\mathcal{V}/\mathcal{M})$, see [17]. In particular, \mathcal{L} does not satisfy the main conjecture. On the other hand, when p is unramified in \mathcal{M} , anti-cyclotomic specializations of \mathcal{L} are known to satisfy the main conjectures, due to Hida and Tilouine [11]. Note that the assumption on the odd prime p being unramified in \mathcal{M} rules out possibility for \mathcal{M} to contain a non-trivial p -th root of unity. When \mathcal{M} contains non-trivial p -power roots of unity, only after our modification, \mathcal{L} is compatible with \mathcal{L}^u . Based on this compatibility, we believe that the modified measure \mathcal{L} satisfied the Iwasawa main conjecture, although we are unable to prove it.

Now we consider the μ -invariants of \mathcal{L} . When p is unramified in \mathcal{M} , due to the work of Hida, the anti-cyclotomic μ -invariants of \mathcal{L} , specialized with respect to a character, can be computed from the p -adic valuations of the Fourier coefficients of the Eisenstein series which gave rise to \mathcal{L} . Hida also computed the p -adic valuations of Fourier coefficients, and, under some technical assumptions proved that anti-cyclotomic μ -invariants vanish. Hsieh removed the technical assumptions that were necessary for the proof of vanishing of μ -invariants, by introducing the Whittaker model that we recalled in the earlier part of the present Section. Despite of the generality for which they can prove the vanishing of μ -invariants, the assumption that p is unramified in \mathcal{M} has never been removed. Our computation shows that the original measure of Katz, without the modifications we made here, may have strictly positive μ -invariants, say m .

When \mathcal{M} contains a primitive p^r -th root of unity, then we prove that m is at least r , as a consequence of the modification. When \mathcal{M} is obtained by adjoining p^r -th roots of unity to an imaginary quadratic field, then we expect more. Hida's formula for the anti-cyclotomic μ -invariants crucially depends on one of his theorems, which we call linear independence theorem. His paper contains a proof for linear independence theorem for p unramified in \mathcal{M} . In a private communication, he expressed that it is likely that the statement itself remains true without the assumption on p being unramified in \mathcal{M} . Taking the linear independence theorem for granted, one can show that the μ -invariant an anti-cyclotomic specialization of the modified measure \mathcal{L} vanishes, under the necessary assumptions on the specialization character.

4. Transfer congruence

In this section, we prove the transfer congruence, which is the main result of the current paper.

4.1. The normalized diagonal embedding

In this subsection, we introduce the normalized diagonal embedding which we denote by Δ , and study its effect on q -expansions on Hilbert modular forms. As before, \mathcal{F}/\mathcal{F}' is a degree p extension of totally real fields, and Δ will be a slight modification of $\tilde{\Delta}$, which were introduced in Subsection 2.5. Unfortunately, in order to have a good normalized Δ , we need to impose a condition on \mathcal{F}/\mathcal{F}' which is stronger than (P) imposed therein. Throughout this section, we will assume that

(P') The relative different $\mathfrak{d}_{\mathcal{F}/\mathcal{F}'}$ is $p\mathcal{O}$.

Clearly, (P') implies (P), which is introduced in Subsection 2.5. Furthermore, whenever (P') is true, we always take $d_{\mathcal{F}/\mathcal{F}'}$ in (P) to be p .

Definition 4.1.1. Recall that $\tilde{\Delta}$ was defined in (2.5.2). Define the normalized diagonal embedding Δ to be

$$(4.1.2) \quad \Delta: X'_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty) \rightarrow X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$$

$$(4.1.3) \quad x \mapsto \begin{bmatrix} p^{-1} & 0 \\ 0 & p \end{bmatrix} \cdot \tilde{\Delta}(x) = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} x \begin{bmatrix} 1 & 0 \\ 0 & p^{-1} \end{bmatrix}.$$

It is easy to see that if f is an automorphic form on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$, then the pull-back of f along Δ which denote by Δ^*f is an automorphic form on $X'_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty)$. The strategy for the proof of our main result is to compare an automorphic form f on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$ and f' on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty)$ by comparing the q -expansions of Δ^*f and f' . In order to do that, it is important to express the q -expansion of Δ^*f in terms of f . Before we formulate it precisely, we introduce some notation. Let f be a holomorphic automorphic form on $X_+ \times \mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^\infty)$. Suppose that we are given a finite idele $g^\infty \in \mathrm{GL}(\mathbb{A}_{\mathcal{F}}^\infty)$, and consider the function F on X_+ which is defined by

$$(4.1.4) \quad F(\tau) = f((\tau, g^\infty)).$$

Let τ_σ to be the σ -component of τ for each $\sigma \in I$, then we have a Fourier expansion of the form

$$(4.1.5) \quad F(\tau) = \sum_{\beta} a_{\beta}(F) \exp \left(2\pi i \sum_{\sigma \in I} \sigma(\beta) \tau_{\sigma} \right)$$

for some $a_\beta(F) \in \mathbb{C}$, where β runs over the set of all totally non-negative elements in \mathcal{F} . In fact, as a function of β , $a_\beta(F)$ is supported on a fractional ideal of \mathcal{F} , but it is irrelevant for our purpose to make that ideal explicit. Now consider a finite idele g'^∞ in $\text{GL}_2(\mathbb{A}_{\mathcal{F}'}^\infty)$. Define f' to be $\Delta^* f$ and define F' to be the restriction of f' to $X'_+ \times \{g'^\infty\}$. Then, F' will also have a Fourier expansion of the form

$$(4.1.6) \quad F'(\tau') = \sum_{\beta'} a'_{\beta'}(F') \exp \left(2\pi i \sum_{\sigma' \in I'} \sigma'(\beta') \tau_{\sigma'} \right).$$

Proposition 4.1.7. *In the situation above, assume in addition that*

$$(4.1.8) \quad g^\infty = \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{c}^{-1} \end{bmatrix}, \text{ and } g'^\infty = \begin{bmatrix} 1 & 0 \\ 0 & (\mathbf{c}')^{-1} \end{bmatrix},$$

and that the natural map $\mathbb{A}_{\mathcal{F}'}^\infty \rightarrow \mathbb{A}_{\mathcal{F}}^\infty$ sends \mathbf{c}' to \mathbf{c} . Then, we have

$$(4.1.9) \quad a_{\beta'}(F') = \sum_{\beta} a_\beta(F),$$

where the sum is taken over the set consisting of $\beta \in \mathcal{F}$ such that $\text{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta) = p\beta'$.

Proof. Let τ' an arbitrary element in X'_+ , and let τ be the element of X_+ such that for each $\sigma \in \Sigma$, τ_σ equals to $\tau'_{\sigma'}$ where σ' is the restriction of σ to \mathcal{F}' . In other words, τ is the image of τ' under the naive diagonal embedding $X'_+ \rightarrow X_+$. The assertion of the proposition follows from a straightforward calculation. Indeed, applying (4.1.3), we have

$$(4.1.10) \quad F'(\tau') = f' \left(\left(\tau', \begin{bmatrix} 1 & 0 \\ 0 & (\mathbf{c}')^{-1} \end{bmatrix} \right) \right)$$

$$(4.1.11) \quad = \Delta^* f \left(\left(\tau', \begin{bmatrix} 1 & 0 \\ 0 & (\mathbf{c}')^{-1} \end{bmatrix} \right) \right)$$

$$(4.1.12) \quad = f \left(\left(p^{-1}\tau, \begin{bmatrix} 1 & 0 \\ 0 & \mathbf{c}^{-1} \end{bmatrix} \right) \right)$$

$$(4.1.13) \quad = F(p^{-1}\tau)$$

$$(4.1.14) \quad = \sum_{\beta} a_\beta(F) \exp \left(2\pi i \sum_{\sigma \in I} \sigma(\beta) p^{-1} \tau_\sigma \right)$$

$$(4.1.15) \quad = \sum_{\beta} a_{\beta}(F) \exp \left(2\pi i \sum_{\sigma' \in I'} \sum_{\sigma|_{\mathcal{F}'}=\sigma'} \sigma(\beta) p^{-1} \tau_{\sigma} \right)$$

$$(4.1.16) \quad = \sum_{\beta} a_{\beta}(F) \exp \left(2\pi i \sum_{\sigma' \in I'} p^{-1} \tau_{\sigma'} \sum_{\sigma|_{\mathcal{F}'}=\sigma'} \sigma(\beta) \right)$$

$$(4.1.17) \quad = \sum_{\beta} a_{\beta}(F) \exp \left(2\pi i \sum_{\sigma' \in I'} p^{-1} \tau_{\sigma'} \operatorname{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta) \right)$$

$$(4.1.18) \quad = \sum_{\beta' \in \mathcal{F}'} \sum_{\beta: \operatorname{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta)=\beta'} a_{\beta}(F) \exp \left(2\pi i \sum_{\sigma' \in I'} p^{-1} \tau_{\sigma'} \beta' \right)$$

$$(4.1.19) \quad = \sum_{\beta' \in \mathcal{F}'} \left(\sum_{\beta: \operatorname{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta)=p\beta'} a_{\beta}(F) \right) \exp \left(2\pi i \sum_{\sigma' \in I'} \tau_{\sigma'} \beta' \right).$$

From this we conclude the assertion of the proposition. □

4.2. Properties of Katz' p -adic modular forms

As promised in Remark 2.3.6, we introduce the notion of p -adic modular forms following Katz. It is stronger than Hida's definition which we stated as Definition 2.3.4, in the sense that a p -adic modular form in the sense of Hida is naturally a p -adic modular form in the sense of Katz. In contrast to the elementary definition of Hida, which uses nothing more than q -expansions, that of Katz is built upon the theory of integral models of Shimura varieties and the Igusa tower. We will not go into them, and we will just summarize some properties of Katz' modular form that we need.

Remark 4.2.1. For the readers who are interested in the definition, not just properties, of Katz' p -adic modular forms, we suggest consulting the paper [12] by Hsieh, the original paper [15] of Katz, and the book [9] of Hida. However, there is some technical complications that need to be pointed out. The compactification of the integral model of Shimura variety and the Igusa tower that need to be constructed first appeared in the thesis of Rapoport. However, the thesis contained a mistake, which makes the proof of q -expansion principle for p -adic modular forms incomplete when p divides the discriminant of the totally real field being considered. Note that the excluded cases are precisely what interest us, while the most of literature deals with the opposite situation in which p is unramified in it. The work [5]

of Deligne and Pappas fixes the problem, from which we can deduce the q -expansion principle along the smooth locus of the Shimura variety. Over the ordinary locus, the two moduli problems defined by Deligne-Pappas and Rapoport agree, whence the cusps and the ordinary CM points belong to the same component of the special fiber modulo p . In particular, we can apply the q -expansion principle to the CM points $x(a)$ that are considered in the current article.

As before, \mathcal{F} will denote a totally real field and we fix an ideal \mathfrak{c} of \mathcal{F} , which plays the role of a polarization ideal. Let K be an open compact subgroup of $GL_2(\mathbb{A}_{\mathcal{F}}^{\infty})$. We keep the conditions on K that we imposed in Subsection 2.2. Let \mathbb{Q}_p^{ur} be the maximal unramified extension of \mathbb{Q}_p , and let \mathcal{I} be the p -adic completion of the valuation ring of \mathbb{Q}_p^{ur} . For a p -adic ring R which is also an \mathcal{I} -algebra, we define $V(\mathfrak{c}, K; R)$ to be the space of Katz p -adic modular forms with coefficients in R defined in 2.5.3. of [12].

We now want to explain some properties of the space $V(\mathfrak{c}, K; R)$ which will be needed later. We begin with q -expansions. Recall that we defined the formal power series $R[[q^L]]$ for a lattice L of \mathcal{F} in (2.2.7). Then, $V(\mathfrak{c}, K; R)$ is endowed with the injective q -expansion homomorphism

$$(4.2.2) \quad V(\mathfrak{c}, K; R) \hookrightarrow R[[q^L]]$$

$$(4.2.3) \quad f \mapsto \sum_{\beta} a_{\beta}(f)q^{\beta}$$

for some L . If we view $a_{\beta}(F)$ as a function of a variable $\beta \in \mathcal{F}$, then it is supported on the set of totally positive elements in L .

The next property of Katz p -adic modular form is its relation with classical automorphic forms. Recall that $M_k(\mathfrak{c}, K_1^n, R)$ was defined for a subring R of \mathbb{C} in (2.2.10). Assume that R_0 is a subring of \mathbb{C} such that $i_p(R_0)$ is contained in a subring R of \mathbb{C}_p which is again an \mathcal{I} -algebra. Then we have a natural map

$$(4.2.4) \quad M_k(\mathfrak{c}, K_1^n, R_0) \rightarrow V(\mathfrak{c}, K; R)$$

$$(4.2.5) \quad f \mapsto \widehat{f}$$

and \widehat{f} is called the p -adic avatar of f . The p -adic avatar \widehat{f} of a Hilbert modular form f in $M_k(\mathfrak{c}, K_1^n, R_0)$ is characterized the property that the q -expansion of f in as a Hilbert modular form is equal to the q -expansion of \widehat{f} as a p -adic modular form.

The next property of Katz' p -adic modular form is that we have a natural injective map from the space of p -adic modular forms in the sense of Hida.

Recall that the latter was defined in Definition 2.3.4, and $V_0(\mathfrak{c}, K; R)$ denotes the space of them. Assume that R is an \mathcal{I} -algebra. We have a canonical map

$$(4.2.6) \quad V_0(\mathfrak{c}, K; R) \rightarrow V(\mathfrak{c}, K; R)$$

which is characterized by the preservation of the q -expansion. That is, denoting by i the inclusion (4.2.6) temporarily, to say that for every $f \in V_0(\mathfrak{c}, K; R)$, the q -expansion of $i(f)$ is equal to the formal power series that defines F . From now, we identify $V_0(\mathfrak{c}, K; R)$ as a subspace of $V(\mathfrak{c}, K; R)$.

Another property of Katz' p -adic modular forms that distinguish it from Hida's is that it is functorial in the coefficients. Let R and R' be two p -adic rings that are algebras over \mathcal{I} . For any \mathcal{I} -algebra homomorphism $\alpha: R \rightarrow R'$, we have a canonical map

$$(4.2.7) \quad \alpha_*: V(\mathfrak{c}, K; R) \longrightarrow V(\mathfrak{c}, K; R').$$

In terms of q -expansions, α_* is characterized by the natural map $R[[q]] \rightarrow R'[[q]]$ induced by α .

The last property of Katz' p -adic modular form that we will need is the evaluation homomorphism. For each CM point $x(a)$, we have

$$(4.2.8) \quad V(\mathfrak{c}, K; R) \longrightarrow R$$

$$(4.2.9) \quad F \mapsto F(x(a))$$

which satisfies the following properties. Firstly, for $\alpha: R \rightarrow R'$, we have

$$(4.2.10) \quad \alpha(F(x(a))) = (\alpha_*F)(x(a)).$$

Also, we have

$$(4.2.11) \quad f(x(a)) = \widehat{f}(x(a)).$$

4.3. A map between p -adic modular forms

In this subsection, we keep the assumptions from the previous section, and we study a map between p -adic modular forms induced by Δ . In particular, we work with a degree p extension \mathcal{F}/\mathcal{F}' such that the relative different $\mathfrak{d}_{\mathcal{F}/\mathcal{F}'}$ is generated by p . Also, we fix quadratic CM extension $\mathcal{M}'/\mathcal{F}'$ with CM type Σ' , and define \mathcal{M} to be $\mathcal{M}'\mathcal{F}$. Let δ' be an element in \mathcal{M}' satisfying the polarization conditions (pol-1), (pol-2), and (pol-3) for $\mathcal{M}'/\mathcal{F}'$. Let \mathfrak{c}' be the ideal of \mathcal{F}' associated to δ' by the condition (pol-3). Let δ be $p\delta' \in \mathcal{M}$. Then,

by our discussion in Subsection 2.5, δ satisfies the polarization conditions for \mathcal{M}/\mathcal{F} . Also, the polarization ideal \mathfrak{c} associated to δ equals $\mathfrak{c}' \cdot \mathcal{O}$.

We will use the notation from Subsection 2.3 and Section 3. Furthermore, we take ideals \mathfrak{C} of \mathcal{F} and \mathfrak{C}' in \mathcal{F}' in such a way that $\mathfrak{C}'\mathcal{O} = \mathfrak{C}$. Let K (resp. K') be the open compact subgroup in $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}}^{\infty})$ (resp. $\mathrm{GL}_2(\mathbb{A}_{\mathcal{F}'}^{\infty})$) introduced in Section 3. By shrinking K' if necessary, Δ^* induces a map

$$(4.3.1) \quad \Delta^* : M_k(\mathfrak{c}, K_1^n, \mathbb{C}) \rightarrow M_{pk}(\mathfrak{c}', K_1'^m, \mathbb{C}).$$

Recall that $V(\mathfrak{c}, K; R)$ denotes the space of R -adic modular forms. Let R_0 be a subring of $\overline{\mathbb{Q}}$ such that $i_p(R_0)$ is contained in the valuation ring of \mathbb{C}_p , and let R be the completion of $i_p(R_0)$ in \mathbb{C}_p . Then there is a canonical embedding

$$(4.3.2) \quad M_k(\mathfrak{c}, K_1^n, R) \rightarrow V(\mathfrak{c}, K; R)$$

$$(4.3.3) \quad f \mapsto \widehat{f}$$

which is compatible with the q -expansions on both sides. We claim that Δ^* in fact induces a map between Λ -adic forms

$$(4.3.4) \quad \Delta^* : V_0(\mathfrak{c}, K; \Lambda) \longrightarrow V_0(\mathfrak{c}', K'; \Lambda),$$

Indeed, if $\widehat{\chi} \in \mathfrak{X}$, $f \in V_0(\mathfrak{c}, K; \Lambda)$, then $(\Delta^*(f))(\widehat{\chi})$ equals $\Delta^*(f(\widehat{\chi}))$ at least as two formal q -expansions. Since $f(\widehat{\chi})$ belongs to $M_k(\mathfrak{c}, K, \mathbb{C})$ for a Zariski dense set of characters $\widehat{\chi}$, it follows that $(\Delta^*(f))(\widehat{\chi}')$ belongs to $M_{kp}(\mathfrak{c}', K', \mathbb{C})$ for such characters $\widehat{\chi}'$. It follows that $\Delta^* f$ belongs to $V_0(\mathfrak{c}', K'; \Lambda)$.

4.4. Proof of the main theorem

In this subsection, assuming the condition (P') and two more conditions (I) and (C) which will be defined below, we prove Theorem 4.4.11, the main theorem of the current paper. We will introduce two p -adic modular forms and deduce the transfer congruence between p -adic L -functions from the congruence between these two p -adic modular forms and applying the q -expansion principle. We begin with formulating the q -expansion principle that we are going to use.

Theorem 4.4.1 (*q-expansion principle*). *Let R be a p -adic ring. Let f be an R -adic modular form in $V(\mathfrak{c}, K; R)$. Suppose that f has q -expansion*

$$(4.4.2) \quad f(q) = \sum_{\beta} a_{\beta}(f)q^{\beta}.$$

Let $x(1)$ be the CM point defined in Subsection 2.4. Suppose that there is an ideal J of R such that for all β , $a_\beta(f)$ belongs to J . Then we have

$$(4.4.3) \quad f(x(1)) \in J.$$

Proof. Let $\mathcal{O}_{\mathbb{C}_p}$ be the valuation ring of \mathbb{C}_p . Let Y be a Zariski dense set of homomorphisms $\phi: R \rightarrow \mathcal{O}_{\mathbb{C}_p}$ such that $f(\phi)$ has a q -expansion

$$(4.4.4) \quad f(\phi) = \sum_{\beta} i_p(a_\beta(f_\phi))q^\beta$$

for some $f_\phi \in M_k(\mathfrak{c}, K_1^n, i_p^{-1}(\mathcal{O}_{\mathbb{C}_p}))$. Such Y exists by definition of R -adic modular forms. Let J_ϕ be the ideal of $\mathcal{O}_{\mathbb{C}_p}$ generated by the image of J under $\phi: R \rightarrow \mathcal{O}_{\mathbb{C}_p}$. Then, of course $a_\beta(f(\phi)) \equiv 0$ modulo J_ϕ . As $x(1)$ is an integral point on the Shimura variety, the q -expansion principle implies that $f_\phi(x(1))$ belongs to J_ϕ . Now $f(x(1))$ is, by definition, the element of R such that $\phi(f(x(1))) = f_\phi(x(1))$. Such $f(x(1))$ is unique since Y is Zariski dense for R . Then it follows that $f(x(1)) \in J$. \square

Now we define the relevant Λ -adic forms. Fix a set of representatives for U/U_{alg} , and introduce a linear combination of Eisenstein series

$$(4.4.5) \quad E(\mathfrak{c}) = \mathcal{C} \cdot \sum_{u \in U/U_{\text{alg}}} \sum_{a \in \mathcal{D}} \text{rec}_{\mathcal{M}}(a)E(\mathfrak{c}(a); u)[[a] \in V(\mathfrak{c}, K; \Lambda)].$$

By the action of the operator $[[a]$ on $\mathbb{E}_{\chi, u}^h$ described in Proposition (3.4.21), $E(\mathfrak{c})$ is independent of the choice of \mathcal{D} . We record an important property of $E(\mathfrak{c})$.

Proposition 4.4.6. *The p -adic L -function \mathcal{L} of Definition (3.8.2) satisfies*

$$(4.4.7) \quad E(\mathfrak{c})(x(1)) = \mathcal{L}$$

where \mathfrak{c} is associated to δ by (pol-3).

Proof. For $\widehat{\chi} \in \mathfrak{X}_+$, we have

$$(4.4.8) \quad E(\mathfrak{c})(x(1))(\widehat{\chi}) = \mathcal{C}(\widehat{\chi}) \sum_{u \in U/U_{\text{alg}}} \sum_{a \in \mathcal{D}} \widehat{\chi}(a)E(\mathfrak{c}(a); u)(\widehat{\chi})[[a](x(1))$$

$$(4.4.9) \quad = \mathcal{C}(\widehat{\chi}) \sum_{u \in U/U_{\text{alg}}} \sum_{a \in \mathcal{D}} \widehat{\chi}(a)E(\mathfrak{c}(a); u)(\widehat{\chi})(x(a))$$

$$(4.4.10) \quad = \int_Z \widehat{\chi} d\mathcal{L}.$$

The second equality follows from the definition of the operator $[[a]]$. Indeed, we defined $[[a]]$ to be the translation $|(\varsigma_f^{-1} \varrho(a) \varsigma_f)$, which sends $x(1)$ to $x(a)$ according to our definition of CM points. The third equality directly follows from the definition of \mathcal{L} . □

The transfer congruence, which is the main result of current paper is the following. We remind the reader that the condition **(P')** was introduced in the beginning of Subsection 4.1, and the conditions **(I)** and **(C)** will be defined below. All three conditions **(P')**, **(I)**, and **(C)** will be proved in the next subsection when $\mathcal{M} = \mathcal{M}'(\mu_{p^r})$ for some $r \geq 2$. Also, see Remark 4.5.26 for a discussion on these conditions.

Theorem 4.4.11. *Suppose that the conditions **(P')**, **(I)** and **(C)** hold. Then we have the transfer congruence*

$$(4.4.12) \quad \mathcal{L}_{\Sigma, \mathfrak{c}' \circ, p\delta'} \equiv \text{ver}(\mathcal{L}'_{\Sigma', \mathfrak{c}', \delta'}) \pmod{T}.$$

Note that we brought back the subscripts of the p -adic L -functions, which tell us the particular choice of CM types, the conductors, and the polarizations. To lighten the notation, we will often suppress the subscripts. The rest of the current subsection will be devoted to the proof of above theorem. We outline the strategy of the proof. In order to show that

$$(4.4.13) \quad \mathcal{L} \equiv \text{ver}(\mathcal{L}') \pmod{T}$$

it suffices to show that

$$(4.4.14) \quad \Delta^* E(\mathfrak{c})(x'(1)) \equiv \text{ver}_* E'(\mathfrak{c}')(x'(1)) \pmod{T}$$

because $\Delta(x'(1)) = x(1)$. By applying the q -expansion principle, in the form of Theorem 4.4.1, applied to $\Delta^* E(\mathfrak{c})$ and $\text{ver}_* E'(\mathfrak{c}')$, (4.4.14) follows from

$$(4.4.15) \quad a_{\beta'}(\Delta^* E(\mathfrak{c})) \equiv a_{\beta'}(\text{ver}_* E'(\mathfrak{c}')) \pmod{T}$$

for every $\beta' \in \mathcal{F}'$. We will prove (4.4.15).

Let us write the β -th Fourier coefficient of $E(\mathfrak{c}(a); u)$ as

$$(4.4.16) \quad a_{\beta}(E(\mathfrak{c}(a); u)) = A(\beta, \mathfrak{c}(a); u)$$

and similarly define $A'(\beta', \mathbf{c}'(a'); u')$ for $E'(\mathbf{c}'(a'); u')$. In particular, if we define $B(\beta, \mathbf{c})$ and $B'(\beta', \mathbf{c}')$ to be the β -th Fourier coefficient of $E(\mathbf{c})$ and the β' -th Fourier coefficient of $E'(\mathbf{c}')$ respectively, then

$$(4.4.17) \quad B(\beta, \mathbf{c}) = \mathcal{C} \cdot \sum_{a \in \mathcal{D}} \text{rec}_{\mathcal{M}}(a) \sum_{u \in U/U_{\text{alg}}} A(\beta, \mathbf{c}(a); u)$$

holds, and similarly

$$(4.4.18) \quad B'(\beta', \mathbf{c}') = \mathcal{C}' \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \sum_{u' \in U'/U'_{\text{alg}}} A'(\beta', \mathbf{c}'(a'); u')$$

holds. By the description about the effect of Δ on q -expansion given in Proposition 4.1.7, the assertion of (4.4.15) is equivalent to the assertion that for each totally positive $\beta' \in \mathcal{F}'$

$$(4.4.19) \quad \sum_{\beta} B(\beta, \mathbf{c}) \equiv \text{ver}(B'(\beta', \mathbf{c}')) \pmod{T}$$

holds, where the sum indexed by β is taken over the set $\{\beta | \beta \in \mathcal{F}, \text{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta) = p\beta'\}$.

Either side of (4.4.19) does not depend on the choice of representatives that we make, but we need to choose representatives that are preserved by the action of G . The condition (I) requires that this is in fact possible to do so.

(I) One can choose the representatives for Cl_- and U/U_{alg} to be G -sets.

In other words, the condition (I) requires that every element in Cl_-^G can be represented by a G -invariant ideal, and similarly every coset in $(U/U_{\text{alg}})^G$ contains an element of U^G . Since $Cl'_- \subset Cl_-$, and $U'/U'_{\text{alg}} \subset U/U_{\text{alg}}$, the condition (I) implies that we can choose a G -set \mathcal{D} of representatives for Cl_- which extends any given set \mathcal{D}' of representatives for Cl'_- . Similarly, we can choose a G -set of representatives for U/U_{alg} extending any given set of representatives for U'/U'_{alg} . In the rest of the subsection, we fix such a representatives.

The next two propositions are the criterions which we will use to prove (4.4.19).

Proposition 4.4.20. *Recall that $G = \text{Gal}(\mathcal{M}/\mathcal{M}')$ acts on Z , which extends to an action on Λ . Suppose we have an element $\lambda \in \Lambda$ of the form*

$$(4.4.21) \quad \lambda = \sum_{\gamma \in W} \lambda_{\gamma}$$

where the sum is taken over a finite set W with G -action, and $\lambda_\gamma \in \Lambda$. Let the action of G on $\gamma \in W$ be written as $\gamma \mapsto \gamma^g$ for $g \in G$. Let W^G be the subset of W consisting of the elements of W that are fixed by G . Then λ belongs to the trace ideal T if

$$(4.4.22) \quad g\lambda_\gamma = \lambda_{\gamma^g}$$

for all $\gamma \in W - W^G$ and all $g \in G$, and

$$(4.4.23) \quad \lambda_\gamma \in p\Lambda$$

for all $\gamma \in W^G$.

Proof. Define

$$(4.4.24) \quad \bar{\lambda}_\gamma = \begin{cases} \lambda_\gamma & \text{if } \gamma \in W - W^G \\ p^{-1}\lambda_\gamma & \text{if } \gamma \in W^G \end{cases}$$

for each $\gamma \in W$. By the assumptions, $\bar{\lambda}_\gamma$ is well defined and belongs to Λ . It is easy to see that λ is the image of

$$(4.4.25) \quad \sum_{\gamma \in W/G} \bar{\lambda}_\gamma$$

under the trace map, hence the proof is complete. \square

A variant of the previous proposition is the following.

Proposition 4.4.26. *Keep the notation from Proposition 4.4.20. Identify Z with the image of Z in Λ under the natural map $Z \rightarrow \Lambda$. Suppose we have an element $\lambda \in \Lambda$ of the form*

$$(4.4.27) \quad \lambda = \sum_{\gamma \in W} a_\gamma z_\gamma$$

Then λ belongs to the trace ideal T if

$$(4.4.28) \quad gz_\gamma = z_{\gamma^g}$$

for any $\gamma \in W$ and any $g \in G$,

$$(4.4.29) \quad a_\gamma = a_{g\gamma}$$

for any $\gamma \in W - W^G$, and

$$(4.4.30) \quad a_\gamma \in p\mathbb{Z}_p$$

for any $\gamma \in W^G$.

Proof. It is a special case of Proposition 4.4.20, where we have taken λ_γ to be of the form $a_\gamma z_\gamma$. \square

We introduce a condition from which we deduce (4.4.19), which will be proved later under a mild assumption.

(C) Let $G = \text{Gal}(\mathcal{M}/\mathcal{M}')$. We can choose \mathcal{D} to be a G -set. Furthermore, we have

$$(4.4.31) \quad \mathcal{C} \cdot \sum_{a \in \mathcal{D}^G} \text{rec}_{\mathcal{M}}(a) = \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \right)$$

holds.

Proposition 4.4.32. *Assume (I) and (C). Then (4.4.19) holds.*

Proof. Unfolding the definition, (4.4.19) is

$$(4.4.33) \quad \mathcal{C} \cdot \sum_{u \in U/U_{\text{alg}}} \sum_a \sum_\beta A(\beta, \mathbf{c}(a); u) \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{u' \in U'/U'_{\text{alg}}} \sum_{a'} A'(\beta', \mathbf{c}'(a'); u') \right)$$

where the sum on the left hand side is indexed over the triples (β, a, u) , where $u \in U/U_{\text{alg}}$, $a \in \mathcal{D}$, and $\beta \in \mathcal{F}$ such that $\text{Tr}(\beta) = p\beta'$, and the sum on the right hand side is indexed over the pairs (u', a') where $u' \in U'/U'_{\text{alg}}$ and $a' \in \mathcal{D}'$.

We first show G acts on the term $A(\beta, \mathbf{c}(a); u)$ by

$$(4.4.34) \quad gA(\beta, \mathbf{c}(a); u) = A(\beta^g, \mathbf{c}(a^g); u^g).$$

Recall the definitions

$$(4.4.35) \quad A^{(p)}(\beta, \mathbf{c}) = \text{rec}^\infty(\beta) \text{Norm}_{\mathcal{F}/\mathbb{Q}}(\beta^{-1}) \prod_{v \nmid p} A(\beta, v, \mathbf{c}_v),$$

$$(4.4.36) \quad A(\beta, \mathbf{c}; u) = A^{(p)}(\beta, \mathbf{c}) \text{rec}_{\Sigma_p}(\beta) \mathbb{I}_{u(1+\varpi_p \mathcal{O}_p)}(\beta),$$

from which we deduce that

$$(4.4.37) \quad gA(\beta, \mathbf{c}; u)$$

$$(4.4.38) \quad = gA^{(p)}(\beta, \mathbf{c}) \times \text{grec}_{\Sigma_p}(\beta) \times \mathbb{I}_{u(1+\varpi_p \circ_p)}(\beta)$$

$$(4.4.39) \quad = gA^{(p)}(\beta, \mathbf{c}) \times \text{rec}_{\Sigma_p}(\beta^g) \times \mathbb{I}_{u^g(1+\varpi_p \circ_p)}(\beta^g).$$

Therefore (4.4.34) is reduced to

$$(4.4.40) \quad gA^{(p)}(\beta, \mathbf{c}(a)) = A^{(p)}(\beta^g, \mathbf{c}(a^g)),$$

which is further reduced, using (4.4.35), to the assertion that

$$(4.4.41) \quad g \prod_{v|v'} A(\beta, v, \mathbf{c}(a)_v) = \prod_{v|v'} A(\beta^g, v, \mathbf{c}(a^g)_v)$$

holds for each $v' \nmid p$. Indeed, first we observe

$$(4.4.42) \quad g \prod_{v|v'} A(\beta, v, \mathbf{c}(a)_v) = \prod_{v|v'} gA(\beta, v, \mathbf{c}(a)_v)$$

$$(4.4.43) \quad = \prod_{v|v'} A(\beta^g, v^g, (\mathbf{c}(a)_v)^g)$$

where the second equality follows from formulae in Lemma 3.6.2. Continuing the computation, we obtain

$$(4.4.44) \quad \prod_{v|v'} A(\beta^g, v^g, (\mathbf{c}(a)_v)^g) = \prod_{v|v'} A(\beta^g, v^g, \mathbf{c}(a^g)_{v^g})$$

$$(4.4.45) \quad = \prod_{v^g|v'} A(\beta^g, v^g, \mathbf{c}(a^g)_{v^g})$$

$$(4.4.46) \quad = \prod_{v|v'} A(\beta^g, v, \mathbf{c}(a^g)_v)$$

where we permuted the index set by $v \mapsto v^g$ in the second equality.

Define the index set W to be

$$(4.4.47) \quad W = \{(\beta, a, u) \mid \text{Tr}_{\mathcal{F}/\mathcal{F}'}(\beta) = p\beta', a \in \mathcal{D}, u \in U/U_{\text{alg}}\}$$

on which G acts by

$$(4.4.48) \quad g(\beta, a, u) = (\beta^g, a^g, u^g).$$

In other words, the triple summation appearing in the left hand side of (4.4.33) is taken over the set W . By Proposition 4.4.26, the validity of (4.4.34) implies that

$$(4.4.49) \quad \sum_{(\beta, a, u) \in W - W^G} A(\beta, \mathfrak{c}(a); u) \in T$$

and it follows that

$$(4.4.50) \quad \mathcal{C} \cdot \sum_{(\beta, a, u) \in W - W^G} A(\beta, \mathfrak{c}(a); u) \in T$$

because T is an ideal.

Now it is sufficient to prove

$$(4.4.51) \quad \mathcal{C} \cdot \sum_{(\beta, a, u) \in W^G} \text{rec}_{\mathcal{M}}(a) A(\beta, \mathfrak{c}(a); u) \\ \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{(u', a')} \text{rec}_{\mathcal{M}'}(a') A'(\beta', \mathfrak{c}'(a'); u') \right) \pmod{T}$$

in order to show Proposition 4.4.32. In fact, the terms on the left hand side with $u \notin U'$ are zero, since $\beta^g = \beta$ and $\text{Tr}(\beta) = p\beta'$ imply $\beta = \beta'$, and for those u we have $\mathbb{I}_{u(1+\varpi_n \mathcal{O}_n)}(\beta) = 0$, whence $A(\beta, \mathfrak{c}(a); u)$ is zero. We have reduced (4.4.51) to the assertion

$$(4.4.52) \quad \mathcal{C} \cdot \sum_{(u', a)} \text{rec}_{\mathcal{M}}(a) A(\beta', \mathfrak{c}(a); u) \\ \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{(u', a')} \text{rec}_{\mathcal{M}}(a) A'(\beta', \mathfrak{c}'(a'); u') \right) \pmod{T},$$

where u' varies in U' in both sides, and a' varies in \mathcal{D}' on the right hand side, and a varies among elements of \mathcal{D} such that $\mathfrak{c}(a^g) = \mathfrak{c}(a)$. By identifying $\mathcal{D}^G = \mathcal{D}'$, we write

$$(4.4.53) \quad \mathcal{C} \cdot \sum_{(u', a')} \text{rec}_{\mathcal{M}}(a) A(\beta', \mathfrak{c}(a'); u) \\ \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{(u', a')} \text{rec}_{\mathcal{M}}(a) A'(\beta', \mathfrak{c}'(a'); u') \right) \pmod{T},$$

and the index sets on both sides are the same. In particular, we can further reduce (4.4.53) to the assertion that for each $u' \in U'$

$$(4.4.54) \quad \mathcal{C} \cdot \sum_{a'} \text{rec}_{\mathcal{M}}(a') A(\beta', \mathbf{c}(a'); u') \\ \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{a'} \text{rec}_{\mathcal{M}}(a) A'(\beta', \mathbf{c}'(a'); u') \right) \pmod{T}$$

holds. We rewrite (4.4.54) equivalently in the form

$$(4.4.55) \quad \mathcal{C} \cdot \sum_{a'} \text{rec}_{\mathcal{M}}(a') \times \mathbb{I}_{u'(1+\varpi_p \mathcal{O}_p)}(\beta') \times \text{rec}_{\Sigma_p}(\beta') \times \prod_{v' \nmid p} \left(\prod_{v|v'} A(\beta', v, \mathbf{c}(a')_v) \right) \\ \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{a'} \text{rec}_{\mathcal{M}}(a') \times \mathbb{I}_{u'(1+\varpi'_p \mathcal{O}'_p)}(\beta') \times \text{rec}_{\Sigma'_p}(\beta') \right. \\ \left. \times \prod_{v' \nmid p} A(\beta', v', \mathbf{c}'(a')_{v'}) \right) \pmod{T}.$$

Since we assumed (C), it suffices to show that

$$(4.4.56) \quad \mathbb{I}_{u'(1+\varpi_p \mathcal{O}_p)}(\beta') \text{rec}_{\Sigma_p}(\beta') = \text{ver} \left(\mathbb{I}_{u'(1+\varpi'_p \mathcal{O}'_p)}(\beta') \text{rec}_{\Sigma'_p}(\beta') \right)$$

holds, and for each $v' \nmid p$ and each $a' \in \mathcal{D}'$,

$$(4.4.57) \quad \prod_{v|v'} A(\beta', v, \mathbf{c}(a')_v) \equiv \text{ver} \left(A(\beta', v', \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

holds. Indeed, we deduce

$$(4.4.58) \quad \mathcal{C} \cdot \sum_{a \in \mathcal{D}^G} \text{rec}_{\mathcal{M}}(a) \prod_{v' \nmid p} \left(\prod_{v|v'} A(\beta', v, \mathbf{c}(a)_v) \right)$$

$$(4.4.59) \quad \equiv \mathcal{C}' \cdot \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \cdot \text{ver} \left(\prod_{v' \nmid p} A(\beta', v', \mathbf{c}'(a')_{v'}) \right)$$

(4.4.60)

$$\equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \right) \cdot \text{ver} \left(\prod_{v' \nmid p} A(\beta', v', \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

where the first and the second congruence follows from (4.4.57) and (C), respectively. By multiplying (4.4.56) to the congruence

$$(4.4.61) \quad \mathcal{C} \cdot \sum_{a \in \mathcal{D}^G} \text{rec}_{\mathcal{M}}(a) \prod_{v' \nmid p} \left(\prod_{v|v'} A(\beta', v, \mathbf{c}(a)_v) \right)$$

$$(4.4.62) \quad \equiv \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \prod_{v' \nmid p} A(\beta', v', \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

we obtain (4.4.55), which is equivalent to (4.4.54).

From the definition of u and u' (4.4.56) follows immediately, and we now prove (4.4.57) by dividing it into several lemmas.

Lemma 4.4.63. *Suppose v' splits in \mathcal{F} , v' splits in \mathcal{M}' , and the place w' of \mathcal{M}' lying above v' divides \mathfrak{F} . Then, the assertion of (4.4.57) is true.*

Proof. From Lemma 3.6.2, we observe that the assertion of (4.4.57) is just

$$(4.4.64) \quad \prod_{v|v'} \text{rec}_w(\beta) \mathbb{I}_{\mathcal{O}_v^\times}(\beta') \equiv \text{ver} \left(\text{rec}_{w'}(\beta') \mathbb{I}_{\mathcal{O}_{v'}^\times}(\beta') \right) \pmod{T},$$

which follows immediately from the definition of ver in terms of ideles. In fact, the equality holds in that case as well. \square

Lemma 4.4.65. *Suppose v' splits in \mathcal{F} , and v' does not divide \mathfrak{D} . Further assume that v' is not ramified in \mathcal{F} , which is satisfied if we assume (P). Then, the assertion of (4.4.57) is true.*

Proof. If we use the formulae in Lemma 3.6.2, in this case (4.4.57) becomes

(4.4.66)

$$\prod_{v|v'} \left(\sum_{j=0}^{\text{val}_v(\beta' \mathbf{c}(a')_v)} \text{rec}_w(\varpi_w^j \mathbf{c}(a')_v) |\varpi_w|_w^{-j} \mathbb{I}_{\mathcal{O}_v}(\beta' \mathbf{c}(a')_v) \right)$$

$$(4.4.67) \quad \equiv \text{ver} \left(\sum_{j=0}^{\text{val}_{v'}(\beta' \mathbf{c}'(a')_{v'})} \text{rec}_{w'}(\varpi_{w'}^j \mathbf{c}'(a')_{v'}) | \varpi_{w'}' |_{w'}^{-j} \mathbb{I}_{\mathcal{O}_{v'}}(\beta' \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

because v' does not divide \mathfrak{D} . We will apply Proposition 4.4.26 after rearranging the terms of (4.4.66). Define

$$(4.4.68) \quad n_v = \text{val}_v(\beta' \mathbf{c}(a')_v)$$

and we take the set W to be

$$(4.4.69) \quad W = \{(j_v)_{v|v'} \mid j_v = 0, 1, 2, \dots, n_v\}$$

consisting of tuples of integers indexed by the set of places v of \mathcal{F} dividing v' . We equip W with the G -action

$$(4.4.70) \quad ((j_v)_{v|v'})^g = (j_{v^{g^{-1}}})_{v|v'}$$

given by the opposite action of G on the indices. Expanding the product in (4.4.66), we obtain the sum

$$(4.4.71) \quad \sum_{j \in W} \lambda_j$$

where j denotes the tuple $(j_v)_{v|v'}$, and for each $j \in W$, λ_j is given by

$$(4.4.72) \quad \prod_{v|v'} \text{rec}_w(\varpi_w^{j_v} \mathbf{c}(a')_v) | \varpi_w |_{w'}^{-j_v} \mathbb{I}_{\mathcal{O}_v}(\beta' \mathbf{c}(a')_v).$$

By routine calculations, letting $h = g^{-1}$ for simplicity, we obtain

$$(4.4.73) \quad g\lambda_j = g \prod_{v|v'} \text{rec}_w(\varpi_w^{j_v} \mathbf{c}(a')_v) | \varpi_w |_{w'}^{-j_v} \mathbb{I}_{\mathcal{O}_v}(\beta' \mathbf{c}(a')_v)$$

$$(4.4.74) \quad = \prod_{v|v'} \text{rec}_{w^g}(\varpi_{w^g}^{j_v} \mathbf{c}(a')_{v^g}) | \varpi_{w^g} |_{w^g}^{-j_v} \mathbb{I}_{\mathcal{O}_{v^g}}(\beta' \mathbf{c}(a')_{v^g})$$

$$(4.4.75) \quad = \prod_{v|v'} \text{rec}_w(\varpi_w^{j_{v^h}} \mathbf{c}(a')_v) | \varpi_w |_{w'}^{-j_{v^h}} \mathbb{I}_{\mathcal{O}_v}(\beta' \mathbf{c}(a')_v)$$

$$(4.4.76) \quad = \lambda_{j^g},$$

which is the first condition of Proposition 4.4.20. We deduce that

$$(4.4.77) \quad \sum_{j \in W - W^G} \lambda_j \in T$$

and it remains to show that

$$(4.4.78) \quad \sum_{j \in W^G} \lambda_j \equiv \text{ver} \left(\sum_{j=0}^{\text{val}_{v'}(\beta' \mathbf{c}'(a')_{v'})} \text{rec}_{w'}(\varpi_{w'}^j \mathbf{c}'(a')_{v'}) | \varpi_{w'}^{-j} \mathbb{I}_{\mathcal{O}_{v'}}(\beta' \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

holds. Firstly, it is clear that W^G consists of the parallel tuples $(j_v)_{v|v'}$ such that $j_v = n$ for some $n = 0, 1, 2, \dots, \text{val}_v(\beta' \mathbf{c}'(a')_v)$. By our assumption, v' is unramified in \mathcal{F} . Noting that our \mathbf{c} is fixed by G , we observe

$$(4.4.79) \quad \text{val}_{v'}(\beta' \mathbf{c}'(a')_{v'}) = \text{val}_v(\beta' \mathbf{c}'(a')_v)$$

from which we deduce that (4.4.78) holds as an equality. The proof of the lemma is complete. \square

Lemma 4.4.80. *Suppose v' splits in \mathcal{F} , and v' is either inert or ramified in \mathcal{M}' . Then, the assertion of (4.4.57) is true.*

Proof. According to the definition of $A(\beta', v, \mathbf{c}(a')_v)$,

$$(4.4.81) \quad \begin{aligned} & A(\beta', v, \mathbf{c}(a')_v) \\ &= \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}} \text{rec}_v(x + 2^{-1}\theta_v)^{-1} \psi_v \left(\frac{-\beta' x}{d_{\mathcal{F}_v}} \right) \end{aligned}$$

given in Lemma 3.6.7, for any pair of sufficiently large integers j_0 and j_1 . Since it does not depend on the finite idele $\mathbf{c}(a')_v$, and we will consider a fixed β' , we simply write

$$(4.4.82) \quad A(v) = A(\beta', v, \mathbf{c}(a')_v)$$

and similarly write

$$(4.4.83) \quad A'(v') = A'(\beta', v', \mathbf{c}'(a')_{v'})$$

temporarily. Recall that we defined Remark 2.4.18. Note that

$$(4.4.84) \quad \prod_{v|v'} \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) = \psi_{v'} \left(\frac{-pt'_{v'}}{2d_{\mathcal{F}_v}} \right) = \psi_{v'} \left(\frac{-t'_{v'}}{2d_{\mathcal{F}'_{v'}}} \right)$$

holds. Also note that

$$(4.4.85) \quad \text{Vol}(\mathfrak{l}^{j_1}, dx_v) = \text{Vol}(\mathfrak{l}'^{j_1}, dx')$$

holds, where dx_v and dx' are Haar measures on \mathcal{F}_v and $\mathcal{F}'_{v'}$, such that

$$(4.4.86) \quad \text{Vol}(\mathcal{O}_v, dx_v) = \text{Vol}(\mathcal{O}'_{v'}, dx') = 1.$$

Of course, dx_v and dx are the same, and the subscript merely specifies the place v . Also note that

$$(4.4.87) \quad g \cdot \text{rec}_v(x + 2^{-1}\theta_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right) = \text{rec}_v(x^g + 2^{-1}\theta_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right)$$

for any $g \in G$ and any $x \in \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}$. Using these properties, one can show the assertion of the lemma by an argument similar to the proof of Lemma 4.4.65. One may take the index set W to be

$$(4.4.88) \quad W = \{(x_v)_{v|v'} \mid x_v \in \mathfrak{l}_v^{-j_0}/\mathfrak{l}_v^{j_1}\}$$

where \mathfrak{l}_v is the maximal ideal of \mathcal{O}_v , and the G -action on W is given by

$$(4.4.89) \quad ((x_v)_{v|v'})^g = (x_{v^{g^{-1}}})_{v|v'}$$

which is the inverse action on the indices similar to (4.4.70). We omit the details. \square

Lemma 4.4.90. *Suppose v' is inert in \mathcal{F} , and v' does not divide \mathfrak{D}' . Then, the assertion of (4.4.57) is true.*

Proof. In this case, there is a unique place v of \mathcal{F} lying above v' . Because v' is inert in \mathcal{F} , we have

$$(4.4.91) \quad |\varpi_{v'}|_{v'}^p = |\varpi_v|_v$$

and, in particular, we have

$$(4.4.92) \quad |\varpi_{v'}|_{v'}^p \equiv |\varpi_v|_v \pmod{p}.$$

Also, since v is unramified over v' , we have

$$(4.4.93) \quad \text{val}_{v'}(\beta' \mathbf{c}(a')_{v'}) = \text{val}_v(\beta' \mathbf{c}(a')_v).$$

The assertion of the lemma is

$$(4.4.94) \quad \sum_{j=0}^{\text{val}_v(\beta \mathbf{c}(a')_v)} \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v) |\varpi_v|^{-j} \mathbb{I}_{\mathcal{O}_v}(\beta \mathbf{c}(a')_v)$$

$$(4.4.95) \quad \equiv \text{ver} \left(\sum_{j=0}^{\text{val}_{v'}(\beta \mathbf{c}(a')_{v'})} \text{rec}_{\mathcal{M}',v'}(\varpi_{v'}^j \mathbf{c}'(a')_{v'}) |\varpi_{v'}|^{-j} \mathbb{I}_{\mathcal{O}_{v'}}(\beta' \mathbf{c}'(a')_{v'}) \right) \pmod{T}$$

which equivalent to

$$(4.4.96) \quad \sum_{j=0}^n \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v) |\varpi_v|^{-j} \mathbb{I}_{\mathcal{O}_v}(\beta \mathbf{c}(a')_v)$$

$$(4.4.97) \quad \equiv \sum_{j=0}^n \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v) |\varpi_{v'}|^{-j} \mathbb{I}_{\mathcal{O}_v}(\beta \mathbf{c}(a')_v) \pmod{T}$$

where we have written $n = \text{val}_{v'}(\beta' \mathbf{c}(a')_{v'}) = \text{val}_v(\beta' \mathbf{c}(a')_v)$. We apply Proposition 4.4.26 to

$$(4.4.98) \quad \sum_{j=0}^n \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v) \left(|\varpi_v|^{-j} - |\varpi_{v'}|^{-j} \right) \mathbb{I}_{\mathcal{O}_v}(\beta \mathbf{c}(a')_v).$$

Since \mathbf{c} is the image of \mathbf{c}' , it is fixed by G , and hence

$$(4.4.99) \quad g \cdot \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v) = \text{rec}_{\mathcal{M},v}(\varpi_v^j \mathbf{c}(a')_v)$$

and the criterion of Proposition 4.4.26 is satisfied by our previous observation (4.4.92). The proof of the lemma is complete. \square

Lemma 4.4.100. *Suppose v' is inert in \mathcal{F} , and v' is splits in \mathcal{M}' . Then, the assertion of (4.4.57) is true.*

Proof. From the formula of Lemma 3.6.2, it immediately follows from the fact that the equality

$$(4.4.101) \quad \text{ver} \left(\text{rec}_{\mathcal{M}',v'}(\beta') \mathbb{I}_{\mathcal{O}_{v'}}(\beta') \right) = \text{rec}_{\mathcal{M},v}(\beta') \mathbb{I}_{\mathcal{O}_v}(\beta')$$

holds. In particular, the congruence claimed in (4.4.57) holds. \square

Lemma 4.4.102. *Suppose v' is inert in \mathcal{F} , and v' is either inert or ramified in \mathcal{M}' . Then, the assertion of (4.4.57) is true.*

Proof. Keeping the notation from Lemma 4.4.80, we begin with the definition

$$(4.4.103) \quad A(v) = \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}} \text{rec}_v(x + 2^{-1}\boldsymbol{\theta}_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right)$$

given in Lemma 3.6.7, for any pair of sufficiently large integers j_0 and j_1 . Increasing j_0 and j_1 if necessary, we have the same definition

$$(4.4.104) \quad A'(v') = \psi_{v'} \left(\frac{-t'_{v'}}{2d_{\mathcal{F}'_{v'}}} \right) \text{Vol}(\mathfrak{l}'^{j_1}, dx) \sum_{x \in \mathfrak{l}'^{-j_0}/\mathfrak{l}'^{j_1}} \text{rec}_{v'}(x + 2^{-1}\boldsymbol{\theta}_{v'})^{-1} \psi_{v'} \left(\frac{-\beta'x}{d_{\mathcal{F}'_{v'}}} \right)$$

with the same pair of integers j_0 and j_1 that we used for (4.4.103). Note that

$$(4.4.105) \quad \psi_{v'} \left(\frac{-t'_{v'}}{2d_{\mathcal{F}'_{v'}}} \right) = \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right)$$

since $\psi_v = \psi_{v'} \circ \text{Tr}_{\mathcal{F}/\mathcal{F}'}$, $d_{\mathcal{F}_v} = pd_{\mathcal{F}'_{v'}}$, and $t'_{v'} = t_v$. Also note that $\boldsymbol{\theta}_v$ is the image of the $\boldsymbol{\theta}_{v'}$ under the diagonal embedding. Using these two facts, we obtain

$$(4.4.106) \quad \begin{aligned} & \text{ver}(A'(v')) \\ &= \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}'^{j_1}, dx') \sum_{x \in \mathfrak{l}'^{-j_0}/\mathfrak{l}'^{j_1}} \text{rec}_v(x + 2^{-1}\boldsymbol{\theta}_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right) \end{aligned}$$

where dx' denotes the Haar measure on $\mathcal{O}'_{v'}$ such that $\text{Vol}(\mathcal{O}'_{v'}, dx') = 1$. Since v' is inert in \mathcal{F} , we have

$$(4.4.107) \quad \text{Vol}(\mathfrak{l}'^{j_1}, dx')^p = \text{Vol}(\mathfrak{l}^{j_1}, dx)$$

and, in particular,

$$(4.4.108) \quad \text{Vol}(\mathfrak{l}'^{j_1}, dx') \equiv \text{Vol}(\mathfrak{l}^{j_1}, dx) \pmod{p}$$

holds. From the equation (4.4.106), we obtain

$$(4.4.109) \quad \begin{aligned} & \text{ver}(A'(v')) \\ & \equiv \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}} \text{rec}_v(x + 2^{-1}\theta_{v'})^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right) \end{aligned}$$

modulo T . Now we observe that

$$(4.4.110) \quad (\mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1})^G = \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}.$$

Indeed, one can easily show (4.4.110) by induction on $j_0 + j_1$. So (4.4.103) becomes, letting $W = \mathfrak{l}^{-j_0}/\mathfrak{l}^{j_1}$,

$$(4.4.111) \quad \begin{aligned} A(v) = & \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in W^G} \text{rec}_v(x + 2^{-1}\theta_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right) \\ & + \psi_v \left(\frac{-t_v}{2d_{\mathcal{F}_v}} \right) \text{Vol}(\mathfrak{l}^{j_1}, dx) \sum_{x \in W - W^G} \text{rec}_v(x + 2^{-1}\theta_v)^{-1} \psi_v \left(\frac{-\beta'x}{d_{\mathcal{F}_v}} \right). \end{aligned}$$

Applying Proposition 4.4.26 to the difference of (4.4.109) and (4.4.111), we conclude the lemma. \square

Combining the lemmas that we have proved, we conclude (4.4.57). The proof of Proposition 4.4.32 is complete. \square

We have completed the proof of Theorem 4.4.11.

4.5. Verifying the conditions (P'), (I) and (C)

In this subsection, we show that (P'), (I) and (C) hold under mild assumptions. For a discussion of these assumptions, see Remark 4.5.26.

Proposition 4.5.1. *Suppose that $\mu_{p^{r-1}} \subset \mathcal{M}'$, $\mathcal{M} = \mathcal{M}'(\mu_{p^r})$ for some $r \geq 2$. Further assume that $\mathcal{M}'/\mathbb{Q}(\mu_{p^{r-1}})$ is unramified at the unique prime of $\mathbb{Q}(\mu_{p^{r-1}})$ lying above p . Then (P') holds for \mathcal{M}/\mathcal{M}' . In particular, (P) holds when \mathcal{M}' is given by $\mathcal{M}_0(\mu_{p^{r-1}})$ for a p -ordinary CM field \mathcal{M}_0 which is unramified at p .*

Proof. Let φ be the Euler totient function. From conductor-discriminant formula, the discriminant of $\mathbb{Q}(\mu_{p^r})$ is given by

$$(4.5.2) \quad e_r := \sum_{j=1}^r (\varphi(p^j) - \varphi(p^{j-1}))p^j,$$

because, for each $j \geq 1$, there are $\varphi(p^j) - \varphi(p^{j-1})$ distinct Dirichlet characters of conductor p^j . Solving a recurrence relation, for every $r \geq 2$, we obtain the formula $\mathfrak{d}_{\mathbb{Q}(\mu_{p^r})/\mathbb{Q}(\mu_{p^{r-1}})} = p\mathcal{O}_{\mathbb{Q}(\mu_{p^r})}$ for the relative different.

Consider the diagram

$$(4.5.3) \quad \begin{array}{ccccc} & & \mathcal{M} & & \\ & & / \quad | \quad \backslash & & \\ \mathbb{Q}(\mu_{p^r}) & & \mathcal{M}' & & \mathcal{F} \\ | & / & \backslash & & | \\ \mathbb{Q}(\mu_{p^{r-1}}) & & & & \mathcal{F}' \end{array}$$

of field extensions. We first observe that $\mathcal{M}/\mathbb{Q}(\mu_{p^r})$ is unramified by our assumption. On the other hand, the extensions \mathcal{M}/\mathcal{F} and $\mathcal{M}'/\mathcal{F}'$ are always unramified. We give an argument for \mathcal{M}/\mathcal{F} , since the same argument works for $\mathcal{M}'/\mathcal{F}'$. Since \mathcal{M} is p -ordinary, the extension \mathcal{M}/\mathcal{F} is unramified at every place lying above p in particular. However, $\mathcal{F}(\mu_{p^r})$ is a non-trivial subextension of \mathcal{M}/\mathcal{F} since \mathcal{F} is totally positive. Since \mathcal{M}/\mathcal{F} is quadratic, \mathcal{M} is equal to $\mathcal{F}(\mu_{p^r})$. It follows from the properties of the cyclotomic fields that the extension \mathcal{M}/\mathcal{F} is unramified outside of p .

By the transitive property of relative different ideals, we have

$$(4.5.4) \quad \mathfrak{d}_{\mathcal{M}/\mathcal{M}'} = \mathfrak{d}_{\mathbb{Q}(\mu_{p^r})/\mathbb{Q}(\mu_{p^{r-1}})} \cdot \mathcal{R} = p\mathcal{R}$$

and

$$(4.5.5) \quad \mathfrak{d}_{\mathcal{M}/\mathcal{M}'} = \mathfrak{d}_{\mathcal{F}/\mathcal{F}'} \cdot \mathcal{R}.$$

From these to equalities, it follows that $\mathfrak{d}_{\mathcal{F}/\mathcal{F}'} = p\mathcal{O}$, which is (P'). □

We introduce some notation that are necessary to analyze the condition (C). Let us decompose

$$(4.5.6) \quad Cl_- = A \oplus B, \quad Cl'_- = A' \oplus B'$$

where A and A' are the maximal p -primary subgroups of Cl_- and Cl'_- respectively. Then the transfer map induces an isomorphism

$$(4.5.7) \quad J_p: B' \xrightarrow{\sim} B^G.$$

However, the map $J_p: A' \rightarrow A^G$ is not necessarily an isomorphism. The cokernel of $A' \rightarrow A^G$ is described by the ramification of \mathcal{F}/\mathcal{F}' .

Proposition 4.5.8. *Suppose that $\mathcal{M} = \mathcal{M}'(\mu_{p^{r+1}})$ for some positive integer r . Then we have*

$$(4.5.9) \quad \text{Coker}(A' \rightarrow A^G) \cong \prod_{v'} \mathbb{Z}/p\mathbb{Z}$$

where the product is taken over the set of places of \mathcal{F}' lying over p that are ramified in \mathcal{F}' . Moreover, each factor of $\mathbb{Z}/p\mathbb{Z}$ is generated by the ideal class

$$(4.5.10) \quad \mathfrak{p}\bar{\mathfrak{p}}^{-1}$$

where \mathfrak{p} is the prime ideal associated to the unique element of Σ_p whose restriction to \mathcal{F}' is v' .

Proof. See the Corollary 1.3.7 of [8]. □

Proposition 4.5.11. *Suppose the condition of Proposition 4.5.8 holds. Further assume that \mathcal{F}/\mathcal{F}' is ramified at every place of \mathcal{F}' lying above p . Then the condition (C) holds.*

Proof. As before, we fix representatives \mathcal{D} and \mathcal{D}' for Cl_- and Cl'_- respectively. In particular, we choose \mathcal{D} so that the diagonal embedding maps \mathcal{D}' into \mathcal{D} , and we choose \mathcal{D} to be a G -set with respect to the natural action of G on ideles. We further fix the decompositions

$$(4.5.12) \quad \mathcal{D} = \mathcal{A} \times \mathcal{B}$$

$$(4.5.13) \quad \mathcal{D}' = \mathcal{A}' \times \mathcal{B}'$$

where $\mathcal{A}, \mathcal{B}, \mathcal{A}'$, and \mathcal{B}' are representatives for A, B, A' , and B' respectively. We may also assume that \mathcal{A} and \mathcal{B} are G -sets so that the decomposition $\mathcal{D} = \mathcal{A} \times \mathcal{B}$ becomes a decomposition of a G -set, and that the natural diagonal embedding maps \mathcal{A}' and \mathcal{B}' into \mathcal{A} and \mathcal{B} respectively.

The map (4.5.7) being an isomorphism is now equivalent to the map

$$(4.5.14) \quad \mathcal{B}' \rightarrow \mathcal{B}^G$$

being a bijection. On the other hand, the conclusion of Proposition 4.5.8 in terms of the \mathcal{A} and \mathcal{A}' can be reformulated as the assertion that we can choose \mathcal{A} so that we have

$$(4.5.15) \quad \mathcal{A}^G = \prod_j \left(\mathcal{A}' \cdot \prod_w \left(\frac{\varpi_w}{\varpi_{\bar{w}}} \right)^{j_w} \right)$$

where j runs over the set

$$(4.5.16) \quad \{(j_w)_{w \in \Sigma_p} \mid j_w = 0, 1, 2, \dots, p-1\}$$

of Σ_p -tuples of integers. The bijection (4.5.15) given above implies that

$$(4.5.17) \quad \sum_{a \in \mathcal{A}^G} \text{rec}_{\mathcal{M}}(a) = \left(\prod_{w \in \Sigma_p} \left(\sum_{j_w=0}^{p-1} \frac{\text{rec}_w(\varpi_w)}{\text{rec}_{\bar{w}}(\varpi_{\bar{w}})} \right) \right) \sum_{a' \in \mathcal{A}'}$$

holds. Multiplying \mathcal{C} to both sides, we obtain

$$(4.5.18) \quad \mathcal{C} \cdot \sum_{a \in \mathcal{A}^G} \text{rec}_{\mathcal{M}}(a) = \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{A}'}$$

It is not very difficult to obtain (C) from this. Indeed,

$$(4.5.19)$$

$$(4.5.20) \quad \begin{aligned} \mathcal{C} \cdot \sum_{a \in \mathcal{D}^G} \text{rec}_{\mathcal{M}}(a) &= \left(\mathcal{C} \cdot \sum_{a \in \mathcal{A}^G} \text{rec}_{\mathcal{M}}(a) \right) \times \left(\sum_{b \in \mathcal{B}^G} \text{rec}_{\mathcal{M}}(b) \right) \\ &= \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{A}'} \text{rec}_{\mathcal{M}'}(a') \right) \times \text{ver} \left(\sum_{b' \in \mathcal{B}'} \text{rec}_{\mathcal{M}'}(b') \right) \end{aligned}$$

$$(4.5.21) \quad = \text{ver} \left(\mathcal{C}' \cdot \sum_{(a', b') \in \mathcal{A}' \times \mathcal{B}'} \text{rec}_{\mathcal{M}'}(a'b') \right)$$

$$(4.5.22) \quad = \text{ver} \left(\mathcal{C}' \cdot \sum_{a' \in \mathcal{D}'} \text{rec}_{\mathcal{M}'}(a') \right)$$

after routine calculations. The proof of the proposition is complete. □

Proposition 4.5.23. *Suppose that $\mathcal{M} = \mathcal{M}'(\mu_{p^r})$ with $r \geq 2$. Then (I) holds.*

Proof. Corollary 1.3.6 of [8] shows that \mathcal{D} can be chosen to be a G -set. In order to show that it is possible to choose a G -set of representatives for U/U_{alg} , look at the following exact sequence

$$(4.5.24) \quad U^G \rightarrow (U/U_{\text{alg}})^G \rightarrow H^1(G, U_{\text{alg}})$$

obtained from the long exact sequence of cohomology groups. The condition (I) requires $H^1(G, U_{\text{alg}}) = 0$. Note that U_{alg} consists of roots of unity of odd order in \mathcal{R} . It follows that U_{alg} is a cyclic group, and furthermore G acts faithfully if $\mathcal{M} = \mathcal{M}'(\mu_{p^r})$. Lemma 1.2.15 of [8] shows that $H^1(G, M) = 0$ when p is an odd prime and M is a cyclic faithful G -module. The proposition is proved. \square

Corollary 4.5.25. *Let \mathcal{K} be an imaginary quadratic field and let p be an odd prime that splits in \mathcal{K} . For an integer $r \geq 2$, put $\mathcal{M} = \mathcal{K}(\mu_{p^r})$ and $\mathcal{M}' = \mathcal{K}(\mu_{p^{r-1}})$. Then all of the conditions (P'), (I), and (C) hold.*

Proof. It is clear that the extension \mathcal{M}/\mathcal{M}' satisfies the assumptions of Proposition 4.5.1, Proposition 4.5.8, and Proposition 4.5.11. \square

Remark 4.5.26. We explain why the condition (P'), (I), and (C) are considered as mild. Suppose we have a tower of CM fields consisting of \mathcal{M}_r for each positive integer r , such that $\mathcal{M}_r \subset \mathcal{M}_{r+1}$ is a degree p extension for all r . Let \mathcal{M}_∞ be the union of the all \mathcal{M}_r , and suppose that \mathcal{M}_∞ is Galois over \mathcal{M}_1 with the Galois group $\text{Gal}(\mathcal{M}_\infty/\mathcal{M})$ being isomorphic to \mathbb{Z}_p . Let \mathcal{F}_r be the maximal totally real subfield of \mathcal{M}_r . If we let \mathcal{F}_∞ be the union of all \mathcal{F}_r , then \mathcal{F}_∞ is exactly the maximal totally real subfield of \mathcal{M}_∞ , and it is Galois over \mathcal{F}_1 with the Galois group $\text{Gal}(\mathcal{F}_\infty/\mathcal{F})$ being isomorphic to \mathbb{Z}_p . Under the validity of Leopoldt's conjecture for \mathcal{F}_1 , which we do not know in full generality yet, \mathcal{F}_∞ must be the cyclotomic \mathbb{Z}_p -extension of \mathcal{F}_1 . Then it is easy to see that the extension $\mathcal{M}_{r+1}/\mathcal{M}_r$ is generated by a p -power root of unity when r is sufficiently large. Note that the Leopoldt's conjecture is proved by Brumer for abelian totally real number fields. A different reason can be given by looking at the proof of Proposition 4.5.23. If G acts faithfully on U_{alg} , then \mathcal{M} is necessarily of the form $\mathcal{M} = \mathcal{M}'(\mu_{p^r})$ for some $r \geq 2$. Hence, the surjectivity of $U^G \rightarrow (U/U_{\text{alg}})^G$ implies that \mathcal{M} must be of the form $\mathcal{M}'(\mu_{p^r})$ for some $r \geq 2$.

5. Applications to the false Tate curve extensions

The current section has two aims. The first one is to explain the relation of our transfer congruence to the existence of non-commutative p -adic L -functions, and the second is to study the explicit congruence between L -values which is implied by our work.

Roughly speaking, in order to prove the non-commutative Iwasawa main conjecture for a given motive and a p -adic Lie extension, it is sufficient to prove various commutative Iwasawa main conjecture for intermediate extensions and prove certain non-commutative Kummer congruences between

these commutative p -adic L -functions. This strategy was successfully applied for the Tate motives over totally real fields in the works of Kakde and Ritter-Weiss. We want to explain what are the relevant intermediate extensions for the false Tate curve extensions, and how to deduce the necessary non-commutative Kummer congruence between them from our transfer congruence. Unfortunately, we do not know at present all of the commutative main conjectures that are necessary for the non-commutative one, in contrast to the situation of the Tate motives over totally real fields for which the commutative main conjecture is known in a wide generality.

While our speculations on the non-commutative Iwasawa main conjecture will rely on other unknown conjectures, our work unconditionally imply the congruence between special values of L -functions. We will study the explicit form of such congruences over the false Tate curve extension in Subsection 5.3.

5.1. Algebraic preliminaries

In this subsection, we start with a compact p -adic Lie group G . We always assume that G has a closed normal subgroup H such that $\Gamma = G/H$ is isomorphic to \mathbb{Z}_p , and explain in general and vague terms what are the non-commutative congruences for it. In the case when H is abelian, which is our main concern of this paper, will state precisely the description of K_1 -groups of Iwasawa algebra $\Lambda(G)$ in terms of the transfer congruence. For more details and generalizations, see [4]. Following [3], we define

$$(5.1.1) \quad S = \{\lambda \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)\lambda \text{ is finitely generated as a left } \Lambda(H)\text{-module.}\}.$$

As shown in Theorem 2.4 of [3], $S \subset \Lambda(G)$ is an Ore set, and we denote the localization of $\Lambda(G)$ at S by $\Lambda(G)_S$. The completion of $\Lambda(G)_S$ with respect to the p -adic topology is denoted by $\widehat{\Lambda(G)_S}$. Strictly speaking, S depends on G and H , but we omit G and H from the notation. In practice, G is given as a Galois group, and Γ corresponds to the cyclotomic \mathbb{Z}_p -extension.

For any topological ring R , we define $K_1(R)$ by

$$(5.1.2) \quad K_1(R) = \mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)]^-$$

where $\mathrm{GL}(R)$ is the inductive limit $\lim_{\rightarrow n} \mathrm{GL}_n(R)$ with respect to the inclusions $[a] \mapsto \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, and $[\mathrm{GL}(R), \mathrm{GL}(R)]^-$ is the closure of the commutator subgroup $[\mathrm{GL}(R), \mathrm{GL}(R)]$ of $\mathrm{GL}(R)$.

When G is abelian, $\Lambda(G)$ is a semi-local ring and $K_1(\Lambda(G)) = \Lambda(G)^\times$ and $K_1(\Lambda(G)_S) = \Lambda(G)_S^\times$. One successful approach to understanding $K_1(\Lambda(G))$ for a non-commutative G is to describe it in terms of abelian subquotients of G . To be precise, one defines a family of abelian subquotients $\{G_i | i \in I\}$ for some index set I and a family of maps $\theta^i: K_1(\Lambda(G)) \rightarrow K_1(\Lambda(G_i))$, in the hope that studying the map

$$(5.1.3) \quad \theta = \prod_{i \in I} \theta^i: K_1(\Lambda(G)) \rightarrow \prod_{i \in I} K_1(\Lambda(G_i)) = \prod_{i \in I} \Lambda(G_i)^\times$$

shed some light on the structure of $K_1(\Lambda(G))$. One tries to show θ is injective, or at least describe its kernel, and also describe the image. The relations that an I -tuple $(\mathcal{L}_i)_i$ needs to satisfy in order to be in the image of θ is called non-commutative congruences. The transfer congruence proved in Theorem 4.4.11 is one example of such non-commutative congruences. When H is pro- p and abelian, then this is in fact sufficient. Indeed, for every integer $r \geq 0$, consider the unique closed subgroup Γ_r of Γ with $[\Gamma_r : \Gamma] = p^r$. Let G_r be the inverse image of Γ_r in G and let G_r^{ab} be the abelianization of G_r . Since G_r is of finite index in G , we have a norm map $\text{Nr}_r = K_1(\Lambda(G)) \rightarrow K_1(\Lambda(G_r))$. Similarly, we have the norm map $\text{Nr}_{r',r} = K_1(\Lambda(G_{r'})) \rightarrow K_1(\Lambda(G_r))$ whenever $r' \leq r$. Also we have a map $K_1(\Lambda(G_{r'})) \rightarrow K_1(\Lambda(G_r^{\text{ab}}))$ induced by the natural projection $G_{r'} \rightarrow G_r^{\text{ab}}$. Define θ^r

$$(5.1.4) \quad \theta^r: K_1(\Lambda(G)) \rightarrow K_1(\Lambda(G_r)) \rightarrow K_1(\Lambda(G_r^{\text{ab}}))$$

to be the composition of the two maps. Similarly, we define the maps

$$(5.1.5) \quad \theta_S^r: K_1(\Lambda(G)_S) \rightarrow K_1(\Lambda(G_r)_S) \rightarrow K_1(\Lambda(G_r^{\text{ab}})_S)$$

$$(5.1.6) \quad \widehat{\theta}_S^r: K_1(\widehat{\Lambda(G)}_S) \rightarrow K_1(\widehat{\Lambda(G_r)}_S) \rightarrow K_1(\widehat{\Lambda(G_r^{\text{ab}})}_S).$$

For each positive integer r , let $\text{ver}_r: \Lambda(G_{r-1}^{\text{ab}}) \rightarrow \Lambda(G_r^{\text{ab}})$ be the map induced by the transfer map $G_{r-1}^{\text{ab}} \rightarrow G_r^{\text{ab}}$ on the group elements. We have a trace map $\Lambda(G_r^{\text{ab}}) \rightarrow \Lambda(G_{r-1}^{\text{ab}})$ with respect to the action of G_r/G_{r-1} , and let T_r be the image. Then T_r is an ideal in $\Lambda(G_r^{\text{ab}})$ and we write $\widehat{T}_{r,S} = T_r \Lambda(\widehat{G_r^{\text{ab}}})_S$.

Theorem 5.1.7. *Assume that H is pro- p and abelian. The maps*

$$(5.1.8) \quad \theta: K_1(\Lambda(G)) \rightarrow \prod_{r \geq 0} \Lambda(G_r^{\text{ab}})^\times$$

$$(5.1.9) \quad \widehat{\theta}_S: K_1(\widehat{\Lambda(G)}_S) \rightarrow \prod_{r \geq 0} \Lambda(G_r^{\text{ab}})_S^\times$$

are injective. The image of θ consists of (x_r) satisfying

- (MS1) $\text{Nr}_{j,i}(x_j) = x_i$ for all $0 \leq i \leq j$.
- (MS2) x_i is fixed under the action of Γ for all i .
- (MS3) $x_i \equiv \text{ver}_i(x_{i-1})$ modulo T_i for all $i \geq 1$.

The image of $\widehat{\theta}_S$ is described by the first two conditions and the congruence modulo $\widehat{T}_{i,S}$.

Remark 5.1.10. The conditions (MS1) and (MS2) are minimal compatibility conditions. For a general G , the transfer congruence (MS3) is not sufficient, and we need to consider different kinds of congruences as described in [14, 18].

Remark 5.1.11. It is sometimes necessary to use an extension of \mathbb{Z}_p as the coefficient for the Iwasawa algebra. When the coefficient ring is unramified, it is proved in [14] that the same result holds after twisting ver_i by the Frobenius on the coefficient ring.

5.2. Specialization to the false Tate curve extensions

In this subsection, we will specialize to the false Tate curve extension of imaginary quadratic fields, and discuss the non-commutative p -adic L -function along it. More precisely, we fix an imaginary quadratic field

$$(5.2.1) \quad \mathcal{M}_0 = \mathbb{Q}(\sqrt{-D_0})$$

for a positive square-free integer D_0 , and an odd prime p which splits in \mathcal{M}_0 . Fix an integer m which is a p -th power free and $|m|_{\mathbb{R}} > 1$. Define

$$(5.2.2) \quad \mathcal{M}_r = \mathcal{M}_0(\mu_{p^r})$$

for each non-negative integer r , and define

$$(5.2.3) \quad \mathcal{K}_\infty = \bigcup_{r=0}^\infty \mathcal{M}_r(m^{\frac{1}{p^r}})$$

to be the two dimensional p -adic Lie extension of \mathcal{M}_0 . It easily follows from the Kummer theory that the Galois group $\text{Gal}(\mathcal{K}_\infty/\mathcal{M}_0)$ is isomorphic to the semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, where \mathbb{Z}_p^\times acts on \mathbb{Z}_p by the multiplication.

We need a preliminary reduction step before we apply the result of the previous subsection. Consider the open subgroup $\mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)$ of index $p-1$ in $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. Consider the map

$$(5.2.4) \quad \phi: K_1(\Lambda(\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times)) \longrightarrow K_1(\Lambda(\mathbb{Z}_p^\times)) \times K_1(\Lambda(\mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)))$$

$$(5.2.5) \quad \lambda \longmapsto (\lambda_0, \lambda_1)$$

where λ_0 is the image under map induces by the natural projection $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_p^\times$, and λ_1 is the image of the norm map. Since $1+p\mathbb{Z}_p$ is an open subgroup of \mathbb{Z}_p^\times , we have a norm map

$$(5.2.6) \quad \phi_0: K_1(\Lambda(\mathbb{Z}_p^\times)) \longrightarrow K_1(\Lambda(1+p\mathbb{Z}_p))$$

and we have a map

$$(5.2.7) \quad \phi_1: K_1(\Lambda(\mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p))) \longrightarrow K_1(\Lambda(1+p\mathbb{Z}_p))$$

induce by the projection map.

Proposition 5.2.8. *A pair*

$$(5.2.9) \quad (\lambda_0, \lambda_1) \in K_1(\Lambda(\mathbb{Z}_p^\times)) \times K_1(\Lambda(\mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)))$$

lies in the image of ϕ if and only if $\phi_0(\lambda_0) = \phi_1(\lambda_1)$.

Proof. We omit the proof. □

The above proposition is the reason why the non-commutative congruences for the group $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ only involve the subquotients of $\mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)$. Our strategy to prove existence of a p -adic L -function for $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ is to construct λ_0 and λ_1 satisfying the above compatibility condition. In order to construct λ_1 , we apply Theorem 5.1.7 to the group $G = \mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)$. The open subgroups G_r correspond to the groups $\text{Gal}(\mathcal{K}_\infty/\mathcal{M}_r)$, whose abelianizations are given by

$$(5.2.10) \quad G_r^{\text{ab}} = \text{Gal}(\mathcal{M}_r(\mu_{p^\infty}, m^{\frac{1}{p^r}})/\mathcal{M}_r).$$

Fix a CM type Σ_0 for \mathcal{M}_0 , which is p -ordinary, then for each $r \geq 1$, \mathcal{M}_r has a p -ordinary CM type Σ_r induced from \mathcal{M}_0 . For simplicity, let $\mathcal{M} = \mathcal{M}_1$, and let Σ be the CM type of \mathcal{M} . suppose we have an algebraic Hecke character

$$(5.2.11) \quad \chi: \mathbb{A}_{\mathcal{M}}^\times \longrightarrow \mathbb{C}^\times$$

whose infinity type is $k\Sigma$ with a positive integer k , and unramified at all places dividing p .

Remark 5.2.12. For example, such χ can be obtained from the Hecke character χ_0 of \mathcal{M}_0 whose infinity type $1\Sigma_0$, and $\chi_0|_{\mathbb{A}_{\mathbb{Q}}^\times}$ is the product of the quadratic character of \mathcal{M}_0/\mathbb{Q} and the adelic norm on $\mathbb{A}_{\mathbb{Q}}^\times$. We may take χ to be the character

$$(5.2.13) \quad \chi_0^k \circ \text{Norm}: \mathbb{A}_{\mathcal{M}}^\times \rightarrow \mathbb{C}^\times$$

whose infinity type is $k\Sigma$. We will come back to this situation in the next subsection.

By composing χ with the norm map $\mathbb{A}_{\mathcal{M}_r}^\times \rightarrow \mathbb{A}_{\mathcal{M}}^\times$, we obtain

$$(5.2.14) \quad \chi_r: \mathbb{A}_{\mathcal{M}_r}^\times \rightarrow \mathbb{C}^\times$$

for each $r \geq 1$.

Let \mathfrak{C} be the conductor of χ , which is an ideal of \mathcal{M} relatively prime to p . Fix a polarization $\delta \in \mathcal{M}$, with polarization ideal \mathfrak{c} . Now we are in the situation of the main results of our paper. In particular, for each $r \geq 1$, we obtain the p -adic L -function

$$(5.2.15) \quad \mathcal{L}_r \in \Lambda(Z_r)$$

of Definition 3.8.2, where Z_r is the Galois group

$$(5.2.16) \quad \lim_{\infty \leftarrow n} \text{Gal}(\mathcal{M}_r(p^n \mathfrak{C})/\mathcal{M}_r)$$

introduced in (2.3.7). Let $\mathcal{L}_r(\chi_r)$ be the branch of \mathcal{L}_r along G_r with respect to χ_r . That is to say, $\mathcal{L}_r(\chi_r)$ is the unique element of $\Lambda(G_r^{\text{ab}})$ such that

$$(5.2.17) \quad \int_{G_r^{\text{ab}}} \phi d\mathcal{L}_r(\chi) = \int_{Z_r} \tilde{\phi} \tilde{\chi} d\mathcal{L}$$

for every continuous function $\phi: G_r^{\text{ab}} \rightarrow \mathbb{Z}_p$, where $\tilde{\phi}$ denotes the pull-back of ϕ along the natural projection map $Z_r \rightarrow G_r^{\text{ab}}$.

Remark 5.2.18. When χ arises from an imaginary quadratic field in the manner explained in Remark 5.2.12, then we let $\mathcal{L}_0(\chi_0)$ to be the branch of \mathcal{L}_0 along $G^{\text{ab}} = \text{Gal}(\mathcal{M}_\infty/\mathcal{M}_0)$ with respect to χ_0 . If we put $\lambda_0 = \mathcal{L}_0(\chi_0)$ and $\lambda_1 = \mathcal{L}_1(\chi_1)$, then λ_0 and λ_1 satisfies the compatibility condition in Proposition 5.2.8, in the sense that if we let

$$(5.2.19) \quad \phi_0: \Lambda(\mathbb{Z}_p^\times) \longrightarrow \Lambda(1 + p\mathbb{Z}_p)$$

be the norm map and let

$$(5.2.20) \quad \phi_1: \Lambda(\mathbb{Z}_p/p\mathbb{Z}_p \times (1 + p\mathbb{Z}_p)) \rightarrow \Lambda(1 + p\mathbb{Z}_p)$$

be the natural projection, then we have $\phi_0(u \cdot \lambda_0) = \phi_1(\lambda_1)$ for a p -adic unit $u \in \mathbb{Z}_p^\times$.

As a consequence of Theorem 4.4.11, we establish the transfer congruence between $\mathcal{L}_r(\chi_r)$ for $r \geq 1$. The factor u was computed in the proof of Theorem 7.2 in [17], where we worked with $p\mathcal{L}_1$ instead of \mathcal{L}_1 .

Theorem 5.2.21. *We have*

$$(5.2.22) \quad \text{ver}_{r-1}(\mathcal{L}_{r-1}(\chi)) = \mathcal{L}_r(\chi) \pmod{T_r}$$

for each $r \geq 2$.

Proof. The key fact is the commutativity of the diagram

$$(5.2.23) \quad \begin{array}{ccc} Z_{r-1} & \longrightarrow & G_{r-1}^{\text{ab}} \\ \downarrow & & \downarrow \\ Z_r & \longrightarrow & G_r^{\text{ab}} \end{array}$$

where the two vertical maps are transfer maps, and the horizontal maps are the natural projections. Having observed this, it is easy to see the congruence from the characterization (5.2.17) of $\mathcal{L}_r(\chi_r)$ in terms of \mathcal{L}_r , and the transfer congruence between \mathcal{L}_r . \square

Although Theorem 5.2.21 verifies (MS3) of Theorem 5.1.7, we do not know yet whether

$$(5.2.24) \quad \mathcal{L}_r(\chi_r) \in \Lambda(G_r^{\text{ab}})_S^\times$$

holds for all $r \geq 1$. We first observe that the conditions (5.2.24) for $r \geq 0$ are rather strongly dependent to each other.

Proposition 5.2.25. *Suppose that (5.2.24) holds for $r = 0$. Then it holds for all $r \geq 0$.*

Proof. We proceed by induction. Since G_r^{ab} is one dimensional for every

$r \geq 0$, an element $\lambda \in \Lambda(G_r^{\text{ab}})$ belongs to $\Lambda(G_r^{\text{ab}})_S^\times$ if and only if λ is not a zero divisor in $\Lambda(G_r^{\text{ab}})/p\Lambda(G_r^{\text{ab}})$.

From $r = 0$ to $r = 1$, we use the observation made in Remark 5.2.18, that $\mathcal{L}_0(\chi_0)$ and $\mathcal{L}_1(\chi_1)$ satisfies a compatibility condition with respect to ϕ_0 and ϕ_1 . Since ϕ_0 maps a non-zero divisor to a non-zero divisor, and ϕ_1 maps a zero divisor to a zero divisor, we have the induction step from $r = 0$ to $r = 1$. The remaining induction steps can be verified similarly by comparing $\mathcal{L}_r(\chi_r)$ and $\mathcal{L}_{r-1}(\chi_{r-1})$ using relevant norm and projection maps. \square

Unfortunately, we do not know how to theoretically prove (5.2.24) for $r = 0$, and we assume it only for the rest of the current subsection. If we further assume that $\mathcal{L}_r(\chi_r)$ satisfies the commutative Iwasawa main conjecture for every r , then it will follow that there exists a non-commutative p -adic L -function in $K_1(\Lambda(G)_S)$, which will satisfy the non-commutative Iwasawa main conjecture. Without the assumption on the commutative main conjectures, we need to work with the completion of localized Iwasawa algebras.

Corollary 5.2.26. *Suppose (5.2.24). Then there exists an element*

$$(5.2.27) \quad \mathcal{L}(G) \in K_1(\widehat{\Lambda(G)}_S)$$

which satisfies

$$(5.2.28) \quad \widehat{\theta}_S^r(\mathcal{L}(G)) = \mathcal{L}_r(\chi_r)$$

for every $r \geq 0$, where $\widehat{\theta}_S^r$ was defined in (5.1.6).

Proof. The existence of certain element $\mathcal{L}(G)$ in $K_1(\widehat{\Lambda(G)}_S)$ follows from Theorem 5.1.7, combined with Proposition 5.2.8. We need to verify then the conditions of Theorem 5.1.7 and Proposition 5.2.8 are satisfied the family $\widehat{\theta}_S^r(\mathcal{L}(G))$. The condition (MS3) is satisfied by Theorem 4.4.11, and the other conditions, including one for Proposition 5.2.8, follow from the interpolation formula of \mathcal{L}_r . \square

The discussion on the interpolation property of $\mathcal{L}(G)$ is postponed to Subsection 5.4, since we first need to classify the Artin representations of G , which we will treat in the next subsection.

5.3. Congruence between special values of L -functions

In this subsection, we want to discuss the concrete congruences between special values of L -functions, which can be deduced from the work of the current

paper. We keep the notation from the previous subsection. In particular, we will focus on the family of characters

$$(5.3.1) \quad \chi_r: \mathbb{A}_{\mathcal{M}_r}^\times \longrightarrow \mathbb{C}^\times$$

of infinity type $k\Sigma_r$ for a fixed positive integer k , and all $r \geq 1$, such that χ_{r+1} is the composition of χ_r with the norm map $\mathbb{A}_{\mathcal{M}_{r+1}}^\times \rightarrow \mathbb{A}_{\mathcal{M}_r}^\times$. For example, one may start with a Hecke character χ_0 of \mathcal{M}_0 whose infinity type of Σ_0 , as described in Remark 5.2.12.

We will consider two families of congruences. A special case of the first family of congruences was studied in [17], but the proof was conditional. Here we have unconditional result which holds in general. The second family arises from main result in Theorem 4.4.11, which illustrates the non-commutative nature of the transfer congruence. Indeed, they are congruence between special values of L -functions of *different* degrees, while the family of L -functions considered in the commutative Iwasawa theory have the same degree.

Let us first describe the irreducible representations of G with finite image on a $\overline{\mathbb{Q}}_p$ -vector space. The classification we give here can be verified easily from the character theory of finite groups, but we simply state the results. For each r , there is an irreducible representation

$$(5.3.2) \quad \rho_r: G \rightarrow \mathrm{GL}_{\varphi(p^r)}(\mathbb{Q}_p)$$

of dimension $\varphi(p^r)$, where φ is the Euler totient function. It is the representation induced from a character η_r of G_r which we define now.

Definition 5.3.3. Define a character η_r of G_r to be a lift of any character

$$(5.3.4) \quad \mathrm{Gal}(\mathcal{M}_r(m^{\frac{1}{p^r}})/\mathcal{M}_r) \rightarrow \overline{\mathbb{Q}}_p^\times$$

whose order is exactly p^r .

The representation ρ_r is independent of the choice of η_r , and it can be in fact defined over \mathbb{Z} . All the other irreducible representations of G are constructed by twisting ρ_r . Precisely speaking, for an irreducible representation ρ of G on a finite dimensional $\overline{\mathbb{Q}}_p$ -vector space, there exists a one dimensional character ξ of G such that ρ is of the form $\rho_r \otimes \xi$ for some r . On the other hand, if we have two characters ξ_1 and ξ_2 of G , then $\rho_r \otimes \xi_1$ is isomorphic to $\rho_r \otimes \xi_2$ if and only if the restrictions of ξ_1 and ξ_2 to G_r are the same.

Apart from the irreducible ones, we will consider

$$(5.3.5) \quad \sigma_r: G \rightarrow \mathrm{GL}_{\varphi(p^r)}(\mathbb{Q}_p)$$

which is the representation induced from the trivial character of G_r . Of course, σ_r can be defined over \mathbb{Z} , and it decomposes into the sum of $\varphi(p^r)$ one dimensional representations over $\overline{\mathbb{Q}}_p$.

Both ρ_r and σ_r are defined over \mathbb{Z} , and it makes sense to ask if they are congruent modulo p . Indeed, one can easily see that they are congruent modulo p , so we expect a congruence between canonically normalized special values of the corresponding twists of an L -function. In other words, if we let

$$(5.3.6) \quad L(\chi_0, \rho, s)$$

be the complex L -function of χ_0 twisted by ρ , then the special values of

$$(5.3.7) \quad L(\chi_0, \sigma_r, s), \text{ and } L(\chi_0, \rho_r, s)$$

at critical points are expected to be congruent modulo p , after normalizing them in a canonical way. From Artin's formalism, we have

$$(5.3.8) \quad L(\chi_0, \rho_r) = L(\chi_r, \eta_r, s)$$

and

$$(5.3.9) \quad L(\chi_0, \sigma_r) = L(\chi_r, s)$$

so we use our p -adic L -functions $\mathcal{L}_r(\chi_r)$ to deduce the desired congruences.

Definition 5.3.10. Define

$$(5.3.11) \quad \mathcal{L}(\chi_0, \rho_r, n) = \int_{Z_r} \eta_r \widehat{\kappa}^n d\mathcal{L}_r(\chi_0)$$

and

$$(5.3.12) \quad \mathcal{L}(\chi_0, \sigma_r, n) = \int_{Z_r} \widehat{\kappa}^n d\mathcal{L}_r(\chi_0)$$

where κ is the norm character defined in (3.7.10).

For $n = 1, 2, \dots, k - 1$, we see from the interpolation formula (3.8.10) that $\mathcal{L}(\chi_0, \rho_r, n)$ and $\mathcal{L}(\chi_0, \sigma_r, n)$ are the normalized special values of $L(\chi_0, \rho_r, n)$ and $L(\chi_0, \sigma_0, n)$, respectively.

Theorem 5.3.13. *With the notation as above, we have*

$$(5.3.14) \quad \mathcal{L}(\chi_0, \rho_r, n) \equiv \mathcal{L}(\chi_0, \sigma_r, n) \pmod{p}$$

for each $n = 1, 2, \dots, k - 1$.

Proof. Observe first that $\mathcal{L}(\chi_0, \rho_r, n)$ belongs to \mathbb{Z}_p , although the character η_r takes values in $\mathbb{Z}_p(\mu_{p^r})$. It is essentially because of the fact that if η_r is of the form $g \circ \eta'_r$ for some $g \in \text{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$ and a $\overline{\mathbb{Q}}_p$ -valued character η'_r of G_r , the ρ_r is the induced representation of either η_r or η'_r . Therefore, from the interpolation formula, we see that

$$(5.3.15) \quad \int_{Z_r} \eta_r \widehat{\kappa}^n d\mathcal{L}_r(\chi_0) = \int_{Z_r} \eta'_r \widehat{\kappa}^n d\mathcal{L}_r(\chi_0)$$

for such η_r and η'_r . Since $\widehat{\kappa}$ and $\widehat{\chi}_0$ take values in \mathbb{Z}_p^\times , and \mathcal{L}_r is defined over \mathbb{Z}_p , it follows that $\mathcal{L}(\chi_0, \rho_r, n)$ is contained in \mathbb{Z}_p . Since η_r is congruent to the trivial character modulo the maximal ideal of $\mathbb{Z}_p(\mu_{p^r})$, the congruence (5.3.14) follows. \square

Remark 5.3.16. For any modular form with weight at least 2, the congruence similar to (5.3.14) is expected to hold. Indeed, it was verified numerically in [6] for an elliptic curve with $(p, r) = (5, 1)$, and in [2] for modular forms of weight at least 4 with $(p, r) = (3, 1)$. Here we provide a theoretical proof when the relevant modular form is of CM type. The interpolation formula of Katz p -adic L -function given here and the interpolation formula of [2] are compared in [17] for $r = 1$ case, but the comparison for $r \geq 1$ is similar. The problem with our previous approach in [17] was that the interpolation formula of Katz p -adic L -function was not the same as the prediction from the non-commutative Iwasawa theory. It is why the author had to introduce Hypothesis 4 in [17]. On the other hand, the numerical values obtained in [2] and [6] suggest that the prediction by the non-commutative Iwasawa theory is the correct one. By dividing out U_{alg} when we define the p -adic L -function in Definition 3.8.2, we obtain the p -adic L -function that is compatible with the prediction of the non-commutative Iwasawa theory.

Now we discuss the second family of congruences which arises from the transfer congruence of Theorem 4.4.11. In order to do so, we first study the effect of composing the transfer homomorphism to the character η_r .

Lemma 5.3.17. *Let $r \geq 2$, and let η_r be any character as in Definition 5.3.3. Let η'_{r-1} be the composition of $\eta_r \circ \text{ver}_r$, where ver_r is the transfer homomorphism*

$$(5.3.18) \quad \text{ver}_r : G_{r-1}^{\text{ab}} \longrightarrow G_r^{\text{ab}}.$$

Then η_{r-1} is of order exactly p^{r-1} , and satisfies the condition of Definition 5.3.3. Namely, η'_{r-1} is a lift of a character

$$(5.3.19) \quad \text{Gal}(\mathcal{M}_{r-1}(m^{\frac{1}{p^{r-1}}})/\mathcal{M}_{r-1}) \longrightarrow \overline{\mathbb{Q}}_p^\times$$

whose order is exactly p^{r-1} .

Proof. It can be verified easily using the power residue symbol. Let \mathfrak{q} be any prime of \mathcal{M}_r which is prime to $p \cdot m$. Let q be the cardinality of the residue field of \mathcal{M}_r at \mathfrak{q} . Consider the p^r -th power residue symbol

$$(5.3.20) \quad \left(\frac{m}{\mathfrak{q}} \right)_{p^r} \in \mu_{p^r} \subset \mathcal{M}_r$$

which is characterized by the property that

$$(5.3.21) \quad \left(\frac{a}{\mathfrak{q}} \right)_{p^r} \equiv a^{\frac{q-1}{p^r}} \pmod{\mathfrak{q}}$$

for every $a \in \mathcal{O}_{\mathcal{M}_r}$ relatively prime to p and the residue characteristic of \mathfrak{q} . If we interpret the power residue symbol as a character of Z_r using ideal theoretic Artin reciprocity map, then it is of order exactly p^r , giving rise to η_r . Now a proof of the lemma is reduced to the assertion that

$$(5.3.22) \quad \prod_{\mathfrak{q}|\mathfrak{l}} \left(\frac{m}{\mathfrak{q}} \right)_{p^r} = \left(\frac{m}{\mathfrak{l}} \right)_{p^{r-1}}$$

holds for each prime \mathfrak{l} of \mathcal{M}_{r-1} prime to $p \cdot m$.

Let l be the cardinality of the residue field of \mathcal{M}_{r-1} at \mathfrak{l} . We prove the above equality by dividing it into two cases. If \mathfrak{l} splits in \mathcal{M}_r , then the residue field of any \mathfrak{q} dividing \mathfrak{l} will be the same as l . Therefore, the left hand side of (5.3.22) is equal to

$$(5.3.23) \quad \prod_{\mathfrak{q}|\mathfrak{l}} m^{\frac{l-1}{p^r}} = m^{\frac{l-1}{p^{r-1}}}$$

modulo \mathfrak{q} , so we obtain (5.3.22). If \mathfrak{l} is inert in \mathcal{M}_r , then $q = l^p$, and the left hand side of (5.3.22) is

$$(5.3.24) \quad m^{\frac{l^p-1}{p^r}} = \left(m^{\frac{l-1}{p^{r-1}}} \right)^b$$

where b is given by

$$(5.3.25) \quad b = \frac{1 + l + \cdots + l^{p-1}}{p}.$$

We claim that b is congruent to 1 modulo p^{r-1} , which will imply (5.3.22). The key fact is that l is congruent to 1 modulo p^{r-1} , because the residue

field at \mathfrak{l} contains all p^{r-1} -th roots of unity. Once we observe this, we can write $l = 1 + ap^{r-1}$ with an integer a . Applying the binomial expansion to each powers of l and rearranging the sum, we obtain the expression

$$(5.3.26) \quad 1 + l + \dots + l^{p-1} = p + (1 + 2 + \dots + p - 1) \cdot ap^{r-1} + a' \cdot p^{2r-2}$$

for some integer a' . Since $r \geq 2$, we have $2r - 3 \geq r - 1$, and since p is odd p divides $1 + 2 + \dots + p - 1$. Therefore b is congruent to 1 modulo p^{r-1} . \square

As a consequence of the previous lemma, we establish the second family of congruences.

Theorem 5.3.27. *For each $r \geq 2$, we have the congruence*

$$(5.3.28) \quad \mathcal{L}(\chi_0, \rho_r, n) \equiv \mathcal{L}(\chi_0, \rho_{r-1}, n) \pmod{p}$$

for any integer n .

Proof. Since

$$(5.3.29) \quad \mathcal{L}(\chi_0, \rho_r, n) \equiv \mathcal{L}(\chi_0, \rho_r, n') \pmod{p}.$$

for any pair of integers n and n' , the congruence is insensitive to a choice of n . So we lose no generality by taking $n = 0$. The assertion of the theorem will follow from the observation that for any $\lambda \in T_r$, where T_r is the trace ideal of $\Lambda(G_r^{\text{ab}})$, we have

$$(5.3.30) \quad \int_{G_r^{\text{ab}}} \eta_r d\lambda \in p\mathbb{Z}_p$$

provided that we know a priori the fact that the value on the left hand side belongs to \mathbb{Z}_p . If we take

$$(5.3.31) \quad \lambda = \mathcal{L}_r(\chi_r) - \text{ver}_r(\mathcal{L}_{r-1}(\chi_{r-1}))$$

then the assertion of the theorem will follow from combining (5.3.30) with Lemma 5.3.17.

We now prove (5.3.30). Observe first that for any $g \in \text{Gal}(\mathcal{M}_r/\mathcal{M}_{r-1})$, g acts on both G_r^{ab} and the values of the character η_r , and the action is equivariant in the following sense. For any such g and $z \in G_r^{\text{ab}}$, we have

$$(5.3.32) \quad \eta_r(g \cdot z) = \eta_r(z)^g.$$

From the characterization of T_r given in Proposition 4.4.26, it follows that (5.3.30) holds. \square

Remark 5.3.33. We note that the congruence (5.3.28) shows a genuinely non-abelian characteristic, being a congruence between L -functions of different degree.

Remark 5.3.34. The author tried to compute the L -values to numerically verify the congruence (5.3.28), without any success. If we allow k to be at least 3, then the Euler product converges for at least one critical point, so one is able to obtain a series converging to $L(\chi_0, \rho_r, k)$ from Euler product. However, for $r = 2$ case, which is the smallest among the relevant, the conductor of the L -function will be at least $N \cdot p^{p(2p-3)}$, where N is the conductor of χ_0 . The conductors at primes dividing m , and the conductor arising from ramification in $\mathbb{Q}_p(m^{1/p^r})/\mathbb{Q}_p$ need to be multiplied to this to obtain the actual conductor, which is bound to be very large. If we look at the table of CM elliptic curves, the smallest one for which 3 is good ordinary is the unique CM elliptic curve of conductor 121. It follows that the conductor of $L(\chi_0, \rho_2, s)$ is at least $121 \cdot 3^9$, which is greater than two million. It seems to the author that the numerical verification of (5.3.28) for modular forms, either of CM type or not, is a challenge from the computational point of view.

5.4. The interpolation formula for $\mathcal{L}(G)$

In this subsection, we discuss the interpolation formula for $\mathcal{L}(G)$ and compare it with the prediction of non-commutative Iwasawa theory. First we recall the meaning of the value of an element $\Theta \in K_1(\Lambda(G)_S)$ at a representation of G on a finite dimensional \mathbb{Q}_p -vector space. Throughout, ρ will denote a representation of G of the form

$$(5.4.1) \quad \rho = \rho_r \otimes \xi$$

where the ρ_r is the irreducible representation introduced in (5.3.2), and ξ is a finite order character of G^{ab} . Recall that κ was defined to be the adelic norm character, whose p -adic avatar was denoted by $\widehat{\kappa}$. In the paragraphs following Lemma 3.3 of [3], it is defined how to define, for each integer n , the value of Θ at the representation $\rho\widehat{\kappa}^n$. We denote the value as

$$(5.4.2) \quad \int_G \rho\widehat{\kappa}^n d\Theta$$

which is meant to give hints to the interpretation of Θ as a measure in the commutative case.

Remark 5.4.3. In the literature, one often writes a representation of G as $\rho\phi^n$, where ϕ is the restriction of $\widehat{\kappa}$ to the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} . In

fact, as one can see easily from our description of irreducible representation of G given after Definition 5.3.3, these make no difference when $r \geq 1$.

As one can expect from our construction of $\mathcal{L}(G)$, the interpolation formula of $\mathcal{L}(G)$ is determined by the interpolation formula of \mathcal{L}_r given in (3.8.10), and our intention is to provide an interpolation formula in terms of intrinsic invariants of ρ and n , which do not involve the intermediate fields. Unfortunately, we will have to leave some factors involve the intermediate fields, and we will contend ourselves by comparing the interpolating factors with those predicted by the non-commutative Iwasawa theory. To make the computation simpler, we will assume:

(Inert) Every prime divisor of m is inert in \mathcal{M}_0 .

Recall that we write ρ in the form $\rho = \rho_r \otimes \xi$. We fix a character η_r of G_r^{ab} whose induced representation of ρ_r . Also, we denote by ξ_r the restriction of ξ to G_r^{ab} . We will identify the adelic characters with Galois characters using the Artin reciprocity maps in this subsection.

Let us consider the periods Ω_∞ appearing in the interpolation formula (3.8.10). For each r , let Σ^r be the CM type of \mathcal{M}_r . Then Ω_∞ is a tuple $(\Omega_{\infty,\sigma})_{\sigma \in \Sigma^r}$ with $\Omega_{\infty,\sigma} \in \mathbb{C}^\times$ for each σ . To emphasize the dependence on \mathcal{M}_r , we often write $\Omega_\infty(\mathcal{M}_r)$ instead of Ω_∞ . Define $\Omega \in \mathbb{C}^\times$ to be

$$(5.4.4) \quad \Omega = \delta_0 \cdot \Omega_\infty(\mathcal{M}_0).$$

The key observation is that we have

$$(5.4.5) \quad \sigma(\delta_r) \cdot \Omega_{\infty,\sigma}(\mathcal{M}_r) = \Omega$$

for every $r \geq 0$ and any $\sigma \in \Sigma^r$. Precisely speaking, we can choose the periods so that (5.4.5) holds, as it was proved in Proposition 5.1 of [17]. For the characters of the form

$$(5.4.6) \quad \chi = \chi_r \kappa_r^n \eta_r \xi_r$$

where χ_r is constructed by composing the norm map to χ_0 , the values of n for which χ belongs the interpolation range are given by

$$(5.4.7) \quad n = 0, 1, 2, \dots, k - 1,$$

and the infinity type of χ is given by

$$(5.4.8) \quad (k - 2n)\Sigma + (1 - c)n\Sigma$$

respectively. Thus we can rewrite the power of Ω_∞ appearing in the denominator in (3.8.10) as

$$(5.4.9) \quad \Omega_\infty^{(k-2n)\Sigma+2n\Sigma} = \Omega^{k\Sigma} \delta_r^{-k\Sigma}.$$

Next we consider the epsilon factors. For the moment, let us view ρ as a representation on a complex vector space, using the embeddings i_p and i_∞ . Then, for the unique prime \mathfrak{p} in the p -adic CM type of \mathcal{M}_r , we have

$$(5.4.10) \quad \epsilon_{\mathfrak{p}}(0, \eta_r \xi_r \chi_r \kappa_r^n, \psi_{\mathfrak{p}}) = \kappa^n \chi_0(C_{p_w}(\rho)) \epsilon_{\mathfrak{p}}(0, \eta_r \xi_r, \psi_{\mathfrak{p}})$$

where $C_{p_w}(\rho)$ is the p_w -part of the conductor of ρ . Define α to be

$$(5.4.11) \quad \alpha = (\chi_r)_{\mathfrak{p}}(\varpi_{\mathfrak{p}})$$

where \mathfrak{p} is as above and $\varpi_{\mathfrak{p}}$ is the uniformizer at \mathfrak{p} . If we let $e_p(\rho)$ be the p -adic valuation of $C_{p_w}(\rho)$, then we have

$$(5.4.12) \quad \kappa^n \chi_0(C_{p_w}(\rho)) = \left(\frac{\alpha}{p^n}\right)^{e_p(\rho)}.$$

Next we consider the ratio

$$(5.4.13) \quad \frac{L(0, \chi_w)}{L(1, \chi_w^{-1})}$$

appearing in (3.8.10). Let p_w be the unique place in the p -adic CM type of \mathcal{M}_0 , and define the polynomial $P_{p_w}(\rho, X)$ to be the polynomial in X such that

$$(5.4.14) \quad P_{p_w}(\rho, p^{-s})^{-1}$$

is the Euler factor of the Artin L -function attached to ρ . If ρ is an unramified linear character, then $P_{p_w}(\rho, X) = 1 - \rho(\phi_{p_w})X$, where ϕ_{p_w} is the (geometric) Frobenius element in the Galois group. By the elementary argument given in the proof of Lemma 4.2 of [17], we have

$$(5.4.15) \quad L(0, \chi_w) = P_{p_w}\left(\rho, \frac{\alpha}{p^n}\right)^{-1}.$$

Similarly, letting ρ^\wedge be the contragredient of ρ , we have

$$(5.4.16) \quad L(1, \chi_w^{-1}) = P_{p_w}\left(\rho^\wedge, \frac{p^{n-1}}{\alpha}\right)^{-1}.$$

Collecting our formulae, for χ of the form (5.4.6), the right hand side of (3.8.10) becomes

$$(5.4.17) \quad L^{p\mathfrak{C}}(\chi, 0) \cdot \mathcal{C}_\infty(\chi) \cdot \frac{\chi_{\mathfrak{p}}(2\delta)\delta^{k\Sigma}}{(\mathrm{Im}(\delta))^{n\Sigma}\epsilon_{\mathfrak{p}}(0, \eta_r\xi_r, \psi_{\mathfrak{p}})\sqrt{|D_{\mathcal{F}}|_{\mathbb{R}}}} \cdot \frac{\pi^{n\Sigma}\Gamma_\Sigma((k-n)\Sigma)}{\Omega^{k\Sigma}} \\ \cdot \left(\frac{p^n}{\alpha}\right)^{e_p(\rho)} \cdot \frac{P_{p_w}(\rho^\wedge, \frac{p^{n-1}}{\alpha})}{P_{p_w}(\rho, \frac{\alpha}{p^n})}$$

because $\mathcal{M}_r/\mathcal{F}_r$ is unramified everywhere and $\mathfrak{C}_+ = 1$ by (Inert). It becomes

$$(5.4.18) \quad L^{p\mathfrak{C}}(\chi, 0) \cdot \mathcal{C}_\infty(\chi) \cdot \frac{\chi_{\mathfrak{p}}(2\delta)\delta^{k\Sigma}p^{e_p(\rho)}}{(\mathrm{Im}(\delta))^{n\Sigma}\epsilon_{\mathfrak{p}}(0, \eta_r\xi_r, \psi_{\mathfrak{p}})\sqrt{|D_{\mathcal{F}}|_{\mathbb{R}}}} \cdot \frac{\pi^{n\Sigma}\Gamma_\Sigma((k-n)\Sigma)}{\Omega^{k\Sigma}} \\ \cdot \left(\frac{p^{n-1}}{\alpha}\right)^{e_p(\rho)} \cdot \frac{P_{p_w}(\rho^\wedge, \frac{p^{n-1}}{\alpha})}{P_{p_w}(\rho, \frac{\alpha}{p^n})}$$

after a slight modification in the second and fourth factor. The L -function can be written, using Artin formalism, as

$$(5.4.19) \quad L^{p\mathfrak{C}}(\chi, 0) = L^{pC}(\chi_0, \rho, k-n),$$

where $L(\chi_0, \rho, s)$ is the L -function of χ_0 over \mathcal{M}_0 twisted by ρ , and C is the norm of \mathfrak{C} to \mathcal{M}_0 , and the superscript pC means that the Euler factors at primes dividing pC are removed. The first factor $\mathcal{C}_\infty(\chi)$ is simply $1 - \alpha p^{2k}$, which is in fact independent of ρ .

The resulting interpolation formula still involves intermediate fields, but the author is not able to give other form of interpolation formula, which looks substantially nicer than this, and would like to give some remarks on the interpolation factors. The last two factors are what appear in the conjectural interpolation formula of non-commutative p -adic L -function given in [3]. The first factor, which is a p -adic unit, does not appear therein, but appears in the interpolation formula of Hida’s three variable Rankin-Selberg p -adic L -function, which is given in Theorem 1, § 10.4 of [10]. This factor is natural since we worked with all $k \geq 1$, which gives rise to a Hida family. For the second factor, It would be nice to obtain a simpler formula it, but the author does not know a better one. The third factor consists of the expected gamma factor and the archimedean period, and Ω can be identified with the Neron period of an elliptic curve up to a p -adic unit. Indeed, one can see it from

(5.4.4), since $\Omega_\infty(\mathcal{M}_0)$ is by definition a Neron period of an elliptic curve, and δ_0 is a p -adic unit.

Acknowledgement

The author would like to thank his advisor John Coates for giving him warm encouragement throughout the project. He also would like to thank T. Bouganis, R. Greenberg, M. Hsieh, and M. Kakde for helpful conversations. He is also grateful to the referee for helpful comments, as well as for pointing several errors in an earlier version. This work was supported by NRF (National Research Foundation of Korea) Grant funded by the Korean Government (NRF 2012 Fostering Core Leaders of the Future Basic Science Program), by Priority Research Center Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2013053914), and by IBS-R003-D1.

References

- [1] D. Bump. *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, 55. Cambridge University Press, Cambridge, 1997.
- [2] J. Coates, T. Dokchitser, Z. Liang, W. Stein, R. Sujatha. *Non-commutative Iwasawa theory for modular forms*, Proc. London Math. Soc. (2013). doi: 10.1112/plms/pds061.
- [3] J. Coates, T. Fukaya, K. Kato, O. Venjakob, R. Sujatha, *The GL_2 -main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes etudes Sci. No. 101 (2005) 163–208.
- [4] J. Coates, P. Schneider, R. Sujatha, O. Venjakob (Eds.). *Noncommutative Iwasawa Main Conjectures over Totally Real Fields*, Springer Proceedings in Mathematics and Statistics, Vol. 29, 2013.
- [5] P. Deligne, G. Pappas. *Singularities des espaces de modules de Hilbert, en les caracteristiques divisant le discriminant*, Compositio Mathematica 90 (1994) 59–79.
- [6] T. Dokchitser, V. Dokchitser. *Computations in non-commutative Iwasawa theory*, Proc. London Math. Soc. (3) 94 (2006) 211–272.
- [7] T. Fukaya and K. Kato. *A formulation of conjectures on p -adic zeta functions in noncommutative Iwasawa theory*, Proceedings of the St.

Petersburg Mathematical Society. Vol. XII, 1–85, Amer. Math. Soc. Transl. Ser. 2, 219.

- [8] R. Greenberg. *Topics in Iwasawa theory*, unpublished, available online at <http://www.math.washington.edu/~greenber/book.pdf>.
- [9] H. Hida, *p -adic automorphic forms on Shimura varieties*, Springer Monographs in Mathematics. Springer-Verlag, New York, 2004. xii+390 pp. ISBN: 0-387-20711-2.
- [10] H. Hida, *Elementary theory of L -functions and Eisenstein series*, London Mathematical Society Student Texts, 26. Cambridge University Press, Cambridge, 1993.
- [11] H. Hida, J. Tilouine, *Anti-cyclotomic Katz p -adic L -functions and congruence modules*, Ann. Scient. Ec. Norm. Sup. 26 (1993) 189–259.
- [12] M. Hsieh. *On the μ -invariant of anticyclotomic p -adic L -functions for CM fields*, to appear in J. Reine Angew. Math. (DOI:10.1515/crelle-2012-0056).
- [13] M. Hsieh. *On the non-vanishing of Hecke L -values modulo p* , American Journal of Mathematics 134 (2012), no. 6, 1503–1539.
- [14] M. Kakde. *The main conjecture of Iwasawa theory for totally real fields*, Invent. Math. 193 (2013), no. 3, 539–626.
- [15] N. Katz. *p -adic L -function for CM fields*, Invent. Math. 49 (1978), no. 3, 199–297.
- [16] K. Kato. *K_1 of Some Non-Commutative Completed Group Rings*, K-Theory 34 (2005), no. 2, 99–140.
- [17] D. Kim. *p -adic L -functions over the false Tate curve extensions*, Mathematical Proceedings of the Cambridge Philosophical Society, 155, pp 483–498. doi:10.1017/S0305004113000431.
- [18] J. Ritter, A. Weiss. *On the “main conjecture” of equivariant Iwasawa theory*, J. Amer. Math. Soc. 24 (2011), no. 4, 1015–1050.
- [19] J. Tate. *Number theoretic background*, Automorphic forms, representations and L -functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 3–26, Proc. Sympos. Pure Math., XXXIII.

DOHYEONG KIM
IBS CENTER FOR GEOMETRY AND PHYSICS
POSTECH MATHEMATICAL SCIENCE BLDG, #108
77, CHEONGAM-RO, NAM-GU
POHANG, GYEONGBUK, 37673
KOREA
E-mail address: dohyeong@ibs.re.kr

RECEIVED OCTOBER 15, 2014