CM PERIODS, L-VALUES AND THE CM MAIN CONJECTURE

HARUZO HIDA

Contents

1. Introduction

The purpose of this paper is three folds:

(1) To give a concise proof of rationality and integrality result (due to Shimura [S] and Katz [K]) of the special values of (archimedean and p-adic) arithmetic modular forms at CM points (Sections 3 and 4);

(2) To construct a two variable p-adic measure interpolating critical Hecke L-values of imaginary quadratic fields (Section 5);

(3) To give a brief sketch of a proof of the anticyclotomic main conjecture in the Iwasawa theory of CM fields (Section 7).

We follow [S] to prove the rationality of the special values of classical arithmetic modular forms and their derivatives (Theorem 3.2). The new proof of p-integrality statements due to Katz (Theorem 4.4) is a modification of the argument of Shimura and can be easily generalized to Hilbert modular forms and beyond. Out of this p-integrality theorems, we can easily construct the measure. The Hilbert modular version of the measure (Theorem 6.1) is used to formulate the main conjecture and the anti-cyclotomic version (Conjecture 6.2). We admit a proposition reducing the

Date: October 2, 2005.

Conference talks at Hakuba (Japan) on September 26–27, 2005; the author is partially supported by the NSF grants: DMS 0244401 and DMS 0456252 and by the Clay Mathematical Institute as a Clay Research Scholar at the Analysis in Number Theory program at Centre de Recherches Mathématiques in Montréal (Canada) in September 2005.

proof of Conjecture 6.2 to a p-integrality statement of Petersson inner products of weight 2 p-integral Hilbert modular forms and a cetain well-specified CM form (Proposition 6.3), and we give a very brief sketch of how to prove the p-integrality of the Petersson inner product. There are two keys to the proof. One is the expression of the inner product of the CM form and a product of two weight 1 forms as a special values at a CM point of the residue of a series (called Shimura series generalizing Eisenstein series), and another is to write down integrally a given p-integral form as a sum of the products of two weight 1 forms (cf. [H05a]). Verifying the p-integrality of the q-expansion of the residue, we conclude the p-integrality of the special value (and hence the inner products) by the q-expansion principle. All the details of the proof of the conjecture are in [H05b], [H05c] and [HMI] Chapter 5.

2. Elliptic modular forms

What are modular forms? In the easiest cases of elliptic modular forms, if we write $w = {}^t(w_1, w_2)$ linearly independent complex numbers (with $\mathrm{Im}(z) > 0$ ($z = w_1/w_2$)), a weight k modular form is a holomorphic function f of w satisfying $f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) w\right) = f(w)$ and $f(aw) = a^{-k} f(w)$ for $a \in \mathbb{C}^\times$ as everybody knows. We want to prove algebraicity and integrality of the value $f(w)$ when w is a basis of an imaginary quadratic field (up to a canonical period), and further generalize this to Hilbert modular case. This is due to Damerell, Weil, Shimura and Katz.

To do this, we need to give algebraic interpretation of modular form (see [AME], [GME] and [PAF] Chapter 2). Pick two linearly independent numbers $w = (w_1, w_2) \in \mathbb{C}^2$. Writing u for the variable on $\mathbb{C}$, the quotient $\mathbb{C}/L_w$ for $L_w = \mathbb{Z}w_1 + \mathbb{Z}w_2$ gives rise to a pair (E, ω) of elliptic curves and the differential $\omega = du$ of first kind (nowhere vanishing differential). Indeed, $E(\mathbb{C}) \cong \mathbb{C}/L_w$, and we can embed E into $\mathbf{P}^2$ via $u \mapsto (x(u), y(u), 1) \in \mathbf{P}^2(\mathbb{C})$ by Weierstrass $\mathcal{P}$-functions

$$x(u) = \mathcal{P}(u; L_w) = \frac{1}{u^2} + \sum_{0 \neq \ell \in L_w} \left\{ \frac{1}{(u-\ell)^2} - \frac{1}{\ell^2} \right\} = \frac{1}{u^2} + \frac{g_2}{20} u^2 + \frac{g_3}{28} u^4 + \cdots$$

and $y = \frac{dx}{du}$, where $g_2(w) = 60 \sum_{0 \neq \ell \in L_w} \ell^{-4}$ and $g_3(w) = 140 \sum_{0 \neq \ell \in L_w} \ell^{-6}$. Then the relation is $y^2 = 4x^3 - g_2 x - g_3$ and $\omega = du = \frac{dx}{y}$. The pair w can be recovered by ω so that $w_i = \int_{\gamma_i} \omega$ for a basis (γ_1, γ_2) of $H_1(E(\mathbb{C}), \mathbb{Z})$.

Conversely, start with a pair $(E, \omega)_{/A}$ defined over a ring A made of an elliptic curve (a smooth curve of genus 1 with a specific point $0 = 0_E \in E(A)$) and a nowhere vanishing differential ω. Then take a parameter u around 0 so that $\omega = du$. Write $[0]$ for the relative Cartier divisor given by 0. Since the line bundle $\mathcal{L}(m[0])$ (made of meromorphic function having pole at 0 of order at most m) is free of rank m if $m > 0$ (by the existence of ω), we can find $x \in H^0(E, \mathcal{L}(2[0]))$ having a pole of order 2 whose Laurent expansion has its leading term u^{-2}. If $6^{-1} \in A$, there is a unique way of normalizing x so that $y^2 = 4x^3 - g_2 x - g_3$ for a unique pair

$(g_2 = g_2(E,\omega), g_3 = g_3(E,\omega)) \in A^2$. Since $E_{/A}$ is smooth, this pair (g_2, g_3) has to satisfy $\Delta = g_2^3 - 27g_3^2 \in A^\times$. This shows

$$\{(E,\omega)_{/A}\}/\cong \overset{\text{1 to 1 and onto}}{\leftrightarrow} \{(g_2,g_3) \in A^2 | \Delta \in A^\times\}$$
$$= \mathrm{Hom}_{alg}(\mathbb{Z}[\frac{1}{6}, g_2, g_3, \frac{1}{\Delta}], A) = \mathrm{Spec}(\mathbb{Z}[\frac{1}{6}, g_2, g_3, \frac{1}{\Delta}])(A).$$

Since all these functions g_2, g_3 and Δ has Fourier expansions in $\mathbb{Z}[\frac{1}{6}][[q]]$ for $q = \exp(2\pi i z)$, we can think of the Tate curve

$$\mathrm{Tate}(q) = \mathrm{Proj}(\mathbb{Z}[\frac{1}{6}][[q]][x,y,z]/(y^2z - (4x^3 - g_2(q)xz^2 - g_3(q)z^3)).$$

As shown by Tate, $\mathrm{Tate}(q)(\overline{\mathbb{Q}}_p[[q]]) \supset (\overline{\mathbb{Q}}_p[[q]])^\times/q^{\mathbb{Z}}$, we have a natural inclusion $i_{can} : \mu_N \hookrightarrow \mathrm{Tate}(q)[N]$ and $\phi_{can} : \mathbb{Z}/N\mathbb{Z} \cong q^{N^{-1}\mathbb{Z}}/q^{\mathbb{Z}} \hookrightarrow \mathrm{Tate}(q)[N]$. The Tate curve also has a canonical differential $\omega_{can} = \frac{dx}{y}$. The Tate curve is an elliptic curve over $\mathbb{Z}[\frac{1}{6}][[q]][q^{-1}]$ because $q|\Delta$. Let B be a $\mathbb{Z}[\frac{1}{6}]$-algebra. This motivate the following algebraic definition (cf. [GME] 2.6.5) of B-integral elliptic modular forms of level $\Gamma_1(N)$ as functions of (E,ω) satisfying

- (G0) f assigns a value $f((E,i,\omega)_{/A}) \in A$ for any triple $(E, i : \mu_N \hookrightarrow E[N], \omega)_{/A}$ defined over an B-algebra A. Here A is also a variable.
- (G1) $f((E,i,\omega)_{/A}) \in A$ depends only on the isomorphism class of $(E,i,\omega)_{/A}$.
- (G2) If $\varphi : A \to A'$ is an B-algebra homomorphism, we have $f((E,i,\omega)_A \otimes A') = \varphi(f((E,i,\omega)_{/A})$.
- (G3) $f((E,i,a\cdot\omega)_{/A}) = a^{-k}f(E,i,\omega)$ for $a \in A^\times$.
- (G4) $f(q) = f((\mathrm{Tate}(q), i_{can}, \omega_{can})_{/B[[q]][q^{-1}]}) \in B[[q]]$.

The space of modular forms will be written as $G_k(N;B)$. By definition, $G_k(1;B) = \bigoplus_{4a+6b=k} Bg_2^a g_3^b$, and $G_k(N, \mathbb{Z}[\frac{1}{6}]) \otimes \mathbb{C} = G_k(N,\mathbb{C})$. Also, if $f \in G_k(N,\mathbb{C})$, $f(q)$ with $q = \exp(2\pi z)$ gives the Fourier expansion of f at the cusp ∞.

Fix a prime $p \geq 5$. We call a $\mathbb{Z}_p$-algebra A a p-adic algebra if $A = \varprojlim_n A/p^nA$. Thus $\mathbb{Z}_p$ is a p-adic algebra but $\mathbb{Q}_p$ is not. Take a p-adic algebra B. The space of B-integral p-adic modular form $V(B)$ is a collection of rules f assigning a value $f((E, i : \mu_{p^\infty})_{/A}) \in A$ for p-adic B-algebras A satisfying the following condition:

- (V0) f assigns a value $f((E,i)_{/A}) \in A$ for any couple $(E, i : \mu_{p^\infty} \hookrightarrow E[p^\infty])_{/A}$ defined over a p-adic B-algebra A. Here A is also a variable.
- (V1) $f((E,i)_{/A}) \in A$ depends only on the isomorphism class of $(E,i)_{/A}$.
- (V2) If $\varphi : A \to A'$ is an B-algebra homomorphism continuous under the p-adic topology, we have $f((E,i)_A \otimes A') = \varphi(f((E,i)_{/A})$.
- (V3) $f(q) = f((\mathrm{Tate}(q), i_{can})_{/B[[q]][q^{-1}]}) \in B[[q]]$.

By definition, $V(B)$ is a p-adic B-algebra.

Since the knowledge of $\mu_{p^\infty/\mathbb{Z}_p} = \varinjlim_n \mu_{p^n/\mathbb{Z}_p}$ is equivalent to the knowledge of $\widehat{\mathbb{G}}_{m/\mathbb{Z}_p} = \mathrm{Spf}(\varprojlim_n \mathbb{Z}_p[t,t^{-1}]/(t^n-1))$, $i : \mu_{p^\infty} \hookrightarrow E$ induces an identification i :

$\widehat{\mathbb{G}}_m \cong \widehat{E} = \varprojlim_n E[p^n]^\circ$. Since $\widehat{\mathbb{G}}_m$ has a canonical differential $\frac{dt}{t}$, i induces a nowhere vanishing differential $\omega_p = i_* \frac{dt}{t}$. Thus $f \in G_k(p^n; B)$ can be regarded as a p-adic modular form by $f((E, i : \mu_{p^\infty} \to E[p^\infty])_{/A}) = f(E, i|_{\mu_{p^n}}, i_* \frac{dt}{t}) \in A$. Thus we have a canonical B-linear map $G_k(N; B) \to V(B)$. The following fact is called the q-expansion principle (following from the two facts that the irreducibility of the Igusa curve over $\mathbb{F}_p$ and the existence of the Tate curve; see [PAF] 3.2.8 and [GME] 2.5):

(Q0) $f(q) = 0 \iff f = 0$ for any f in $V(B)$ or in $G_k(N; B)$. In particular, $G_k(p^n; B) \to V(B)$ is an injection, and functions in the image satisfies $f(E, a \cdot i) = a^{-k} f(E, i)$ for $a \in \mathbb{Z}_p^\times$.

(Q1) Let $f_n \in V(B)$ be a sequence. Then f_n converges p-adically in $V(B) \iff f_n(q)$ converges p-adically in $B[[q]] \iff f_n((E, i))/A)$ converges p-adically for all $(E, i))/A$ and all p-adic B-algebra A.

(Q2) If B_0 is a $\mathbb{Z}[\frac{1}{6}]$-algebra p-adically dense in B, $G_k(p^\infty; B_0) = \bigcup_n G_k(p^n; B_0)$ is dense in $V(B)$ for any $k \geq 2$.

(Q3) If $f \in V(B) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $f(q) \in B[[q]]$, then $f \in V(B)$, assuming B is flat over $\mathbb{Z}_p$.

An elliptic curve $E_{/A}$ is said to have complex multiplication if $\mathrm{End}(E_{/A})$ contains the integer ring R of an imaginary quadratic field $M \subset \mathbb{C}$. If $E(\mathbb{C}) = \mathbb{C}/L_w$ has complex multiplication, $R \cdot L_w \subset L_w$, thus we have a representation $\rho : M^\times \hookrightarrow GL_2(\mathbb{Q})$ such that $\alpha w = \rho(\alpha) w$ for $\alpha \in M^\times$. Since $\rho(\alpha)(z) = \frac{az+b}{cz+d}$ ($\rho(\alpha) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$) and $z = w_1/w_2$ corresponds to the same elliptic curve, we have $\rho(\alpha)(z) = z$. Suppose that E has complex multiplication by R. Then by the Shimura–Taniyama theory, E is defined over a number field M', and by a result of Serre–Tate E is defined over a valuation ring R' of M' the residual characteristic p. Suppose further p splits into a product of two primes $\mathfrak{p}\overline{\mathfrak{p}}$ in R. Then we may assume that $E[\mathfrak{p}^\infty]_{/R'}$ is isomorphic to μ_{p^∞} after extending scalar to the strict henselization $\mathcal{W} \subset \overline{\mathbb{Q}}$ of R'. Pick $\omega \in H^0(E, \Omega_{E/\mathcal{W}})$ so that $H^0(E, \Omega_{E/\mathcal{W}}) = \mathcal{W}\omega$. We fix two isomorphisms $i : \mu_{p^\infty/\mathcal{W}} \cong E[\mathfrak{p}^\infty] \subset E[p^\infty]_{/\mathcal{W}}$ and $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$ for a fractional ideal $\mathfrak{a} \supset R$ with $\mathfrak{a}_p = R_p$. Thus we may assume that $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}z$ ($z \in M^\times$). Let $W = \varprojlim_n \mathcal{W}/p^n\mathcal{W}$. Then we have two numbers $\Omega_\infty \in \mathbb{C}^\times$ and $\Omega_p \in W^\times$ such that

$$\omega = \Omega_\infty du = \Omega_p i_* \frac{dt}{t}.$$

We have

Theorem 2.1. *Let $f \in G_k(p^n; \mathcal{W})$. Write $f_p \in V(W)$ (resp. $f_\infty \in G_k(p^n; \mathbb{C})$) the corresponding p-adic modular form (resp. the corresponding holomorphic modular form). If $(E, \omega)_{/\mathcal{W}}$ has complex multiplication by R in which p splits, we have*

$$\frac{f_\infty(z)}{\Omega_\infty^k} = \frac{f_\infty(E, i, du)}{\Omega_\infty^k} = \frac{f_p(E, i, i_* \frac{dt}{t})}{\Omega_p^k} = f(E, i, \omega) \in \mathcal{W}.$$

Remark 2.2. Replacing $\mathcal{W}$ by its quotient field, the assertion of the theorem is valid if $f = \frac{f}{g}$ finite at (E, i, du) for $h \in G_{k+k'}(p^n; \mathcal{W})$ and $g \in G_{k'}(p^n; \mathcal{W})$ for an obvious reason.

3. Invariant differential operators

Shimura studied the effect on modular forms of the following differential operators on the upper half complex plane $\mathfrak{H}$ indexed by $k \in \mathbb{Z}$:

$$\delta_k = \frac{1}{2\pi\sqrt{-1}}\left(\frac{\partial}{\partial z} + \frac{k}{2y\sqrt{-1}}\right) \quad \text{and} \quad \delta_k^r = \delta_{k+2r-2}\cdots\delta_k, \tag{3.1}$$

where $r \in \mathbb{Z}$ with $r \geq 0$. For more details of these operators, see [LFE] 10.1. Here are easy identities:

Exercise 3.1. *Show the following formulas:*

(1) $\delta_{k+\ell}(fg) = g\delta_k f + f\delta_\ell g$.
(2) $\delta_k^r(f|_k\alpha) = (\delta_k^r f)|_{k+2r}\alpha$ *for a holomorphic function* $f : \mathfrak{H} \to \mathbb{C}$, *where*

$$f|_k\alpha(z) = \det(\alpha)^{k/2} f(\alpha(z))(cz+d)^{-k}$$

for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *with positive determinant.*

Therefore if $f \in G_k(N; \mathbb{C})$, $\delta_k^r(f)$ satisfies $\delta_k^r(f)|_{k+2r}\gamma = \delta_k^r(f)$ for all $\gamma \in \Gamma_1(N)$. Although $\delta_k^r(f)$ is not a holomorphic function, defining

$$\delta_k^r(f)(w) = w_2^{-k-2r}\delta_k^r(f)(z),$$

we have a well-defined homogeneous modular form. In this sense, $\delta_k^r(f)$ is a real-analytic modular form on $\Gamma_1(N)$ of weight $k + 2r$.

An important point Shimura found is that the differential operator preserves rationality property at CM points of (arithmetic) modular forms, although it does not preserve holomorphy. We shall describe the rationality. Here is the rationality result of Shimura [S]:

Theorem 3.2 (G. Shimura)**.** *Let the notation and the assumption be as in* Theorem 2.1. *For* $f \in G_k(N; \overline{\mathbb{Q}})$, *we have*

$$\frac{(\delta_k^r f)(z)}{\Omega_\infty^{k+2r}} = \frac{(\delta_k^r f)(E, i, du)}{\Omega_\infty^{k+2r}} \in \overline{\mathbb{Q}}. \tag{S}$$

Proof. We follow the argument of Shimura in [S]. Since

$$(\delta_k^r f)(E, du) = w_2^{-k-2r}(\delta_k^r f)(z) = (\delta_k^r f)(z)$$

for $z = w_1/w_2 \in \mathfrak{H}$ (and $w_2 = 1$), we need to show $\frac{(\delta_k^r f)(z)}{\Omega_\infty^{k+2r}} \in \overline{\mathbb{Q}}$. When $r = 0$, the result follows from Theorem 2.1. We have $\rho : M^\times \hookrightarrow GL_2(\mathbb{Q})$ given by $\left(\begin{smallmatrix} z\alpha \\ \alpha \end{smallmatrix}\right) = \rho(\alpha)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$ for $\alpha \in M^\times$. Then $\rho(\alpha)(z) = z$. Writing $\rho(\alpha) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have $cz + d = \alpha$. Apply δ_k to

$f|_k\rho(\alpha) = fh$, by Exercise 3.1, we have $(\delta_k f)|_{k+2}\rho(\alpha) = (\delta_k f)h + f(\delta_0 h)$. Specializing this equality at z, we have

$$\begin{aligned}\alpha^{-k-2}(\delta_k f)(z) = (\delta_k f)|_{k+2}\rho(\alpha)(z) = (\delta_k f)(z)h(z) + f(z)(\delta_0 h)(z)\\ = (\delta_k f)(z)\alpha^{-k} + f(z)(\delta_0 h)(z),\end{aligned}$$

because $h(z) = (f|_k\rho(\alpha))(z)/f(z) = \alpha^{-k}$. Then we have

$$(\delta_k f)(z) = \alpha^k(\alpha^{-2} - 1)^{-1} f(z)(\delta_0 h)(z).$$

Note that $\delta_0 h$ is a meromorphic modular form of weight 2 defined over $\overline{\mathbb{Q}}$ by the q-expansion principle. Thus $\frac{\delta_0 h(z)}{\Omega_\infty^2} \in \overline{\mathbb{Q}}$ (Remark 2.2), and this proves the result when $r = 1$. We repeating this process r times. By the Leibnitz formula, $\delta_k^r(fh) = \sum_{0\le s\le r}\binom{r}{s}\delta_k^s f\delta_0^{r-s}h$. Form this we get

$$\delta_k^r(f)|_{k+2r}\rho(\alpha) = (\delta_k^r f)h + \sum_{0<s\le r}\binom{r}{s}(\delta_k^{r-s}f)(\delta_0^s h).$$

Evaluating this at z, we finally get

$$(\delta_k^r f)(z) = \alpha^k(\alpha^{-2r} - 1)^{-1}\sum_{0<s\le r}\binom{r}{s}(\delta_k^{r-s}f)(z)(\delta_0^s h)(z). \tag{3.2}$$

Note that $\delta_0^s h = \delta_2^{s-1}\delta_0 h$, and as we have already observed, $\delta_0 h$ is a meromorphic $\overline{\mathbb{Q}}$-rational modular form finite at z. Then by the induction hypothesis, we get the desired rationality. $\square$

Remark 3.3. Choosing $g \in G_{k+2r}(N;\mathcal{W})$ with $g(z) \neq 0$ under the notation of the above proof, Shimura actually proved in [S] that $\frac{\delta_k^r f(z)}{g(z)} \in \overline{\mathbb{Q}}$, which is equivalent to the above theorem by Theorem 2.1.

Remark 3.4. For a given $f \in G_k(N;\overline{\mathbb{Q}})$ as above, defining the transformation equation

$$P(X, f) = \prod_{\gamma\in\Gamma_1(N)\backslash SL_2(\mathbb{Z})}(X - f|_k\gamma) = \sum_{j=0}^{d} a_j(z)X^j,$$

we have $a_j \in G_{kd-jd}(1;\mathcal{W})$. Thus $a_j = Q_j(g_2, g_3)$ for a isobaric polynomial Q_j with coefficients in oQ. If (E,ω) is defined by $y^2 = 4x^3 - g_2(E,\omega)x - g_3(E,\omega)$, $f(E,i,\omega)$ satisfies $\sum_{j=0}^{d} Q_j(g_2(E,\omega), g_3(E,\omega))X^j = 0$. Thus this gives an algorithm to compute the value $f(E,i,\omega)$. Once we know the value $f(E,i,\omega) = \frac{f(E,i,du)}{\Omega_\infty^k}$, we can then compute $\frac{\delta_k^r(f(z))}{\Omega_\infty^{k+2r}}$ following the above proof (in particular, the induction process).

4. p-Adic differential operators

On $V(W)$, we have a more standard differential operator $d = \delta_0$ whose effect on q-expansion is $d(\sum_n a_n q^n) = \sum_n n a_n q^n$. An elementary construction of d can be given as follows. Pick $f \in G_k(N;\mathcal{W}) \subset G_k(N;\mathbb{C})$. Then for any function $\phi : \mathbb{Z}/p^r\mathbb{Z} \to \mathcal{W}$, we define its Fourier transform $\phi^* : \mathbb{Z}/p^r\mathbb{Z} \to \mathcal{W}$ by $\phi^*(x) = \sum_{u\in\mathbb{Z}/p^r\mathbb{Z}} \phi(u)\mathbf{e}(xu/p^r)$, where $\mathbf{e}(x) = \exp(2\pi i x)$.

Exercise 4.1. *Prove* $(\phi^*)^*(x) = p^r\phi(-x)$.

We define

$$f|\phi(z) = p^{-r} \sum_{u \mod \mathbb{Z}/p^r\mathbb{Z}} \phi^*(-u) f(z + \frac{u}{p^r}). \tag{4.1}$$

Then we have $(\sum_n a_n q^n)|\phi) = \sum_n \phi(n) a_n q^n \in G_k(Np^{2r};\mathcal{W})$.

Exercise 4.2. *Define* $\phi|x(u) = \phi(xu)$ *for* $x \in (\mathbb{Z}/p^r\mathbb{Z})^\times$. *For* $f \in G_k(N;\mathbb{C})$, *prove that* $(f|\phi)|_k\gamma = (f|_k\gamma)|(\phi|ad^{-1})$ *if* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_1(N)\cap\Gamma_0(p^{2r})$. *In particular* $f|\phi \in G_k(N;\mathbb{C})$. (Hint: Use the strong approximation theorem of $SL(2)$ and the formula: $\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & u/p^r \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & (a^{-1}d)u/p^r - a^{-1}b \\ 0 & 1\end{smallmatrix}\right)$; see also [IAT] Proposition 3.64.)

Then choosing $\phi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathcal{W}$ so that $\phi_n(u) \equiv u \mod p^n\mathcal{W}$, the q-expansion $\lim_{n\to\infty}(f|\phi_n)$ converges p-adically to the q-expansion of df. By the q-expansion principle, $G_k(p^\infty;\mathcal{W})$ is dense in $V(W)$, we have a unique $df \in V(W)$. Thus $d^r f(E, i_*\frac{dt}{t}) \in W$ is well defined. The effect of d^r on the q–expansion of a modular form is given by

$$d^r \sum_n a(n)q^n = \sum_n a(n)n^r q^n. \tag{4.2}$$

We can let $a \in \mathbb{Z}_p^\times$ acts on $f \in V(R)$ by $f|a(E,i) = f|\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right)(E,i) = f(E, a\cdot i)$.

Lemma 4.3. *If* $f \in G_k(N;\mathcal{W})$, *then we have*

$$(d^r f)|\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right) = a^{-k-2r}(d^r f)$$

for $a \in \mathbb{Z}_p^\times$.

Proof. We can approximate p-adically $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right)$ by an element $\gamma_n \in \Gamma_1(N)\cap\Gamma_0(p^{2n})$ so that $\gamma_n \equiv g \mod p^n M_2(\mathbb{Z}_p)$. By Exercise 4.2, we have

$$df|a = \lim_{n\to\infty} f|\phi_n|_k\gamma_n = a^{-k}\lim_{n\to\infty} f|\gamma_n|(\phi_n|a^2) = a^{-k-2}df$$

because $\phi_n(u) \equiv u \mod p^n\mathcal{W}$. Then iterating this formula r times, we get the formula in the lemma. □

Katz interpreted the differential operator d in terms of the Gauss-Manin connection of the universal elliptic curve over the modular curve $X_1(N)$ and gave a purely algebro-geometric definition of the operator d^r acting on $V(R)$ for any p-adic W-algebra R

(see Katz's paper [K]). Since his definition of d^r is purely algebro-geometric, it is valid for classical modular forms and p–adic modular forms at the same time. An important formula given in [K] (2.6.7) is as follows.

Theorem 4.4 (N. M. Katz)**.** *Let the notation and the assumption be as in* Theorem 2.1 *For $f \in G_k(p^n;\mathcal{W})$, we have*

$$\frac{(d^r f)(E,i)}{\Omega_p^{k+2r}} = \frac{(\delta_k^r f)(E,i,du)}{\Omega_\infty^{k+2r}} \in \mathcal{W}. \tag{K}$$

We give here a proof similar to the argument which proves Theorem 3.2.

Proof. We use the notation introduced in the proof of Theorem 3.2. In particular, take $\pm 1 \neq \alpha \in M^\times$) with $\alpha\overline{\alpha} = 1$.

After identifying algebro-geometric forms and analytic ones by q-expansions via the fixed two embeddings $\overline{\mathbb{Q}}_p \supset \mathcal{W} \subset \mathbb{C}$, we see that $d = \frac{1}{2\pi i}\frac{\partial}{\partial z}$. We write $\mathcal{A} = \mathcal{A}(N;\overline{\mathbb{Q}}) = \bigcup_k \{\frac{f}{g} | f, g \in G_k(N;\overline{\mathbb{Q}})\}$. Thus for meromorphic functions $h(x) \in \mathcal{A}$, we have,

$$d(h \circ \rho(\alpha)) = \frac{1}{2\pi i}\frac{\partial h(\rho(\alpha)(z))}{\partial z} = \alpha^{-2}\frac{1}{2\pi i}\frac{\partial h}{\partial z}((\rho(\alpha)(z)) = \alpha^{-2}(dh) \circ \rho(\alpha).$$

Since $dh = g_1/g_2$ for $g_1 \in G_{k+2}(N;\mathcal{W})$ and $g_2 \in G_k(N;\mathcal{W})$ for sufficiently large k, we have (Remark 2.2)

$$\frac{(dh)(E, i_*\frac{dt}{t})}{\Omega_p^2} = (dh)(E,\omega) \in \overline{\mathbb{Q}}. \tag{4.3}$$

Since $\frac{f(E,i_*\frac{dt}{t})}{\Omega_p^k} = f(E,\omega) \in \mathcal{W}$, we first show

$$\frac{(d^r f)(E,i)}{\Omega_p^{k+2r}} = \frac{(\delta_k^r f)(E,i,du)}{\Omega_\infty^{k+2r}} \in \overline{\mathbb{Q}}$$

by induction on r. When $r = 0$, this follows from Theorem 2.1. To treat $r > 0$, take $f \in G_k(N;\mathcal{W})$, and define $h \in \mathcal{A}$ by $f|_k\rho(\alpha) = fh$ as in the proof of Theorem 3.2.

Apply d to $f|_k\rho(\alpha) = fh$, we have $(df)|_{k+2}\rho(\alpha) = (df)h + f(dh)$. Specializing this equality at (E,ω), we get from Lemma 4.3

$$\alpha^{-k-2}(df(E,i)) = ((df)|_{k+2}\rho(\alpha))(E,i) = (df)(E,i)h(E) + f(E,i)(dh)(E,i).$$

Since $h(E) = (f|_k\rho(\alpha))(E,i)/f(E,i) = \alpha^{-k}$, we have

$$(df)(E,i) = \alpha^k(\alpha^{-2}-1)^{-1}f(z)(dh)(E,i).$$

Thus we have again proved $\frac{dh(E,i_*\frac{dt}{t}))}{\Omega_p^2} \in \overline{\mathbb{Q}}$, and also this proves the result when $r = 1$. We repeat this process r times. By the Leibnitz formula, we have $d^r(fh) =$

$\sum_{0\le s\le r}\binom{r}{s}d^s f d^{r-s}h$. Form this we get

$$d^r(f)|_{k+2r}\rho(\alpha)=(d^r f)h+\sum_{0<s\le r}\binom{r}{s}(d^{r-s}f)(d^s h).$$

Evaluating this at (E,i), we get

$$(d^r f)(E,i)=\alpha^k(\alpha^{-2r}-1)^{-1}\sum_{0<s\le r}\binom{r}{s}(d^{r-s}f)(E,i)(d^s h)(E,i).$$

Dividing by Ω_p^{k+2r}, we finally get

$$\frac{(d^r f)(E,i)}{\Omega_p^{k+2r}}=\alpha^k(\alpha^{-2r}-1)^{-1}\sum_{0<s\le r}\binom{r}{s}\frac{(d^{r-s}f)(E,i)}{\Omega_p^{k+2r-2s}}\frac{(d^s h)(E,i)}{\Omega_p^{2s}}.$$

By the induction hypothesis, we have, for $s>0$,

$$\frac{(d^{r-s}f)(E,i)}{\Omega_p^{k+2r-2s}}=\frac{(\delta_k^{r-s}f)(E,i,du)}{\Omega_\infty^{k+2r-2s}}$$

and

$$\frac{(d^s h)(E,i)}{\Omega_p^{2s}}=\frac{(d^{s-1}dh)(E,i)}{\Omega_p^{2s}}=\frac{(\delta_2^{s-1}dh)(E,i,du)}{\Omega_\infty^{2s}}.$$

Replacing each term as above by the corresponding archimedean term, we recover the right-hand-side of (3.2) divided by Ω_∞^{k+2r}. Then by the induction hypothesis, we get the desired identity:

$$\frac{(d^r f)(E,i)}{\Omega_p^{k+2r}}=\frac{(\delta_k^r f)(E,i,du)}{\Omega_\infty^{k+2r}}$$

inside $\overline{\mathbb{Q}}$. Since the left-hand-side of the above identity is in W, we conclude the identity in $\mathcal{W}=W\cap\overline{\mathbb{Q}}$. $\square$

We note that all this process of proving algebraicity and integrality applies to Hilbert modular forms after an appropriate adjustment.

5. Katz measure

We consider the binomial polynomial $\binom{x}{m}$. We consider the differential operator $\binom{d}{m}$. Then we have

$$\binom{d}{m}(\sum_n a_n q^n)=\sum_n\binom{n}{m}a_n q^n.$$

In particular, $\binom{n}{m}a_n\in R$ if $a_n\in R$ for a p-adic algebra R. This shows $\binom{d}{m}:V(R)\to V(R)$. In particular, $\binom{d}{m}f(E,\omega)\in W$ if $f\in G_k(p^n;W)$. By Mahler's theorem, a given continuous function $\phi:\mathbb{Z}_p\to W$ can be expanded uniquely as $\phi(x)=\sum_{m\ge 0}c_m(\phi)\binom{x}{m}$ for $c_m(\phi)\in W$ tending to 0 as $m\to\infty$. Thus defining $\int_{\mathbb{Z}_p}\binom{x}{m}df(x)=\binom{d}{m}f(E,i)$, we have a unique p-adic measure $df : \mathcal{C}(\mathbb{Z}_p; W) \to W$, where $\mathcal{C}(\mathbb{Z}_p; W)$ is the p-adic Banach space of continuous functions on $\mathbb{Z}_p$ with values in W. Thus, we have

Theorem 5.1. *Let the notation be as in* Theorem 2.1, *and suppose $f \in G_k(p^n; \mathcal{W})$. If $\phi(x) = \sum_{m\geq 0} c_m(\phi)\binom{x}{m} \in \mathcal{C}(\mathbb{Z}_p; W)$, we have*

$$\int_{\mathbb{Z}_p} \phi(x) df(x) = \phi(x) = \sum_{m\geq 0} c_m(\phi) \binom{d}{m} f(E, i).$$

In particular, we have

$$\frac{\int_{\mathbb{Z}_p} x^r df(x)}{\Omega_p^{k+2r}} = \frac{d^r f(E,i)}{\Omega_p^{k+2r}} = \frac{\delta_k^r f(E, du)}{\Omega_\infty^{k+2r}} \in \mathcal{W}.$$

Recall the Eisenstein series

$$g_k(w) = \sum_{0\neq \ell \in L_w} \ell^{-k}.$$

After a division by a simple nonzero constant, writing the new series as G_k, this series G_k has the following q-expansion :

$$G_k(q) = 2^{-1}\zeta(1-k) + \sum_{n>0} q^n \sum_{0<\delta|n} \delta^{k-1}.$$

Thus defining $E_k = G_k|\mathbf{1}$ for the characteristic function $\mathbf{1}$ of $(\mathbb{Z}/p\mathbb{Z})^\times$ on $(\mathbb{Z}/p\mathbb{Z})$ in order to remove coefficients of q^{mp} for $m = 0, 1, \dots,$ we get

$$E_k(q) = \sum_{n>0, p\nmid n} q^n \sum_{0<\delta|n} \delta^{k-1}.$$

Then writing $\binom{x}{m} = \sum_{j=0}^{m} c_j x^j$, we find

$$\binom{\mathcal{E}}{m} = \sum_j c_j E_{j+1} = \sum_{n>0, p\nmid n} q^n \sum_{0<\delta|n} \binom{\delta}{m} \in \mathbb{Z}[[q]],$$

which has integral q-expansion. Thus we can create two variable measure $dE : \mathcal{C}(\mathbb{Z}_p^2; W) \to W$ as follows.

Theorem 5.2 (N. Katz)**.** *Let the notation be as in* Theorem 2.1. *There exists a measure $dE : \mathcal{C}(\mathbb{Z}_p^2; W) \to W$ such that*

$$\int_{\mathbb{Z}_p^2} \binom{x}{m}\binom{y}{n} dE = \binom{d}{m}\binom{\mathcal{E}}{n}(E, i) \in W$$

for all integers $n \geq 0$ and $m \geq 0$.

If E is given by Gauss' lemniscate: $y^2 = 1 - x^4 \cong y^2 = 4x^3 - 4x$, we have $R = \mathbb{Z}[i]$ for $i = \sqrt{-1}$, $\Omega_\infty = \int_0^1 du = \int_0^\infty \frac{dx}{\sqrt{1-x^4}} dx$, and

$$g_k(E, \omega) = \Omega_\infty^{-k} \sum_{0 \neq \alpha \in \mathbb{Z}[i]} \alpha^{-k} = \Omega_\infty^{-k} L(0, \lambda_k),$$

where $\lambda_k((\alpha)) = \alpha^{-k}$. More generally, the differential operator δ_k^r brings λ_k into λ' with $\lambda_{k+r,-r}((\alpha)) = \alpha^{-k}(\overline{\alpha}/\alpha)^r$, and we get a p-adic measure interpolating $\frac{L(0,\lambda_{k+r,-r})}{\Omega_\infty^{k+2r}(2\pi i)^{-r}}$ over $\mathbb{Z}_p^2$. For a general imaginary quadratic field M, one needs to make a combination of the above type of measures to get this type of p-adic interpolation of Hecke L-values. Indeed, writing $Cl(p^n)$ for the ray class group of M modulo p^n, the limit $C = \varprojlim_n Cl(p^n) = \bigsqcup_{\mathfrak{a} \in Cl} [\mathfrak{a}] R_p^\times / \{\pm 1\}$. Each $\mathfrak{a}$ gives rise to an elliptic curve with complex multiplication by R with $E_\mathfrak{a}(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$. Since we assumed that p splits in R, $R_p \cong \mathbb{Z}_p^2$ as algebras. By the above construction, we have a measure $dE_\mathfrak{a}$ associated to $E_\mathfrak{a}$ on the coset $[\mathfrak{a}] R_p^\times / \{\pm 1\}$. In this way, Katz proved

Theorem 5.3 (N. Katz)**.** *Let M be an imaginary quadratic field in which the prime p splits. Then there exists a measure $d\mu$ on C such that for a Hecke character λ with $\lambda((\alpha)) = \alpha^{-k}\overline{\alpha}^j$ for $\alpha \equiv 1 \mod p^n$ for some $n > 0$, writing its p-adic avatar as $\widehat{\lambda}$,*

$$\frac{\int_C \widehat{\lambda} d\mu}{\Omega_p^{k+j}} = c(\lambda)(1 - \lambda(\overline{\mathfrak{p}}))(1 - \lambda(\mathfrak{p})^{-1} p^{-1}) \frac{L(0, \lambda)}{(2\pi i)^{-j} \Omega_\infty^{k+j}} \in \mathcal{W}[\lambda],$$

where $0 \leq j < k$ and $\mathcal{W}[\lambda]$ is the ring generated over $\mathcal{W}$ by $\lambda(\mathfrak{a})$ for $\mathfrak{a}$ running over all fractional ideals of M prime to p. For the simple constant $c(\lambda)$, see [K] (5.3.0).

6. Anticyclotomic main conjectures

Now we need to work over a totally real field. Fix a totally real field F with integer ring O and a totally imaginary quadratic extension M/F with integer ring R. We suppose that p is unramified in $F/\mathbb{Q}$. Such an M is called a CM field from the time of Shimura–Taniyama. Fix two embeddings $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then each embedding $\sigma \in I = \mathrm{Hom}_{\text{field}}(M, \overline{\mathbb{Q}})$ gives rise to a p-adic absolute value $|x|_{p,\sigma} = |i_p(\sigma(x))|_p$. Let $\Sigma \subset I$ such that $I = \Sigma \sqcup \Sigma c$ for the generator $c \in \mathrm{Gal}(M/F)$ and any p-adic absolute value associated to $\sigma \in \Sigma$ is not induced by elements in Σc. Such a subset exists only if

(ord) every prime factor $\mathfrak{p}$ of p in O splits in R.

In place of CM elliptic curves (E, ω), now we have a CM abelian variety $(X, \omega)_{/\mathcal{W}}$ such that $X(\mathbb{C}) = \mathbb{C}^\Sigma / R^\Sigma$, where $R^\Sigma = \{(i_\infty(\sigma(x)))_{\sigma \in \Sigma}\} \subset \mathbb{C}^\Sigma | x \in R\}$. Here $H^0(X, \Omega_{X/\mathcal{W}}) = (\mathcal{W} \otimes_\mathbb{Z} R)\omega$. At ∞, we have variables $u = (u_\sigma)$ of $\mathbb{C}^\Sigma$. Then $\omega_\infty = du = \sum_\sigma du_\sigma$ satisfies $H^0(X, \Omega_{X/\mathbb{C}}) = (\mathbb{C} \otimes_\mathbb{Z} R) du$. At p, note that Σ gives p-adic places which in turn gives rise to a set of prime ideals $\mathfrak{P}_\sigma$. Let $\mathbf{P}$ be the product of $\mathfrak{P}_\sigma$ for $\sigma \in \Sigma$. Then we can identify $X[\mathbf{P}^\infty]$ with $\mu_{p^\infty} \otimes_\mathbb{Z} O$ over $\mathcal{W}$. This induces an isomorphism of formal groups $i : \widehat{\mathbb{G}}_m \otimes_{\mathbb{Z}} O \cong \widehat{X}$; so, we have $\omega_p = i_*(\frac{dt}{t} \otimes 1)$, which satisfies $H^0(X, \Omega_{X/W}) = (W \otimes_{\mathbb{Z}} R)\omega_p$. Thus we can define $\Omega_p = (\Omega_p^\sigma)_{\sigma \in \Sigma} \in (W^\times)^\Sigma$ and $\Omega_\infty = (\Omega_\infty^\sigma)_{\sigma\in\Sigma} \in (\mathbb{C}^\times)^\Sigma$ by $\omega = \Omega_\infty \omega_\infty$ and $\omega = \Omega_p \omega_p$. For $k = \sum_{\sigma\in\Sigma} k_\sigma \sigma \in \mathbb{Z}[\Sigma]$, we write $\Omega_?^k = \prod_\sigma (\Omega_?^\sigma)^{k_\sigma}$ for $? = \infty, p$. We also write Σ for $\sum_{\sigma\in\Sigma}\sigma$.

Let $Cl(p^n)$ be the ray class group of M modulo p^n and put $C = \varprojlim_n Cl(p^n)$. Then in exactly the same manner as in the proof of Theorem 5.3, Katz proved in [K] the following result.

Theorem 6.1 (N. Katz). *Let the notation and the assumption be as above. Then there exists a measure $d\mu$ on C such that for a Hecke character λ with $\lambda((\alpha)) = \alpha^{-k\Sigma}\alpha^{-\kappa(1-c)}$ with either $0 < k \in \mathbb{Z}$ and $0 \le \kappa \in \mathbb{Z}[\Sigma]$ or $k \le 1$ and $\kappa \ge (1-k)\Sigma$ for $\alpha \equiv 1 \mod p^n$ for some $n > 0$,*

$$\frac{\int_C \widehat{\lambda} d\mu}{\Omega_p^{k\Sigma+2\kappa}} = c(\lambda)\prod_\sigma \left[(1-\lambda(\overline{\mathfrak{P}}_\sigma))(1-\lambda(\mathfrak{P}_\sigma)^{-1}N(\mathfrak{P}_\sigma)^{-1})\right]\frac{L(0,\lambda)}{(2\pi i)^{-\kappa}\Omega_\infty^{k\Sigma+2\kappa}} \in \mathcal{W}[\lambda],$$

where $\mathcal{W}[\lambda]$ is the ring generated over $\mathcal{W}$ by $\lambda(\mathfrak{a})$ for $\mathfrak{a}$ running over all fractional ideals of M prime to p. For the simple constant $c(\lambda)$, see [K] (5.3.0)*.*

We split $C = \Delta \times \mathbf{\Gamma}$ for a finite group Δ and a torsion-free subgroup $\mathbf{\Gamma}$. The group $\mathbf{\Gamma}$ has a natural action of $\mathrm{Gal}(M/F)$. We define $\mathbf{\Gamma}^+ = H^0(\mathrm{Gal}(M/F), \Gamma)$ and $\mathbf{\Gamma}_- = \mathbf{\Gamma}/\mathbf{\Gamma}^+$. Write $\pi_- : C \to \Gamma_-$ and $\pi_\Delta : C \to \Delta$ for the two projections. Take a character $\varphi : \Delta \to W^\times$, and regard it as a character of C through the projection: $C \twoheadrightarrow \Delta$. The Katz measure $d\mu$ on C associated to the CM type Σ as in Theorem 6.1 induces the anticyclotomic φ–branch $d\mu_\varphi^-$ by

$$\int_{\mathbf{\Gamma}_-} \phi d\mu_\varphi^- = \int_C \phi(\pi_-(z))\varphi(\pi_\Delta(z))d\mu(z). \tag{6.1}$$

We write $L_p^-(\varphi)$ for this measure $d\mu_\varphi^-$ regarding it as an element of the algebra $\Lambda^- = W[[\mathbf{\Gamma}_-]]$ made up of measures with values in W.

We look into arithmetic of the unique $\mathbb{Z}_p^{[F:\mathbb{Q}]}$–extension M_∞^- of M on which we have $c\sigma c^{-1} = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(M_\infty^-/M)$ for complex conjugation c. The extension M_∞^-/M is called the anticyclotomic tower over M. Writing $M(p^\infty)$ for the ray class field over M modulo p^∞, we identify C with $\mathrm{Gal}(M(p^\infty)/M)$ via the Artin reciprocity law. Then $\mathrm{Gal}(M(p^\infty)/M_\infty^-) = \Gamma^+ \times \Delta$ and $\mathrm{Gal}(M_\infty^-/M) = \mathbf{\Gamma}_-$. We then define M_Δ by the fixed field of $\mathbf{\Gamma}$ in $M(p^\infty)$; so, $\mathrm{Gal}(M_\Delta/M) = \Delta$. Since φ is a character of Δ, φ factors through $\mathrm{Gal}(M_\infty^- M_\Delta/M)$. Let $L_\infty/M_\infty^- M_\Delta$ be the maximal p–abelian extension unramified outside Σ_p. Each $\gamma \in \mathrm{Gal}(L_\infty/M)$ acts on the normal subgroup $X = \mathrm{Gal}(L_\infty/M_\infty^- M_\Delta)$ continuously by conjugation, and by the commutativity of X, this action factors through $\mathrm{Gal}(M_\Delta M_\infty^-/M)$. Then we look into the $\mathbf{\Gamma}_-$–module: $X[\varphi] = X \otimes_{\Delta,\varphi} W$.

A character φ of Δ is called *anticyclotomic* if $\varphi(c\sigma c^{-1}) = \varphi^{-1}$. If φ is anticyclotomic, then we can find a finite order Hecke character ψ of M such that $\varphi(\sigma) =$

$\psi^{1-c}(\sigma) = \psi(\sigma)\psi(c\sigma c^{-1})^{-1}$. As is well known, $X[\varphi]$ is a Λ^-–module of finite type, and in many cases, it is known to be a torsion module by the work of Taylor–Wiles and K. Fujiwara under the following conditions:

(H0) φ is anticyclotomic.
We choose ψ as above with $\psi^{1-c} = \varphi$.

(H1) The character φ regarded as a Galois character is nontrivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/F[\sqrt{p^*}])$ ($p^* = (-1)^{(p-1)/2}p$). This implies that the representation $\mathrm{Ind}_M^F(\psi \mod \mathfrak{m}_W)$ for the maximal ideal $\mathfrak{m}_W$ of W is absolutely irreducible over $\mathrm{Gal}(\overline{\mathbb{Q}}/F[\sqrt{p^*}])$.

(H2) The character φ regarded as a Galois character is nontrivial on the decomposition group of $\mathfrak{P}$ for all prime factors $\mathfrak{P}|p$ in R.

If one assumes the Σ–Leopoldt conjecture for abelian extensions of M, we know that $X[\varphi]$ is a torsion module over Λ^- always. If $X[\varphi]$ is a torsion Λ^-–module, we can think of the characteristic element $\mathcal{F}^-(\varphi) \in \Lambda^-$ of the module $X[\varphi]$. If $X[\varphi]$ is not of torsion over Λ^-, we simply put $\mathcal{F}^-(\varphi) = 0$. Here is a conjecture made in [HT].

Conjecture 6.2. *The Λ^--module $X[\varphi]$ is a torsion module, and $\mathcal{F}^-(\varphi) = L_p^-(\varphi)$ up to units in Λ^-.*

A Hilbert modular Hecke eigenform θ is called of CM-type by R if its p-adic Galois representation is isomorphic to $\mathrm{Ind}_M^K \widehat{\lambda}$ for a Hecke character λ of M. For the character $\widehat{\lambda}$, we define its Teichmüller projection by $\psi_\lambda = \lim_{n\to\infty} \widehat{\lambda}^{p^{nf}}$, where f is the residual degree of the maximal ideal of $\mathbb{Z}_p[\lambda]$.

The proof of this conjecture under (H0–2) boils down to the following statement:

Proposition 6.3. *Let θ be a CM Hecke eigenform whose Galois representation is isomorphic to* $\mathrm{Ind}_M^F \widehat{\lambda}$ *for $\kappa = 0$ and $k = 1$. Define $\varphi(\sigma) = \psi_\lambda(\sigma)\psi_\lambda(c\sigma c^{-1})^{-1}$. Under* (H0–2)*, if for any $\mathcal{W}$-integral Hilbert modular form of p-power level with the same weight* 2*, the same level and the same Neben character as θ, the Petersson inner product $\frac{W(\lambda^{1-c})(\theta,f)}{(2\pi i)^{-2\Sigma}\Omega_\infty^{2\Sigma}}$ is p-integral, then* Conjecture 6.2 *follows for φ, where $W(\lambda^{1-c})$ is the Gauss sum of λ^{1-c}.*

This follows from a detailed analysis of the congruence number of θ and the size of the Selmer group of λ^{1-c}. We admit this fact. See [H05b] and [H05c].

7. Petersson inner product

For each fractional ideal $\mathfrak{c}$, we need to consider

$$\Gamma_0(p^n, \mathfrak{c}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(O) \middle| c \in p^n(\mathfrak{c}^*)^{-1}, a, d \in O\ b \in \mathfrak{c}^* \right\},$$

where $\mathfrak{c}^* = \{x \in F | \mathrm{Tr}_{F/\mathbb{Q}}(x\mathfrak{c}) \subset \mathbb{Z}\}$. We write $\Gamma_0(p^n)$ for $\Gamma_0(p^n, O)$. Then Hilbert modular Hecke operators $T(\mathfrak{n})$ acts on the product $\bigoplus_{\mathfrak{c}} G_2(\Gamma_0(p^n, \mathfrak{c}), \varepsilon; R)$ (for a Neben character ε modulo p^n) taken over $\mathfrak{c}$ running in a complete representative set for the strict ideal classes of F. To make things simple, we just assume that the strict class number of F is trivial so that we have $G_2(p^n,\varepsilon;R) = G_2(\Gamma_0(p^n),\varepsilon;R)$. A modular form $f \in G_2(p^n,\varepsilon;\mathbb{C}))$ has q-expansion of the following form:

$$f(q) = a(0,f) + \sum_{0\neq\xi\in F} a(\xi,f)q^{\xi},$$

where $q^{\xi} = \exp(2\pi i\mathrm{Tr}(\xi z))$. Here $a(\xi,f) = 0$ if $0 \neq \xi$ is not in $F_+^{\times} \cap O$. Also $f \in G_2(p^n,\varepsilon;R) \iff a(\xi,f) \in R$ for all ξ. The inner product is given by

$$(\theta,f) = \int_{\Gamma_0(p^n)\backslash\mathfrak{H}^I} \overline{\theta(z)}f(z)dxdy.$$

To study the p-integrality of (θ,f), we consider the Shimura series defined in the following way: Let $(z,w) \in \mathfrak{H}^I \times \mathfrak{H}^I$ and $v \in M_2(F)$. Put

$$[v;z,w] = ((w_\sigma,1)^t\sigma(v)\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\left(\begin{smallmatrix}z_\sigma\\1\end{smallmatrix}\right))_\sigma$$

as a tuple of numbers indexed by $\sigma \in I$. Then define $[v;z,w]^k = \prod_\sigma[\sigma(v);z_\sigma,w_\sigma]^k$. Take a locally constant compactly supported function $\phi : M_2(F_{\mathbb{A}}^{(\infty)}) \to \mathcal{W}$ with $\phi(\varepsilon x) = \phi(x)$ for $\varepsilon \in O_+^{\times}$. Then the Shimura series for $GL(2)\times GL(2)$ is defined for $0 < k \in \mathbb{Z}$ in [S1] II (4.11) by

$$\begin{aligned}(7.1)\quad H(z,w;s) &= H_k(z,w;s;\phi,g)\\ &= \sum_{0\neq\alpha\in M_2(F)/O_+^{\times}} \phi(\alpha)a(-\det(\alpha),g)[\alpha;z,w]^{-k}\left|[\alpha;z,w]\right|^{-2s}\end{aligned}$$

for $(z,w) \in \mathfrak{H}^I \times \mathfrak{H}^I$. Here g is a Hilbert modular in $G_\ell(\Gamma_0(p^n),\varepsilon)$. The following facts are known (see [S1], [H05b] and [H05c]):

- (S0) This series is a generalization of Eisenstein series, because if we take $g = 1$ (so $\ell = 0$), the series gives an Eisenstein series for $GL(2)\times GL(2)$ over F.
- (S1) The series (7.1) converges absolutely and locally uniformly with respect to all variables s,z,w if $\mathrm{Re}(s) \gg 0$ and can be continued meromorphically to the whole $s \in \mathbb{C}$.
- (S2) Choose $z_0 \in \mathfrak{H}^I \cap M^{\Sigma}$ on which (X,i,ω) sits. Define $\rho : M \to M_2(F)$ by $\rho(\alpha)\left(\begin{smallmatrix}z_0\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}z_0\alpha\\\alpha\end{smallmatrix}\right)$. We can find $b \in M_2(F)$ such that $M \oplus M = M \otimes_F M \cong M_2(F)$ by $\alpha\otimes\beta \mapsto \rho(\alpha)v\rho(\beta^c)$. Take $\phi_L,\phi_R : M \to \mathcal{W}$ (locally constant compactly supported functions), and define $\phi = \phi_L \otimes \phi_R : M_2(F) \to \mathcal{W}$. Then if $\ell = k$, $H_k(z,w;s;\phi,g)$ has a pole of order ≤ 1 at $s = 1$. Define $\phi_{k,L}(\alpha) = \alpha^{k\Sigma}\phi(\alpha)$. Then $\mathrm{Res}_{s=1}H_k(z_0,z_0;s;\phi,g) \sim (\theta(\phi_{k,L}),g\theta(\phi_R))$.
- (S3) Define $\Psi_g(z,w) = c\cdot\mathrm{Res}_{s=1}H_k(z,w;s;\phi,g)$ for a suitable normalization constant (which is a p-adic unit). Then this modular form has the following q-expansion for $q = \exp(2\pi z)$

$$\Psi_g(z,w) = \sum_{\alpha\in\Gamma_0(p^n)\backslash M_2(F),\det(\alpha)\gg 0} \phi^*(\epsilon\alpha)q^{\det(\alpha)}g|_k\alpha(w),$$

where ϕ^* is the partial Fourier transform with respect to (a,b) for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(F_{\mathbb{A}}^{(\infty)})$. Thus "basically" Ψ_g is integral if ϕ^* is integral and if the p-component of ϕ^* has support in the Eichler order of conductor p^n.

Choosing ϕ_L well, we may assume that $\theta(\phi_{1,L}) = \theta$ (the CM Hecke eigenform associated to λ). Thus if all $\mathcal{W}$-integral form f of weight 2 with character ε is an integral linear combination of $\theta(\phi_R)g$ moving around g and ϕ_R, we get the integrality as in the proposition.

If $[F:\mathbb{Q}]$ is even, we have a definite quaternion algebra everywhere unramified at finite place. Thus we can embed $M \hookrightarrow B$ and split $B = M \oplus M$ as above. Every modular form is a "rational" linear combination of theta series of B (the Jacquet-Langlands correspondence). Thus every weight 2 modular forms is a linear combination of $\theta(\phi_1)\theta(\phi_2)$ for $\phi_j : M \to \mathcal{W}$, and we may take $\phi_R = \phi_1$ and $g = \theta(\phi_2)$. Thus we need to prove $\mathcal{W}$-integrality of the Jacquet-Langlands correspondence. This can be done under (H0–2). So we get the p-integrality of (θ, f) under suitable assumptions if $[F:\mathbb{Q}]$ is even. In fact, by a base-change argument, the anticyclotomic conjecture can be proven for any F unramified at p under (H0–2) as long as $p \geq 5$. All the details of the above argument can be found in [H05c].

References

Books

[AME] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Math. Studies **108**, Princeton University Press, Princeton, NJ, 1985.

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.

[HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, Oxford University Press, In press

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, and Iwanami Shoten, Tokyo, 1971.

[LFE] H. Hida, *Elementary Theory of L-Functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, England, 1993.

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.

[MFM] T. Miyake, *Modular Forms*, Springer, New York-Tokyo, 1989.

[PAF] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, 2004, Springer

Articles

[H05a] H. Hida, The integral basis problem of Eichler, IMRN **2005:34** (2005), 2101–2122

[H05b] H. Hida, Non-vanishing modulo p of Hecke L-values and application, to appear in the Durham symposium proceedings, 2005 (downloadable at www.math.ucla.edu/~hida)

[H05c] H. Hida, Anticyclotomic main conjectures, preprint, 2004, (downloadable at `www.math.ucla.edu/~hida`)

[HT] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, Inventiones Math. **117** (1994), 89–147

[K] N. M. Katz, p-adic L-functions for CM fields, Inventiones Math. **49** (1978), 199–297.

[S] G. Shimura, On some arithmetic properties of modular forms of one and several variables, Ann. of Math. **102** (1975), 491–515 ([75c] in vol. II of the collected works)

[S1] G. Shimura, On certain zeta functions attached to two Hilbert modular forms: I. The case of Hecke characters, II. The case of automorphic forms on a quaternion algebra, I: Ann. of Math. **114** (1981), 127–164; II: ibid. 569–607 ([81b–c] in vol. III of the collected works).