2. Lecture 2: Values of modular forms at CM points

To extend the result of the previous section to Hecke L-values of imaginary quadratic fields, we recall modular forms and CM periods.

2.1. 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 this can be generalized to Hilbert modular case and beyond (see [AAF]). 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 $\wp$-functions

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

and $y = \frac{dx}{du}$, where $g_2(w) = 60 \sum_{0 \neq l \in L_w} l^{-4}$ and $g_3(w) = 140 \sum_{0 \neq l \in L_w} l^{-6}$. 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

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

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 $\phi_{can,N} : \mu_N \hookrightarrow \mathrm{Tate}(q)[N]$. 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 $(E, \phi_N : \mu_N \hookrightarrow E[N], \omega)$ satisfying

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

The space of modular forms will be written as $G_k(N;B) = G_k(\Gamma_1(N);B)$. 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 $p \geq 5$ and a positive integer N prime to p. 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 $V(B) = V_{\Gamma_1(N)}(B)$ is a collection of rules f assigning a value $f((E,\phi_p : \mu_{p^\infty} \hookrightarrow E[p^\infty], \phi_N)_{/A}) \in A$ for p-adic B-algebras A satisfying the following condition:

- (V0) f assigns a value $f((E,\phi_p,\phi_N)_{/A}) \in A$ for any couple $(E,\phi_p,\phi_N)_{/A}$ defined over a p-adic B-algebra A. Here A is also a variable.
- (V1) $f((E,\phi_p,\phi_N)_{/A}) \in A$ depends only on the isomorphism class of $(E,\phi_p,\phi_N)_{/A}$.

(V2) If $\varphi : A \to A'$ is an B-algebra homomorphism continuous under the p-adic topology, we have $f((E, \phi_p, \phi_N)_A \otimes A') = \varphi(f((E, \phi_p, \phi_N)_{/A})$.

(V3) $f(q) = f((\mathrm{Tate}(q), \phi_{can,p}, \alpha \circ \phi_{can,N})_{/B[[q^{1/N}]][q^{-1/N}]}) \in B[[q^{1/N}]]$. for any automorphism $\alpha \in \mathrm{Aut}_{\text{gp scheme}}(\mathrm{Tate}(q)[N]_{/B[[q^{1/N}]][q^{-1/N}]})$.

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 $\widehat{\mathbb{G}}_{m/\mathbb{Z}_p} = \mathrm{Spf}(\varprojlim_n \mathbb{Z}_p[t, t^{-1}]/(t^n - 1))$, $\phi_p : \mu_{p^\infty} \hookrightarrow E$ induces an identification $\widehat{\phi}_p : \widehat{\mathbb{G}}_m \cong \widehat{E} = \varprojlim_n E[p^n]^\circ$. Since $\widehat{\mathbb{G}}_m$ has a canonical differential $\frac{dt}{t}$, $\widehat{\phi}_p$ induces a nowhere vanishing differential $\omega_p = \widehat{\phi}_{p,*}\frac{dt}{t}$. Thus $f \in G_k(p^n; B)$ can be regarded as a p-adic modular form by $f((E, \phi_p, \phi_N)_{/A}) = f(E, \phi_p|_{\mu_{p^n}}, \phi_N, \omega_p) \in A$. 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 $G_k(Np^n; B)$. In particular, $G_k(Np^n; B) \to V(B)$ is an injection, and functions in the image satisfies $f(E, a \cdot \phi_p, \phi_N) = a^{-k} f(E, \phi_p, \phi_N)$ 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 $B[[q]] \iff f_n((E, \phi_p, \phi_N))/A)$ converges p-adically for all $(E, \phi_p, \phi_N))/A$ and all p-adic B-algebra A.

(Q2) If B_0 is a $\mathbb{Z}[\frac{1}{6}]$-algebra p-adically dense in B, $G_k(Np^\infty; B_0) = \bigcup_n G_k(Np^n; B_0)$ is p-adically 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 an order $\mathfrak{O}'$ of the integer ring $\mathfrak{O}$ of an imaginary quadratic field $M \subset \mathbb{C}$. An order of $\mathfrak{O}$ means a subring of finite index. If $E(\mathbb{C}) = \mathbb{C}/L_w$ has complex multiplication, for $\mathfrak{O}' = \{\alpha \in M | \alpha \cdot L_w \subset L_w\}$, $\mathfrak{O}' \cdot L_w \subset L_w$, 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 $\mathfrak{O}'$. Then by the finiteness of isomorphism class over $\mathbb{C}$ of CM elliptic curves, E is defined over a number field K, and by a result of Serre–Tate E is defined over a valuation ring $\mathfrak{V} \subset \mathcal{W}$ of K of residual characteristic p.

For an ideal $\mathfrak{m} \subset \mathfrak{O}'$, we can think of the kernel of multiplication by $\mathfrak{m}$:

$$E[\mathfrak{m}](A) = \{x \in E(A) | \mathfrak{m}x = 0\} = \bigcap_{\alpha \in \mathfrak{m}} E[\alpha](A).$$

For the moment, we suppose further p splits into a product of two primes $\mathfrak{p}\overline{\mathfrak{p}}$ in $\mathfrak{O}'$ (so $\mathfrak{O}_p = \mathfrak{O}'_p$). Let $E[\mathfrak{p}^\infty] = \bigcup_n E[\mathfrak{p}^n]$. Then we may assume that $E[\mathfrak{p}^\infty]_{/\mathfrak{V}}$ is isomorphic to μ_{p^∞} after extending scalar to the strict henselization $\mathcal{W} \subset \overline{\mathbb{Q}}$ of $\mathfrak{V}$; so, we have $\phi = \phi_p : \mu_{p^\infty} \cong E[\mathfrak{p}^\infty]$. If $p = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathfrak{O}$ but not in $\mathfrak{O}'$ (so, $\mathfrak{O}'$ is an order of conductor divisible by p), we just assume that E has an isogeny $E' \xrightarrow{\pi} E$ defined over $\mathcal{W}$ such that E' has complex multiplication by $\mathfrak{O}$ and $\mathrm{Ker}(\pi) \cap E'[\mathfrak{p}^\infty] = 0$. Under this setting, $\phi' : \mu_{p^\infty} \cong E'[\mathfrak{p}^\infty]$ induces $\phi = \phi_p = \pi \circ \phi'_p : \mu_{p^\infty} \hookrightarrow E[p^\infty]$. We study later in details the sheaf $\Omega_{E/\mathcal{W}}$ of differentials on the scheme E. An important point is that its global sections $H^0(E, \Omega_{E/\mathcal{W}})$ is a free $\mathcal{W}$-module of rank 1. Pick $\omega \in H^0(E, \Omega_{E/\mathcal{W}})$ so that $H^0(E, \Omega_{E/\mathcal{W}}) = \mathcal{W}\omega$. As explained above, we fix two embeddings $\phi_p : \mu_{p^\infty/\mathcal{W}} \hookrightarrow E[p^\infty]_{/\mathcal{W}}$ and $E(\mathbb{C}) = \mathbb{C}/i_\infty(\mathfrak{a})$ for a fractional ideal $\mathfrak{a} \supset \mathfrak{O}'$. In this case, we write $E = E(\mathfrak{a})$. 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

$$\omega = \Omega_\infty du = \Omega_p \widehat{\phi}_{p,*}\frac{dt}{t}.$$

We have the following fact basically from definition:

Theorem 2.1. *Let $f \in G_k(\Gamma_1(Np^n); \mathcal{W})$. Write $f_p \in V_{\Gamma_1(N)}(W)$ (resp. $f_\infty \in G_k(\Gamma_1(Np^n); \mathbb{C})$) the corresponding p-adic modular form (resp. the corresponding holomorphic modular form). If $(E = E(\mathfrak{a}), \omega)_{/\mathcal{W}}$ has complex multiplication by $\mathfrak{O}$ in which p splits, we have*

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

The theorem is stated for modular forms on $\Gamma_1(Np^n)$ though we only explained those of level $\Gamma_1(p^r)$.

Remark 2.2. Replacing $\mathcal{W}$ by its quotient field, the assertion of the theorem is valid if $f = \frac{h}{g}$ finite at (E, ϕ_N, du) for $h \in G_{k+k'}(\Gamma_1(Np^n); \mathcal{W})$ and $g \in G_{k'}(\Gamma_1(Np^n); \mathcal{W})$ for an obvious reason.

Remark 2.3. To have well defined p-adic period Ω_p, a key point here is to have a canonical $\phi_p : \mu_{p^\infty} \hookrightarrow E[p^\infty]$ for a CM elliptic curve E not E having multiplication by the full integer ring $\mathfrak{O}$. Indeed, we give a canonical ϕ_p even if $E(\mathbb{C}) = \mathbb{C}/i_\infty(\mathfrak{a})$ for a lattice $\mathfrak{a}$ in M with $\mathfrak{a}_p$

not equal to $\mathfrak{O}_p$. Then the above theorem is valid intact over a finite extension $\mathcal{W}'/\mathcal{W}$ for such $E(\mathfrak{a})$ defined over $\mathcal{W}'$ as is clear form the proof. The minimum ring $\mathcal{W}'$ is given by $\mathcal{W}[\mu_{p^n}]$ for n depending on how far $\mathfrak{a}_p$ differs from $\mathfrak{O}_p$. So we state the result afterward including $E(\mathfrak{a})$.

2.2. **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 $k \in \mathbb{Z}$:

$$\delta_k = \frac{1}{2\pi\sqrt{-1}}\left(\frac{\partial}{\partial z} + \frac{k}{2y\sqrt{-1}}\right) \quad \text{and} \quad \delta_k^r = \delta_{k+2r-2}\cdots\delta_k, \tag{2.1}$$

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

Exercise 2.4. *Show the following formulas:*

(1) $\delta_{k+l}(fg) = g\delta_k f + f\delta_l g$.
(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 $f \in G_k(\Gamma_1(N);\mathbb{C})$, $\delta_k^r(f)$ 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. Here we call $z \in \mathfrak{H}$ a *CM point* if $z \in \mathfrak{H} \cap i_\infty(M)$ for an imaginary quadratic field M. Then $\mathfrak{a} = i_\infty^{-1}(\mathbb{Z}+\mathbb{Z}z) \subset M$ is a lattice, and we have a CM elliptic curve $E(\mathfrak{a})$ with multiplication by $\mathfrak{O}(\mathfrak{a}) = \{\alpha \in M | \alpha\mathfrak{a} \subset \mathfrak{a}\}$ as in Remark 2.3. We shall describe the rationality. Here is the rationality result of Shimura [Sh75]:

Theorem 2.5 (G. Shimura)**.** *Let the notation be as above; in particular, z is a CM point of $\mathfrak{H}$. For $f \in G_k(\Gamma_1(N);\overline{\mathbb{Q}})$, we have*

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

In this theorem, z is just a CM point, and it is nothing to do with the prime p we have chosen. Thus we do not need to assume that the prime p split in the imaginary quadraric field $M = \mathbb{Q}[z]$.

Proof. We follow the argument of Shimura in [Sh75]. Since

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

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 $\alpha \in M \setminus \mathbb{Q}$. 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 $f|_k\rho(\alpha) = fh$ (putting $h = (f|_k\rho(\alpha))/f$), by Exercise 2.4, we have $(\delta_k f)|_{k+2}\rho(\alpha) = (\delta_k f)h + f(\delta_0 h)$. Specializing this equality at z and assuming $\det(\rho(\alpha)) = N(\alpha) = 1$, 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 $h(z) = (f|_k\rho(\alpha))(z)/f(z) = \alpha^{-k}$. As $\alpha^2 \neq 1$, 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, $\delta_k^r(fh) = \sum_{0 \leq s \leq r} \binom{r}{s} \delta_k^s f \delta_0^{r-s} h$. Form this we get

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

Evaluating this at z, we finally get

$$(\delta_k^r f)(z) = \alpha^k(\alpha^{-2r} - 1)^{-1} \sum_{0 < s \leq r} \binom{r}{s} (\delta_k^{r-s} f)(z)(\delta_0^s h)(z). \tag{2.2}$$

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 2.6. Choosing $g \in G_{k+2r}(\Gamma_1(N); \mathcal{W})$ with $g(z) \neq 0$ under the notation of the above proof, Shimura actually proved in [Sh75] 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 2.7. For a given $f \in G_k(\Gamma_1(N);\overline{\mathbb{Q}})$ 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 an isobaric polynomial Q_j with coefficients in $\overline{\mathbb{Q}}$. If (E,ω) is defined by $y^2 = 4x^3 - g_2(E,\omega)x - g_3(E,\omega)$, $f(E,\phi_N,\phi_p,\omega)$ 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 $f(E,\phi_N,\phi_p,\omega)$. Once we know the value $f(E,\phi_N,\phi_p,\omega) = \frac{f(E,\phi_N,du)}{\Omega_\infty^k}$, we can then compute $\frac{\delta_k^r(f(z))}{\Omega_\infty^{k+2r}}$ following the above proof (in particular, the induction process).

2.3. ***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 $f \in G_k(\Gamma_1(N);\mathcal{W}) \subset G_k(\Gamma_1(N);\mathbb{C})$. 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 2.8. *Prove* $(\phi^*)^*(x) = p^r\phi(-x)$.

We define

$$f|\phi(z) = p^{-r} \sum_{u \mod \mathbb{Z}/p^r\mathbb{Z}} \phi^*(-u) f(z + \frac{u}{p^r}). \tag{2.3}$$

Then we have $(\sum_n a_n q^n)|\phi) = \sum_n \phi(n) a_n q^n \in G_k(\Gamma_1(Np^{2r});\mathcal{W})$.

Exercise 2.9. *Define* $\phi|x(u) = \phi(xu)$ *for* $x \in (\mathbb{Z}/p^r\mathbb{Z})^\times$. *For* $f \in G_k(\Gamma_1(N);\mathbb{C})$, *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* $f|\phi \in G_k(\Gamma_1(N);\mathbb{C})$.

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 limit principle, $G_k(p^\infty;\mathcal{W})$ is dense in $V(W)$, we have a unique $df \in V(W)$. Thus $d^r f(E, \widehat{\phi}_{p,*}\frac{dt}{t}) \in W$ is well defined. The effect of d^r on the q–expansion of a modular form is given by

$$d^r \sum_n a(n)q^n = \sum_n a(n)n^r q^n. \tag{2.4}$$

We can let $a \in \mathbb{Z}_p^\times$ acts on $f \in V(R)$ by

$$f|a(E,\phi_N,\phi_p) = f|\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right)(E,\phi_N,\phi_p) = f(E, a\cdot\phi_p).$$

Lemma 2.10. *If $f \in G_k(\Gamma_1(N);\mathcal{W})$, then we have*

$$(d^r f)|\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right) = a^{-k-2r}(d^r f) \quad \textit{for } a \in \mathbb{Z}_p^\times.$$

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 2.9,

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

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

The above action of a (or $g \in T_1(\mathbb{Z}_p)$) is the local one concentrated at p (as ϕ_N is intact), where $T_1(A)$ is the subgroup of $SL_2(A)$ made of diagonal matrices for any ring A. We have a global action $f \mapsto f|\gamma$ for $\gamma \in G(\mathbb{Z}_{(p)})$. Since γ change the level structure ϕ_N, the definition is more involved. For that, we actually need to extend level structure to the prime-to-p Tate module $\eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong V^{(p)}(E) = \left(\varprojlim_{p\nmid m} E[m]\right)\otimes_{\mathbb{Z}}\mathbb{Q}$ so that we can let γ act by $\eta^{(p)} \mapsto \eta^{(p)}\circ\gamma$. This is tantamount to introducing the structure of Shimura curve. Define

$$(d^r f)|\rho(\alpha)(E,\phi_p,\eta^{(p)}) := (d^r f)(E,\phi_p\circ\alpha_{\mathfrak{p}},\eta^{(p)}\circ\rho^{(p)}(\alpha)).$$

Here we just note the following fact:

Lemma 2.11. *Recall an elliptic curve $E(\mathfrak{a})$ with complex multiplication by an imaginary quadratic field M in which p splits into $(p) = \mathfrak{p}\overline{\mathfrak{p}}$. Define $\rho : \mathfrak{O}_{(p)}^\times \hookrightarrow G(\mathbb{Z}_p\times\mathbb{A}^{(p\infty)})$ by $\alpha^{(p)}\circ\eta^{(p)} = \eta^{(p)}\circ\rho(\alpha)$ and $\rho_p(\alpha) = \begin{pmatrix} \alpha_{\mathfrak{p}} & 0 \\ 0 & \alpha_{\overline{\mathfrak{p}}}\end{pmatrix}$. Then for $f \in G_k(\Gamma_1(Np^m);\mathcal{W})$, if $N(\alpha) = 1$, we have $d(f|\rho(\alpha)) = \alpha_{\mathfrak{p}}^2(df|\rho(\alpha))$ and*

$$((d^r f)|\rho(\alpha))(E(\mathfrak{a}),\phi_p,\eta^{(p)}) = \alpha_{\mathfrak{p}}^{-k-2r}\cdot d^r f(E(\mathfrak{a}),\phi_p,\eta^{(p)}).$$

Proof. By deformation theory of $E(\mathfrak{a})$, the differential operator d commutes with the action $\eta^{(p)} \mapsto \eta^{(p)}\circ g$ for $g \in SL_2(\mathbb{A}^{(p\infty)})$. Then the effect of d on the operation $f \mapsto f|\rho(\alpha)$ can be computed by Lemma 2.10. Note that $(E(\mathfrak{a}),\phi_p\circ\alpha_{\mathfrak{p}},\eta^{(p)}\circ\rho^{(p)}(\alpha)) \cong (E(\mathfrak{a}),\phi_p,\eta^{(p)})$ by complex multiplication. $\square$

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 [K78a]). 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 [K78a] (2.6.7) is as follows.

Theorem 2.12 (N. Katz)**.** *Let the notation and the assumption be as in* Theorem 2.1*; in particular, $E(\mathfrak{a})_{/\mathcal{W}'}$ is a CM elliptic curve associated to a lattice $\mathfrak{a} \subset M$ for an imaginary quadratic field M in which p splits, where $\mathcal{W}'$ is a discrete valuation ring finite flat over $\mathcal{W}$ over which $E(\mathfrak{a})$ is defined. For $f \in G_k(p^n; \mathcal{W}')$, we have*

$$\text{(K)} \qquad \frac{(d^r f)(E(\mathfrak{a}), \phi_N, \phi_p)}{\Omega_p^{k+2r}} = \frac{(\delta_k^r f)(E(\mathfrak{a}), \phi_N, du)}{\Omega_\infty^{k+2r}} \in \mathcal{W}'.$$

If $\mathfrak{a}$ is a fractional ideal of $\mathfrak{O}$, we can take $\mathcal{W}' = \mathcal{W}$ as explained earlier. We can always find a nowhere vanishing differential ω in $\Omega_{E(\mathfrak{a})/\mathcal{W}'}$ as $\mathcal{W}'$ is a discrete valuation ring, and as before $\omega = \Omega_p \widehat{\phi}_{p,*} \frac{dt}{t}$. We give here a proof similar to the argument which proves Theorem 2.5.

Proof. We use the notation introduced in the proof of Theorem 2.5; so, $\mathfrak{a} = i_\infty^{-1}(\mathbb{Z} + \mathbb{Z}z)$ for $z \in \mathfrak{H}$. We take $\pm 1 \neq \alpha \in M^\times$) with $\alpha\overline{\alpha} = 1$. Let $E = E(\mathfrak{a})$.

After identifying algebro-geometric forms and analytic ones by q-expansions via the fixed two embeddings $\mathbb{C}_p \xleftarrow{i_p} \mathcal{W}' \xrightarrow{i_\infty} \mathbb{C}$, we see that $d = \frac{1}{2\pi i}\frac{\partial}{\partial z}$. We write $\mathcal{A} = \mathcal{A}(N; \overline{\mathbb{Q}}) = \bigcup_k \{\frac{f}{g} | f, g \in G_k(\Gamma_1(N); \overline{\mathbb{Q}})\}$. 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 $g_1 \in G_{k+2}(\Gamma_1(N); \mathcal{W}')$ and $g_2 \in G_k(\Gamma_1(N); \mathcal{W}')$ for sufficiently large k, we have (Remark 2.2)

$$\text{(2.5)} \qquad \frac{(dh)(E, \phi_N, \widehat{\phi}_{p,*}\frac{dt}{t})}{\Omega_p^2} = (dh)(E, \phi_N, \omega) \in \overline{\mathbb{Q}}.$$

Since $\frac{f(E, \widehat{\phi}_{p,*}\frac{dt}{t})}{\Omega_p^k} = f(E, \phi_N, , \omega) \in \mathcal{W}'$, we first show

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

by induction on r. When $r = 0$, this follows from Theorem 2.1. To treat $r > 0$, take $f \in G_k(\Gamma_1(N); \mathcal{W}')$, and define $h \in \mathcal{A}$ by $f|_k\rho(\alpha) = fh$ as in the proof of Theorem 2.5.

Apply d to $f|_k\rho(\alpha) = fh$, we have $(df)|_{k+2}\rho(\alpha) = (df)h + f(dh)$. Specializing this equality at (E, ϕ_N, ω), we get from Lemma 2.11

$$\begin{aligned}\alpha^{-k-2}(df(E, \phi_N, \phi_p)) &= ((df)|_{k+2}\rho(\alpha))(E, \phi_N, \phi_p)\\ &= (df)(E, \phi_N, \phi_p)h(E) + f(E, \phi_N, \phi_p)(dh)(E, \phi_N, \phi_p).\end{aligned}$$

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

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

Thus we have again proved $\frac{dh(E,\phi_N,\widehat{\phi}_{p,*}\frac{dt}{t}))}{\Omega_p^2} \in \overline{\mathbb{Q}}$, 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, ϕ_N, ϕ_p), we get for $C = \frac{\alpha^k}{(\alpha^{-2r}-1)}$

$$(d^r f)(E, \phi_N, \phi_p) = C \cdot \sum_{0<s\le r} \binom{r}{s} (d^{r-s}f)(E, \phi_N, \phi_p)(d^s h)(E, \phi_N, \phi_p).$$

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

$$\frac{(d^r f)(E, \phi_N, \phi_p)}{\Omega_p^{k+2r}} = C \cdot \sum_{0<s\le r} \binom{r}{s} \frac{(d^{r-s}f)(E, \phi_N, \phi_p)}{\Omega_p^{k+2r-2s}} \frac{(d^s h)(E, \phi_N, \phi_p)}{\Omega_p^{2s}}.$$

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

$$\begin{aligned}\frac{(d^{r-s}f)(E, \phi_N, \phi_p)}{\Omega_p^{k+2r-2s}} &= \frac{(\delta_k^{r-s}f)(E, \phi_N, du)}{\Omega_\infty^{k+2r-2s}},\\ \frac{(d^s h)(E, \phi_N, \phi_p)}{\Omega_p^{2s}} &= \frac{(d^{s-1}dh)(E, \phi_N, \phi_p)}{\Omega_p^{2s}} = \frac{(\delta_2^{s-1}dh)(E, \phi_N, du)}{\Omega_\infty^{2s}}.\end{aligned}$$

Replacing each term as above by the corresponding archimedean term, we recover the right-hand-side of (2.2) divided by Ω_∞^{k+2r}. Then by the induction hypothesis, we get the desired identity:

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

inside $\overline{\mathbb{Q}}$. Since the left-hand-side of the above identity is in the completion W' of $i_p(\mathcal{W}')$ in $\mathbb{C}_p$, we conclude the identity in $\mathcal{W}' = i_p^{-1}(W')$. $\square$

Remark 2.13. We note that this process of proving algebraicity and p-integrality applies to Hilbert modular forms and beyond after an appropriate adjustment (as Shimura's argument proving Theorem 2.5 has been generalized to unitary/symplectic Shimura varieties by himself in [AAF] Chapter III). Therefore, the use of Gauss–Manin connection to study this type of algebraicity is not necessary (though is more conceptual). In particular, if $\mathfrak{a}_p \neq \mathfrak{O}_p$, the proof via Gauss–Manin connection is more involved, because one needs to make scalar extension of the ring of definition of $E(\mathfrak{O})$ to split the Hodge-filtration on $H^1_{DR}(E(\mathfrak{a}))$ in an appropriate manner (see [K78a] (2.4.2)). We note that [K78a] does cover the case $\mathfrak{a}_p \neq \mathfrak{O}_p$.