* Big Galois representations and p-adic L-functions First lecture

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

June 17 2011

*A 105 minutes talk at Université de Paris Nord. The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949 and by Clay Mathematics institute as a senior scholar.

We have Galois representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\Lambda)$ for $\Lambda = \mathbb{Z}_p[[T]]$ associated to p-adic analytic families of Hecke eigen cusp forms.

Supposing that ρ does not have abelian image over $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ for any quadratic field $M/\mathbb{Q}$ (non CM condition), we want to show that the image $\mathrm{Im}(\rho)$ is big!

Under some mild conditions, we prove that

- $\mathrm{Im}(\rho) \supset \{x \in SL_2(\Lambda) | x \equiv 1 \mod \mathfrak{c}\} =: \Gamma(\mathfrak{c})$ for a Λ-ideal $\mathfrak{c} \neq 0$. Taking this $\mathfrak{c}$ as large as possible, we call $\mathfrak{c}$ the conductor of ρ.

- Taking the reflexive closure $\bigcap_{(\lambda)\supset\mathfrak{c}}(\lambda)$ which is a principal ideal (L), we want to determine (L). We ask:

  Is L related to a p-adic L-function?

§1. Notation

To define the family $\mathcal{F}$ we study, we introduce some notation. Fix

- An odd prime $p \geq 5$;
- a positive cube-free integer N $(p \nmid N)$;
- two field embeddings $\mathbb{C} \hookleftarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Consider the space of cusp form

$$S_{k+1,\psi} = S_{k+1}(\Gamma_0(Np^{r+1}), \psi) \quad (r \geq 0)$$

of weight "$k+1$" with Nebentypus ψ.

Let the rings

$$\mathbb{Z}[\psi] \subset \mathbb{C} \text{ and } \mathbb{Z}_p[\psi] \subset \overline{\mathbb{Q}}_p$$

be generated by $\psi(n)$ $(n = 1, 2, \dots)$ over $\mathbb{Z}$ and $\mathbb{Z}_p$.

The Hecke algebra over $\mathbb{Z}$ is

$$h = \mathbb{Z}[\psi][T(n)|n = 1, 2, \cdots] \subset \mathrm{End}(S_{k+1,\psi}).$$

Put $h_{k+1,\psi} = h \otimes_{\mathbb{Z}[\psi]} \mathbb{Z}_p[\psi]$.

Sometimes our $T(p)$ is written as $U(p)$ as the level is divisible by p.

§2. Big Hecke algebra

The ordinary part $h^{ord}_{k+1,\psi} \subset h_{k+1,\psi}$ is the **maximal ring direct summand** on which $U(p)$ is invertible; so,

$$h^{ord} = e \cdot h \quad \text{for} \quad e = \lim_{n\to\infty} U(p)^{n!}.$$

Let $\psi_1 = \psi_N \times$the tame p-part of ψ. Then, we have a unique 'big' Hecke algebra $\mathbf{h} = \mathbf{h}_{\psi_1}$ such that

- $\mathbf{h}$ is free of finite rank over $\mathbb{Z}_p[[T]]$ with

$T(n) \in \mathbf{h}$ $(n = 1, 2, \ldots;\ T(p) = U(p))$

- Let $\gamma = 1 + p$. If $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$

is a character,

$$\mathbf{h}/(1 + T - \psi(\gamma)\varepsilon(\gamma)\gamma^k)\mathbf{h} \cong h^{ord}_{k+1,\varepsilon\psi_k}$$

for $\psi_k := \psi_1\omega^{1-k}$, sending $T(n)$ to $T(n)$, where ω is the Teichmüller character.

§3. Galois representation

Each **irreducible component**

$$\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$$

with normalization $\mathrm{Spec}(\widetilde{\mathbb{I}})$ has a **Galois representation**

$$\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\widetilde{\mathbb{I}})$$

with **coefficients** in $\mathbb{I}$ (or its quotient field) such that

$$\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l)$$

(for the image $a(l)$ in $\mathbb{I}$ of $T(l)$) for almost all primes ℓ.

We regard $P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ as an algebra homomorphism $P : \mathbb{I} \to \overline{\mathbb{Q}}_p$, and we put $\rho_P = P \circ \rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{Q}}_p)$.

§4. Analytic family

A point P of Spec$(\mathbb{I})(\overline{\mathbb{Q}}_p)$ is called

arithmetic

if $P(1+T-\varepsilon\psi_k(\gamma)\gamma^k)=0$ for $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$.

If P is arithmetic, we have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_0(Np^{r(P)}), \varepsilon\psi_k)$ such that

$$f_P|T(n) = a_P(n)f_P \quad (n = 1, 2, \dots)$$

for $a_P(n) := P(a(n)) \in \overline{\mathbb{Q}}_p$.

We write $\varepsilon_P = \varepsilon$ and $k(P) = k$.

Thus $\mathbb{I}$ gives rise to an **analytic family**

$$\mathcal{F}_{\mathbb{I}} = \{f_P | \text{arithemtic } P \in \text{Spec}(\mathbb{I})\}.$$

§5. CM component and CM family

We call a Galois representation ρ **CM** if there exists an open subgroup $G \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that the semi-simplification $(\rho|_G)^{ss}$ has abelian image over G.

We call $\mathbb{I}$ a *CM component* if $\rho_{\mathbb{I}}$ is CM.

If $\mathbb{I}$ is a CM component, it is known that for an imaginary quadratic field M in which p splits, there exists a Galois character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{I}}^{\times}$ such that $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$.

If $\rho_P \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi_P$ for some arithmetic point P, $\mathbb{I}$ is a CM component.

§6. As $D_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ representation.

Let $V(\mathbb{I}) = \widetilde{\mathbb{I}}^2$ be the representation space of $\rho_{\mathbb{I}}$. We have the following exact sequence of D_p-modules coming from connected-étale sequence of Tate modules of modular jacobians:

$$0 \to V^\circ(\mathbb{I}) \to V(\mathbb{I}) \to V(\mathbb{I})^{et} \cong \widetilde{\mathbb{I}} \to 0$$

under suitable assumptions; so, we have

$$\begin{aligned} &\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = T(l) \quad (l \nmid Np), \\ &\rho_{\mathbb{I}}^{\mathrm{ss}}([\gamma^s, \mathbb{Q}_p]) \sim \begin{pmatrix} (1+T)^s & 0 \\ 0 & 1 \end{pmatrix} \text{ and} \\ &\rho_{\mathbb{I}}^{\mathrm{ss}}([p, \mathbb{Q}_p]) \sim \begin{pmatrix} * & 0 \\ 0 & a(p) \end{pmatrix}, \quad \text{(Gal)} \end{aligned}$$

where $\gamma^s = (1+p)^s \in \mathbb{Z}_p^\times$ for $s \in \mathbb{Z}_p$ and $[x, \mathbb{Q}_p]$ is the local Artin symbol.

§7. Assumptions enforced.

Pick and fix a non CM component $\mathbb{I}$ of prime-to-p level N. Write $\overline{\rho} = \rho_{\mathfrak{m}} = (\rho_{\mathbb{I}} \mod \mathfrak{m})$ for the maximal ideal $\mathfrak{m}$ of $\mathbb{I}$. and assume $p \geq 5$ and the following condition throughout

(R) $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix} \overline{\epsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ with $\overline{\delta}$ unramified and $\overline{\epsilon} \neq \overline{\delta}$.

Consider the following conditions:

(s) There exists $g \in D_p$ with $\rho_{\mathbb{I}}(g)$ having eigenvalues α, β in $\mathbb{Z}_p$ such that $\alpha^2 \not\equiv \beta^2 \mod \mathfrak{m}_{\mathbb{I}}$;
(u) $\rho_{\mathbb{I}}(D_p)$ contains a non-trivial unipotent element $g \in GL_2(\mathbb{I})$;
(v) $\rho_{\mathbb{I}}(D_p)$ contains a unipotent element $g \in GL_2(\mathbb{I})$ with $g \not\equiv 1 \mod \mathfrak{m}_{\mathbb{I}}$.

§8. Existence of the level.

Our first goal is:

Theorem I. *Suppose one of the two conditions* (s) *or* (u). *Then*

1. *There exist a representation ρ equivalent to $\rho_{\mathbb{I}}$ with values in $GL_2(\widetilde{\mathbb{I}})$ such that $G := \mathrm{Im}(\rho) \cap SL_2(\Lambda)$ contains $\Gamma_{\Lambda}(\mathfrak{a})$.*

2. *If $\mathfrak{c}$ is the Λ-ideal maximal among $\mathfrak{a}$ with $G \supset \Gamma(\mathfrak{a})$, the ideal $\mathfrak{c}_P \subset \Lambda_P$ localized at a prime divisor P only depends on the isomorphism class $[\rho_{\mathbb{I}}]$ as long as ρ_P is absolutely irreducible.*

3. *In particular, if $\overline{\rho} = \rho_{\mathfrak{m}}$ for the maximal ideal $\mathfrak{m}$ of $\mathbb{I}$ is absolutely irreducible, the reflexive closure (L) of $\mathfrak{c}$ is independent of the choice of ρ with $G \supset \Gamma(\mathfrak{a}) \neq 1$.*

§9. Lie algebra of a p-profinite group $\mathcal{G}$.

Set-up: • A: a semi-local p-profinite ring.

• Define $\Theta : SL_2(A) \to \mathfrak{sl}_2(A)$ and $C : SL_2(A) \to Z(A)$ for the center $Z(A)$ of $M_2(A)$ by

$$\Theta(x) = x - \frac{1}{2}\mathrm{Tr}(x)1_2,\ \zeta(x) = \frac{1}{2}(\mathrm{Tr}(x) - 2)1_2$$

for $1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

• For a p-profinite subgroup $\mathcal{G} \subset SL_2(A)$, define L by the closed additive subgroup of $\mathfrak{sl}_2(A)$ generated by $\Theta(x)$ for all $x \in \mathcal{G}$.

• Put $C = \mathrm{Tr}(L \cdot L)$.

• Define $\mathcal{M}_1^0(\mathcal{G}) = L$ and $\mathcal{M}^0(\mathcal{G}) = [L, L]$.

• $[L, L] \subset L,\ C \cdot L \subset L$.

• L is a Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{sl}_2(A)$.

• Put $\mathcal{M}_1(\mathcal{G}) = C \cdot 1_2 \oplus \mathcal{M}_1^0(\mathcal{G})$ and

$$\mathcal{M}(\mathcal{G}) = \mathcal{M}_2(\mathcal{G}) = C \cdot 1_2 \oplus \mathcal{M}^0(\mathcal{G}),$$

which is a closed Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{gl}_2(A)$.

• Define $\mathcal{H} = \mathcal{H}_2$ for

$$\mathcal{H}_j = SL_2(A) \cap (1 + \mathcal{M}_j(\mathcal{G})).$$

§10. A theorem of Pink

Theorem 1 (Pink). *Let the notation be as above. Let $\mathcal{G} \subset SL_2(A)$ be a p-profinite subgroup. Then we have*

(1) $\mathcal{H}_1$ and $\mathcal{H}$ are p-profinite subgroups of $SL_2(A)$;

(2) $\mathcal{G}$ is a normal closed subgroup of $\mathcal{H}_1$;

(3) $\mathcal{H} = (\mathcal{H}_1, \mathcal{H}_1) = (\mathcal{G}, \mathcal{G})$ (the topological commutator subgroup).

- $\mathcal{G} \mapsto \mathcal{M}_j(\mathcal{G})$ (resp. $\mathcal{G} \mapsto \mathcal{M}_j^0(\mathcal{G})$) is a covariant functor from p-profinite subgroups of $SL_2(A)$ into closed Lie $\mathbb{Z}_p$-subalgebras of $\mathfrak{gl}_2(A)$ (resp. $\mathfrak{sl}_2(A)$).
- $\mathcal{M}_j(\mathcal{G})$ and $\mathcal{M}_j^0(\mathcal{G})$ are stable under the **adjoint** action $x \mapsto gxg^{-1}$ of the normalizer $N(\mathcal{G}) \subset SL_2(A)$.
- For an A-ideal $\mathfrak{a}$ and for $\overline{\mathcal{G}}_{\mathfrak{a}} = (\mathcal{G} \mod \mathfrak{a}) = (\mathcal{G} \cdot \Gamma_A(\mathfrak{a}))/\Gamma_A(\mathfrak{a})$, $\mathcal{M}_j^0(\overline{\mathcal{G}}_{\mathfrak{a}}) \subset \mathfrak{sl}_2(A/\mathfrak{a})$ is the image of $\mathcal{M}_j^0(\mathcal{G})$ under $x \mapsto (x \mod \mathfrak{a})$.

§11. A proof of Theorem I, Step 1.

- We only give the proof under (R) and (s) and $\mathbb{I} = \Lambda$.
- Write $\mathcal{B}$ for the upper triangular Borel subgroup of $GL(2)$.
- Let $j = \lim_{n\to\infty} \rho_{\mathbb{I}}(g)^{p^n}$ for $g \in D_p$ in (s).
- By conjugating $\rho_{\mathbb{I}}$ by an element in $\mathcal{B}(\mathbb{I})$, we may assume

$$j = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta' \end{pmatrix} \quad \text{with } \zeta, \zeta' \in \mu_{p-1}(\mathbb{Z}_p),\ \zeta^2 \neq \zeta'^2$$

and

- $\mathcal{T} = \left\{ \begin{pmatrix} (1+T)^s & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset \rho_{\mathbb{I}}(D_p)$.
- Let $G = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma(\mathfrak{m})$.
- We have two eigenspaces $\mathfrak{u} = \mathcal{M}^0(G)[z]$ for $z = \zeta\zeta'^{-1}$ and $\mathfrak{u}_t = \mathcal{M}^0(G)[z^{-1}]$ of $\mathcal{M}^0(G)$ under the adjoint action $Ad(j)$. These are upper and lower nilpotent subalgebras.
- By the adjoint action of $\mathcal{T}$, $\mathfrak{u}$ and $\mathfrak{u}_t$ are Λ-modules (or abelian Lie Λ-algebras).
- If $\mathfrak{u} \neq 0$ and $\mathfrak{u}_t \neq 0$, then $[\mathfrak{u}, \mathfrak{u}_t] \neq 0$, $[\mathfrak{u}, [\mathfrak{u}, \mathfrak{u}_t]] \neq 0$ and $[\mathfrak{u}_t, [\mathfrak{u}, \mathfrak{u}_t]] \neq 0$ generate Lie Λ-subalgebra of $\mathfrak{sl}_2(\Lambda)$ of rank 3; so, we are done, since $G \supset (G, G) = SL_2(\Lambda) \cap (1 + \mathcal{M}(G))$.

§12. Non-triviality of $\mathfrak{u}$ and $\mathfrak{u}_t$.

- Note that $\det(\rho_{\mathbb{I}}([\gamma^s, \mathbb{Q}_p])) = (1+T)^s$.
- $\mathbb{H} = \{x \in \mathrm{Im}(\rho_{\mathbb{I}}) | \det(\rho_{\mathbb{I}})(x) \in \Gamma,\ x \equiv 1 \bmod \mathfrak{m}\}$ is an open subgroup of $\mathrm{Im}(\rho_{\mathbb{I}})$.
- Replacing G by $G \cap \mathbb{H}$, we have $\mathbb{H} = \mathcal{T} \ltimes G$.
- Pick $P \in \mathrm{Spec}(\Lambda)$. For any $X \subset GL_2(\Lambda)$, writing $\overline{X}_P$ for the image of X in $GL_2(\Lambda/P)$, we have $\overline{\mathbb{H}}_P = \overline{\mathcal{T}}_P \ltimes \overline{G}_P$; so, the reduction map $G \to \overline{G}_P$ is **onto**.
- Thus $\mathfrak{u} = \mathcal{M}^0(G)[z] \to \mathcal{M}^0(\overline{G}_P)[z] =: \overline{\mathfrak{u}}_P$ is **onto** by Pink's construction.
- Since $\mathbb{I}$ is a non CM component, for an **arithmetic** P, f_P does not have complex multiplication.
- By Ribet and Momose, $\overline{G}_P$ contains an open subgroup of $SL_2(\mathbb{Z}_p)$, and therefore $\overline{\mathfrak{u}} \neq 0$, which implies $\mathfrak{u} \neq 0$.
- Similarly, $\mathfrak{u}_t \neq 0$.

§13. Deciding the level; set-up.

We assume that the prime-to-p conductor of $\overline{\rho}$ is equal to N. We split our study following the shape of $\overline{\rho}$:

Case SL: $\mathrm{Im}(\overline{\rho}) \supset SL_2(\mathbb{F}_p)$.
Case A: $\mathrm{Im}(\overline{\rho})$: either a tetrahedral, octahedral or icosahedral type.
Case D: $\overline{\rho}$ is **induced** from a quadratic extension M which is either real or p does not split in M (dihedral image).
Case CM: $\overline{\rho}$ is **induced** from an imaginary quadratic extension M in which p splits.
Case R: $\overline{\rho}$ is **reducible**.

In Cases D and CM, we write $\overline{\rho} = \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ and assume that $\overline{\psi}^-(\sigma) = \overline{\psi}(\sigma c \sigma^{-1} c^{-1})$ (for $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inducing a non-trivial automorphism of M) has order ≥ 3 **ramified** at p. In Case CM, let $L^-_{\overline{\psi}^-}$ be the product of the anticyclotomic Katz p-adic L-function of branch character reducing to $\overline{\psi}^-$ mod $\mathfrak{m}$.

In Case R, write $\overline{\rho} = \overline{\theta} \oplus \overline{\psi}$, and assume that θ **ramified** at p with $\overline{\theta\psi}^{-1}$ having order ≥ 3. Then **no two cases overlaps**.

§14. Theorem

Our second goal is:

Theorem II. *Suppose* (R) *and one of the conditions* (s) *and* (v)*. Take a non CM cuspidal component* $\mathbb{I}$ *of prime-to-*p *cube-free level* N *and write* $(L(\mathbb{I}))$ *for the reflexive closure of the conductor of* $\mathbb{I}$*. Then*
Case SL: *Assume* $p \geq 7$*. Then* $L(\mathbb{I}) = 1$*.*
Case A: $T|L(\mathbb{I})|T^n$ *for an integer* $n > 0$*.*
Case D: $L(\mathbb{I})|((1+T)^{p^m} - 1)^2$ *for* $m \gg 0$*.*
Case CM: *Assume* $p \nmid \varphi(N)$*. Then* $L(\mathbb{I})|(L_{\overline{\psi}^-})^2$*.*
Case R: *Suppose* $p \nmid \varphi(N)$*. Then* $L(\mathbb{I})$ *is a factor of the primitive Kubota-Leopoldt* p*-adic* L*-function whose branch character modulo* p *is* $\overline{\psi}^{-1}\overline{\theta}\omega$*.*

Plainly, Cases CM and R in the theorem relate the level to p-adic L-functions. Out of the Galois representation of level L, one would be able to construct non-trivial Galois 1-cocycle with values in $Ad(\rho \mod L)$ not too much ramified; so, Cases A and D could be related to a certain p-adic L-function (possibly not yet constructed) if the cocycle gives Selmer cocycle.

§15. $P \nmid L(\mathbb{I})$ if $\mathrm{Im}(\rho_P) \cap SL_2(\mathbb{Z}_p)$ open.

By the proof of the existence of level, we find $\overline{\mathfrak{u}} \neq 0$ and $\overline{\mathfrak{u}}_t \neq 0$. Let

$\mathfrak{a} = \{a \in \Lambda | \left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{u}\}$, $\mathfrak{b} = \{b \in \Lambda | \left(\begin{smallmatrix} 0 & 0 \\ b & 0 \end{smallmatrix}\right) \in \mathfrak{u}_t\}$.

Then it is easy to see $\mathfrak{c} \supset \mathfrak{ab}$. In particular, $\mathfrak{c}$ is prime to P.

Thus in these two cases, we have $P \nmid L(\mathbb{I})$. In particular, in Case CM,

$$P | L(\mathbb{I}) \Leftrightarrow \rho_P \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi_P$$

for a Galois character Ψ_P. Thus we study congruence of $\rho_{\mathbb{I}}$ and $\mathrm{Ind}_M^{\mathbb{Q}} \mathbf{\Phi}$ for the universal character $\mathbf{\Phi}$ deforming $\overline{\psi}$ without extra ramification.

§16. CM components

We start a sketch of a proof in Case CM when N is the discriminant of M.

Let Spec($\mathbb{T}$) be the connected component of Spec($\mathbf{h}$) containing Spec($\mathbb{I}$), and write Spec($\mathbb{T}_{cm}$) for the union of all CM component of Spec($\mathbb{T}$).

Let $Cl_M(p^\infty)$ and $Cl_M^-(p^\infty)$ for its maximal anti-cyclotomic quotient $Cl_M^-(p^\infty) = Cl_M(p^\infty)/Cl_M(p^\infty)^{1+c}$. Let Z be the **maximal p-profinite quotient** of $Cl_M^-(p^\infty)$. Then by theta series, we have

$$\mathbb{T}_{cm} \cong W[[Z]] \text{ which is } \textbf{Gorenstein}.$$

As is well known, by ramification of ψ^- at p, we have

$\mathbb{T}$ is a **Gorenstein ring** flat over Λ.

Write Υ for the maximal torsion-free quotient of Z.

§17. Congruence module.

Write Spec($X^{\perp}$) for the complementary union of irreducible components of a union Spec(X) of irreducible components of Spec($\mathbb{T}$).

By the solution of anticyclotomic main conjecture, If $\mathbb{J}$ is a CM irreducible component with $\rho_{\mathbb{J}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$, we have

$$\begin{aligned}\mathrm{Spec}(\mathbb{J}) \cap \mathrm{Spec}(\mathbb{J}^{\perp}) &= \mathrm{Spec}(\mathbb{J} \otimes_{\mathbb{T}} \mathbb{J}^{\perp}) \\ &\cong \mathrm{Spec}(W[[\Upsilon]]/(h \cdot L(\Psi^{-}))),\end{aligned}$$

for the Ψ^{-} branch of the Katz measure and the class number h of M.

From the above formula, by Gorensteinness of $\mathbb{T}$ and $\mathbb{T}_{cm}$, we can compute

$$\begin{aligned}\mathrm{Spec}(\mathbb{T}_{cm}) \cap \mathrm{Spec}(\mathbb{T}_{cm}^{\perp}) &= \mathrm{Spec}(\mathbb{T}_{cm} \otimes_{\mathbb{T}} \mathbb{T}_{cm}^{\perp}) \\ &\cong \mathrm{Spec}(W[[Z]]/(L^{-}(\overline{\psi}^{-})))\end{aligned}$$

for the $\overline{\psi}^{-}$ projection $L^{-}(\overline{\psi}^{-})$ of the anticyclotomic Katz measure.

§18. Last steps.

Recall our simplifying assumption $\mathbb{I} \cong \Lambda$. Note $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T}_{cm}^{\perp})$. The annihilator $\mathfrak{x}$ of $\mathrm{Spec}(\mathbb{I}) \cap \mathrm{Spec}(\mathbb{T}_{cm})$ is the minimal ideal of $\mathbb{I}$ such that

$$\rho_{\mathbb{I}} \equiv \mathrm{Ind}_M^{\mathbb{Q}} \boldsymbol{\Phi} \mod \mathfrak{x}$$

for the universal character $\boldsymbol{\Phi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z]] \cong \mathbb{T}_{cm}$.

Thus we have $\mathbb{I}/\mathfrak{x}$ is a sujective image of $W[[Z]]/(L(\overline{\psi}^{-}))$. This implies $\mathfrak{x} \supset (L^{-}_{\overline{\psi}^{-}})$. Plainly $\mathfrak{x} = \mathfrak{a}$ for $\mathfrak{a} \cong \mathfrak{u}$ as Λ-modules.

§19. Conclusion.

We want to show $\mathfrak{x}^2 \subset \mathfrak{c}$. Let $D = \mathrm{Im}(\overline{\rho})$ which is a dihedral group of order prime to p. We can lift D to $\widetilde{D} \subset \mathrm{Im}(\rho_{\mathbb{I}})$ so that $j, J \in \widetilde{D} \cap \rho_{\mathbb{I}}(D_p)$ and

$$J = \lim_{n \to \infty} \rho_{\mathbb{I}}(c)^{p^n} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus $\mathfrak{b}$ made of $\mathfrak{u}_t = J\mathfrak{u}J^{-1}$ is also equal to $\mathfrak{x}$. Then $\mathfrak{c} \supset \mathfrak{a}\mathfrak{b} = \mathfrak{x}^2$.

§20. Case SL.

In this case, if $p \geq 7$, $SL_2(\mathbb{F}_p)$ cannot be lifted to $GL_2(A)$ for any characteristic 0 ring A. Thus if $P \nmid (p)$, $\mathcal{M}^0(\overline{G}_P)$ is non-zero Lie $\mathbb{Z}_p$-algebra on which $\mathrm{Im}(\overline{\rho}) \supset SL_2(\mathbb{F}_p)$ acting by the irreducible adjoint representation; so, $\mathcal{M}^0(\overline{G}_P)$ contains an open subalgebra of a conjugate of $\mathfrak{sl}_2(\mathbb{Z}_p)$; so, $\mathrm{Im}(\rho_P)$ contains an open subgroup of $SL_2(\mathbb{Z}_p)$; so, $P \nmid L(\mathbb{I})$.

If $P|(p)$, we can take
$\mathbb{H} = \{x \in \mathrm{Im}(\rho_{\mathbb{I}})|(x \mod \mathfrak{m}) \text{ is upper unipotent}\}$.
The $\overline{\mathbb{H}}_P$ normalized by $\mathcal{T}$ is infinite containing non-zero Λ-modules $\overline{\mathfrak{u}}$ and $\overline{\mathfrak{u}}_t$; so, $\mathfrak{c} \supset \mathfrak{u}\mathfrak{u}_t$ is prime to P.

We conclude $L(\mathbb{I}) = 1$.