HIDA THEORY

NOTES TAKEN BY PAK-HIN LEE

Abstract. These are notes from the (ongoing) Student Number Theory Seminar on Hida theory at Columbia University in Fall 2017, which is organized by David Hansen and Samuel Mundy.

Contents

Last updated: November 10, 2017. Please send corrections and comments to phlee@math.columbia.edu. We thank Samuel Mundy for proofreading and editting these notes.

1. Lecture 1 (September 7, 2017): Samuel Mundy
Ribet's Converse to Herbrand's Theorem

1.1. **Introduction.** Let p be an odd prime, and $\omega : G_{\mathbf{Q}} \to \mu_{p-1} \subseteq \mathbf{Z}_p^\times$ be the Teichmüller character (so that $\sigma\zeta_p = \zeta_p^{\omega(\sigma)}$ for all $\sigma \in G_{\mathbf{Q}}$).

For any $\mathbf{Z}_p[G_{\mathbf{Q}}]$-module M and $\varphi \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})^\wedge$, write $M^\varphi = \{m \in M \mid \sigma m = \varphi(\sigma)m\}$ to be the φ-eigenspace of M.

Let B_n be the n-th Bernoulli number.

Today we are going to prove Ribet's converse to Herbrand's theorem:

Theorem 1.1 (Ribet)**.** *Let m be an odd integer with $3 \le m \le p-2$. If $p \mid B_{p-m}$, then $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^{\omega^m} \neq 0$.*

Remark. We have $v_p(B_{p-1}) = -1$ and $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\omega = 0$.

The idea is to deduce properties of Galois representations attached to automorphic representations of GL_1 using those for GL_2.

1.2. **Modular forms.** Fix embeddings $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p} \hookrightarrow \mathbf{C}$. For $N \ge 1$ an integer, $\psi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ a Dirichlet character, and $A \subseteq \mathbf{C}$ a subring containing $\mathbf{Z}[\psi]$, write

$$S_k(N,\psi,A) = \left\{\text{cusp forms } f = \sum_{n=1}^\infty a_n(f)q^n \text{ of weight } k\text{, level } N\text{, nebentypus } \psi \mid a_n(f) \in A\right\}$$

where $q = e^{2\pi i z}$. Denote by $\mathbf{T}_k(N,\psi,A)$ the sub-A-algebra of $\mathrm{End}_A(S_k(N,\psi,A))$ generated by the Hecke operators $T(n)$ for all n.

We define a pairing

$$\begin{aligned} S_k(N,\psi,A) \times \mathbf{T}_k(N,\psi,A) &\to A \\ \langle f,h\rangle &\mapsto a_1(f|h). \end{aligned}$$

In particular, $\langle f, T(n)\rangle = a_n(f)$.

Theorem 1.2. *This pairing is perfect.*

Theorem 1.3. *Let B be an A-algebra with $\phi : A \to B$. Under the isomorphism*

$$\mathrm{Hom}_A(\mathbf{T}_k(N,\psi,A), B) \simeq S_k(N,\psi,A) \otimes_A B,$$

the A-algebra homomorphisms $\mathrm{Hom}_{A\text{-alg}}(\mathbf{T}_k(N,\psi,A),B)$ correspond to the normalized eigenforms, i.e., $f = \sum a_n(f)q^n \in S_k(N,\psi,A)\otimes_A B \subset B[[q]]$ with $a_1(f) = 1$ such that for all $h \in \mathbf{T}_k(N,\psi,A)$, there exists $c \in B$ such that $\phi(f|h) = c\phi(f)$, where the corresponding homomorphism on the LHS sends an operator to its eigenvalue.

Theorem 1.4. *Let $f = \sum_{n=1}^\infty a_n(f)q^n \in S_k(N,\psi,A)$ be a normalized eigenform. Then there exists a continuous Galois representation $\rho_f : G_{\mathbf{Q}} \to \mathrm{Aut}(V)$ with $\dim_{\overline{\mathbf{Q}_p}}(V) = 2$ such that*

1. *ρ_f is irreducible;*
2. *for all $\ell \nmid pN$, ρ_f is unramified at ℓ;*
3. *for all $\ell \nmid pN$, $\mathrm{tr}\,\rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$;*
4. *for all $\ell \nmid pN$, $\det\rho_f(\mathrm{Frob}_\ell) = \psi(\ell)\ell^{k-1}$.*

Definition 1.5. A normalized eigenform $f \in S_k(1,\overline{\mathbf{Q}_p})$ is *ordinary* if $|a_p(f)|_p = 1$.

Theorem 1.6 (Mazur–Wiles)**.** *If f is ordinary, then there exists a basis v_1, v_2 of V such that*

$$\rho_f|_{G_{\mathbf{Q}_p}} = \begin{pmatrix} \alpha^{-1}\chi^{k-1} & * \\ & \alpha \end{pmatrix},$$

where $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is the cyclotomic character (i.e., $\sigma\zeta = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_{p^\infty}$), and $\alpha : G_{\mathbf{Q}_p} \to \overline{\mathbf{Q}_p}^\times$ is the unramified character such that $\alpha(\mathrm{Frob}_p)$ is the unit root of $X^2 - a_p(f)X + p^{k-1}$.

1.3. **Proof of Ribet's theorem.** The proof consists of the following steps.

Step 0: Let κ by any finite field of characteristic p. Then

$$\begin{aligned}
\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p]^{\omega^m} \otimes_{\mathbf{F}_p} \kappa &\cong \mathrm{Hom}_{G_{\mathbf{Q}}}(G^{\mathrm{ab,unr}}_{\mathbf{Q}(\zeta_p)}, \kappa(\omega^m)) \\
&\cong H^1_{\mathrm{unr}}(G_{\mathbf{Q}(\zeta_p)}, \kappa(\omega^m))^{G_{\mathbf{Q}}} \\
&\overset{\mathrm{Res}^{-1}}{\cong} H^1_{\mathrm{unr}}(G_{\mathbf{Q}}, \kappa(\omega^m)) \\
&\cong \mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa, \kappa(\omega^m)) \\
&\cong \mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa(\omega^{p-1-m}), \kappa).
\end{aligned}$$

Step 1 (Construction of an eigenform): Let

$$E_k(z) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty}\left(\sum_{d|n} d^{k-1}\right) q^n$$

be the Eisenstein series of weight k, where $k \geq 4$ is even. The following facts are classical:

(1) $\zeta(1-k) = -B_k/k$.
(2) $v_p(B_k) < 0 \Leftrightarrow p-1 \mid k \Leftrightarrow v_p(B_k) = -1$.
(3) $E_k \in M_k(1, \mathbf{C})$. If $p-1 \nmid k$, then $E_k \in M_k(1, \mathbf{Z}_p)$ by (2).
(4) If $m \equiv n \pmod{p-1}$, then $B_m \equiv B_n \pmod{p}$.

Note that

$$\begin{aligned}
E_4(z) &= \frac{1}{240} + q + \cdots, \\
E_6(z) &= \frac{-1}{504} + q + \cdots.
\end{aligned}$$

Let $k \geq 4$ and $k \equiv p - m \pmod{p-1}$. Write $k = 4a + 6b$ where $a, b \geq 0$. Then define

$$G_k = (240E_4)^a(-504E_6)^b = 1 + \sum_{n=1}^{\infty} a_n q^n$$

where $a_n \in \mathbf{Z}$. Let

$$F_k = E_k - \frac{\zeta(1-k)}{2} G_k = \sum_{n=1}^{\infty} b_n q^n$$

where $b_n = \frac{B_k}{2k} a_n + \sum_{d|n} d^{k-1}$.

Now assume $p \mid B_{p-m}$. Then by (4), $p \mid B_k$ and so $b_n \equiv \sum_{d|n} d^{k-1} \pmod{p}$. Thus the map

$$\mathbf{T}_k(1, \mathbf{Z}_p) \to \mathbf{F}_p$$

$$T(n) \mapsto \sum_{d|n} d^{k-1} \pmod p$$

is a $\mathbf{Z}_p$-algebra homomorphism, corresponding to $F_k \pmod p$.

Let $\mathfrak{m} \subseteq \mathbf{T}_k(1, \mathbf{Z}_p)$ be the kernel, and $\mathfrak{p} \subseteq \mathfrak{m}$ be a minimal prime. Let f be the eigenform corresponding to the homomorphism

$$\mathbf{T}_k(1, \mathbf{Z}_p) \to A := \mathbf{T}_k(1, \mathbf{Z}_p)/\mathfrak{p} \hookrightarrow \mathcal{O}_L,$$

where $L := \operatorname{Frac} A$. Then $f \in S_k(1, \mathcal{O}_L)$ and $f \equiv F_k \pmod \lambda$, where $\lambda \in \mathcal{O}_L$ is a uniformizer.

Step 2 (Analysis of ρ_f): Write $f = \sum_{n=1}^{\infty} c_n q^n$. Then

$$c_p \equiv \sum_{d|p} d^{k-1} \equiv 1 + p^{k-1} \equiv 1 \pmod \lambda,$$

so f is ordinary. Let $v_1, v_2 \in V_{\rho_f}$ such that

$$\rho_f|_{G_{\mathbf{Q}_p}} = \begin{pmatrix} \alpha^{-1}\chi^{k-1} & * \\ & \alpha \end{pmatrix}.$$

Let $\sigma_0 \in G_{\mathbf{Q}_p}$ be an element such that $\chi^{k-1}(\sigma_0) \not\equiv 1 \pmod \lambda$ (possible since $k-1$ is odd, so $p - 1 \nmid k - 1$). Write $\beta := \chi^{k-1}(\sigma_0)$. Replacing v_1 by $\alpha(\sigma_0)v_1$ and v_2 by $\alpha^{-1}(\sigma_0)v_2 +$ (something) $\cdot\, v_1$, we may assume

$$\rho_f(\sigma_0) = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}.$$

For $\sigma \in \mathcal{O}_L[G_{\mathbf{Q}}]$, let $\rho_f(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$.

Lemma 1.7.

(1) *For all $\sigma, \tau \in \mathcal{O}_L[G_{\mathbf{Q}}]$, we have $a_\sigma, d_\sigma, b_\sigma c_\tau \in \mathcal{O}_L$ and*

$$a_\sigma \equiv \omega^{k-1}(\sigma), \quad d_\sigma \equiv \mathbb{1}(\sigma), \quad b_\sigma c_\tau \equiv 0 \pmod \lambda,$$

where $\mathbb{1}$ is the trivial $G_{\mathbf{Q}}$-character, and $\omega^{k-1}, \mathbb{1}$ are extended by linearity to $\mathcal{O}_L[G_{\mathbf{Q}}]$.

(2) *$C = \{c_\sigma \mid \sigma \in \mathcal{O}_L[G_{\mathbf{Q}}]\}$ is a nonzero fractional ideal.*

(3) *$c_\sigma = 0$ for all $\sigma \in I_\ell$ and primes ℓ.*

Proof. Omitted; play with matrix coefficients using information about the trace. □

Step 3 (Construction of the lattice): Let $M_1 = \mathcal{O}_L v_1$, $M_2 = C v_2$ and $M = M_1 \oplus M_2 \subseteq V_{\rho_f}$. This is $G_{\mathbf{Q}}$-stable, generated over $\mathcal{O}_L[G_{\mathbf{Q}}]$ by v_1.

Let $\kappa = \mathcal{O}_L/\lambda$ and $\overline{M} = M/\lambda M$.

Claim. $\overline{M_2} := M_2/\lambda M_2 \subseteq \overline{M}$ is a $G_{\mathbf{Q}}$-stable line with trivial action.

Let $m_2 \in M_2$, so $m_2 = c_\tau v_2$ for some $c_\tau \in C$. If $\sigma \in G_{\mathbf{Q}}$, then

$$\rho_f(\sigma) m_2 = c_\tau b_\sigma v_1 + c_\tau d_\sigma v_2 \equiv d_\sigma m_2 = \mathbb{1}(\sigma) m_2 = m_2 \pmod \lambda$$

which proves the claim.

Let $\overline{M_1} = M_1/\lambda M_1$. Then $\overline{M_1} \cong \kappa(\omega^{k-1})$ by a similar argument, and there is a short exact sequence

$$0 \to \kappa \to \overline{M} \to \kappa(\omega^{k-1}) \to 0$$

which is:

- nonsplit over $G_{\mathbf{Q}}$ because, if it were, $\overline{M_2} \cong \kappa$ would be a quotient and hence the image of v_1 would belong to the kernel by this quotient. This is because σ_0 acts as $\beta \not\equiv 1 \pmod{\lambda}$ on v_1, but v_1 generates $\overline{M}$ over $G_{\mathbf{Q}}$. Hence the kernel is all of $\overline{M}$, a contradiction.
- split over I_ℓ for all ℓ because $\mathcal{O}_L v_1 \pmod{\lambda}$ is a stable line under I_ℓ, since

$$\rho(\sigma)v_1 = a_\sigma v_1 + c_\sigma v_2 \equiv a_\sigma v_1 \pmod{\lambda}.$$

Since $\omega^{k-1} = \omega^{p-1-m}$, this extension gives a nontrivial class in $\mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa(\omega^{p-1-m}), \kappa)$. This finishes the proof of Theorem 1.1.

2. Lecture 2 (September 14, 2017): Samuel Mundy Basic Iwasawa Theory

2.1. **$\mathbf{Z}_p$-extensions and Iwasawa's theorem.** Last time we understood better the structure of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$ as a $G_{\mathbf{Q}}$-module. A natural question is: What about $\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}$?

Theorem 2.1 (Iwasawa)**.** *There exist integers n_0 and μ, λ, κ such that for all $n > n_0$,*

$$\#\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}[p^\infty] = p^{\mu p^n + \lambda n + \kappa}.$$

This statement *a priori* does not have anything to do with the Galois structure of class groups, but the proof relies heavily on that.

Recall that $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$. Let $\mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 0} \mathbf{Q}(\zeta_{p^n})$. Then

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}) \simeq \mathbf{Z}_p^\times,$$
$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}(\zeta_p)) \simeq \mathbf{Z}_p.$$

The element $1 - \zeta_{p^n} \in \mathcal{O}_{\mathbf{Q}(\zeta_{p^n})} = \mathbf{Z}[\zeta_{p^n}]$ generates the (totally ramified) prime above $p \in \mathbf{Z}$. With these facts we are ready to study basic Iwasawa theory.

Definition 2.2. Let K_0 be a number field. A $\mathbf{Z}_p$*-extension* of K_0 is an algebraic extension K_∞/K_0 such that $\mathrm{Gal}(K_\infty/K_0) \simeq \mathbf{Z}_p$ topologically; equivalently, it is a tower of finite extensions

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n$$

such that $\mathrm{Gal}(K_n/K_0) \simeq \mathbf{Z}/p^n\mathbf{Z}$.

Proposition 2.3. *Let K_∞/K_0 be a $\mathbf{Z}_p$-extension. Then:*

1. *Some prime is ramified in K_∞.*
2. *For any ramified prime $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$, there exists n_0 such that if $\mathfrak{q} \subseteq \mathcal{O}_{K_{n_0}}$ is such that $\mathfrak{q} \mid \mathfrak{p}$, then $\mathfrak{q}$ is totally ramified in K_∞/K_{n_0}.*
3. *Every ramified prime lies over $p \in \mathbf{Z}$.*

Proof.

1. The maximal unramified abelian extension of K_0 is finite over K_0.
2. Let $\mathfrak{p}$ be ramified in K_∞/K_0, and $I_{\mathfrak{p}} \subseteq \mathrm{Gal}(K_\infty/K_0) \simeq \mathbf{Z}_p$ be the inertia group at $\mathfrak{p}$. This is nontrivial and closed. Thus $I_{\mathfrak{p}} \simeq p^{n_0}\mathbf{Z}_p$ for some n_0, so $I_{\mathfrak{p}} = \mathrm{Gal}(K_\infty/K_0)$.

(3) Let $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$ be ramified in K_∞. By local class field theory,

$$\mathrm{Gal}(K_{0,\mathfrak{p}}^{\mathrm{ab}}/K_{0,\mathfrak{p}}) \cong \widehat{K_{0,\mathfrak{p}}^\times} \simeq \pi^{\widehat{\mathbf{Z}}} \times \mathcal{O}_{K_{0,\mathfrak{p}}}^\times$$

corresponding to the unramified and ramified parts respectively, so by (2) we get an infinite subgroup of $\mathcal{O}_{K_{0,\mathfrak{p}}}^\times$ isomorphic to $\mathbf{Z}_p$, forcing $K_{0,\mathfrak{p}}$ to have residue characteristic p. □

Proposition 2.4. *Let L/K be an extension of number fields such that some prime in K is totally ramified in L. Then the norm map*

$$\mathrm{Nm} : \mathrm{Cl}_L[p^\infty] \to \mathrm{Cl}_K[p^\infty]$$

is surjective.

Remark. This is true without taking p-primary parts and essentially the same proof will work. It is also true if the ramified prime is at infinity.

Proof. Let M_0/K be the maximal unramified abelian p-extension of K, and M_1 that for L. Then M_0 and L are linearly disjoint over K (i.e., $M_0 \cap L = K$ in any $\overline{K}$).

$$\begin{tikzcd}[column sep=small]
 & & M_1 \arrow[dl, dash] \\
 & LM_0 \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & M_0 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Since LM_0/L is an unramified abelian p-extension, it is contained in M_1. Then by class field theory, the diagram

$$\begin{tikzcd}
\mathrm{Cl}_L[p^\infty] \arrow[r, "\sim", "\mathrm{Art}"'] \arrow[d, "\mathrm{Nm}"'] & \mathrm{Gal}(M_1/L) \arrow[d, two heads, "\text{restriction to } M_0"] \\
\mathrm{Cl}_K[p^\infty] \arrow[r, "\sim", "\mathrm{Art}"'] & \mathrm{Gal}(M_0/K)
\end{tikzcd}$$

commutes. □

This suggests that we should look at

$$C := \varprojlim_{n \geq 0} \mathrm{Cl}_{K_n}[p^\infty],$$

where the inverse limit is taken with respect to Nm. Write $\Gamma_n = \mathrm{Gal}(K_n/K_0)$. Since $\mathrm{Cl}_{K_n}[p^\infty]$ is a $\mathbf{Z}_p[\Gamma_n]$-module, C is a module over

$$\Lambda := \varprojlim_{n \geq 0} \mathbf{Z}_p[\Gamma_n],$$

where the inverse limit is taken with respect to restriction maps $\Gamma_m \twoheadrightarrow \Gamma_n$ if $m \geq n$.

Theorem 2.5 (Iwasawa). *C is a finitely generated torsion Λ-module.*

We will see how Theorem 2.1 follows from this.

2.2. **Λ-modules.** We need to first understand the structure of Λ. Let $\gamma \in \Gamma := \mathrm{Gal}(K_\infty/K_0) \subseteq \Lambda^\times$ be a topological generator. An observation due to Serre is that:

Proposition 2.6 (Serre)**.** *There is an isomorphism*

$$\Lambda \simeq \mathbf{Z}_p[[T]]$$

of topological rings, induced by $\gamma - 1 \mapsto T$.

Proof. Omitted; see Lang's *Cyclotomic Fields I and II*, Chapter 5. □

Corollary 2.7 (Nakayama's lemma)**.** *If M is a compact Λ-module and $M/TM = M/(\gamma - 1)M$ is finitely generated over $\mathbf{Z}_p$, then any set of generators in M/TM lifts to a set of generators in M. In particular, M is finitely generated.*

Definition 2.8. A *quasi-isomorphism* of Λ-modules M, N is a map $\varphi : M \to N$ such that there exists an exact sequence

$$0 \to A \to M \xrightarrow{\varphi} N \to B \to 0$$

with A, B of finite cardinality.

Quasi-isomorphism is an equivalence relation.

Theorem 2.9 (Weierstrass preparation)**.** *Let $f \in \mathbf{Z}_p[[T]]$ be a nonconstant power series. Then there exist a unique integer $n \geq 0$ and unique $g, u \in \mathbf{Z}_p[[T]]$ such that g is* distinguished *and $u \in \mathbf{Z}_p[[T]]^\times$, and*

$$f = p^n ug.$$

(A monic polynomial $g = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ is distinguished *if $p \mid a_i$ for all $i = 0, \cdots, n-1$.)*

Theorem 2.10. *Let M be a finitely generated Λ-module. Then there exist integers r, n_i and distinguished f_j (where $i \in I$ and $j \in J$ with I and J finite) such that*

$$M \overset{\text{q-iso}}{\simeq} \Lambda^r \oplus \bigoplus_{i\in I} \Lambda/(p^{n_i}) \oplus \bigoplus_{j \in J} \Lambda/(f_j).$$

2.3. **Proof of Iwasawa's theorem.** We will prove Theorem 2.1 and Theorem 2.5 in the case when there is only one ramified prime $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$ above p.

Proof of Theorem 2.5. For simplicity, we further assume that $\mathfrak{p}$ is totally ramified in K_∞/K_0. Then we make the main

Claim. $C/(\gamma - 1)C \simeq \mathrm{Cl}_{K_0}$.

Let M_n/K_n be the maximal unramified abelian p-extension, and $M_\infty := \bigcup_{n\geq 0} M_n$, so M_∞/K_∞ is the maximal unramified pro-p abelian extension. Let $G_C := \mathrm{Gal}(M_\infty/K_\infty) \cong C$, $G := \mathrm{Gal}(M_\infty/K_0)$ and $\Gamma = \mathrm{Gal}(K_\infty/K_0)$.

Claim (Subclaim 1)*.* If $I \subset G$ is the inertia at $\mathfrak{p}$, then $G \simeq G_C \rtimes I$.

There is an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(M_\infty/K_\infty) & \longrightarrow & \mathrm{Gal}(M_\infty/K_0) & \longrightarrow & \mathrm{Gal}(K_\infty/K_0) & \longrightarrow & 1. \\ & & \| & & \| & & \| & & \\ & & G_C & & G & & \Gamma & & \end{array}$$

Since $\mathfrak{p}$ is totally ramified in K_∞, I surjects onto Γ and has empty intersection with G_C. This proves $\Gamma \simeq I$ and subclaim 1.

Let $\Gamma \simeq I$ act on G_C by conjugation. Then this action is the same as that on C: $\mathrm{Frob}_{\sigma\mathfrak{q}} = \sigma \,\mathrm{Frob}_{\mathfrak{q}}\, \sigma^{-1}$.

Claim (Subclaim 2). Let G' be the commutator subgroup of G. Then $G' = (\gamma - 1)G$.

Let $g \in G$. Then $(\gamma - 1)g = \tilde{\gamma} g \tilde{\gamma}^{-1} g^{-1} \in G'$, where $\tilde{\gamma}$ is a lift of γ to I. Conversely, $G/(\gamma-1)G$ is the largest quotient where Γ acts trivially. So conjugation by elements in I is trivial, and since G_C is abelian and $G = G_C \rtimes I$, we have that $G/(\gamma - 1)G$ is abelian and hence $(\gamma - 1)G \subseteq G'$. This proves subclaim 2.

To prove the main claim that $C/(\gamma-1)C \simeq \mathrm{Cl}_{K_0}[p^\infty]$, it is the same to prove

$$G_C/(\gamma-1)G_C \cong \mathrm{Gal}(M_0/K_0).$$

Note $(\gamma-1)G_C = (\gamma-1)G$ (because if $g \in G_C$, $\iota \in I$ and $\gamma \in \Gamma$, then picking a lift $\tilde{\gamma} \in I$, we have $(\gamma-1)g\iota = \tilde{\gamma} g \iota \tilde{\gamma}^{-1} \iota^{-1} g^{-1} = \tilde{\gamma} g \iota \iota^{-1} \tilde{\gamma}^{-1} g^{-1} = (\gamma - 1)g$; the reverse inclusion is trivial). Then

$$\begin{aligned} G_C/(\gamma-1)G_C &= G_C/(\gamma-1)G \\ &\cong G/I \cdot (\gamma-1)G \\ &= G/I \cdot G' \\ &= \mathrm{Gal}(M_0/K_0). \end{aligned}$$

This proves the main claim.

Since $\mathrm{Cl}_{K_0}[p^\infty] = C/(\gamma-1)C$ is finite, by Nakayama's lemma C is finitely generated. Write

$$C \overset{\text{q-iso}}{\simeq} \Lambda^r \oplus \bigoplus \Lambda/(p^{n_i}) \oplus \bigoplus \Lambda/(f_j).$$

Then since $\Lambda^r/(\gamma-1)\Lambda^r \simeq \mathbf{Z}_p^r$, we have $r = 0$. This proves Theorem 2.5. $\square$

Remark. Since $C/(\gamma^{p^n}-1)C$ is finite, we see that f_j is coprime to $(1+T)^{p^n} - 1$ for all j, n.

Finally, let us prove Theorem 2.1: There exist n_0 and μ, λ, κ such that for all $n > n_0$,

$$\#\mathrm{Cl}_{K_n}[p^\infty] = p^{\mu p^n + \lambda n + \kappa}.$$

Exercise.

(1) $\#\Lambda/(p^m, \gamma^{p^n} - 1) = p^{mp^n}$.

(2) Let f be a distinguished polynomial coprime to $(1+T)^{p^n} - 1$ for all n. Then there exists n_0 such that if $n > n_0$, then $\#\Lambda/(f, \gamma^{p^n}-1) = p^{\deg(f)n + c}$ for some $c = c(f)$.

Proof of Theorem 2.1. Replacing K_0 by K_n where $n \gg 0$, we may assume the ramified prime is totally ramified. Then setting $\mu = \sum_i n_i$ and $\lambda = \sum_j \deg f_j$, we get (by the previous exercise and remark) κ such that

$$\#\mathrm{Cl}_{K_n}[p^\infty] = \#C/(\gamma^{p^n}-1)C = p^{\mu p^n + \lambda n + \kappa}$$

for sufficiently large n. $\square$

Remark. For the cyclotomic extension $\mathbf{Q}(\zeta_{p^\infty})$, it is known that $\mu = 0$; this is the Ferrero–Washington theorem.

3. Lecture 3 (September 21, 2017): Samuel Mundy
p-adic Properties of L-functions

3.1. **Class number formulas.** Fix an odd prime p and embeddings $\mathbf{Q} \hookrightarrow \overline{\mathbf{Q}_p} \hookrightarrow \mathbf{C}$. Denote $K = \mathbf{Q}(\zeta_{p^n})$ throughout.

Definition 3.1.

(1) A character $\psi : \mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \to \mathbf{C}^\times$ is *odd* if $\psi(c) = -1$ for the complex conjugation c, and *even* otherwise (so $\psi(c) = 1$).

(2) Given ψ, $L(s,\psi)$ is the complex analytic function continuing $\sum_{n=1}^\infty \frac{\psi'(n)}{n^s}$, where ψ' is the *primitive* character associated with ψ. (In particular, $L(s,1) = \zeta(s)$ and not $(1-p^{-s})\zeta(s)$.)

(3) Let $K^+ = \mathbf{Q}(\zeta_{p^n})^+ := \mathbf{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$, so $[K : K^+] = 2$. Let $h = \#\mathrm{Cl}_K$, $h^+ = \#\mathrm{Cl}_{K^+}$ and $h^- = h/h^+$.

Remark. $\mathrm{Nm} : \mathrm{Cl}_K \to \mathrm{Cl}_{K^+}$ is surjective, since K/K^+ is totally ramified at ∞. This implies $h^- \in \mathbf{Z}$.

We collect the following standard facts.

Theorem 3.2.

(1) *Dirichlet's class number formula: Let $\zeta_L(s)$ be the Dedekind zeta function for a number field L. Then*
$$\mathrm{Res}_{s=1}\, \zeta_L(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_L h_L}{\#\mu_L\sqrt{|\Delta_L|}},$$
where the regulator is $\mathrm{Reg}_L = \det\log|\sigma_i\alpha_j|$ for a $\mathbf{Z}$-basis $\{\alpha_j\}$ of $\mathcal{O}_L^\times/$torsion. In particular, we have
$$\mathrm{Res}_{s=1}\, \zeta_K(s) = \frac{(2\pi)^{N/2}\mathrm{Reg}_K h}{2p^n\sqrt{|\Delta_K|}} \text{ and } \mathrm{Res}_{s=1}\, \zeta_{K^+}(s) = \frac{2^{N/2}\mathrm{Reg}_{K^+} h^+}{2\sqrt{|\Delta_{K^+}|}},$$
where $N = [K:\mathbf{Q}] = (p-1)p^{n-1}$.

(2) *Let $\psi : \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$ have conductor $m(\psi)$, and write*
$$\Lambda(s,\psi) := \begin{cases} m(\psi)^{s/2}\pi^{-s/2}\Gamma(\frac{s}{2})L(s,\psi) & \text{if } \psi \text{ is even,} \\ m(\psi)^{s/2}\pi^{-s/2}\Gamma(\frac{s+1}{2})L(s,\psi) & \text{if } \psi \text{ is odd.} \end{cases}$$
Then
$$\Lambda(s,\psi) = \frac{\sqrt{\psi(-1)m(\psi)}}{S(\psi)}\Lambda(1-s,\psi),$$
where $S(\psi)$ is the Gauss sum.

(3) $\displaystyle\prod_{\psi\neq 1} S(\psi) = i^{N/2}\sqrt{|\Delta_K|}$ *and* $\displaystyle\prod_{\substack{\psi\neq 1\\ \psi \text{ even}}} S(\psi) = \sqrt{|\Delta_{K^+}|}$.

(4) $\mathcal{O}_K^\times = \mu_{p^n}\mathcal{O}_{K^+}^\times$.

(5) *Let $B_{n,\psi}$ be the generalized Bernoulli numbers, defined by*

$$\sum_{a=0}^{m(\psi)-1} \frac{\psi(a)Te^{aT}}{e^{m(\psi)T}-1} = \sum_{n=0}^{\infty} B_{n,\psi}\frac{T^n}{n!}.$$

Then for every integer $n \geq 1$,

$$L(1-n,\psi) = -\frac{B_{n,\psi}}{n}.$$

We have the following formula for h^-.

Theorem 3.3.

$$h^- = 2p^n \prod_{\psi \text{ odd}} \frac{1}{2}L(0,\psi) \left(\overset{(5)}{=} 2p^n \prod_{\psi \text{ odd}} -\frac{1}{2}B_{1,\psi} \right).$$

Proof. Note that

$$\operatorname{Res}_{s=1} \zeta_K(s) = \prod_{\psi \neq 1} L(1,\psi) \text{ and } \operatorname{Res}_{s=1} \zeta_{K^+}(s) = \prod_{\substack{\psi \neq 1 \\ \psi \text{ even}}} L(1,\psi).$$

Then

$$\begin{aligned}
h^- = \frac{h}{h^+} &\overset{(1)}{=} \frac{2^{N/2}\operatorname{Reg}_{K^+}/2\sqrt{|\Delta_{K^+}|}}{(2\pi)^{N/2}\operatorname{Reg}_K/2p^n\sqrt{|\Delta_K|}} \times \prod_{\psi \text{ odd}} L(1,\psi) \\
&\overset{(2)}{=} \frac{\operatorname{Reg}_{K^+}}{\operatorname{Reg}_K} \frac{p^n\sqrt{|\Delta_K|}}{\pi^{N/2}\sqrt{|\Delta_{K^+}|}} \prod_{\psi \text{ odd}} \frac{L(0,\psi)\Gamma(\frac{1}{2})i \cdot m(\psi)^{1/2}}{S(\psi)m(\psi)^{1/2}\pi^{-1/2}\Gamma(1)} \\
&\overset{(4)}{=} \frac{1}{2^{N/2-1}} p^n \pi^{-N/2} \frac{\sqrt{|\Delta_K|}}{\sqrt{|\Delta_{K^+}|}} \left(\prod_{\psi \text{ odd}} L(0,\psi) \right) \left(\prod_{\psi \text{ odd}} S(\psi)^{-1} \right) \pi^{N/2} i^{N/2} \\
&\overset{(3)}{=} 2p^n \prod_{\psi \text{ odd}} \frac{1}{2}L(0,\psi).
\end{aligned}$$

□

Remark. The p-part of h^- is $\prod_{\psi \text{ odd}} \#\mathrm{Cl}_K[p^\infty]^\psi$ (left as an exercise). Recall that $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\omega = 0$ and $v_p(pB_{1,\omega^{-1}}) = 0$. Thus the theorem gives

$$\prod_{\substack{\psi \neq \omega \\ \psi \text{ odd}}} \#\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\psi = \prod_{\substack{\psi \neq \omega^{-1} \\ \psi \text{ odd}}} \#\mathbf{Z}_p/(L(0,\psi)).$$

Therefore, inverting each character on the right hand side, we have

$$\prod_{\substack{\psi \neq \omega \\ \psi \text{ odd}}} \#\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\psi = \prod_{\substack{\psi \neq \omega \\ \psi \text{ odd}}} \#\mathbf{Z}_p/(L(0,\psi^{-1})).$$

In fact this is true without taking products, as we will see in Corollary 3.8. This strengthens Herbrand–Ribet, because $v_p(B_{p-m}) = v_p(B_{1,\omega^{-m}})$.

3.2. **p-adic L-functions.** Fix $\gamma \in \Gamma \subseteq \Lambda^\times$ a topological generator of Γ. Let χ_{cyc} be the cyclotomic character. Let ζ be a p^n-th root of 1 (not necessarily primitive). For $k \in \mathbf{Z}$, let $\phi_{k,\zeta} : \Lambda \to \mathbf{Z}_p[\zeta]$ send γ to $\chi_{\mathrm{cyc}}^k(\gamma)\zeta$.

Theorem 3.4. *Let $\psi : \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \to \mathbf{C}^\times$ be an odd character, and*

$$h_\psi = \begin{cases} \chi_{\mathrm{cyc}}(\gamma)\gamma - 1 & \text{if } \psi = \omega^{-1}, \\ 1 & \text{if } \psi \neq \omega^{-1}. \end{cases}$$

Then there exists $g_\psi \in \Lambda$ such that

$$\frac{\phi_{k,\zeta}(g_\psi)}{\phi_{k,\zeta}(h_\psi)} = L(-k, \psi\psi_\zeta\omega^{-k}),$$

where $\psi_\zeta : \mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \to \mathbf{C}^\times$ sends the image of γ to ζ.

Definition 3.5. g_ψ is called a *p-adic L-function.*

The construction of g_ψ uses Bernoulli measures, whose existence implies the Kummer congruences.

3.3. **Main Conjecture.**

Definition 3.6. For a finitely generated torsion Λ-module M, write

$$M \overset{\text{q-iso}}{\simeq} \bigoplus_i \Lambda/(p^{n_i}) \oplus \bigoplus_j \Lambda/(f_j)$$

as in the classification theorem. Then the *characteristic ideal* of M is

$$\mathrm{Char}(M) := \left(\prod_i p^{n_i} \cdot \prod_j f_j\right)\Lambda.$$

Recall that last time we constructed a finitely generated torsion Λ-module

$$C := \varprojlim_{n \geq 1} \mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}[p^\infty].$$

Let C^ψ be the ψ-eigenspace of C, where $\psi : \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \to \mathbf{C}^\times$ is an odd character.

Remark. We have $C^\psi = \varprojlim_n \left(\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}[p^\infty]^\psi\right)$.

For a Λ-module M, let M^ι be the same Λ-module except with $g \in \Gamma$ acting as g^{-1}.
The goal of the first part of our seminar is to prove the

Theorem 3.7 (Main Conjecture)**.** $\mathrm{Char}(C^{\psi,\iota}) = (g_{\psi^{-1}})$.

Corollary 3.8. *Suppose $\psi \neq \omega$. Then*

$$\#\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\psi = \#\mathbf{Z}_p/(L(0,\psi^{-1})).$$

To prove this we need the

Proposition 3.9. *C (and hence C^ι) has no nonzero finite cardinality Λ-submodules.*

Proof. See Washington P.287–289. ∎

Exercise. If M is a finitely generated torsion Λ-module with no nonzero finite cardinality Λ-submodules, and if $M/(\gamma^{p^n}-1)M$ is finite for all n, then

$$\#M/(\gamma^{p^n}-1)M = \#\Lambda/(\mathrm{Char}(M), \gamma^{p^n}-1).$$

Proof of Corollary 3.8.

$$\begin{aligned}
\#\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\psi &= \#C^\psi/(\gamma-1)C^\psi \\
&= \#C^{\psi,\iota}/(\gamma-1)C^{\psi,\iota} \\
&= \#\Lambda/(\gamma-1, \mathrm{Char}(C^{\psi,\iota})) \quad \text{(by Exercise)} \\
&= \#\Lambda/(\gamma-1, g_{\psi^{-1}}) \quad \text{(by MC)} \\
&= \#\mathbf{Z}_p/(\phi_{0,1}(g_{\psi^{-1}})) \\
&= \#\mathbf{Z}_p/(L(0,\psi^{-1})).
\end{aligned}$$

□

4. Lecture 4 (September 28, 2017): Pak-Hin Lee
Λ-adic modular forms

5. Lecture 5 (October 5, 2017): Pak-Hin Lee
Ordinary Λ-adic forms

6. Lecture 6 (October 12, 2017): Pak-Hin Lee
Hida Theory and Λ-adic Galois Representations

7. Lecture 7 (October 19, 2017): Pak-Hin Lee
Λ-adic Representations via Pseudo-representations

These will be updated soon!

8. Lecture 8 (October 26, 2017): Samuel Mundy
Proof of the Main Conjecture, I

Let p be an odd prime, and $\psi = \omega^m$ where m is odd and ω is the Teichmüller character. Decompose $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}) = \Delta \times \Gamma = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \times \langle\gamma\rangle$. Let $\Lambda = \mathbf{Z}_p[[\Gamma]]$, with the specialization map $\nu_{k,\zeta}$ sending $\gamma \in \Gamma \subseteq \Lambda^\times$ to $\zeta\chi_{\mathrm{cyc}}^k(\gamma)$. We identify $\Gamma = 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$ via the cyclotomic character χ_{cyc}.

Recall there exists a unique $g_\psi \in \Lambda$ such that, writing

$$h_\psi := \begin{cases} \chi_{\mathrm{cyc}}(\gamma)\gamma - 1 & \text{if } \psi = \omega^{-1}, \\ 1 & \text{otherwise,} \end{cases}$$

we have

$$\frac{\nu_{k,\zeta}(g_\psi)}{\nu_{k,\zeta}(h_\psi)} = L(-k, \psi\psi_{\mathrm{cyc}}\omega^{-k})$$

where ψ_ζ sends γ to ζ.

Remark. The g_ψ here is Pak-Hin's $g_{\psi\omega}$, so $g_{\omega^{-1}}$ corresponds to his g_1. We have to switch from even to odd.

Recall that we constructed $X_\infty = \varprojlim_n \mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}[p^\infty]^-$, where the minus sign means the odd part of the eigenspace for complex conjugation. This is a finitely generated Λ-module. Let X_∞^ψ be the ψ-eigenspace, and $X_\infty^{\psi,\iota}$ be X_∞^ψ on which γ acts as γ^{-1}.

Theorem 8.1 (Main Conjecture)**.** $\mathrm{Char}(X_\infty^{\psi,\iota}) = (g_{\psi^{-1}})$.

8.1. **Reduction to one inclusion.** Let us show that it is enough to prove either $\subseteq$ or $\supseteq$. Fix $n \geq 0$. Then we have

$$\begin{aligned}
\prod_{\zeta\in\mu_{p^n}} \prod_{\substack{0\le k\le p-2\\ k \text{ odd}}} \nu_{0,\zeta}(g_{\omega^k}) &= \prod_{\zeta,k} \nu_{0,\zeta}(h_{\omega^k}) L(0,\omega^k\psi_\zeta) \\
&= \prod_{\zeta} \nu_{0,\zeta}(h_{\omega^{-1}}) \cdot \prod_{\zeta,k} L(0,\omega^k\psi_\zeta) \\
&= \left(\prod_{\zeta} (\chi_{\mathrm{cyc}}(\gamma)\zeta - 1)\right) \prod_{\substack{\psi\in\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q})^\wedge\\ \psi \text{ odd}}} L(0,\psi) \\
&= (\chi_{\mathrm{cyc}}^{p^n}(\gamma) - 1)\left(\prod_{\psi} L(0,\psi)\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
v_p\left(\prod_{\zeta,k} \nu_{0,\zeta}(g_{\omega^k})\right) &= v_p(\chi_{\mathrm{cyc}}^{p^n}(\gamma) - 1) + v_p\left(\prod_{\psi} L(0,\psi)\right) \\
&= n + 1 + v_p\left(\#\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^{n+1}})}[p^\infty]^-/p^n\right) \quad \text{(by CNF)} \\
&= 1 + v_p\left(\#X_\infty^\iota/(\gamma^{p^n} - 1)X_\infty^\iota\right) \\
&= v_p\left(\#\Lambda/(\mathrm{Char}(X_\infty^\iota), \gamma^{p^n} - 1)\right) + o(1) \\
&= v_p\left(\#\Lambda/\left(\textstyle\prod_k \mathrm{Char}(X_\infty^{\omega^k,\iota}), \gamma^{p^n} - 1\right)\right) + o(1).
\end{aligned}$$

On the other hand, if ϖ is a uniformizer in $\mathbf{Z}_p[\zeta_{p^n}]$, we have

$$\begin{aligned}
v_p\left(\prod_{\zeta,k} \nu_{0,\zeta}(g_{\omega^k})\right) &= \frac{1}{(p-1)p^{n-1}} v_\varpi\left(\prod_{\zeta,k} \nu_{0,\zeta}(g_{\omega^k})\right) \\
&= \frac{1}{(p-1)p^{n-1}} v_p\left(\prod_{\zeta,k} \#\Lambda_{\mathbf{Z}_p[\zeta_{p^n}]}/(g_{\omega^k}, \gamma - \zeta)\right) \\
&= \frac{1}{(p-1)p^{n-1}} v_p\left(\#\Lambda_{\mathbf{Z}_p[\zeta_{p^n}]}/\textstyle\prod_{k,\zeta}(g_{\omega^k}, \gamma - \zeta)\right) + o(1) \\
&= \frac{1}{(p-1)p^{n-1}} v_p\left(\#\Lambda_{\mathbf{Z}_p[\zeta_{p^n}]}/\left(\textstyle\prod_k g_{\omega^{-k}}, \gamma^{p^n} - 1\right)\right) + o(1) \\
&= v_p\left(\#\Lambda/\left(\textstyle\prod_k g_{\omega^{-k}}, \gamma^{p^n} - 1\right)\right) + o(1),
\end{aligned}$$

where the second equality is sort of like $v_\varpi(\#\mathbf{Z}_p/p) = v_p(\#\mathbf{Z}_p[\zeta_{p^n}]/p)$.

Therefore,

$$v_p\left(\#\Lambda/\left(\textstyle\prod_k \mathrm{Char}(X_\infty^{\omega^k,\iota}), \gamma^{p^n} - 1\right)\right) = v_p\left(\#\Lambda/\left(\textstyle\prod_k g_{\omega^{-k}}, \gamma^{p^n} - 1\right)\right) + o(1).$$

By hypothesis $\prod_k \mathrm{Char}(X_\infty^{\omega^k,\iota})$ either contains or is contained in $\prod_k g_{\omega^{-k}}$, so we must have equality because $\Lambda/(\text{these ideals}, \gamma^{p^n}-1)$ have the same order up to some bounded power of p. Thus we get $\mathrm{Char}(X_\infty^{\omega^k,\iota}) = (g_{\omega^{-k}})$.

8.2. **Proof of Main Conjecture.** We will prove that $\mathrm{Char}(X_\infty^{\psi,\iota}) \subseteq (g_{\psi^{-1}})$.

Let $\Psi : G_{\mathbf{Q}} \overset{\text{proj}}{\to} \Gamma \overset{\chi_{\text{cyc}}}{\to} \mathbf{Z}_p^\times$, and define

$$\mathcal{E}_\psi = g_\psi + h_\psi \sum_{n=1}^{\infty} \left(\sum_{\substack{d \mid n \\ (d,p)=1}} \prod_{\substack{\ell^e \| d \\ \ell \text{ primes}}} \psi\Psi(\mathrm{Frob}_\ell^e) \right) q^n.$$

Remark. My $\nu_{k,\zeta}(\mathcal{E}_\psi)$ is Pak-Hin's $\nu_{k+1,\zeta}(\mathcal{E}_{\psi\omega})$, so

$$v_{k,\zeta}(\mathcal{E}_\psi) \in M_{k+1}^{\mathrm{ord}}(p^N, \psi\omega\psi_\zeta\omega^{-k-1}) = M_{k+1}^{\mathrm{ord}}(p^N, \psi\psi_\zeta\omega^{-k}).$$

This is okay if we built the theory "oddly", and we will assume that we did. Thus $\mathcal{E}_\psi \in \mathbf{M}^{\mathrm{ord}}(1, \psi; \Lambda)$.

Step 1 (Construction of a Λ-adic cusp form):

Exercise. If $p = 3, 5, 7$, then $g_\psi \in \Lambda^\times$ for all ψ odd. Moreover, $g_{\omega^{-1}} \in \Lambda^\times$ for all $p > 2$.

If $p \geq 11$ and $k = 3, 5$, then

$$\nu_{0,1}(g_{\omega^k}) = L(0, \omega^k) = B_{1,\omega^k} \equiv B_{k+1} \pmod{p}.$$

Note $B_4 = -\frac{1}{30}$ and $B_6 = \frac{1}{42}$ which are units in $\mathbf{Z}_p$, so $g_{\omega^k} \in \Lambda^\times$ for $k = 3$ or 5.

Now let $p > 2$. Let $a, b \in \mathbf{Z}_{>0}$ be such that $m + 1 \equiv 4a + 6b \pmod{p-1}$. Then let

$$\mathcal{F} := \mathcal{E}_\psi - g_\psi g_{\omega^3}^{-a} g_{\omega^5}^{-b} \mathcal{E}_{\omega^3}^a \mathcal{E}_{\omega^5}^b \in \mathbf{S}^{\mathrm{ord}}(1, \psi; \Lambda).$$

Step 2 (g_ψ and the Eisenstein ideal): Let $\mathbf{T} = \mathbf{T}^{\mathrm{ord}}(1, \psi; \Lambda)$. Define the *Eisenstein ideal* by

$$I := \langle T_\ell - 1 - \psi\Psi(\mathrm{Frob}_\ell) \text{ for } \ell \neq p, U_p - 1 \rangle \subset \mathbf{T}.$$

The structure map $\Lambda \to \mathbf{T}/I$ is surjective, so denoting the kernel by J we have $\Lambda/J \cong \mathbf{T}/I$.

Claim. $J \subseteq (g_\psi)$.

Proof. If $\psi = \omega^{-1}$, then $(g_\psi) = \Lambda$ so there is nothing to prove. Otherwise, if $\psi \neq \omega^{-1}$, we will show that there exists a surjective $\varphi_I : \mathbf{T}/I \twoheadrightarrow \Lambda/(g_\psi)$ such that the diagram

$$\begin{tikzcd} \Lambda \arrow[rr, "\text{proj}"] \arrow[dr, "\text{structure}"'] & & \Lambda/(g_\psi) \\ & \mathbf{T}/I \arrow[ur, two heads, "\varphi_I"'] & \end{tikzcd}$$

commutes, from which the claim follows.

Consider φ_I defined by

$$\varphi_I : T_\ell \pmod{I} \mapsto a_\ell(\mathcal{F}) \pmod{g_\psi}.$$

This is an algebra homomorphism and fits in the diagram above, so $\mathbf{T}/I \to \Lambda/(g_\psi)$ is surjective. $\square$

Step 3 (Another reduction): The following reduction will be carried out next time.

Proposition 8.2. *To prove the Main Conjecture, it suffices to find a faithful* $\mathbf{T}$*-module* $\mathcal{M}_2$ *and a surjective* Λ*-module map* $X_\infty^{\psi^{-1},\iota} \twoheadrightarrow \mathcal{M}_2/I\mathcal{M}_2$.

Proof. Let R be a Noetherian ring, and M a finitely generated R-module with a finite presentation $R^m \xrightarrow{L} R^n \to M \to 0$. The *Fitting ideal of* M, denoted $\mathrm{Fitt}_R(M)$, is defined to be the ideal in R generated by the $n \times n$ minors of the matrix representing L. We have the following facts:

(0) This is well-defined.
(1) If $M = R/I$, then $\mathrm{Fitt}_R(M) = I$.
(2) $\mathrm{Fitt}_R(M \times N) = \mathrm{Fitt}_R(M) \cdot \mathrm{Fitt}_R(N)$.
(3) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $\mathrm{Fitt}_R(M') \cdot \mathrm{Fitt}_R(M'') \subseteq \mathrm{Fitt}_R(M)$.

Now choose a quasi-isomorphism

$$0 \to M \to \left(\bigoplus_i \Lambda/(f_i)\right) \oplus \left(\bigoplus_j \Lambda/(p^{n_j})\right) \to X_\infty^{\psi^{-1},\iota} \to N \to 0,$$

where M and N are of finite cardinality. Then $M = 0$ because $\bigoplus_i \Lambda/(f_i) \oplus \bigoplus_j \Lambda/(p^{n_j})$ does not have finite submodules. By Facts (1), (2), (3),

$$\mathrm{Fitt}_\Lambda\left(\left(\bigoplus_i \Lambda/(f_i)\right) \oplus \left(\bigoplus_j \Lambda/(p^{n_j})\right)\right) = \prod f_i \cdot \prod p^{n_j} \cdot \mathrm{Fitt}_\Lambda(N) \subseteq \mathrm{Fitt}_\Lambda(X_\infty^{\psi^{-1},\iota}),$$

i.e.,

$$\mathrm{Char}(X_\infty^{\psi^{-1},\iota})\,\mathrm{Fitt}_\Lambda(N) \subseteq \mathrm{Fitt}_\Lambda(X_\infty^{\psi^{-1},\iota}).$$

Since $\#N < \infty$, any Λ-module map $\Lambda \to N$ has kernel with finite index, so choosing $0 \neq n \in N$ (if it exists) we get an exact sequence

$$0 \to \Lambda/I \to N \to N' \to 0$$

where I has finite index in Λ, and $\#N' < \#N$. By induction and Fact (3), we deduce that $\mathrm{Fitt}_\Lambda(N)$ has finite index in Λ.

(4) If $M \twoheadrightarrow N$ is a surjective R-module map, then $\mathrm{Fitt}_R(M) \subseteq \mathrm{Fitt}_R(N)$.

Thus

$$\mathrm{Fitt}_\Lambda(X_\infty^{\psi^{-1},\iota}) \subseteq \mathrm{Fitt}_\Lambda(\mathcal{M}_2/I\mathcal{M}_2)$$

by assumption.

(5) $\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R(M) \pmod{I}$.

Thus

$$\begin{aligned}\mathrm{Fitt}_\Lambda(\mathcal{M}_2/I\mathcal{M}_2) \pmod{J} &= \mathrm{Fitt}_{\Lambda/J}(\mathcal{M}_2/I\mathcal{M}_2)\\ &= \mathrm{Fitt}_{\mathbf{T}/I}(\mathcal{M}_2/I\mathcal{M}_2)\\ &= \mathrm{Fitt}_{\mathbf{T}}(\mathcal{M}_2) \pmod{I}.\end{aligned}$$

(6) If M is a faithful R-module, then $\mathrm{Fitt}_R M = 0$.

So $\mathrm{Fitt}_{\mathbf{T}}(\mathcal{M}_2) = 0$ and hence $\mathrm{Fitt}_\Lambda(\mathcal{M}_2/I\mathcal{M}_2) \subseteq J$. Since $J \subseteq (g_\psi)$, we get

$$\mathrm{Char}(X_\infty^{\psi^{-1},\iota}) \,\mathrm{Fitt}_\Lambda N \subseteq (g_\psi).$$

Let $f_\psi = \prod f_i \prod p^{n_j}$, so $\mathrm{Char}(X_\infty^{\psi^{-1},\iota}) = (f_\psi)$. Then find two coprime elements $\alpha, \beta \in \mathrm{Fitt}_\Lambda N$ and we get $g_\psi \mid f_\psi \alpha$ and $g_\psi \mid f_\psi \beta$. Since Λ is a UFD, this implies $g_\psi \mid f_\psi$ and therefore $\mathrm{Char}(X_\infty^{\psi^{-1},\iota}) \subseteq (g_\psi)$. $\square$