Thm (Iwasawa) $\exists\, n_0, \mu, \lambda, \kappa$ s.t. $\forall n > n_0$

$$\# \, Cl_{\mathbb{Q}(\zeta_{p^n})}[p^\infty] = p^{\mu p^n + \lambda n + \kappa}$$

Recall $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ and $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) \simeq \mathbb{Z}_p$

$(1-\zeta_{p^n})$ generates the (totally ramified) prime above $p \in \mathbb{Z}$.

$\mathcal{O}_{\mathbb{Q}(\zeta_{p^n})} = \mathbb{Z}[\zeta_{p^n}]$

Defn. A $\mathbb{Z}_p$ extn of K_0 (# field) is an alg extn K_∞/K_0 s.t. $Gal(K_\infty/K_0) \simeq \mathbb{Z}_p$

Equiv it's a tower of $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_\infty = \bigcup_{n \geq 0} K_n$

s.t. $Gal(K_n/K_0) \simeq \mathbb{Z}/p^n$

Prop Let K_∞/K_0 be a $\mathbb{Z}_p$-extn

(1) some prime in K_0 is ramified in K_∞/K_0

(2) for any ramified prime $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$, $\exists\, n_0$ s.t. if $\mathfrak{q} \subseteq \mathcal{O}_{K_{n_0}}$ is s.t. $\mathfrak{q} \mid \mathfrak{p}$, then $\mathfrak{q}$ is totally ramified in K_∞/K_{n_0}

(3) every ramified prime lies over $p \in \mathbb{Z}$.

pf. (1) The max'l unr abel extn of K_0 is finite$/K_0$

(2) Let $\mathfrak{p}$, n_0 as in the condition. $I_\mathfrak{p}$ = inertia $\subseteq Gal(K_\infty/K_0)$ nontrivial, closed. So $I_\mathfrak{p} \simeq p^{n_0}\mathbb{Z}_p$, some n_0, so $I_\mathfrak{p} = Gal(K_\infty/K_{n_0})$

(3) Let $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$ ~~$Gal(K_{0,\mathfrak{p}}/K_{0,\mathfrak{p}})$~~ $Gal(K_{0,\mathfrak{p}}^{ab}/K_{0,\mathfrak{p}}) =$

$= \widehat{K_{0,\mathfrak{p}}^\times} \simeq \hat{\mathbb{Z}} \times \mathcal{O}_{K_0,\mathfrak{p}}^\times \longleftarrow$ finite gp $\times$ pro-(char $\mathfrak{p}$) gp

hence char $\mathfrak{p} = p \Rightarrow \mathfrak{p} \mid p$

Prop. Let L/K totally ramified (at some place in K) of # fields

Then $Cl_L[p^\infty] \xrightarrow{Nm} Cl_K[p^\infty]$ is surj.

pf. Let M_0/K be the max'l unr ab p-extn of K_0

M_1/L — — L

Then M_0 and L are linearly disj $/K$. $(M_0 \cap L = K$ in $\bar{K})$

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

use CFT. ∎

$C := \varprojlim_{n \geq 0} Cl_{K_n}[p^\infty]$ (w.r.t Nm maps).

Writing $\Gamma_n = Gal(K_n/K_0)$, $Cl_{K_n}[p^\infty]$ is a $\mathbb{Z}_p[\Gamma_n]$-mod

C is a module over $\Lambda := \varprojlim_{n \geq 0} \mathbb{Z}_p[\Gamma_n]$, limit taken w.r.t. $\Gamma_m \to \Gamma_n$ if $m \geq n$.

Thm (Iwasawa) C is a f.g. torsion Λ-module.
(To be proved later).

Structure of Λ Let $\gamma \in \Gamma = Gal(K_\infty/K_0) \subseteq \Lambda^\times$ be a topological gen.

$$\Gamma \cong \mathbb{Z}_p$$

Observation (Serre) $\Lambda \overset{top.}{\cong} \mathbb{Z}_p[[T]]$, $(\gamma - 1) \longmapsto T$

Cor (Nakayama's lemma) If M is a cpt Λ-module, and $M/TM = M/(\gamma-1)M$ is f.g. over $\mathbb{Z}_p$, then any set of gen's in M/TM lifts to a set of gen's in M. In particular, M is f.g.

Def. A quasi-iso of Λ-modules M, N is a map $\varphi: M \longrightarrow N$ s.t. $|\ker(\varphi)|$ & $|\mathrm{coker}(\varphi)|$ finite.

Thm (Weierstrass Preparation) Let $f \in \mathbb{Z}_p[[T]]$ be a non-constant power series. Then $\exists!\ n \geq 0$ and $\exists!\ g, u \in \mathbb{Z}_p[[T]]$ s.t. g is <u>distinguished</u>, $u \in \mathbb{Z}_p[[T]]^\times$, and

$$f = p^n \cdot u \cdot g$$

$\left(g = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \text{ is distinguished if } p \mid a_i, \forall i \right)$

Thm Let M be a f.g. Λ-mod. Then $\exists$ integers r, n_i and distinguished f_j ($i \in I$, $j \in J$, $\#I, \#J < \infty$), s.t.

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

pf of II (if only one ram. prime and it is totally ramified in K_∞/K_0).
Let $\mathfrak{p} \leq \mathcal{O}_{K_0}$ be the tot. ram. prime. Then

Main Claim $C/(\gamma-1)C \simeq Cl_{K_0}$

Let M_n/K_n be the max'l unr. ab. p-extns, $M_\infty = \bigcup_{n \geq 0} M_n$, so M_∞/K_∞ is the max'l unr. pro p ab extn and
$G_C = Gal(M_\infty/K_\infty) \simeq C$. Let $G = Gal(M_\infty/K_0)$
$\Gamma = Gal(K_\infty/K_0)$.

subclaim 1: If $I \leq G$ is the inertia at $\mathfrak{p}$, then $G = I \cdot G_C$ semidirectly.

pf. $\exists$ ex seq

$$1 \to \underset{G_C}{Gal(M_\infty/K_\infty)} \longrightarrow \underset{G}{Gal(M_\infty/K_0)} \longrightarrow \underset{\Gamma \simeq I}{Gal(K_\infty/K_0)}$$

Since $\mathfrak{p}$ is tot. ram. in K_∞, I surj's onto Γ and has empty intersection w/ G_C. $\square$

~~Rk~~ Let $\Gamma \simeq I$ act on G_C by conj. Then this action is the same as that on C. $\left(Frob_{\sigma q} = \sigma Frob_q \sigma^{-1}\right)$

subclaim 2. $G' =$ comm. subgp of G, then $\overline{G'} = (\gamma-1)G$

pf. $g \in G$, $(\gamma-1)g \triangleq \gamma g \gamma^{-1} g^{-1} \in G'$.
Conversely $G/\overline{(\gamma-1)G}$ is the largest quotient where Γ acts trivially. So conj. by elts in I is trivial and since G_C is abelian & subclaim 1 $\Rightarrow G/(\gamma-1)G$ is abelian $\Rightarrow \overline{(\gamma-1)G} \subseteq \overline{G'}$

$G/(\gamma-1)G$

$\parallel$

Note $(\gamma-1)G_C = (\gamma-1)G$

Pf of Main Claim

$G_C/(\gamma-1)G_C = G_C/(\gamma-1)G$

$\cong G/I\cdot(\gamma-1)G$

$\cdot$ mod I hence $\cdot$ unr. mod $(\gamma-1)G$ hence (by subclaim 2) abelian.

therefore it factors thru $\mathrm{Gal}(M_0/K_\infty)$

But $(\gamma-1)G_C \subseteq \ker(G_C \twoheadrightarrow \mathrm{Gal}(M_0/K_\infty))$ $\square$

By Main Claim $C \overset{\text{q-iso}}{\cong} \Lambda^r \oplus \bigoplus \Lambda/(p^{n_i}) \oplus \bigoplus \Lambda/(f_j)$

since $\Lambda^r/(\gamma-1)\Lambda^r \cong \mathbb{Z}_p^r$, we have $r=0$

Exercise: $\exists\, n_0$, s.t. if $n > n_0$, then $\#\,\Lambda/(f_j, \gamma^{p^n}-1) = p^{\deg(f_j)n + c}$ for some $c = c(f_j)$.

L-fctns

I. Class # formulas. p odd prime. $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ $K = \mathbb{Q}(\zeta_{p^n})$

Defn (a) A character $\psi: \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ is odd if $\psi(\text{cplx conj.}) = -1$

even if otherwise.

(b). Given a ψ, $L(s,\psi)$ is the cplx analytic function continuing

$$\sum_{n=1}^{\infty} \frac{\psi'(n)}{n^s}$$

where ψ' is the primitive char. assoc. w/ ψ.

$L(s,1) = \zeta(s)$.

(c) $K^+ := \mathbb{Q}(\zeta_{p^n})^+ := \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$ so $[K:K^+] = 2$.

Let $h = \#\mathrm{Cl}_K$, $h^+ = \#\mathrm{Cl}_{K^+}$. $h^- = \frac{h}{h^+}$

Rmk. $\mathrm{Cl}_K \xrightarrow{\mathrm{Nm}} \mathrm{Cl}_{K^+}$ is surj since K/K^+ is totally ramified $\Rightarrow h^- \in \mathbb{Z}$

Thm. (1) $$\operatorname*{Res}_{s=1} \zeta_L(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_L h_L}{\#\mu_L\sqrt{|\Delta_L|}} = \begin{cases} (2\pi)^{N/2}\,\mathrm{Reg}_K\, h/2p^n\sqrt{|\Delta_K|}, & \text{if } L=K \\ 2^{N/2}\,\mathrm{Reg}_{K^+} h^+/2\sqrt{|\Delta_{K^+}|}, & \text{if } L=K^+ \end{cases}$$

$N = (p-1)p^{n-1}$

(2) Let $\psi : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ have cond. $M(\psi)$. Then write

$$\Lambda(s,\psi) := \begin{cases} M(\psi)^{s/2}\, \pi^{-s/2}\, \Gamma(s/2)\, L(s,\psi) & \text{if } \psi \text{ even} \\ M(\psi)^{s/2}\, \pi^{-s/2}\, \Gamma\left(\frac{s+1}{2}\right) \cdot L(s,\psi) & \text{if } \psi \text{ odd} \end{cases}$$

Then $\Lambda(s,\psi) = \dfrac{\sqrt{\psi(-1) M(\psi)}}{S(\psi)}\, \Lambda(1-s,\psi)$.

where $S(\psi)$ is a Gauss Sum

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

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

(5) $\sum_{n \geq 0} B_{n,\psi} \frac{T^n}{n!} = \sum_{a=0}^{M(\psi)-1} \dfrac{\psi(a)\, T \cdot e^{aT}}{e^{M(\psi)T} - 1}$

Then if $n \in \mathbb{Z}$, $n \geq 1$, then $L(1-n,\psi) = -\dfrac{B_{n,\psi}}{n}$.

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

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

$$h^- = \frac{h}{h^+} \overset{(1)}{=} \frac{\mathrm{Reg}_{K^+} \sqrt{|\Delta_{K^+}|}}{\pi^{N/2}\, \mathrm{Reg}_K \sqrt{|\Delta_K|}} \cdot p^n \cdot \prod_{\psi \text{ odd}} L(1,\psi).$$

$$\overset{(2)}{=} \frac{\mathrm{Reg}_{K^+}}{\mathrm{Reg}_K} \cdot \frac{p^n \sqrt{|\Delta_K|}}{\sqrt{|\Delta_{K^+}|}} \prod_{\psi \text{ odd}} \left(L(0,\psi)\, \Gamma\left(\tfrac{1}{2}\right) i \cdot \pi^{1/2} / S(\psi) \right) \cdot \pi^{-\frac{N}{2}}$$

$$= \frac{1}{2^{N/2-1}} \cdot p^n \cdot \cancel{\pi^{N/2}} \cdot \frac{\sqrt{|\Delta_K|}}{\sqrt{|\Delta_{K^+}|}} \left(\prod_{\psi \text{ odd}} L(0,\psi) \right) \left(\prod_{\psi \text{ odd}} S(\psi)^{-1} \right) \cdot i^{\frac{N}{2}}$$

$$\overset{(3)}{=} 2 \cdot p^n \cdot \prod_{\psi \text{ odd}} \frac{L(0,\psi)}{2}$$

Rmk. (p-part of h^-) $\overset{\text{Exercise}}{=\!=}$ $\prod_{\psi \text{ odd}} \# Cl_K[p^\infty]^\psi$

Also $Cl_{\mathbb{Q}(\zeta_p)}[p^\infty]^\omega = 0$ $\quad v_p(p \cdot B_{1,\omega}) = 0$

ω: Teichmüller character.

Thus $\prod_{\psi \text{ odd}} \# Cl_{\mathbb{Q}(\zeta_p)}[p^\infty]^\psi = \prod_{\psi \text{ odd}} \# \mathbb{Z}_p / (L(0,\psi))$.

In fact, this is true w/o products

This strengthens Ribet – Herbrand

(b/c $v_p(B_{p-m}) = v_p(B_{1,\omega^m})$ ~~...~~.

II p-adic L-fctn.

Fix $\gamma \in \Gamma \subseteq \Lambda^\times$ a top gen. of Γ. Let χ_{cyc} be the cyclotomic char.

Let ζ be a p^n root of 1. (not nec. primitive)

For $k \in \mathbb{Z}$, let $\phi_{k,\zeta}: \Lambda \longrightarrow \mathbb{Z}_p[\zeta]$ sending γ to $\chi_{cyc}^k(\gamma) \cdot \zeta$

Thm Let $\psi: Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ be an odd char. Then $\exists$ $g_\psi \in \Lambda$ s.t. if we write

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

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

where $\psi_\zeta : Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$

image of $\gamma \longmapsto \zeta$.

Defn. g_ψ is called a p-adic L-fctn.

III Main Conjecture

Defn. For M - f.g. torsion Λ-mod. write $M \overset{\text{q-isog}}{\simeq} \bigoplus_i \Lambda/p^{n_i} \oplus \bigoplus_j \Lambda/(f_j)$ as in the classification. Then the char. ideal of M is $\mathrm{Char}(M) := \left(\prod_i p^{n_i} \prod_j f_j\right) \cdot \Lambda$

Recall Last time we constructed $C := \varinjlim_{n \geq 1} Cl_{\mathbb{Q}(\zeta_{p^n})}[p^\infty]$.

Let C^ψ = ψ-eigenspace of C, $\psi : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{C}^\times$ is an odd char.

Rmk $C^\psi = \varinjlim_n \left(Cl_{\mathbb{Q}(\zeta_{p^n})}[p^\infty]^\psi\right)$

Thm (Main Conj) $\mathrm{Char}(C^\psi) = (g_\psi)$.

Cor. $\# Cl_{\mathbb{Q}(\zeta_p)}[p^\infty]^\psi = \# \mathbb{Z}_p/(L(0,\psi))$. $\psi \neq \omega^{-1}$

pf. First we need Prop: C has no finite cardinality Λ-submodules

Exercise: if M is f.g ~~Λ-mod~~ torsion Λ-mod w/ no finite submod. and if $M/(\gamma^{p^n}-1)M$ is finite $\forall n$, then

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

Now

$$\# Cl_{\mathbb{Q}(\zeta_p)}[p^\infty]^\psi = \# C^\psi/(\gamma-1)C^\psi$$

$$\overset{\text{Ex}}{=} \# \Lambda/(\gamma-1, \mathrm{char}\, C^\psi).$$

$$\overset{\text{MC}}{=} \# \Lambda/(\gamma-1, g_\psi)$$

$$= \# \mathbb{Z}_p/(\phi_{0,1}(g_\psi)) = \# \mathbb{Z}_p/(L(0,\psi)).$$