Goal. Overview of the Herbrand-Ribet thm (Iwasawa theory)

p - odd prime.

$C :=$ p-part of $Cl(\mathbb{Q}(\zeta_p))$

Recall: p-part of $A(\mathbb{Q}(\zeta_p))$ $\rightsquigarrow$ obstruction to naïve proof of Fermat eq'n.

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times \xleftarrow{\sim} G_1(\mathbb{Q}(\mu_p)/\mathbb{Q}) \curvearrowright C$$

↓ representation theory

isotypic decomp.

$$C = \bigoplus_{i=0}^{p-2} C(\overline{K}^i)$$

↑

$G_1(\mathbb{Q}(\mu_p)/\mathbb{Q})$ - equivariant

Rmk. ($C(\overline{K}) = 0$)

Thm. Let $3 \le i \le p-2$ be odd. Then

$$C(\overline{K}^i) \neq 0 \overset{\text{(Herb)}}{\Rightarrow} \overset{\text{(Ribet)}}{\Leftarrow} p \text{ divides } B_{p-i}.$$

$$\left[\frac{t}{e^t - 1} = \sum_{n \ge 0} B_n \frac{t^n}{n!} \right]$$

better

Let $j = p - i$.

$\in \mathbb{Q}$ ↓

RHS $\Leftrightarrow$ $p \mid \zeta(1-j)$

Recollection on ζ.

Prop. If $k \ge 1$, then $\zeta(2k) = \pi^{2k} \left(\frac{(-1)^{k+1} 2^{2k-1} B_{2k}}{(2k)!} \right)$

Pf. $\cot(z) = \frac{\cos(z)}{\sin(z)} = i\frac{e^{iz}+e^{-iz}}{e^{iz}-e^{-iz}} = i\frac{e^{2iz}+1}{e^{2iz}-1} = i\left(1+\frac{2}{e^{2iz}-1}\right)$

$\rightsquigarrow z\cot(z) = iz + \frac{2iz}{e^{2iz}-1} = iz + \sum_{n\geq 0} B_n \frac{(2iz)^n}{n!}$

Take $d\log(\cdot)$: $\sin(z) = z\cdot\prod\left(1-\frac{z^2}{n^2\pi^2}\right)$

$$\cot(z) = \frac{1}{z} + \sum_{n\geq 1} \frac{1}{1-z^2/n^2\pi^2}\cdot\frac{-2z}{n^2\pi^2}$$

$$\Rightarrow z\cot(z) = 1 - 2\sum_{n\geq 1}\frac{z^2}{n^2\pi^2}\sum_{k\geq 0}\left(\frac{z^2}{n^2\pi^2}\right)^k$$

$$= 1 - 2\sum_{n\geq 1}\sum_{k\geq 1}\left(\frac{z^2}{n^2\pi^2}\right)^k$$

Compare coeff's of z^{2k} for $k\geq 1$.

$$\frac{B_{2k}}{(2k)!}\, z^{2k}(-1)^k = \frac{-2}{\pi^{2k}}\zeta(2k). \qquad \blacksquare$$

Recall. Let $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Then ξ has meromorphic continuation w/ functional eq'n $\xi(s) = \xi(1-s)$.

Cor. For $k\geq 1$, $\zeta(1-2k) = -\frac{B_{2k}}{2k}$.

Pf. $\zeta(2k)\pi^{-k}\Gamma(k) = \zeta(1-2k)\,\pi^{-\frac{1-2k}{2}}\,\Gamma\left(\frac{1-2k}{2}\right)$

$$\Rightarrow \zeta(1-2k) = \frac{\pi^{2k}}{(2k)!}(-1)^{k+1}2^{2k-1}B_{2k}\cdot\pi^{-k}(k-1)!\cdot\pi^{\frac{1-2k}{2}}$$

$$\Gamma\left(\frac{1-2k}{2}\right) = \frac{(-4)^k k!\sqrt{\pi}}{(2k)!}$$

$$= -\frac{B_{2k}}{2k}. \quad \blacksquare$$

Reformulation of the condition $C(\mathbb{K}^i) \neq 0$ via CFT:

L = maximal ab everywhere unram p-extension of $\mathbb{Q}(\zeta_p)$

$\mathbb{Q}(\zeta_p)$

$\mathbb{Q}$

Then, non-vanishing of $C(\mathbb{K}^i) \neq 0$

$$\Updownarrow$$

$$\mathrm{Hom}_{\underline{G(\mathbb{Q}(\mu_p)/\mathbb{Q})}}\left(G(L/\mathbb{Q}(\mu_p)), \mathbb{T}_p(\mathbb{K}^i)\right) \neq 0.$$

G !!!

$$= H^1_{\mathcal{L}}\left(\mathbb{Q}(\zeta_p), \mathbb{T}_p(\mathbb{K}^i)\right)^G$$

where $\mathcal{L}$ = Selmer system $\mathcal{L}_v$:

$$\mathcal{L}_v = H^1\left(\Gamma_{\mathbb{F}_v}/I_{\mathbb{F}_v}, \mathbb{T}_p(\mathbb{K}^i)^{I_{\mathbb{F}_v}}\right)$$

is the unram coho $\forall v$.

But $H^1_{\mathcal{L}_{\mathbb{Q}}}(\mathbb{Q}, \mathbb{F}_p(\pi i)) \xrightarrow{\text{res}}_{\sim} H^1_{\mathcal{L}}(\mathbb{Q}(\zeta_p), \mathbb{F}_p(\pi i))^G$

($\mathcal{L}_{\mathbb{Q}}$: everywhere unram.) w/o local cond.'s res is iso b/c

$(|G|, |\mathbb{F}_p|) = 1$.

w/ local condition. Clear that $H^1_{\mathcal{L}_{\mathbb{Q}}} \longrightarrow H^1_{\mathcal{L}}$. Have to check that all elt's of $(H^1_{\mathcal{L}})^G$ (φ) came from $H^1_{\mathcal{L}_{\mathbb{Q}}}$. By assumption, $\forall$ prime ℓ, $(\varphi|_{\mathbb{F}})_{v|\ell} \in \left(\bigoplus H^1(I_{\mathbb{F}})\right)^G$ is zero. But

$$H^1(I_{\mathbb{Q}_\ell}) \longrightarrow \left(\bigoplus_{v|\ell} H^1(I_{\mathbb{F}_v})\right)^G$$

is injection

$\begin{cases} \ell \neq p: \text{ then } I_{\mathbb{Q}_\ell} \cong \Gamma_{\mathbb{F}_v}\ (\mathbb{F}/\mathbb{Q} \text{ unr } @\ell) \\ \ell = p: \ker\left(H^1(I_{\mathbb{Q}_p}) \longrightarrow H^1(I_{\mathbb{F}_p})\right) \\ \qquad = 0 \text{ again by res-inf.} \end{cases}$

Better: since $H^1(\Gamma_{\mathbb{Q}_p}/I_{\mathbb{Q}_p}, \underbrace{\mathbb{F}_p(\pi i)^{I_{\mathbb{Q}_p}}}_{0}) = 0$.

$\Gamma := G$

For $\varphi \in H^1_{\mathcal{L}_{\mathbb{Q}}}(\mathbb{Q}, \mathbb{F}_p(\pi i))$, $\varphi|_{G_{\mathbb{Q}_p}} = 0$ so we

are looking for extensions (non-split)

$$0 \to \mathbb{F}_p(\pi^i) \longrightarrow \bar{\rho} \longrightarrow \mathbb{F}_p \to 0,$$

s.t. $\bar{\rho}: G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ is unr. at all $\ell \neq p$ and is split @ p.

$$\rho \sim \begin{pmatrix} \pi^i & * \\ & 1 \end{pmatrix}$$

$$\rho|_{G_{\mathbb{Q}_p}} \sim \pi^i \oplus 1$$

Can base change $\mathbb{F}_p$ to $\overline{\mathbb{F}_p}$.

Target thm. Let $2 \leq j \leq p-3$ be even then if $\rho|_{I_p} \sim (\omega^{1-j}, 1)$, then $\exists$ non-split $\bar{\rho}: G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p^2)$.

1) $\forall \ell \neq p$, $\bar{\rho}|_{I_{\mathbb{Q}_\ell}} = 1$, $\simeq \begin{pmatrix} \omega^{1-j} & * \\ & 1 \end{pmatrix}$

2) $\bar{\rho}_{G_{\mathbb{Q}_p}} \simeq \omega^{1-j} \oplus 1$.

Rmk. $\exists$ an interpretation of (2) for i even.

Vandiver's conj - $c(\pi^i) = 0$ for even.

Rmk. Hecke proved converse long ago.

where do Galois rep'ns come from? modular forms

Strategy for Ribet's thm. ~~Find~~ Given $p \mid \#\mathrm{Cl}(\mathbb{Q}(\sqrt{-j}))$, find a mod p congruence b/w a cuspidal mod form & an Eisenstein series to produce $\bar{\rho}$.

For Ribet's thm, suffices to use $\Gamma = SL_2(\mathbb{Z})$.

Rmk. Ribet's original proof doesn't work this way. The arg we sketch is a simplification/spec. of Wiles Main Conjecture pf.

Recall $M_k(\Gamma) = \{ f : \mathfrak{h} \to \mathbb{C}$ hol s.t. $\forall \gamma \in \Gamma, f(\gamma z) = j(\gamma, z)^k f(z) \}$

Def. $\gamma \in GL_2(\mathbb{R})^+$, $j(\gamma, z) = cz + d$

"$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$"

Since $f(z+1) = f(z)$, $f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$ $\quad q = e^{2\pi i z}$

"hol @ ∞" $\Leftrightarrow$ $a_n = 0$ for $n < 0$.

f is <u>cuspidal</u> if f vanishes @ ∞, i.e. $a_0 = 0$.

Write $S_k(\Gamma) \subset M_k(\Gamma)$ for the space of cusp forms (both are f.d. $\mathbb{C}$-vector spaces).

<u>Hecke operators</u>.

Another interpretation: let $\mathcal{L} = \{\text{lattices in } \mathbb{C}\}$

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathcal{L} \\ z &\longrightarrow \mathbb{Z}z + \mathbb{Z} \end{aligned} \qquad \text{yields a bijection}$$

$$\Gamma \backslash \mathcal{L} \longrightarrow \mathcal{L}/\text{homothety}.$$

$$\gamma z \longrightarrow \Lambda_{\gamma z} = \cdots = \frac{1}{cz+d}\Lambda_z$$

Can then view mod. forms as f'ns on lattices. If $F: \mathcal{L} \to \mathbb{C}$, F s.t. $F(a\Lambda) = a^{-k}F(\Lambda)$ $f: \mathcal{h} \to \mathbb{C}$ by

$$f(z) = F(\Lambda_z)$$

$$\rightsquigarrow f(\gamma z) = F(\Lambda_{\gamma z}) = F\left(\frac{1}{cz+d}\cdot\Lambda_z\right) = (cz+d)^k F(\Lambda_z)$$
$$= \gamma(\gamma, z)^k f(z).$$

<u>Def</u>. For all $n \geq 1$, define T_n on $\{\mathcal{L} \xrightarrow{F} \mathbb{C}\}$

by $(T_n F)(\Lambda) = \sum_{\substack{\Lambda' \subset \Lambda \\ \text{index } n}} F(\Lambda')$.

On mod. forms, if $f \longleftrightarrow F : \mathcal{L} \to \mathbb{C}$,

set $(T_n f)(z) = n^{k-1} (T_n F)(\Lambda_z) = n^{k-1} \sum_{\substack{\Lambda' \subset \Lambda \\ n}} F(\Lambda')$.

e.g. wt k Eisenstein series

Fix $k > 2$. Set $G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda} \frac{1}{\lambda^k}$ or

equivalently: $G_k : \mathcal{L} \to \mathbb{C}$ by $G_k(z) = G_{2k}(\Lambda_z)$

$$= \sum_{\substack{(m,n) \\ \neq (0,0)}} \frac{1}{(mz+n)^k}$$

1) G_{2k} defines hol fn. on $\mathcal{L}$. Also hol @ ∞

2) $G_{2k} \in M_k(\Gamma)$. In lattice picture,

$$G_{2k}(\alpha\Lambda) = \sum_{\lambda \in \alpha\Lambda} \frac{1}{\lambda^k} = \sum_{\lambda \in \Lambda} \frac{1}{(\alpha\lambda)^k} = \alpha^{-k} G_{2k}(\Lambda).$$

Lemma. G_{2k} is a simultaneous eigenfunction of all Hecke operators T_n.

Pf: ① alg gen'd by Hecke ops T_n is actually gen'd by (homothetics mult by p), and T_p $\forall$ primes

p (pf : if $(m,n)=1$, then CRT $\Rightarrow T_{mn} = T_m T_n$.

∃ recursive formulas for $T_{p^{n+1}}$ in terms of lower powers).

② $(T_p G_k)(\Lambda) = \underbrace{\sum_{\Lambda' \subset \Lambda}}_{p} G_k(\Lambda') = \underbrace{\sum_{\Lambda' \subset \Lambda}}_{p} \sum_{\lambda \in \Lambda'} \frac{1}{\lambda^k}$

For $\lambda \in \Lambda$, two cases: $\lambda \in p\Lambda$: then $\lambda \in \Lambda'$ ∀ index p $p\Lambda' \subset \Lambda$

$\lambda \notin p\Lambda$: then λ appears in exactly one index p sublattice

contribution $\frac{1}{\lambda^k}$

$p+1$ " $|\mathbb{P}^1(\mathbb{F}_p)|$

So $(T_p G_k)(\Lambda) = G_k(\Lambda) + p \cdot G_k(p\Lambda)$

$= G_k(\Lambda) + p^{1-k} G_k(\Lambda)$

$= (1 + p^{1-k}) G_k(\Lambda)$.

Translated to $G_k : \mathcal{h} \to \mathbb{C}$ (recall here $T_p = p^{k-1}$, previous $T_p = p^{k-1}$), we see

$(T_p G_k)(z) = (p^{k-1} + 1) G_k(z) = \sigma_{k-1}(p) G_k(z)$.