2012/4/3 talk II

Recall the following result.

<u>Thm</u> (Herbrand-Ribet)

$p \mid \zeta(1-2m) \Leftrightarrow Cl(\mathbb{Q}(\zeta_p))[p]^{\omega^{1-2m}} \neq \{0\}$ $\lrcorner$

<u>Rmk</u> (1) By analytic class number formula

p divides one of $\zeta(1-2m)$ for $0<2m<p-1$

$\Leftrightarrow Cl(\mathbb{Q}(\zeta_p))[p] \neq \{0\}$

(2) $\Leftarrow$ is due to Herbrand (around 1930?)

$\Rightarrow$ is due to Ribet (1976) $\lrcorner$

From now, we will prove ($\Rightarrow$) of the above thm.

<u>Main strategie</u>

(A) construction of a normalized eigen cuspform f congruent to an Eisenstein series.

(B) find a lattice $T \cong \mathcal{O}^{\oplus 2} \subset V_f \curvearrowleft G_{\mathbb{Q}}$

s.t $T/\varpi T \curvearrowleft G_{\mathbb{Q}}$ is irred.

"locally trivial" at every prime.

Once (A),(B) is established, we have

$(*)\ 0 \longrightarrow \mathbb{F}_q(\mathbb{1}) \longrightarrow T/\varpi T \longrightarrow \mathbb{F}_q(\omega^{1-2m}) \longrightarrow 0 \curvearrowleft G_{\mathbb{Q}}$

with $\mathbb{F}_q = \mathcal{O}/(\varpi)$ by Chebotarev density thm.

$(*)$: non-trivial ext. by (A)

$\Rightarrow$ determines a non-trivial element $C_{(*)} \overset{\neq 0}{\in} H^1(\mathbb{Q}, \mathbb{F}_q(\omega^{2m-1}))$

Property (B) $\Rightarrow$ the image of $C_{(*)}$ via the restriction map:

$$\mathrm{res}: H^1(\mathbb{Q}, \mathbb{F}_p(\omega^{2m-1})) \hookrightarrow H^1(\mathbb{Q}(\zeta_p), \mathbb{F}_p(\omega^{2m-1}))$$
$$\qquad\qquad\qquad\qquad\qquad\qquad \| $$
$$\qquad\qquad\qquad\qquad \mathrm{Hom}(G_{\mathbb{Q}(\zeta_p)}, \mathbb{F}_p(\omega^{2m-1}))$$

is unramified at every prime of $\mathbb{Q}(\zeta_p)$.

Hence $\mathrm{res}(C_{(*)}) \overset{\neq 0}{\in} \mathrm{Hom}(Cl(\mathbb{Q}(\zeta_p))[p]^{\omega^{1-2m}}, \mathbb{F}_q)$

$$\Rightarrow Cl(\mathbb{Q}(\zeta_p))[p]^{\omega^{1-2m}} \neq \{0\}$$

<u>Part (A)</u>

For η : Dir. char. of conductor M and $k \in \mathbb{N}$

$$E_{k,\eta} \overset{\text{def}}{:=} \frac{M^k (k-1)!}{2G(\eta^{-1})(2\pi\sqrt{-1})^k} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\eta^{-1}(n)}{(mMz+n)^k}$$

where $G(\eta^{-1})$ is the Gauss sum

we assume $\eta \neq \mathbb{1}$ for $k \leq 2$

Recall that $E_{k,\eta}$ has the q-expansion as follows

$$E_{k,\eta} = \frac{L(\eta, 1-k)}{2} + \sum_{1\leq n<\infty} \sigma_{k-1,\eta}(n)\, q^n$$

where $\sigma_{k-1,\eta}(n) := \sum_{0<d|n} \eta(d)\, d^{k-1}$

By the well-known congruence,

$$\zeta(1-2m) \equiv L(\omega^{-2m}, -1) \mod p$$

Hence

constant term of $E_{2,\omega^{-2m}}$ is divisible by p.

Let us take $a, b \in \mathbb{Z}$ s.t $a+b \equiv -m \mod p-1$

Put $G_{a,b} = E_{1,\omega^a} E_{1,\omega^b} \in M_2(\Gamma_1(p) : \mathcal{O})^{\omega^{-2m}}$

<u>Claim</u> There exist $a, b \in \mathbb{Z}$ s.t

the constant term of $G_{a,b}$ is a p-unit. $\lrcorner$

By the asymptotic formula on the class numbers obtained by Carlitz et al :

$$(B_p) \quad \begin{aligned} \operatorname{ord}_p \prod_a L(\omega^a, 0) &\leqq \operatorname{ord}_p \# Cl(\mathbb{Q}(\zeta_p))[p] \\ &< \frac{p-1}{4} \end{aligned}$$

and explicit calculation for $p \leq 19$,

Claim is true for all p.

By Claim

$$f' = E_{2,\omega^{-m}} - \frac{L(\omega^{-2m}, -1)}{a_0(G_{a,b})\,2} G_{a,b} \in M_2(\Gamma_1(p);\mathcal{O})^{\omega^{-2m}}$$

has the following property:

(i) congruent to $E_{2,\omega^{-2m}}$ mod (ϖ)

(ii)$'$ "eigenform mod (ϖ)"

(iii)$'$ constant term at $\sqrt{-1}\infty$ is zero.

Recall the following lemma:

<u>Lemma</u>

Let M be a free $\mathcal{O}$-module of finite rank on which we have $\mathcal{O}$-linear endomorphisms $T_1, \cdots, T_n, \cdots$.
If $\bar{v} \in M/\varpi M$ is "eigenvector mod ϖ", there exist a finte ext. $\mathcal{O}'$ and $v \in M_{\mathcal{O}'}$

s.t $\begin{cases} v \text{ is an eigenvector} \\ v \equiv \bar{v} \mod (\varpi) \end{cases}$

$\lrcorner$

Using this lemma, we have $f \in M_2(\Gamma_1(p):\mathcal{O})^{\omega^{-2m}}$ satisfying (i), (iii)$'$ and
(ii) eigenform in $M_2(\Gamma_1(p):\mathcal{O})^{\omega^{-2m}}$

Further, by the decomposition: space of Eisenstein series

$$M_2(\Gamma_1(p):\mathcal{K})^{\omega^{-2m}} = S_2(\Gamma_1(p):\mathcal{K})^{\omega^{-2m}} \oplus \underbrace{E_2(\Gamma_1(p):\mathcal{K})^{\omega^{-2m}}}_{\text{space of Eisenstein series}}$$

($\mathcal{K} = \mathrm{Frac}(\mathcal{O})$)

By the explicit description of eigenbases of $E_2(\Gamma_1(p):\mathcal{K})^{\omega^{-2m}}$, there are no non-zero elements in $E_2(\Gamma_1(p):\mathcal{K})^{\omega^{-2m}}$ satisfying (i) and (iii)'.

$\Rightarrow$ f falls in $S_2(\Gamma_1(p):\mathcal{O})^{\omega^{-2m}}$.

Part (B)

Let $V_f \cong \mathcal{K}^{\oplus 2} \curvearrowleft G_{\mathbb{Q}}$ (homological) Galois rep ass. to f due to Eichler, Shimura

① For any $\mathcal{O}_{\mathcal{K}}$-lattice $T \subset V_f$

$$(T/\varpi T)^{s.s} \cong \mathbb{F}_q(\omega^{1-2m}) \oplus \mathbb{F}_q(\mathbb{1})$$

$\Rightarrow$ $\exists\, \mathcal{O}_{\mathcal{K}}$-lattice $T \subset V_f$

s.t. $0 \longrightarrow \mathbb{F}_q(\mathbb{1}) \longrightarrow T/\varpi T \longrightarrow \mathbb{F}_q(\omega^{1-2m}) \longrightarrow 0$

$\bar{\rho} \curvearrowleft G_{\mathbb{Q}}$

② (Ribet's lemma)

We may assume that the ext. given at ① is non-trivial.

In fact, we take the matrix rep. $M = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ of

$\rho : g \in G_{\mathbb{Q}} \curvearrowright T$.

Note that $c(g) \equiv 0 \bmod \varpi$. We want to show that $\exists g \in G_{\mathbb{Q}}$ s.t $b(g) \not\equiv 0 \bmod \varpi$.

$$\begin{pmatrix} 1 & 0 \\ 0 & \varpi^{n} \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ 0 & \varpi^{-n} \end{pmatrix} = \begin{pmatrix} a(g) & \varpi^{-n} b(g) \\ \varpi^{n} c(g) & d(g) \end{pmatrix}$$

Since $G_{\mathbb{Q}} \curvearrowright V_f$ is irred. by Ribet, $b(g)$ is not identically zero.

replacing T by twisting with $\begin{pmatrix} 1 & 0 \\ 0 & \varpi^{n} \end{pmatrix}$ for $n \gg 0$, we prove the non-triviality of the ext. mod ϖ.

③ Let $J_1(p)$ (resp. $J_0(p)$) be the jacobian var. of the modular curve $X_1(p)$ (resp. $X_0(p)$).

By local Langlands corr. (proved by Carayol), abel. var $J_1(p)/J_0(p)$ has good red. over $k = \mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$.

$\Rightarrow \exists$ abel. var $B_{/\mathbb{Q}} \underset{\text{isog.}}{\sim} J_1(p)/J_0(p)$ s.t. $T/\varpi T \hookrightarrow B(\overline{\mathbb{Q}})[p]$

Let B abelian scheme $/\mathcal{O}_k$

We have a finite flat gp scheme $\mathcal{G}_{/\mathcal{O}_k}$

s.t $T/\varpi T \simeq \mathcal{G}(\bar{k}) \curvearrowleft G_k$

Standard decomp. $0 \to \mathcal{G}^{\cancel{0}\,\mathrm{conn}} \to \mathcal{G} \to \mathcal{G}^{\text{ét}} \to 0$

$e(k) < p-1 \xrightarrow{\text{Raynaud}} \mathcal{G}$ is unique

$\Rightarrow T/\varpi T \supset \mathcal{O}_{k/(\varpi)}(\mathbb{1})$ split!

$T/\varpi T \supset \mathcal{O}_{k/\varpi}(\omega^{1-2m})$ //