Ming-Lun Hsieh

Lecture (1) : Eisenstein congruence on unitary groups

§1 Main Conjecture for CM elliptic curves

Notation:

F : totally real field of degree $d/\mathbb{Q}$
M : imaginary quad field
E : elliptic curves with CM by $\mathcal{O}_M$ $/F$
p : rational prime > 2

Assumption :
E has good ordinary reduction at all places of F above p

F_∞ : the cyclotomic ext $/F$
$\Lambda_F = \mathcal{O}[[\mathrm{Gal}(F_\infty/F)]]$

The p-adic L-function for E is obtained by the specialization of a certain twist of Katz p-adic L for $K = F \cdot M$ to the cyclotomic line

$$\left(\begin{array}{l} \psi_E : \mathrm{Gal}\left(K(E[\mathfrak{p}])/K\right) \longrightarrow \mathrm{Aut}\left(E[\mathfrak{p}]\right) = \mu_{p-1} \hookrightarrow \mathbb{Z}_p^\times \\ p = \mathfrak{p}\cdot\bar{\mathfrak{p}} \text{ in } M \end{array}\right)$$

$$L_p(E) \in \Lambda_F$$

$$\mathrm{Sel}_{F_\infty}(F) = \mathrm{Ker}\left(H^1(F_\infty, E[p^\infty]) \longrightarrow \prod_v H^1(F_{\infty,v}, E)\right)$$

cofinitely generated Λ_F-module

$$F_p(E) = \mathrm{char}_{\Lambda_F} \mathrm{Sel}_{F_\infty}(E)^*$$

Iwasawa Main Conjecture for E (IMC for E) says

$$(F_p(E)) = (L_p(E))$$

Thm (Hsieh)

Suppose

(1) $p \nmid 6 \cdot h_K/h_F \cdot D_F$

$\star$ (2) The root # of $E = 1$

(3) The conductor N_E of E is a product of split primes in K/F

Then $(F_p(E)) \subset (L_p(E))$

Moreover, if we assume $\boxed{K(E[p]) \text{ is abelian over } M}$

Then $(F_p(E)) = (L_p(E))$

$\left(\text{Rubin's result implies IMC if } \underbrace{K(E_{tors})/M}_{\text{abelian}} \right)$

From now on, K is a general CM field with maximal totally real subfield F

(ord) Every prime of F above p splits in K

Σ : p-ordinary CM type

$K_\infty = K_\infty^+ K_\infty^-$: $\left(\begin{array}{ll} K_\infty^+ & \text{cyclotomic } \mathbb{Z}_p\text{-ext} \\ K_\infty^- & \text{anticyclotomic } \mathbb{Z}_p^d\text{-ext} \end{array} \right.$

Def (p-ordinary CM type) $\left(\begin{array}{l} \iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \\ \iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C} \end{array} \right)$

- Σ is a CM-type
- $\Sigma_p = \{ \text{primes induced from } \iota_p \circ \sigma,\ \sigma \in \Sigma \text{ of } K \}$
- Σ is p-ordinary if $\Sigma_p \amalg \overline{\Sigma}_p = \{ \text{primes of } K \text{ above } p \}$
- $\psi : Gal(K'/K) \longrightarrow \overline{\mathbb{Q}}_p^\times$

  K'/K : finite abel ext of K, K' is disjoint from K_∞

with this datum

We have
- Katz p-adic $L \rightsquigarrow L_{\psi,\Sigma} \in \Lambda = \mathcal{O}[\![Gal(K_\infty/K)]\!]$
- $\mathfrak{X}_\Sigma(K_\infty) = Gal(M_\Sigma(K_\infty)/K'_\infty)$
  where $K'_\infty = K' \cdot K_\infty$

$M_\Sigma(K_\infty)$ is the max abelian p-ext of K'_∞ unramified outside Σ_p

$F_{\psi,\Sigma} := char_\Lambda \mathfrak{X}_\Sigma(K_\infty)$

<u>IMC</u> $(L_{\psi,\Sigma}) = (F_{\psi,\Sigma})$

<u>Thm</u> Assume (1) ~ (4)

(1) $(p, 6 \cdot h_K/h_F \cdot D_F) = 1$

(2) ψ is unram at Σ_p^c and for some $a \not\equiv 2 \ (p-1)$
$\psi\omega_K^{-a}$ is unram at Σ_p

(3) $(D_{K/F}, 2) = 1$

(4) the μ-invariant of the (anti) cyclotomic projection of $L_{\psi,\Sigma}$ $\mu^-_{\psi,\Sigma} = 0$

Then $(L_{\psi,\Sigma}) \subset (F_{\psi,\Sigma})$

The method is to study Eisenstein congruence on $U(2,1)/F$

(Rough)

<u>Steps</u> (1) Construct ordinary E.S. on $U(2,1)$ with good constant terms

(2) Show this ES is nonzero modulo p (Murase - Sugano's computation + <u>works</u> of Hida and Hsieh)

$\downarrow$ ✱ This is the place we use condition (3)

(1) + (2) $\Rightarrow$ This exists a tempered ordinary cusp forms congruent to ES.

(3) Use Ribet's lemma $\Rightarrow$ cocycles in H^1

(4) Use some <u>p-adic Hodge theory</u> $\hookrightarrow$ use cond (2)

$\Rightarrow$ cocycles in Sel

<u>Remark</u> If the root # of E is -1, in fact, Bellaiche and Chenevier construct nontrivial elements in Selmer groups for imaginary fields by CAP congruence.

§2. Revisit Wiles's proof of IMC for totally real fields

<u>Assume</u> $p \nmid D_F$

$G = GL(2)/_F$ $\quad$ K open compact $\subseteq G(\mathbb{A}_{F,f})$

K is neat and $K_p = GL_2(\mathcal{O}_F \otimes \mathbb{Z}_p)$

$$\det(K) \cap F_+ \subset (K \cap \underset{\underset{\text{center of } GL_2}{\parallel}}{Z(F)})^2$$

$$\underset{\mathcal{O}_{F+}}{\cap}$$

let $\mathcal{O} \subset \overline{\mathbb{Z}}_{(p)}$ be a discrete valuation ring

$S_G(K)/_{\mathcal{O}}$: Hilbert modular variety

$$S_G(K)(\mathbb{C}) = {}_{G(F)^+}\backslash \mathfrak{h}^d \times G(\mathbb{A}_{F,f})/K$$

$C(K)$: the set of cusps of $S_G(K)/\mathcal{O}$

$\Gamma_F = \mathrm{Gal}(F_\infty/F)$

Fix a generator γ_+ of $\Gamma_F \cong \gamma_+^{\mathbb{Z}_p}$

ε : the cyclotomic character of Γ_F

For each integer k,

$$\begin{aligned} \chi_k : \Gamma_F &\longrightarrow \mathbb{C}_p^\times \\ \gamma &\longmapsto \varepsilon(\gamma)^{1-k} \end{aligned}$$

$$W_+ = \left\{ x \in \mathrm{Spec}\,\Lambda_F(\mathbb{C}_p) \,\middle|\, x = \chi_k \quad k > 1 \right\}$$

$M_{ord}(K, \Lambda)$: the space of ordinary Λ_F-adic modular forms.

$\mathcal{F} \in M_{ord}(K, \Lambda)$ is $\{\mathcal{F}_{[g]}\}_{[g] \in C(K)}$

$$\mathcal{F}_{[g]} = a_{[g]}(0; \mathcal{F}) + \sum_{\beta \in F_+} a_{[g]}(\beta, \mathcal{F}) \in \Lambda_F[\![q^\beta]\!]$$

$\mathcal{F}_{[g]}(\chi_k)$ is the q-expansion of forms in $M_k^{ord}(K_0(p), \omega^{-k}, \mathcal{O})$

then, main results in Hida theory

(1) Control theorem

$$M_{ord}(K,\Lambda)(x_k) = M_k^{ord}(K_0(p), \omega^{-k}, \mathcal{O})$$

$$\forall x_k \in W_+$$

(2) (Fundamental exact seq)

$$0 \longrightarrow \overset{\circ}{M}_{ord}(K,\Lambda) \longrightarrow M_{ord}(K,\Lambda) \xrightarrow[\Phi]{\circledast} \bigoplus_{[g]\in C(K)} \Lambda\cdot[g] \longrightarrow 0$$

cusp forms

(Λ-adic ordinary)

$$\left(\psi : (\mathcal{O}\otimes\mathbb{Z}_p)^\times \longrightarrow \mathbb{C}_p^\times \quad \text{fixed}\right)$$

[cf Chai's paper Appendix to Wiles's paper]

- Eisenstein congruences on $GL(2)/_F$

(1) construct ordinary Λ_F-adic $\mathcal{E} \in M_{ord}(K,\Lambda)$

such that

$$a_{[1]}(0,\mathcal{E}) = L_p^{(\ell)}(\psi)\left(1-\Psi^{-1}\mathcal{E}(\mathrm{Frob}_\ell)\right)$$

const. term for some auxiliary unram prime ℓ in F

$$\mathrm{Tr}\,\rho_{\mathcal{E}}(\mathrm{Frob}_v) = 1 + \Psi(\mathrm{Frob}_v)$$

$$\psi : \mathrm{Gal}(F'/F) \longrightarrow \mathbb{C}_p^\times \quad \text{finite order}$$

$$\Psi : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathcal{O}[[\Gamma_F]]^\times$$

$$g \longmapsto \psi(g)\cdot g|_{F_\infty}$$

$L_p(\psi)$: Deligne-Ribet p-adic L

Assume ψ is odd

(*) • $a_{[g]}(0,\mathcal{E})$ are Λ-multiples of $a_{[1]}(0,\mathcal{E})$

The ideal generated by constant terms at all cusps is $L_p^{[\text{illegible}]}(\psi)\left(1-\Psi^{-1}\varepsilon(\mathrm{Frob}_\ell)\right) =: \mathcal{L}$

- By the fundamental exact sequence,

$\exists\ \mathcal{G}' \in M_{\mathrm{ord}}(K,\Lambda)$ such that

$$\mathcal{F} := \mathcal{E} - \mathcal{L}\cdot\mathcal{G}' \in M^{\circ}_{\mathrm{ord}}(K,\Lambda)$$

• Note that $\mathcal{F} \equiv \mathcal{E} \pmod{\mathcal{L}}$

and $a_{[1]}(1,\mathcal{F}) \equiv \underline{a_{[1]}(1,\mathcal{E}) \equiv 1} \pmod{\mathcal{L}}$

(*)

[key
difficult for unitary groups]

Assume $(\mathcal{L}) \neq \Lambda \Rightarrow a_{[1]}(1,\mathcal{F})$ is a unit

<u>Def</u>

$$\lambda_{\mathcal{F}} : h^{\mathrm{ord}}(K,\Lambda) \longrightarrow \Lambda$$
$$T \longmapsto \frac{a_{[1]}(1,\mathcal{F}|_T)}{a_{[1]}(1,\mathcal{F})}$$

then,

$$\lambda_{\mathcal{F}} : \frac{h^{\mathrm{ord}}(K,\Lambda)}{I_\Psi} \longrightarrow \frac{\Lambda}{(\mathcal{L})} \quad \Lambda\text{-alg. hom}$$

$$I_\Psi := \left(T_v - (\Psi(\mathrm{Frob}_v)+1)\right), \quad T_v = K_v\begin{pmatrix}1 & \\ & \varpi_v\end{pmatrix}K_v$$

<u>Eisenstein ideal</u>

$I_\Psi \neq h^{\mathrm{ord}}(K,\Lambda)$ let $\mathfrak{m}$ be the maximal ideal of $h^{\mathrm{ord}}(K,\Lambda)$ containing I_Ψ

- Let $h_{\mathcal{E}} = h^{\mathrm{ord}}(K, \Lambda)_{\mathfrak{m}}$

  <u>The Eisenstein component</u>

  $h_{\mathcal{E}}$ is reduced, local, finite $/\Lambda$

- Let Eis_{Ψ} be the ideal of Λ s.t.

$$\frac{\Lambda}{\mathrm{Eis}_{\Psi}} \cong \frac{h^{\mathrm{ord}}(K, \Lambda)}{I_{\Psi}}$$

$$\lambda \longmapsto \lambda \cdot 1$$

Then, we proved $\mathrm{Eis}_{\Psi} \subseteq (\mathcal{L})$

(L|E)

§. Pseudo representations (Routine part)

By the existence of Galois rep attached to Hilbert modular forms,

one can construct a pseudo character

$$T : G_F \longrightarrow h_{\mathcal{E}} \quad \text{s.t. } T \equiv 1 + \Psi \pmod{I_{\Psi}}$$

- one can get genuine Galois rep

$$\rho : G_F \longrightarrow GL_2(K)$$

$$K = \mathrm{Frac}\, h_{\mathcal{E}}$$

$$\mathrm{Tr}\,\rho = T$$

Use results in Chap 1 of Bellaiche - Chenevier,

Because $T \equiv 1 + \Psi \pmod{I}$

$\Psi \not\equiv 1 \pmod{\mathfrak{m}}$ (Ψ is odd!)

$\Rightarrow$ T is residually multiplicity-free

We can get (GMA) generalized matrix algebra

$$\rho(h_{\xi}[G_F]) \approx \begin{pmatrix} R & R_{12} \\ R_{21} & R \end{pmatrix} \qquad R = h_{\xi}$$

$\cap$ Frac R — R_{ij} is a fractional ideal in $K = \mathrm{Frac} R$

with the property that $R_{ji} \cdot R_{ij} \subset I_{\Psi}$

Write $\rho(g) = (a_{ij}(g))_{i,j=1\sim 2}$

Then,

$$a_{11} \equiv \Psi \pmod{I}$$
$$a_{22} \equiv \mathbb{1} \pmod{I}$$

◎ Lattice construction

let $v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Define $L = \rho(R[G]) \cdot v_2 \subset K^2 = Kv_1 \oplus Kv_2$

★ L is a lattice (by irreducibility of Gal rep.)

Let $L_1 = R_{12} \cdot v_1$, $L_2 = R \cdot v_2$

$$L = L_1 \oplus L_2 \text{ as } R\text{-modules}$$

$$0 \longrightarrow L_1(\Psi) \otimes R/I \longrightarrow L/IL \longrightarrow R/I\,(1) \longrightarrow 0$$

lemma $L(\Psi^{-1})$ has no R-module quotient on which G acts trivially
(no trivial $R[G]$-module quotient)

pf. By Nakayama's lemma
$+\ \Psi \not\equiv 1 \pmod{m}$ $\lrcorner$

- Construction of cocycles

$$
\begin{tikzcd}
c : \left(L_1/IL_1\right)^* = \mathrm{Hom}\left(R_{12}/IR_{12}, \mathbb{Q}_p/\mathbb{Z}_p\right) \arrow[d] \\
H^1(F, \Phi \otimes (R/I)^*) \arrow[d, hook, "\text{injective! } (\Phi \not\equiv 1 \pmod{m})"] \\
H^1(F, \Phi \otimes \Lambda^*)
\end{tikzcd}
$$

$f \longmapsto$

$$c^f_\sigma(r) = f(r\, a_{12}(\sigma)) \quad (r \in R,\ \sigma \in G_F)$$

<u>Prop</u> c is injective

<u>proof</u> previous lemma + Galois cohomology

Image of c satisfies the local condition at p

<u>Idea</u> $\rho \sim \begin{pmatrix} \Phi & * \\ 0 & 1 \end{pmatrix} \bmod I_\Phi$

$\Phi(\chi_k) \sim \varepsilon^{1-k}$

$$\rho\big|_{I_v} \sim \begin{pmatrix} 1 & * \\ 0 & \Phi \end{pmatrix}$$

$\Rightarrow$ the image of c splits at $v \mid p$

we assume $\Phi\big|_{I_v} \not\equiv 1 \pmod{P}$ for height one primes P of Λ.

(If $\Phi\big|_{I_v} \equiv 1 \pmod{P}$ <u>trivial zero</u>

$\Rightarrow \Phi(\gamma_+^{p^n}) - 1 \in P \Rightarrow (1+T)\zeta - 1 \in P$ for some $\zeta \in \mu_{p^n}$)

$\Rightarrow$ For any such $\mathfrak{P}$, there exists $t_{\mathfrak{P}} \in \Lambda \setminus \mathfrak{P}$

$$t_{\mathfrak{P}} \left(R_{12}/I R_{12} \right)^* \subset \mathrm{Sel}_F^{(\ell)}(\Psi)$$

$\Rightarrow$ By using Fitting ideal argument

$$\left(\mathrm{Fitt}_\Lambda \, \mathrm{Sel}_F^{(\ell)}(\Psi)\right)_{\mathfrak{P}} \subset (\mathcal{L})_{\mathfrak{P}}$$

$\forall \mathfrak{P}$ away from trivial zeros.

$$\Rightarrow \ell_{\mathfrak{P}}(\mathrm{Sel}_F^{(\ell)}(\Psi)) \geqslant \ell_{\mathfrak{P}}(\mathcal{L}) = \ell_{\mathfrak{P}}\left(L_p(\Psi)\,(1-\Psi^{-1}\varepsilon(\mathrm{Frob}_\ell))\right)$$

By $0 \longrightarrow \mathrm{Sel}_F(\Psi) \longrightarrow \mathrm{Sel}_F^{(\ell)}(\Psi) \longrightarrow H^1(D_\ell, \Psi \otimes \Lambda^*)$

$$\Rightarrow \ell_{\mathfrak{P}}(\mathrm{Sel}_F^{(\ell)}(\Psi)) \leqslant \ell_{\mathfrak{P}}(\mathrm{Sel}_F(\Psi)) + \underbrace{\ell_{\mathfrak{P}}(H^1(D_\ell, \Psi \otimes \Lambda^*))}_{\ell_{\mathfrak{P}}(1-\Psi^{-1}\varepsilon(\mathrm{Frob}_\ell))}$$

$$\Rightarrow \ell_{\mathfrak{P}}(L_p(\Psi)) \leqslant \ell_{\mathfrak{P}}(\mathrm{Sel}_F(\Psi))$$

$\forall \mathfrak{P}$ away from trivial zeros. $\boxtimes$

(cf Ribet
$\rho : G \longrightarrow GL_2(\mathbb{Z}_p)$ (generically irreducible, residually reducible)
$\hookrightarrow$ find a lattice s.t. $\bar{\rho} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$, or $\begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix}$)