Modular constructions of Galois cohomology classes with prescribed local properties

(Ribet's Method)

Samit Dasgupta

University of California, Santa Cruz

June 15, 2010

Goal of the lectures

Let $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let E be a field, and let

$$\chi : G_{\mathbf{Q}} \longrightarrow E^{\times}$$

be a continuous character.

We will be interested in constructing classes

$$[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi)).$$

(Continuous cohomology)

Typically E will be a finite extension of $\mathbf{F}_p$ or $\mathbf{Q}_p$.

Goal of the lectures

Let $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let E be a field, and let

$$\chi : G_{\mathbf{Q}} \longrightarrow E^{\times}$$

be a continuous character.

We will be interested in constructing classes

$$[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi)).$$

(Continuous cohomology)

Typically E will be a finite extension of $\mathbf{F}_p$ or $\mathbf{Q}_p$.

Goal of the lectures

Let $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let E be a field, and let

$$\chi : G_{\mathbf{Q}} \longrightarrow E^{\times}$$

be a continuous character.

We will be interested in constructing classes

$$[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi)).$$

(Continuous cohomology)

Typically E will be a finite extension of $\mathbf{F}_p$ or $\mathbf{Q}_p$.

Prescribed local behavior

Let $G_p \subset G_{\mathbf{Q}}$ denote a decomposition group at p.

This corresponds to taking an embedding $\overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_p$, with $G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

We will want to control the local images

$$[\kappa]_p = \mathrm{res}^{G_{\mathbf{Q}}}_{G_p}[\kappa] \in H^1(G_p, E(\chi)).$$

For instance, we may want $[\kappa]_p = 0$ when a certain L-function vanishes, or $[\kappa]_p$ related to a p-adic L-function.

Prescribed local behavior

Let $G_p \subset G_{\mathbf{Q}}$ denote a decomposition group at p.

This corresponds to taking an embedding $\overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_p$, with $G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

We will want to control the local images

$$[\kappa]_p = \mathrm{res}^{G_{\mathbf{Q}}}_{G_p}[\kappa] \in H^1(G_p, E(\chi)).$$

For instance, we may want $[\kappa]_p = 0$ when a certain L-function vanishes, or $[\kappa]_p$ related to a p-adic L-function.

Examples of problems attacked with this method

- Converse to Herbrand's Theorem
  (Ribet)
- Iwasawa's Main Conjecture
  (Mazur-Wiles, Wiles, Skinner-Urban)
- Mazur–Tate–Teitelbaum Conjecture
  (Greenberg–Stevens)
- Gross–Stark Conjecture
  (D, Darmon, R. Pollack)

Examples of problems attacked with this method

- Converse to Herbrand's Theorem
  (Ribet)
- Iwasawa's Main Conjecture
  (Mazur-Wiles, Wiles, Skinner-Urban)
- Mazur–Tate–Teitelbaum Conjecture
  (Greenberg–Stevens)
- Gross–Stark Conjecture
  (D, Darmon, R. Pollack)

Examples of problems attacked with this method

- Converse to Herbrand's Theorem
  (Ribet)
- Iwasawa's Main Conjecture
  (Mazur-Wiles, Wiles, Skinner-Urban)
- Mazur–Tate–Teitelbaum Conjecture
  (Greenberg–Stevens)
- Gross–Stark Conjecture
  (D, Darmon, R. Pollack)

Examples of problems attacked with this method

- Converse to Herbrand's Theorem
(Ribet)
- Iwasawa's Main Conjecture
(Mazur-Wiles, Wiles, Skinner-Urban)
- Mazur–Tate–Teitelbaum Conjecture
(Greenberg–Stevens)
- Gross–Stark Conjecture
(D, Darmon, R. Pollack)

Steps in Ribet's Method

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.

- Step 2: Construct a family of (ordinary) cusp forms with knowledge of the Fourier coefficients, e.g. a_p related to L_p.

- Step 3: Specialize the Galois representation associated to the family at a point where it is reducible. Extract a cohomology class from the reducible representation.

- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.
- Step 2: Construct a family of (ordinary) cusp forms with knowledge of the Fourier coefficients, e.g. a_p related to L_p.
- Step 3: Specialize the Galois representation associated to the family at a point where it is reducible. Extract a cohomology class from the reducible representation.
- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.

- Step 2: Construct a family of (ordinary) cusp forms with knowledge of the Fourier coefficients, e.g. a_p related to L_p.

- Step 3: Specialize the Galois representation associated to the family at a point where it is reducible. Extract a cohomology class from the reducible representation.

- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.
- Step 2: Construct a family of (ordinary) cusp forms with knowledge of the Fourier coefficients, e.g. a_p related to L_p.
- Step 3: Specialize the Galois representation associated to the family at a point where it is reducible. Extract a cohomology class from the reducible representation.
- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Ribet's converse to Herbrand

Let $A =$ ideal class group of $\mathbf{Q}(\mu_p)$, let $C = A \otimes \mathbf{F}_p$.
Canonical character

$$\omega : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \cong \mathbf{F}_p^\times$$

Then

$$C = \bigoplus_{i=0}^{p-2} C(\omega^i),$$

where

$$C(\omega^i) = \{c \in C : \sigma(c) = \omega^i(\sigma) \cdot c \text{ for all } \sigma \in G_{\mathbf{Q}}\}.$$

Theorem (Ribet)

Let j be even, $2 \le j \le p-3$. Then $p \mid B_j$ implies $C(\omega^{1-j}) \neq 0$.

Ribet's converse to Herbrand

Let $A =$ ideal class group of $\mathbf{Q}(\mu_p)$, let $C = A \otimes \mathbf{F}_p$.
Canonical character

$$\omega : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \cong \mathbf{F}_p^\times$$

Then

$$C = \bigoplus_{i=0}^{p-2} C(\omega^i),$$

where

$$C(\omega^i) = \{c \in C : \sigma(c) = \omega^i(\sigma) \cdot c \text{ for all } \sigma \in G_{\mathbf{Q}}\}.$$

Theorem (Ribet)

Let j be even, $2 \leq j \leq p-3$. Then $p \mid B_j$ implies $C(\omega^{1-j}) \neq 0$.

Ribet's converse to Herbrand

Let $A =$ ideal class group of $\mathbf{Q}(\mu_p)$, let $C = A \otimes \mathbf{F}_p$.
Canonical character

$$\omega : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \cong \mathbf{F}_p^\times$$

Then

$$C = \bigoplus_{i=0}^{p-2} C(\omega^i),$$

where

$$C(\omega^i) = \{c \in C : \sigma(c) = \omega^i(\sigma) \cdot c \text{ for all } \sigma \in G_{\mathbf{Q}}\}.$$

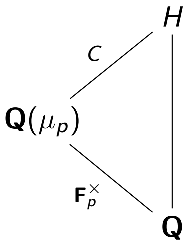
Theorem (Ribet)

Let j be even, $2 \leq j \leq p-3$. Then $p \mid B_j$ implies $C(\omega^{1-j}) \neq 0$.

Step 1: Reformulation

By class field theory, $C = \mathrm{Gal}(H/\mathbf{Q}(\mu_p))$, where

H = maximal abelian unramified ext of $\mathbf{Q}(\mu_p)$ with exponent p.



Conjugation action

$\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \cong \mathbf{F}_p^\times$ acts on $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ by conjugation:

$$\sigma(\tau) = \tilde{\sigma}\tau\tilde{\sigma}^{-1},$$

where $\tilde{\sigma} \in \mathrm{Gal}(H/\mathbf{Q})$ lifts σ.

This corresponds to the usual Galois action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on ideal classes C.

$\mathrm{Gal}(H/\mathbf{Q}) \cong C \rtimes \mathbf{F}_p^\times$.

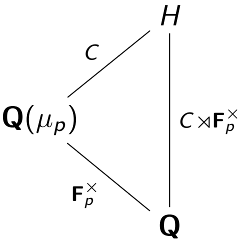
Conjugation action

$\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \cong \mathbf{F}_p^\times$ acts on $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ by conjugation:

$$\sigma(\tau) = \tilde{\sigma}\tau\tilde{\sigma}^{-1},$$

where $\tilde{\sigma} \in \mathrm{Gal}(H/\mathbf{Q})$ lifts σ.

This corresponds to the usual Galois action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on ideal classes C.



$\mathrm{Gal}(H/\mathbf{Q}) \cong C \rtimes \mathbf{F}_p^\times$.

Therefore, with $\chi = \omega^{1-j}$, we see that $C(\chi) \neq 0$ is equivalent to the existence of an abelian extension $H/\mathbf{Q}(\mu_p)$ such that:

- $H/\mathbf{Q}(\mu_p)$ is unramified;
- $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ has size p;
- The conjugation action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ is via χ.

In this situation,

$$\mathrm{Gal}(H/\mathbf{Q}) \cong \mathbf{F}_p \rtimes \mathbf{F}_p^{\times}.$$

Let $\kappa : G_{\mathbf{Q}} \to \mathbf{F}_p$ denote projection onto first factor.

Therefore, with $\chi = \omega^{1-j}$, we see that $C(\chi) \neq 0$ is equivalent to the existence of an abelian extension $H/\mathbf{Q}(\mu_p)$ such that:

- $H/\mathbf{Q}(\mu_p)$ is unramified;
- $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ has size p;
- The conjugation action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on $\mathrm{Gal}(H/\mathbf{Q}(\mu_p))$ is via χ.

In this situation,

$$\mathrm{Gal}(H/\mathbf{Q}) \cong \mathbf{F}_p \rtimes \mathbf{F}_p^\times.$$

Let $\kappa : G_{\mathbf{Q}} \to \mathbf{F}_p$ denote projection onto first factor.

κ is a 1-cocycle for χ:

$$\kappa(\sigma\tau) = \kappa(\sigma) + \chi(\sigma)\kappa(\tau).$$

We get a non-trivial class

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi)).$$

Since κ is unramified, we find that

$$\mathrm{res}_{I_\ell}^{G_{\mathbf{Q}}}[\kappa] \in H^1(I_\ell, \mathbf{F}_p(\chi))$$

is trivial for all ℓ.

These steps are reversible: the splitting field of an unramified non-trivial $[\kappa]$ gives the desired H.

κ is a 1-cocycle for χ:

$$\kappa(\sigma\tau) = \kappa(\sigma) + \chi(\sigma)\kappa(\tau).$$

We get a non-trivial class

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi)).$$

Since κ is unramified, we find that

$$\mathrm{res}^{G_{\mathbf{Q}}}_{I_\ell}[\kappa] \in H^1(I_\ell, \mathbf{F}_p(\chi))$$

is trivial for all ℓ.

These steps are reversible: the splitting field of an unramified non-trivial $[\kappa]$ gives the desired H.

κ is a 1-cocycle for χ:

$$\kappa(\sigma\tau) = \kappa(\sigma) + \chi(\sigma)\kappa(\tau).$$

We get a non-trivial class

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi)).$$

Since κ is unramified, we find that

$$\mathrm{res}^{G_{\mathbf{Q}}}_{I_\ell}[\kappa] \in H^1(I_\ell, \mathbf{F}_p(\chi))$$

is trivial for all ℓ.

These steps are reversible: the splitting field of an unramified non-trivial $[\kappa]$ gives the desired H.

κ is a 1-cocycle for χ:

$$\kappa(\sigma\tau) = \kappa(\sigma) + \chi(\sigma)\kappa(\tau).$$

We get a non-trivial class

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi)).$$

Since κ is unramified, we find that

$$\mathrm{res}^{G_{\mathbf{Q}}}_{I_\ell}[\kappa] \in H^1(I_\ell, \mathbf{F}_p(\chi))$$

is trivial for all ℓ.

These steps are reversible: the splitting field of an unramified non-trivial $[\kappa]$ gives the desired H.

Cohomology classes and Galois representations

The cocycle

$$\kappa \in Z^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi))$$

gives a Galois representation:

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

defined by

$$\rho(\sigma) = \begin{pmatrix} 1 & \kappa(\sigma)\chi^{-1}(\sigma) \\ 0 & \chi^{-1}(\sigma) \end{pmatrix}$$

In order to show the existence of κ, we will construct ρ.

Yoga: Galois representations come from modular forms.

Cohomology classes and Galois representations

The cocycle

$$\kappa \in Z^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi))$$

gives a Galois representation:

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

defined by

$$\rho(\sigma) = \begin{pmatrix} 1 & \kappa(\sigma)\chi^{-1}(\sigma) \\ 0 & \chi^{-1}(\sigma) \end{pmatrix}$$

In order to show the existence of κ, we will construct ρ.

Yoga: Galois representations come from modular forms.

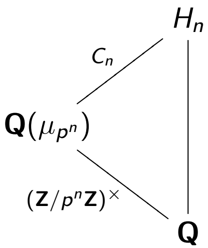
(Special case of) Iwasawa's Main Conjecture

From now on

$$\omega : G_{\mathbf{Q}} \to (\mathbf{Z}/p\mathbf{Z})^{\times} \to \mathbf{Z}_p^{\times}$$

is the Teichmuller character.

For j even, $2 \leq j \leq p-3$, there is a p-adic L-function $L_p(\omega^j, s)$.



$C_\infty := \varprojlim C_n$ has an action of

$$\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \cong \mathbf{Z}_p^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (1 + p\mathbf{Z}_p).$$

Let g = topological generator of $1 + p\mathbf{Z}_p$, and suppose $\gamma \mapsto (1, g)$.

(Consequence of) Iwasawa's Main Theorem

Theorem (Mazur-Wiles)

If $L_p(\omega^j, s) = 0$ for $s \in \mathbf{Z}_p$, then g^s is an eigenvalue of γ acting on

$$(C_\infty \otimes \mathbf{Q}_p)(\omega^{1-j}).$$

Step 1: Reformulation

If $L_p(\omega^j, s) = 0$ for $s \in \mathbf{Z}_p$, then there exists a non-trivial unramified class in

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{Q}_p(\omega^{1-j}\epsilon^s)),$$

where

$$\epsilon : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (1 + p\mathbf{Z}_p)$$

is projection to the second factor.

(Consequence of) Iwasawa's Main Theorem

Theorem (Mazur-Wiles)

If $L_p(\omega^j, s) = 0$ for $s \in \mathbf{Z}_p$, then g^s is an eigenvalue of γ acting on

$$(C_\infty \otimes \mathbf{Q}_p)(\omega^{1-j}).$$

Step 1: Reformulation

If $L_p(\omega^j, s) = 0$ for $s \in \mathbf{Z}_p$, then there exists a non-trivial unramified class in

$$[\kappa] \in H^1(G_{\mathbf{Q}}, \mathbf{Q}_p(\omega^{1-j}\epsilon^s)),$$

where

$$\epsilon : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (1 + p\mathbf{Z}_p)$$

is projection to the second factor.

Construct κ from a Galois representation

$$\rho : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Q}_p)$$

with

$$\rho(\sigma) = \begin{pmatrix} 1 & b(\sigma) \\ 0 & \omega^{j-1}\epsilon^{-s}(\sigma) \end{pmatrix}$$

and $\kappa(\sigma) = b(\sigma)/\omega^{j-1}\epsilon^{-s}(\sigma)$.

Our source for Galois representations is...

Construct κ from a Galois representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$$

with

$$\rho(\sigma) = \begin{pmatrix} 1 & b(\sigma) \\ 0 & \omega^{j-1}\epsilon^{-s}(\sigma) \end{pmatrix}$$

and $\kappa(\sigma) = b(\sigma)/\omega^{j-1}\epsilon^{-s}(\sigma)$.

Our source for Galois representations is...

Modular Forms

Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times, \quad \chi(-1) = (-1)^k$.

A modular form of level N, character χ, and weight k is a holomorphic function $f : \mathcal{H} \to \mathbf{C}$ such that

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = \chi(a) f(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, and

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

Modular forms denoted $M_k(N,\chi)$.

Cusp forms: $a_0 = 0$ for every $f|_\gamma$, denoted $S_k(N,\chi)$.

Hecke operators

For each $\ell \nmid Np$, there is a Hecke operator T_ℓ on $S_k(N, \chi; \mathbf{Z}_p)$ given on q-expansions by:

$$T_\ell\left(\sum_{n=0}^{\infty} a_n q^n\right) = \sum_{n=0}^{\infty} (a_{n\ell} + \chi(\ell)\ell^{k-1} a_{n/\ell}) q^n.$$

Here $a_{n/\ell} = 0$ if $\ell \nmid n$.

Similarly for $\ell \mid N$, we have

$$U_\ell\left(\sum_{n=0}^{\infty} a_n q^n\right) = \sum_{n=0}^{\infty} a_{n\ell} q^n.$$

These operators define a $\mathbf{Z}_p$-algebra called the Hecke algebra $\mathbf{T}_k$.

Hecke operators

For each $\ell \nmid Np$, there is a Hecke operator T_ℓ on $S_k(N, \chi; \mathbf{Z}_p)$ given on q-expansions by:

$$T_\ell\left(\sum_{n=0}^{\infty} a_n q^n\right) = \sum_{n=0}^{\infty}(a_{n\ell} + \chi(\ell)\ell^{k-1}a_{n/\ell})q^n.$$

Here $a_{n/\ell} = 0$ if $\ell \nmid n$.

Similarly for $\ell \mid N$, we have

$$U_\ell\left(\sum_{n=0}^{\infty} a_n q^n\right) = \sum_{n=0}^{\infty} a_{n\ell} q^n.$$

These operators define a $\mathbf{Z}_p$-algebra called the Hecke algebra $\mathbf{T}_k$.

Theorem (Deligne-Serre)

Let $k \geq 1$ and $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \rightarrow \overline{\mathbf{Q}}^\times$ a character. Let $f \in S_k(N, \chi)$ be a cuspidal newform. There exists an irreducible continuous Galois representation

$$\rho : G_{\mathbf{Q}} \longrightarrow GL_2(\overline{\mathbf{Q}}_p)$$

that is unramified outside Np, such that for all $\ell \nmid Np$,

$$trace(\rho(Frob_\ell)) = a_\ell$$

and

$$\det(\rho(Frob_\ell)) = \chi(\ell)\ell^{k-1}.$$

Here

$$f(q) = \sum_{n=1}^{\infty} a_n q^n,$$

so a_ℓ is the eigenvalue of the Hecke operator T_ℓ.

Ordinary forms

The form f is called *ordinary at p* if

$$x^2 - a_p x + \chi(p)p^{k-1}$$

has a root α_p that is a p-adic unit.

If $k > 1$ (or $\chi(p) = 0$) this is equivalent to a_p being a p-adic unit.

Ordinary forms

The form f is called *ordinary at p* if

$$x^2 - a_p x + \chi(p)p^{k-1}$$

has a root α_p that is a p-adic unit.

If $k > 1$ (or $\chi(p) = 0$) this is equivalent to a_p being a p-adic unit.

Ordinary representations

Theorem

Let f be a cuspidal eigenform that is ordinary at p. There is a basis such that the restriction of ρ to G_p has the form

$$\rho|_{G_p} \cong \begin{pmatrix} \eta_1 & * \\ 0 & \eta_2 \end{pmatrix}$$

where $\eta_2 : G_p \to \mathbf{Z}_p^\times$ is the unramified character such that

$$\eta_2(Frob_p) = \alpha_p.$$

Interpolating these representations

For each $k \geq 2$, let f_k be a newform. Suppose that the associated representations

$$\rho_k(\sigma) = \begin{pmatrix} a_k(\sigma) & b_k(\sigma) \\ c_k(\sigma) & d_k(\sigma) \end{pmatrix}$$

have the remarkable property that the function $k \mapsto a_k(\sigma)$ extends to a continuous function $\mathbf{Z}_p \to \overline{\mathbf{Q}}_p$, and similarly for the other matrix coefficients.

Then for any $k \in \mathbf{Z}_p$, we get a Galois representation, and it is certainly possible that these other specializations are reducible.

Interpolating these representations

For each $k \geq 2$, let f_k be a newform. Suppose that the associated representations

$$\rho_k(\sigma) = \begin{pmatrix} a_k(\sigma) & b_k(\sigma) \\ c_k(\sigma) & d_k(\sigma) \end{pmatrix}$$

have the remarkable property that the function $k \mapsto a_k(\sigma)$ extends to a continuous function $\mathbf{Z}_p \to \overline{\mathbf{Q}}_p$, and similarly for the other matrix coefficients.

Then for any $k \in \mathbf{Z}_p$, we get a Galois representation, and it is certainly possible that these other specializations are reducible.

Knowledge of ρ_k

Furthermore, since $\{k \in \mathbf{Z}, k \geq 2\}$ is dense in $\mathbf{Z}_p$, we know the trace and determinant of the representation by continuity.

Finally, if the f_k are all ordinary, we know what the representation looks like when restricted to G_p.

Knowledge of ρ_k

Furthermore, since $\{k \in \mathbf{Z}, k \geq 2\}$ is dense in $\mathbf{Z}_p$, we know the trace and determinant of the representation by continuity.

Finally, if the f_k are all ordinary, we know what the representation looks like when restricted to G_p.

Interpolation, following Iwasawa and Hida

Let $\Lambda = \mathbf{Z}_p[[T]]$.

Let g be a topological generator of $1 + p\mathbf{Z}_p$, e.g. $g = 1 + p$.

For each $k \in \mathbf{Z}_p$, define $\nu_k : \Lambda \to \mathbf{Z}_p^\times$ by

$$\nu_k(1 + T) = g^{k-2}.$$

Every $\lambda \in \Lambda$ represents a function on $\mathbf{Z}_p$, via $k \mapsto \nu_k(\lambda)$.

We call elements of Λ, when viewed as functions on $\mathbf{Z}_p$, *Iwasawa functions*.

Interpolation, following Iwasawa and Hida

Let $\Lambda = \mathbf{Z}_p[[T]]$.

Let g be a topological generator of $1 + p\mathbf{Z}_p$, e.g. $g = 1 + p$.

For each $k \in \mathbf{Z}_p$, define $\nu_k : \Lambda \to \mathbf{Z}_p^\times$ by

$$\nu_k(1 + T) = g^{k-2}.$$

Every $\lambda \in \Lambda$ represents a function on $\mathbf{Z}_p$, via $k \mapsto \nu_k(\lambda)$.

We call elements of Λ, when viewed as functions on $\mathbf{Z}_p$, *Iwasawa functions*.

Interpolation, following Iwasawa and Hida

Let $\Lambda = \mathbf{Z}_p[[T]]$.

Let g be a topological generator of $1 + p\mathbf{Z}_p$, e.g. $g = 1 + p$.

For each $k \in \mathbf{Z}_p$, define $\nu_k : \Lambda \to \mathbf{Z}_p^\times$ by

$$\nu_k(1 + T) = g^{k-2}.$$

Every $\lambda \in \Lambda$ represents a function on $\mathbf{Z}_p$, via $k \mapsto \nu_k(\lambda)$.

We call elements of Λ, when viewed as functions on $\mathbf{Z}_p$, *Iwasawa functions*.

Example: power functions

Consider the function $k \mapsto a^{k-1}$ with $a \in 1 + p\mathbf{Z}_p$.

Let $a = g^\beta$, with $\beta \in \mathbf{Z}_p$.

Let

$$\lambda = a(1+T)^\beta = a \sum_{n=0}^{\infty} \binom{\beta}{n} T^n \in \Lambda.$$

Then

$$\nu_k(\lambda) = \nu_k(a(1+T)^\beta) = a(g^{k-2})^\beta = a^{k-1}.$$

Example: power functions

Consider the function $k \mapsto a^{k-1}$ with $a \in 1 + p\mathbf{Z}_p$.

Let $a = g^\beta$, with $\beta \in \mathbf{Z}_p$.

Let

$$\lambda = a(1+T)^\beta = a \sum_{n=0}^{\infty} \binom{\beta}{n} T^n \in \Lambda.$$

Then

$$\nu_k(\lambda) = \nu_k(a(1+T)^\beta) = a(g^{k-2})^\beta = a^{k-1}.$$

Λ-adic forms

Definition

A Λ-adic form of level Np and character χ is a q-expansion

$$f = \sum_{n=0}^{\infty} a_n q^n \qquad \text{with } a_n \in \Lambda$$

such that for all $k \in \mathbf{Z}$, $k \geq 2$,

$$\nu_k(f) = \sum_{n=0}^{\infty} \nu_k(a_n) q^n \in \mathbf{Z}_p[[q]]$$

is the q-expansion of a modular form $f_k \in M_k(Np, \chi\omega^{1-k}; \mathbf{Z}_p)$.

Here $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ is the Teichmuller character.

Λ-adic cusp forms

A Λ-adic form f is called a cusp form if for all $k \in \mathbf{Z}, k \geq 2$, the classical form f_k is a cusp form.

Note that this implies, but is not equivalent to, $a_0 = 0$.

The space of Λ-adic modular forms of level N and character χ is denoted $\mathscr{M}(N, \chi)$, and the subspace of cusp forms is denoted $\mathscr{S}(N, \chi)$.

Λ-adic cusp forms

A Λ-adic form f is called a cusp form if for all $k \in \mathbf{Z}, k \geq 2$, the classical form f_k is a cusp form.

Note that this implies, but is not equivalent to, $a_0 = 0$.

The space of Λ-adic modular forms of level N and character χ is denoted $\mathscr{M}(N, \chi)$, and the subspace of cusp forms is denoted $\mathscr{S}(N, \chi)$.

Λ-adic Hecke operators

For each $\ell \nmid Np$, there is a Hecke operator T_ℓ on the space of Λ-adic forms such that

$$\nu_k(T_\ell f) = T_\ell \nu_k(f).$$

The formula for T_ℓ is:

$$T_\ell(\sum a_n q^n) = \sum_{n=0}^{\infty} (a_{n\ell} + \chi(\ell)\lambda_\ell a_{n/\ell}) q^n,$$

where $\lambda_\ell \in \Lambda$ such that $\nu_k(\lambda) = \langle \ell \rangle^{k-1}$. Here

$$\langle \ell \rangle = \ell/\omega(\ell) \equiv 1 \pmod{p}.$$

Λ-adic Hecke operators

For each $\ell \nmid Np$, there is a Hecke operator T_ℓ on the space of Λ-adic forms such that

$$\nu_k(T_\ell f) = T_\ell \nu_k(f).$$

The formula for T_ℓ is:

$$T_\ell(\sum a_n q^n) = \sum_{n=0}^{\infty} (a_{n\ell} + \chi(\ell)\lambda_\ell a_{n/\ell}) q^n,$$

where $\lambda_\ell \in \Lambda$ such that $\nu_k(\lambda) = \langle \ell \rangle^{k-1}$. Here

$$\langle \ell \rangle = \ell/\omega(\ell) \equiv 1 \pmod{p}.$$

Λ-adic Hecke algebra

Similarly there is a Λ-adic operator U_ℓ for $\ell \mid Np$.

The operators T_ℓ for $\ell \nmid Np$ and U_ℓ for $\ell \mid Np$ define a Λ-algebra called the Hecke algebra $\mathbf{T}$.

Eisenstein Series

Let $k \in \mathbf{Z}$, $k \geq 2$,

$$\eta : (\mathbf{Z}/a\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times, \qquad \psi : (\mathbf{Z}/b\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$$

be characters such that $\eta\psi(-1) = (-1)^k$.

There is a modular form $E_k(\eta, \psi) \in M_k(ab, \eta\psi)$ with q-expansion

$$E_k(\eta, \psi)(q) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n} \eta\left(\frac{n}{d}\right) \psi(d) d^{k-1} q^n,$$

where

$$a_0 = \begin{cases} \frac{1}{2} L(\psi, 1-k) & \text{if } \eta = 1 \text{ (with } a = 1) \\ 0 & \text{otherwise.} \end{cases}$$

Eisenstein Series

Let $k \in \mathbf{Z}$, $k \geq 2$,

$$\eta : (\mathbf{Z}/a\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times, \qquad \psi : (\mathbf{Z}/b\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$$

be characters such that $\eta\psi(-1) = (-1)^k$.

There is a modular form $E_k(\eta, \psi) \in M_k(ab, \eta\psi)$ with q-expansion

$$E_k(\eta, \psi)(q) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n} \eta\left(\frac{n}{d}\right) \psi(d) d^{k-1} q^n,$$

where

$$a_0 = \begin{cases} \frac{1}{2} L(\psi, 1-k) & \text{if } \eta = 1 \text{ (with } a = 1) \\ 0 & \text{otherwise.} \end{cases}$$

Weight 1 Eisenstein Series

The same is true if $k = 1$, except if $\eta \neq 1$ and $\psi = 1$, the constant term is

$$\frac{1}{2} L(\eta, 0).$$

Note that $E_1(\eta, \psi) = E_1(\psi, \eta)$.

Weight 1 Eisenstein Series

The same is true if $k = 1$, except if $\eta \neq 1$ and $\psi = 1$, the constant term is

$$\frac{1}{2} L(\eta, 0).$$

Note that $E_1(\eta, \psi) = E_1(\psi, \eta)$.

Eisenstein series are eigenforms

The Eisenstein series $E_k(\eta, \psi)$ is an eigenform, with eigenvalue

$$\eta(\ell) + \psi(\ell)\ell^{k-1}$$

for T_ℓ when $\ell \nmid N$ and for U_ℓ when $\ell \mid N$.

$$M_k(N, \chi) = S_k(N, \chi) \oplus \mathrm{Eis}_k(N, \chi)$$

where $\mathrm{Eis}_k(N, \chi)$ is the space spanned by $E_k(\eta, \psi)$ for all η, ψ such that $ab = N$ and $\eta\psi = \chi$.

Eisenstein series are eigenforms

The Eisenstein series $E_k(\eta, \psi)$ is an eigenform, with eigenvalue

$$\eta(\ell) + \psi(\ell)\ell^{k-1}$$

for T_ℓ when $\ell \nmid N$ and for U_ℓ when $\ell \mid N$.

$$M_k(N, \chi) = S_k(N, \chi) \oplus \mathrm{Eis}_k(N, \chi)$$

where $\mathrm{Eis}_k(N, \chi)$ is the space spanned by $E_k(\eta, \psi)$ for all η, ψ such that $ab = N$ and $\eta\psi = \chi$.

p-adic interpolation of Eisenstein Series

Suppose $\eta\psi(-1) = -1$. Consider

$$E_k(\eta, \psi\omega^{1-k}) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n,(d,p)=1} \eta(d)\psi(d)\langle d\rangle^{k-1}q^n,$$

where $\psi\omega^{1-k}$ is always viewed to have modulus divisible by p.

Here $a_0 = 0$ if $\eta \neq 1$, and

$$a_0 = \frac{1}{2}L(\psi\omega^{1-k}, 1-k)$$

if $\eta = 1$.

Note that the Fourier coefficients for $n \geq 1$ are Iwasawa functions.

p-adic interpolation of Eisenstein Series

Suppose $\eta\psi(-1) = -1$. Consider

$$E_k(\eta, \psi\omega^{1-k}) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n,(d,p)=1} \eta(d)\psi(d)\langle d\rangle^{k-1} q^n,$$

where $\psi\omega^{1-k}$ is always viewed to have modulus divisible by p.

Here $a_0 = 0$ if $\eta \neq 1$, and

$$a_0 = \frac{1}{2} L(\psi\omega^{1-k}, 1-k)$$

if $\eta = 1$.

Note that the Fourier coefficients for $n \geq 1$ are Iwasawa functions.

p-adic interpolation of Eisenstein Series

Suppose $\eta\psi(-1) = -1$. Consider

$$E_k(\eta, \psi\omega^{1-k}) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n,(d,p)=1} \eta(d)\psi(d)\langle d\rangle^{k-1} q^n,$$

where $\psi\omega^{1-k}$ is always viewed to have modulus divisible by p.

Here $a_0 = 0$ if $\eta \neq 1$, and

$$a_0 = \frac{1}{2} L(\psi\omega^{1-k}, 1-k)$$

if $\eta = 1$.

Note that the Fourier coefficients for $n \geq 1$ are Iwasawa functions.

Kubota–Leopoldt p-adic L-function

Actually, a_0 is an Iwasawa function as well.

Theorem (Kubota-Leopoldt)

Let $\psi(-1) = 1$, and $\psi \neq 1$. There exists an element $\mathscr{L}(\psi) \in \Lambda$ such that

$$\nu_k(\mathscr{L}(\psi)) = L(\psi\omega^{-k}, 1-k)$$

for all $k \in \mathbf{Z}$, $k \geq 1$.

Notation:

$$L_p(\psi, s) = \nu_{1-s}(\mathscr{L}(\psi))$$

is the p-adic L-function attached to ψ.

Kubota–Leopoldt p-adic L-function

Actually, a_0 is an Iwasawa function as well.

Theorem (Kubota-Leopoldt)

Let $\psi(-1) = 1$, and $\psi \neq 1$. There exists an element $\mathscr{L}(\psi) \in \Lambda$ such that

$$\nu_k(\mathscr{L}(\psi)) = L(\psi\omega^{-k}, 1-k)$$

for all $k \in \mathbf{Z}$, $k \geq 1$.

Notation:

$$L_p(\psi, s) = \nu_{1-s}(\mathscr{L}(\psi))$$

is the p-adic L-function attached to ψ.

Pole of the p-adic zeta function

When $\psi = 1$, there is a pole of $\zeta_p(s) = L_p(1, s)$ at $s = 1$.

Theorem

There exists an element $\mathscr{G} \in \Lambda$ such that

$$\mathscr{L}(1) = \frac{\mathscr{G}}{g^2(1+T)-1} \in Frac(\Lambda)$$

satisfies

$$\nu_k(\mathscr{L}(1)) = \frac{\nu_k(\mathscr{G})}{g^k - 1} = L(\omega^{-k}, 1-k)$$

for all $k \in \mathbf{Z}$, $k \geq 1$.

Furthermore, $\nu_0(\mathscr{G}) \neq 0$.

Pole of the p-adic zeta function

When $\psi = 1$, there is a pole of $\zeta_p(s) = L_p(1, s)$ at $s = 1$.

Theorem

There exists an element $\mathscr{G} \in \Lambda$ such that

$$\mathscr{L}(1) = \frac{\mathscr{G}}{g^2(1+T) - 1} \in \mathit{Frac}(\Lambda)$$

satisfies

$$\nu_k(\mathscr{L}(1)) = \frac{\nu_k(\mathscr{G})}{g^k - 1} = L(\omega^{-k}, 1-k)$$

for all $k \in \mathbf{Z}$, $k \geq 1$.

Furthermore, $\nu_0(\mathscr{G}) \neq 0$.

Λ-adic Eisenstein series

Theorem

Given η, ψ such that $\eta\psi(-1) = -1$, there exists a Λ-adic form $\mathscr{E}(\eta, \psi)$ of level ab and character $\eta\psi$ given by

$$\mathscr{E}(\eta, \psi) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n,(d,p)=1} \eta\left(\frac{n}{d}\right) \psi(d) \lambda_d q^n,$$

and

$$a_0 = \begin{cases} \frac{1}{2}\mathscr{L}(\psi\omega) & \text{if } \eta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

When $\psi = \omega^{-1}$, the constant term $a_0 = \frac{1}{2}\mathscr{L}(1)$ lies in Frac(Λ) and has a pole at $k = 0$.

Λ-adic Eisenstein series

Theorem

Given η, ψ such that $\eta\psi(-1) = -1$, there exists a Λ-adic form $\mathscr{E}(\eta, \psi)$ of level ab and character $\eta\psi$ given by

$$\mathscr{E}(\eta, \psi) = a_0 + \sum_{n=1}^{\infty} \sum_{d|n,(d,p)=1} \eta\left(\frac{n}{d}\right)\psi(d)\lambda_d q^n,$$

and

$$a_0 = \begin{cases} \frac{1}{2}\mathscr{L}(\psi\omega) & \text{if } \eta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

When $\psi = \omega^{-1}$, the constant term $a_0 = \frac{1}{2}\mathscr{L}(1)$ lies in Frac(Λ) and has a pole at $k = 0$.

Step 2: constructing a Λ-adic form

It is harder to show the existence of Λ-adic cusp forms (just as it is harder to show the existence of classical cusp forms).

There are some explicit constructions, for example, families of Θ series.

We will use Λ-adic Eisenstein series to construct Λ-adic cusp forms.

(Remember $\Delta = c_1 \cdot E_4^3 - c_2 \cdot E_6^2$.)

The existence of Λ-adic cuspidal families follows from general theory, much of which was done by Hida.

Step 2: constructing a Λ-adic form

It is harder to show the existence of Λ-adic cusp forms (just as it is harder to show the existence of classical cusp forms).

There are some explicit constructions, for example, families of Θ series.

We will use Λ-adic Eisenstein series to construct Λ-adic cusp forms.

(Remember $\Delta = c_1 \cdot E_4^3 - c_2 \cdot E_6^2$.)

The existence of Λ-adic cuspidal families follows from general theory, much of which was done by Hida.

Iterating U_p

If $f \in S_k(Np, \chi; \mathbf{Z}_p)$ is a U_p-eigenform, then

$$U_p f = a_p f \Longrightarrow U_p^n f = a_p^n f.$$

If f is not ordinary, $a_p^n \to 0$ as $n \to \infty$, so $U_p^n f \to 0$.

If f is ordinary, $a_p^{(p-1)p^n} \to 1$ as $n \to \infty$, so $U_p^{(p-1)p^n} f \to f$.

Hida's ordinary projector

Definition

Define Hida's ordinary projector by

$$e = \lim_{n \to \infty} U_p^{n!} \in \mathbf{T}.$$

e is an idempotent: $e^2 = e$.

If f is an eigenform then $ef = f$ if f is ordinary and $ef = 0$ otherwise.

Hida's control theorem

Define the space of ordinary Λ-adic cusp forms by

$$\mathscr{S}(N,\chi)^o = e\mathscr{S}(N,\chi).$$

Theorem (Hida)

The space of ordinary Λ-adic forms $\mathscr{S}(N,\chi)^o$ is a free Λ-algebra of finite rank, and for every integer $k \geq 2$, we have

$$\nu_k(\mathscr{S}(N,\chi)^o) = S_k(Np,\chi\omega^{1-k})^o.$$

Furthermore, over $\mathrm{Frac}(\Lambda)$, the space $\mathscr{S}(N,\chi)^o$ has a basis of eigenforms.

Step 3: associated Galois representation

Theorem (Hida, Wiles)

Let $f \in \mathscr{S}(N,\chi)^o$ be an ordinary Λ-adic cuspidal eigenform. There exists an irreducible continuous Galois representation

$$\rho : G_{\mathbf{Q}} \to GL_2(\mathrm{Frac}(\Lambda))$$

that is unramified outside Np, such that for all $\ell \nmid Np$,

$$trace(\rho(Frob_\ell)) = a_\ell$$

and

$$\det(\rho(Frob_\ell)) = \chi(\ell)\langle\ell\rangle^{k-1}.$$

It is possible that the specialization of ρ at some $k \in \mathbf{Z}_p$ is reducible.

Step 4: the local restriction

Theorem (Hida, Wiles)

There is a basis such that the restriction of ρ to G_p has the form

$$\rho|_{G_p} \cong \begin{pmatrix} \eta_1 & * \\ 0 & \eta_2 \end{pmatrix}$$

where $\eta_2 : G_p \to \Lambda^\times$ is the unramified character such that

$$\eta_2(Frob_p) = a_p.$$

Steps in Ribet's Method, revisited

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.
- Step 2: Construct an ordinary Λ-adic family of cusp forms with a_p related to L_p.
- Step 3: Specialize the Galois representation associated to the family at a weight $k \in \mathbf{Z}_p$ where it is reducible. Extract a cohomology class $[\kappa]$ from the reducible representation.
- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method, revisited

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.
- Step 2: Construct an ordinary Λ-adic family of cusp forms with a_p related to L_p.
- Step 3: Specialize the Galois representation associated to the family at a weight $k \in \mathbf{Z}_p$ where it is reducible. Extract a cohomology class $[\kappa]$ from the reducible representation.
- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method, revisited

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.

- Step 2: Construct an ordinary Λ-adic family of cusp forms with a_p related to L_p.

- Step 3: Specialize the Galois representation associated to the family at a weight $k \in \mathbf{Z}_p$ where it is reducible. Extract a cohomology class $[\kappa]$ from the reducible representation.

- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Steps in Ribet's Method, revisited

- Step 1: Reformulate problem as stating the existence of a global class $[\kappa] \in H^1(G_{\mathbf{Q}}, E(\chi))$ with a prescribed local restriction, e.g. with $[\kappa]_p$ related to a p-adic L-function L_p.
- Step 2: Construct an ordinary Λ-adic family of cusp forms with a_p related to L_p.
- Step 3: Specialize the Galois representation associated to the family at a weight $k \in \mathbf{Z}_p$ where it is reducible. Extract a cohomology class $[\kappa]$ from the reducible representation.
- Step 4: Use the fact that the family is ordinary to relate the local restriction $[\kappa]_p$ to a_p, and hence to L_p as desired.

Preview of coming attractions

In the remaining lectures, we will describe these steps in the case of the Gross–Stark conjecture.