The method of Eisenstein congruences in Iwasawa theory

Ruichen XU

Géométrie algébrique et théorie des nombres en Bourgogne Franche-Comté

Academy of Mathematics and Systems Science (AMSS), Chinese Academy of Sciences
Laboratoire de Mathématiques de Besançon (LmB), l'Université de Franche-Comté

Mars 28, 2025, À Dijon
Revised: Mars 29, 2025

Contents

1. Iwasawa theory of class groups
2. Iwasawa main conjectures: the machinery of Eisenstein congruences.
3. Iwasawa theory beyond class groups, and our recent work.

Iwasawa theory of class groups: backgrounds

Let F be a number field, i.e., a finite extension of $\mathbb{Q}$. Denote by $\mathcal{O}_F$ its ring of integers.

Key object: The class group $\mathrm{Cl}(F)$ of F, which measures how far $\mathcal{O}_F$ is from being a principal ideal domain (PID) or a unique factorization domain (UFD).

Theorem

The class group $\mathrm{Cl}(F)$ is a finite abelian group.

Iwasawa theory of class groups: backgrounds

Some examples of class groups

1. $\mathrm{Cl}(\mathbb{Q}) = 1$, since $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ is a PID.
2. $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = 2$. In fact, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$, and we have the factorizations:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Gauss's problem

For quadratic fields $F = \mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$, how is the class number

$$h(D) := \#\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$$

distributed?

Iwasawa theory of class groups: Gauss's problem

Gauss's problem

For quadratic fields $F = \mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$, how is the class number $\#\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$ distributed?

Theorem (Heilbronn, 1934)

$h(D) \to \infty$, as $D \to -\infty$.

Theorem (Stark, 1966. Baker, 1971)

*The only **imaginary** quadratic fields of class number one are $\mathbb{Q}(\sqrt{-D})$ with*

$$D = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Remark: The parallel question for *real* quadratic fields is widely open.

Iwasawa theory of class groups: Iwasawa's problem

Gauss's problem

The distribution of class numbers in **horizontal families** of number fields: for example, all number fields F such that $[F:\mathbb{Q}] = 2$.

Iwasawa's problem

Consider Gauss' problem in **vertical families** of number fields

$$F \subset F_1 \subseteq F_2 \subset \cdots \subset F_n \subset \cdots \subset F_\infty$$

such that $\mathrm{Gal}(F_\infty/F) \simeq (\mathbb{Z}_p, +)$. The extension F_∞/F is called a $\mathbb{Z}_p$**-extension** of F, and its intermediate fields are F_n for $n \geq 1$ with $\mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n$.

Example: Cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$

Let $p \geq 3$. Consider the p-cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, that is, adjoining all p-power roots of unity over $\mathbb{Q}$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n)^\times = \mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1) \times (1 + p\mathbb{Z}_p)$$

Then the subfield $\mathbb{Q}_\infty$ of $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ fixed by the subgroup $\mathbb{Z}/(p-1)$ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}$. It is called the **cyclotomic $\mathbb{Z}_p$-extension** of $\mathbb{Q}$.

Remark: $1 + p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p$ via the logarithm map, when $p \geq 3$.

Example: Cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\mu_p)$

Similarly, one checks that $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$ is a $\mathbb{Z}_p$-extension, with the n-th layer being $\mathbb{Q}(\mu_{p^{n+1}})$.

Iwasawa theory of class groups

Iwasawa's problem

Let F_∞/F be a $\mathbb{Z}_p$-**extension** of F with intermediate fields

$$F \subset F_1 \subseteq F_2 \subset \cdots \subset F_n \subset \cdots \subset F_\infty$$

Then how does the sequence $\{\#\mathrm{Cl}(F_n)[p^\infty]\}$ grow?

The key to the problem: consider all these class groups in one single giant object

$$\mathrm{Cl}_\infty := \varprojlim_n \mathrm{Cl}(F_n)[p^\infty].$$

The advantage is that it acquires an action of the **Iwasawa algebra**

$$\Lambda := \mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/F)]\!] \simeq \mathbb{Z}_p[\![T]\!].$$

The upshot: Cl_∞ is a **finitely generated torsion** Λ-module.

Iwasawa theory of class groups

Here comes some commutative algebras of Λ-modules:

Finitely generated torsion Λ-modules are "rigid":

Let M be a finitely generated torsion Λ-module. Then there is a ("unique") map

$$M \to \bigoplus_{i=1}^{r} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{n_j}$$

whose kernel and cokernel are of finite cardinality. Here $f_j(T) \in \mathbb{Z}_p[T]$ are "distinguished polynomials". We can then define the Iwasawa-theoretic invariants of M:

- μ-**invariant**: $\mu(M) := \sum_{i=1}^{r} m_i$,
- λ-**invariant**: $\lambda(M) := \sum_{j=1}^{t} n_j \deg(f_j(T))$,
- **characteristic ideal**: $\mathrm{char}(M) := (p^{\mu(M)} \prod_{j=1}^{t} f_j(T)^{n_j})$, a principal ideal of Λ.

Iwasawa theory of class groups

Recall: The module Cl_∞ is a finitely generated torsion Λ-module. Using homological algebra, we can trace back to finite levels and obtain the following theorem.

Iwasawa's class number formula

$$\#\mathrm{Cl}(F_n)[p^\infty] = p^{\mu p^n + \lambda n + \nu}, \quad \text{for } n \gg 0,$$

where $\mu = \mu(\mathrm{Cl}_\infty)$, $\lambda = \lambda(\mathrm{Cl}_\infty)$, and ν is an integer (possibly negative).

Is this really a big result? Yes and No!

- **Yes**: At least we now understand more about the growth pattern of $\mathrm{Cl}(F_n)[p^\infty]$.
- **No**: "These are merely algebraic tricks; we still do not know the invariants μ, λ, and ν."

The upshot: The goal is to describe the invariants $\mu(\mathrm{Cl}_\infty)$, $\lambda(\mathrm{Cl}_\infty)$, and even the characteristic ideal char(Cl_∞) **analytically**.

Four Themes of Iwasawa Theory (Imprecise):

Let $F_\infty/F = \mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$.

- (A) **Algebraic side**: Cl_∞ is a finitely generated torsion Λ-module.
- (B) **Analytic side** [Kubota-Leopoldt, 1960s]: There exist ***p*-adic *L*-functions** $\mathcal{L}_p \in \Lambda$ encoding the special values of Dirichlet L-functions:

$$\{L(\psi\omega^{-r}\phi^{-1}, 1-r) \mid r \geq 1,\ \phi : \mathrm{Gal}(F_\infty/F) \to \mathbb{C}^\times \text{ of finite order}\}.$$

- (C) **Iwasawa's Main Conjecture** [Mazur-Wiles, 1980s]: As principal ideals of Λ, we have the equality

$$\mathrm{char}(\mathrm{Cl}_\infty) = (\mathcal{L}_p).$$

- (D) $\mu(\mathcal{L}_p) = 0$ [Ferrero-Washington, 1980s], and $\lambda(\mathcal{L}_p)$ is *conjectured* to be zero [Greenberg, 1980s].

Corollary: Granting Greenberg's conjecture, $\#\mathrm{Cl}(\mathbb{Q}(\mu_{p^{n+1}}))[p^\infty]$ is bounded as $n \to \infty$.

Iwasawa Main Conjectures

Today, we focus on **Theme (C)**: Iwasawa's main conjecture of the form

$$\mathrm{char}(\mathrm{Cl}_\infty) = (\mathcal{L}_p).$$

This leads to two divisibilities:

1. $\mathcal{L}_p \mid \mathrm{char}(\mathrm{Cl}_\infty)$: This gives a **lower bound** for Cl_∞.
   Method: Use **Eisenstein congruences** to construct sufficiently many ideal classes.
2. $\mathrm{char}(\mathrm{Cl}_\infty) \mid \mathcal{L}_p$: This gives an **upper bound** for Cl_∞.
   Method: Use **Euler systems** to study relations among ideal classes (speaking very vaguely).

Today, we focus on Eisenstein congruences, i.e., the lower bound for Cl_∞.

Ribet's method

Suppose p divides the numerator of some Bernoulli number B_m with even number $m \in [2, p-3]$, then $\mathrm{Cl}(\mathbb{Q}(\mu_{p^m}))$ has a nontrivial p-torsion element.

Step 1 : Consider the weight m, level $\mathrm{SL}_2(\mathbb{Z})$ Eisenstein series

$$E_m(q = \exp(2\pi \mathrm{i} z)) = \frac{\zeta(1-m)}{2} + \sum_{n \geq 1} \sigma_{m-1}(n) q^n, \quad \sigma_{m-1}(n) := \sum_{d|n} d^{m-1}.$$

Step 2 : Then $p \mid B_m$ implies that p divides the constant term of E_m. Therefore it is plausible to construct a cuspform $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ such that $E_m \equiv f \pmod{p}$.

Step 3 : Translate this to modulo-p congruence of Galois representations, one obtain

$$\rho_f \equiv \rho_{E_m} \equiv \begin{bmatrix} \omega^{m-1} & * \\ 0 & 1 \end{bmatrix} \pmod{p}.$$

The Galois cohomology class $*$ will provide a desired ideal class.

Iwasawa main conjectures: Ribet's method

Example: Ramanujan's congruence

Consider

$$\Delta(q = \exp(2\pi \mathrm{i} z)) := q \prod_{i=1}^{\infty} (1 - q^n)^{24} \in S_{12}(\mathrm{SL}_2(\mathbb{Z})), \quad \mathrm{im}(z) > 0.$$

Then Ramanujan observed that

$$\Delta \equiv E_{12} \mod p = 691.$$

Serre used this to construct a nontrival ideal class of $\mathbb{Q}(\mu_{691})$. This is the starting point of Ribet's method.

Iwasawa theory beyond class groups

Starting with B. Mazur, it was observed that the Iwasawa theory of class groups can be vastly generalized to study the arithmetic of elliptic curves, modular forms, and even general Galois representations.

Suppose we want to study the Iwasawa theory of a modular form $f_0 \in S_k(\Gamma_1(N), \epsilon)$. How does Ribet's method proceed?

Class Groups: The special values $\zeta(1-m)$ over GL_1 correspond to Eisenstein series E_m over GL_2, whose constant term involves $\zeta(1-m)$.

Modular Forms: The L-function $L(f_0, s)$ over GL_2 corresponds to an Eisenstein series $E_{??}$ over $G^{??}$, whose constant term should involve $L(f_0, s)$.

Iwasawa theory beyond class groups: Klingen Eisenstein series

Upshot: The **Klingen Eisenstein series** $E_{f_0}^{\mathrm{Kling}}$ over unitary groups $\mathrm{U}(2,2)$ or $\mathrm{U}(3,1)$ encodes $L(f_0, s)$.

Unitary groups

Let K be an auxiliary imaginary quadratic field such that p splits in K, one defines

$$\mathrm{U}(m,n) := \left\{ g \in \mathrm{GL}_{m+n}(K) : \overline{g}^{\mathrm{t}} \begin{bmatrix} \mathbf{1}_m & 0 \\ 0 & -\mathbf{1}_n \end{bmatrix} g = \begin{bmatrix} \mathbf{1}_m & 0 \\ 0 & -\mathbf{1}_n \end{bmatrix} \right\}.$$

This is called the **unitary group** of signature (m,n). This is an algebraic group over $\mathbb{Q}$. For example,

$$\mathrm{U}(1,1) \simeq \mathrm{GL}_2, \quad \mathrm{U}(2,0) \simeq \text{a nonsplit quaternion algebra.}$$

Iwasawa theory: Klingen Eisenstein series and their p-primitivity

Let's put ourself in the most general case: Let φ_0 be a cuspform over the unitary group $\mathrm{U}(m, n)$, we can define a Klingen Eisenstein series

$$E_{\varphi_0}^{\mathrm{Kling}} : \mathrm{U}(m+1, n+1)(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{C}$$

with constant term essentially the L-function of φ_0. Then "*Step 1* " of Ribet's method works.

The key difficulty: "*Step 2* " of Ribet's method

How to show that the congruence relation "$E_{\varphi_0}^{\mathrm{Kling}} \equiv f \pmod{p}$" is **nontrivial**? In other words, how to show that $E_{\varphi_0}^{\mathrm{Kling}} \not\equiv 0 \pmod{p}$?

Iwasawa theory: Klingen Eisenstein series and their p-primitivity

The key difficulty: "*Step 2*" of Ribet's method

How to show that the congruence relation "$E^{\mathrm{Kling}}_{\varphi_0} \equiv f \pmod p$" is **nontrivial**? In other words, how to show that $E^{\mathrm{Kling}}_{\varphi_0} \not\equiv 0 \pmod p$?

Example on lower rank cases

- Recall the GL_2-case, the p-th coefficient of E_m is $1 + p^{m-1}$, which is nonzero modulo p. Hence $E_m \not\equiv 0 \pmod p$.
- For Kligen Eisenstein series $E^{\mathrm{Kling}}_{f_0}$ over $\mathrm{U}(2,2)$ or $\mathrm{U}(3,1)$, certain Fourier coefficients of $E^{\mathrm{Kling}}_{f_0}$ can be computed. [Skinner-Urban 2014][Wan 2020][Castella-Liu-Wan 2022]

Our work on the GGP period integral of Klingen Eisenstein series

For $E_{\varphi_0}^{\mathrm{Kling}}$ over $\mathrm{U}(m+1, n+1)$, we compute its **Gan-Gross-Prasad period integral** defined as

$$\mathscr{P}_\varphi(E_{\varphi_0}^{\mathrm{Kling}}) := \int_{\mathrm{U}(m+1,n)(\mathbb{Q})\backslash \mathrm{U}(m+1,n)(\mathbb{A}_\mathbb{Q})} E_{\varphi_0}^{\mathrm{Kling}}(\iota(g))\varphi(g)\,\mathrm{d}g,$$

where φ is a cuspform over the smaller group $\mathrm{U}(m+1, n)$, and ι is a canonical embedding $\iota : \mathrm{U}(m+1, n) \hookrightarrow \mathrm{U}(m+1, n+1)$.

Philosophy of period integrals

- To show $E_{\varphi_0}^{\mathrm{Kling}}$ is modulo-p nonvanishing, it suffices to **choose an approprite** φ such that $\mathscr{P}_\varphi(E_{\varphi_0}^{\mathrm{Kling}})$ is nonvanishing modulo p.
- Such period integrals are closed related to **special values of L-function**, and we have more tools on these L-functions.

Our theorem reflects the aforementioned philosophy.

Theorem (X., arXiv:2410.13132)

$$\frac{\mathscr{P}_{\varphi}(E_{\varphi_0}^{\mathrm{Kling}})^2}{|\varphi|\,|\varphi_0|} \approx \mathcal{L}^{\Sigma}\left(\frac{1}{2}, \pi_{\varphi} \times \pi_{\varphi_0}\right) \mathcal{L}^{\Sigma}\left(s_0, \pi_{\varphi}\right) \mathcal{L}^{\Sigma}\left(s_0, \pi_{\varphi}^{\vee}\right),$$

where "$\approx$" means "up to explicit factors at some bad places $v \in \Sigma$", and $\mathcal{L}^{\Sigma}$ denotes appropriately normalized L-functions with local Euler factors at bad places $v \in \Sigma$ removed.

Ongoing work with collaborators: Establishing the modulo-p nonvanishing property of these L-functions by further reducing the rank of φ via theta correspondences.

A byproduct of our theorem: By deforming φ_0 and φ in p-ordinary families of modular forms, we show that the Klingen Eisenstein series E_{φ_0} and its GGP period integrals deform in p-adic families. Consequently, this yields a construction of a p-adic L-function for the Rankin–Selberg product of cusp forms over unitary groups of rank $m+n$ and $m+n+1$.

Thank you!

Slides will be available on my webpage:
`https://xuruichen98.github.io/`

Ruichen XU, `xuruichen21@mails.ucas.ac.cn`