STARK'S CONJECTURES AND HILBERT'S 12TH PROBLEM

Samit Dasgupta

Duke University

Fields Institute, Toronto

Online Seminar—8/26/2020

CLASS FIELD THEORY

Class field theory describes the **Galois group** of the maximal abelian extension of a number field F.

$$\mathrm{Gal}(F^{ab}/F) \cong \mathbf{A}_F^*/\overline{F^*F_\infty^{>0}}$$

The right hand side uses information intrinsic to only F itself.

Explicit class field theory asks for the construction of the field F^{ab}, again using only information intrinsic to F.

KRONECKER–WEBER THEOREM

Let $F = \mathbf{Q}$.

Class field theory:

$$\mathrm{Gal}(\mathbf{Q}^{ab}/\mathbf{Q}) \cong \hat{\mathbf{Z}}^* \cong \prod_p \mathbf{Z}_p^*$$

Explicit class field theory: (Kronecker-Weber)

$$\mathbf{Q}^{ab} = \bigcup_{n=1}^{\infty} \mathbf{Q}(e^{2\pi i/n})$$

COMPLEX MULTIPLICATION

Quadratic imaginary fields.

$$F = \mathbf{Q}(\sqrt{-d}), \qquad d = \text{ positive integer}.$$

> **Theorem**. $F_n = F(j(E), w(E[n]))$ where E is an elliptic curve with complex multiplication by $\mathcal{O}_F$ and $w =$ "Weber function."

Here $j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$ is the usual modular function. For $F = \mathbf{Q}(\sqrt{-d})$, modular functions play the role of the exponential function for $F = \mathbf{Q}$.

HILBERT'S 12TH PROBLEM (1900)

"The theorem that every abelian number field arises from the realm of rational numbers by the composition of fields of roots of unity is due to Kronecker."

"Since the realm of the imaginary quadratic number fields is the simplest after the realm of rational numbers, the problem arises, to extend Kronecker's theorem to this case."

"Finally, the extension of Kronecker's theorem to the case that, in the place of the realm of rational numbers or of the imaginary quadratic field, any algebraic field whatever is laid down as the realm of rationality, seems to me of the greatest importance. I regard this problem as one of the most profound and far-reaching in the theory of numbers and of functions."

APPROACHES USING L-FUNCTIONS

- **Stark** stated a series of conjectures proposing the existence of elements in abelian extensions H/F whose absolute values are related to L-functions (1971-80).
- **Tate** made Stark's conjectures more precise and stated the **Brumer-Stark** conjecture. (1981)
- **Gross** refined the Brumer-Stark conjecture using p-adic L-functions. This is called the **Gross-Stark** conjecture (1981).
- **Rubin** (1996), **Burns** (2007), and **Popescu** (2011) made the higher rank version of Stark's conjectures more precise.
- **Burns**, **Popescu**, and **Greither** made partial progress on Brumer-Stark building on work of **Wiles**.

THE BRUMER-STARK AND GROSS-STARK CONJECTURES

Let F be a **totally real** number field. Let H be a finite **CM** abelian extension F.

- The **Brumer-Stark conjecture** predicts the existence of certain elements $u \in H^*$ called Brumer-Stark units that are related to L-functions of F in a specific way.

- The **Gross-Stark conjecture** predicts that these units are related to p-adic L-functions of F in a specific way.

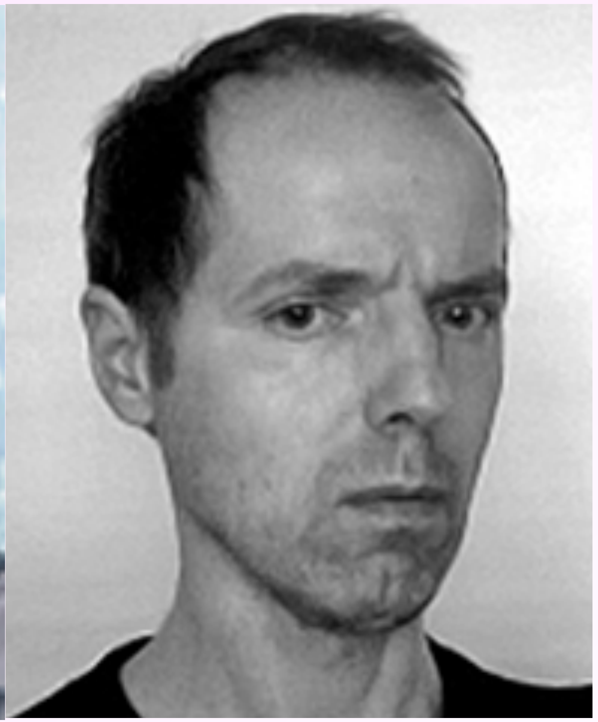
SOME OF MY PRIOR WORK IN THIS AREA

Stated a conjectural **exact formula** for Brumer-Stark units in several joint works, with:

Henri Darmon

Pierre Charollois

Matthew Greenberg



Michael Spiess

SOME OF MY PRIOR WORK IN THIS AREA

Proved the **Gross-Stark** conjecture*

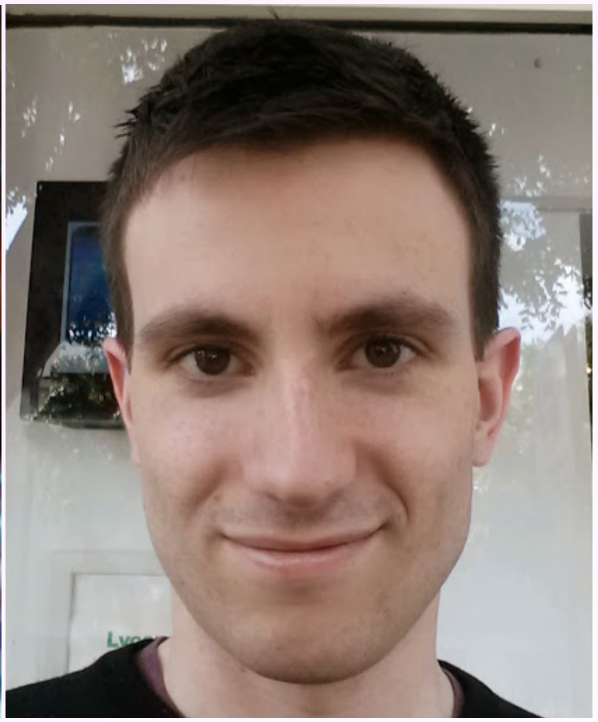
Benedict Gross

in joint works with:

Henri Darmon

Robert Pollack

Mahesh Kakde



Kevin Ventullo

NEW RESULTS* (WITH MAHESH KAKDE)

Theorem 1. The Brumer-Stark conjecture holds if we invert 2 (i.e. up to a bounded power of 2).

Theorem 2. My conjectural exact formula for Brumer-Stark units holds, up to a bounded root of unity.

P-ADIC SOLUTION TO HILBERT'S 12TH PROBLEM

Hilbert's 12th problem is viewed as asking for the construction of the field F^{ab} using analytic functions depending only on F.

The Brumer-Stark units, together with other explicit and easy to describe elements, generate the field F^{ab}.

Our exact formula expresses the Brumer-Stark units as p-adic integrals of analytic functions depending only on F.

Therefore the proof of this conjecture can be viewed as a p-adic solution to Hilbert's 12th problem.

STARK'S CONJECTURE

H/F = finite abelian ext of number fields, $G = \mathrm{Gal}(H/F)$.

v = place of F that splits completely in H .

S = a set of places of F containing the infinite places, ramified places, and v.

$e = \#\mu(H)$.

Conjecture (Stark 1971-80).

There exists $u \in H^*$ such that $|u|_w = 1$ for every place $w \nmid v$ and for every character χ of G,

$$L_S'(\chi,0) = -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\log|u|_{\sigma^{-1}w}.$$

Furthermore, $H(u^{1/e})$ is an abelian extension of F.

Technical remark: For this formulation, must assume at least 3 archimedean or ramified places of F.

INSIDE THE ABSOLUTE VALUE

Stark's formula can be manipulated to calculate $|u|$ under each embedding $H \hookrightarrow \mathbf{C}$.

Can one refine this and propose a formula for u itself?

The presence of the absolute value represents a gap between Stark's Conjecture and Hilbert's 12th problem—if we had an analytic formula for u, this would give a way of constructing canonical nontrivial elements of H.

There are interesting conjectures in this direction by Ren-Sczech and Charollois-Darmon.

THE BRUMER-STARK CONJECTURE

Fix primes $\mathfrak{p}, \mathfrak{q} \subset \mathcal{O}_F$, $\mathfrak{P} \subset \mathcal{O}_H$ above $\mathfrak{p}$.

$S = \{$infinite places, ramified places$\}$.

Conjecture (Tate-Brumer-Stark).

There exists $u \in \mathcal{O}_H[1/\mathfrak{p}]^*$ such that $|u| = 1$ under each embedding $H \hookrightarrow \mathbf{C}$,

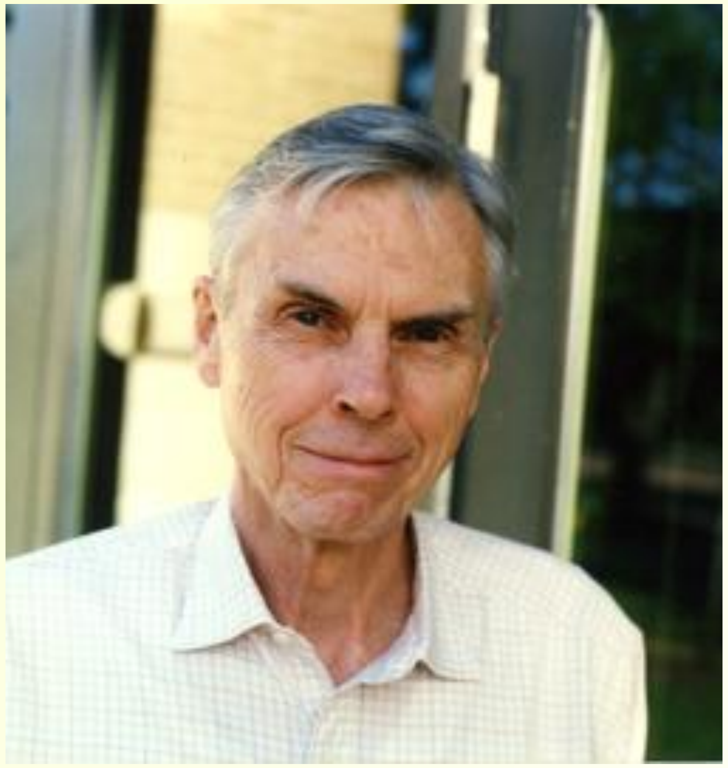
$$L_S(\chi, 0)(1 - \chi(\sigma_\mathfrak{q})\mathrm{N}\mathfrak{q}) = \sum_{\sigma \in G} \chi^{-1}(\sigma) \operatorname{ord}_\mathfrak{P}(\sigma(u))$$

for all characters χ of G, and $u \equiv 1 \pmod{\mathfrak{q}\mathcal{O}_H}$.

Ludwig Stickelberger

Armand Brumer

Harold Stark



John Tate

RESULTS

Theorem (D-Kakde). There exists

$$u \in \mathcal{O}_H[1/\mathfrak{p}]^* \otimes \mathbf{Z}[1/2]$$

satisfying the conditions of the Brumer-Stark conjecture.

There is a "higher rank" version of the Brumer-Stark conjecture due to Karl Rubin. We obtain this result as well, after tensoring with $\mathbf{Z}[1/2]$.

GROUP RINGS AND STICKELBERGER ELEMENTS

Theorem. (Deligne-Ribet, Cassou-Noguès)

There is a unique $\Theta \in \mathbf{Z}[G]$ such that

$$\chi(\Theta) = L_S(\chi^{-1},0)(1 - \chi^{-1}(\sigma_{\mathbf{q}})\mathrm{N}\mathbf{q})$$

for all characters χ of G.

CLASS GROUP

Define

$$\mathrm{Cl}_{\mathfrak{q}}(H) = I(H)/\langle (u) : u \equiv 1 \pmod{\mathfrak{q}\mathcal{O}_H} \rangle.$$

This is a G-module.

Brumer-Stark states: Θ annihilates $\mathrm{Cl}_{\mathfrak{q}}(H)$.

For this, it suffices to prove

$$\boxed{\Theta \in \mathrm{Ann}_{\mathbf{Z}_p[G]}(\mathrm{Cl}_{\mathfrak{q}}(H) \otimes \mathbf{Z}_p)}$$

for all primes p.

STRONG BRUMER-STARK

Theorem. For odd primes p, we have

$$\Theta \in \mathrm{Fitt}_{\mathbf{Z}_p[G]}(\mathrm{Cl}_{\mathfrak{q}}(H)^{\vee,-})$$

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(\mathrm{Cl}_{\mathfrak{q}}(H)^{\vee,-}) \subset \mathrm{Ann}_{\mathbf{Z}_p[G]}(\mathrm{Cl}_{\mathfrak{q}}(H)^{-}).$$

REFINEMENTS: CONJECTURES OF KURIHARA AND BURNS

Theorem. For odd primes p, we have

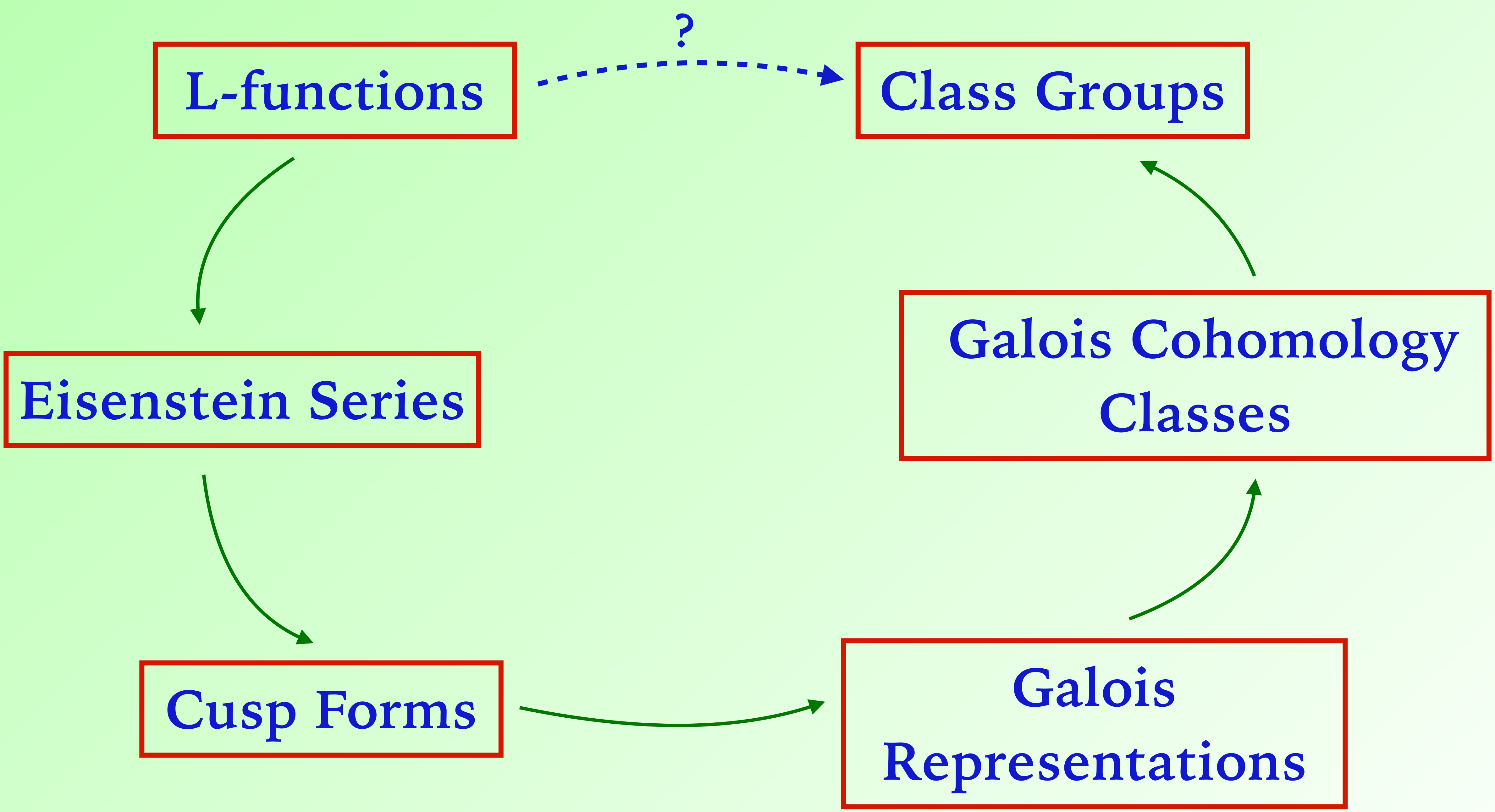
$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(\mathrm{Cl}_{\mathfrak{q}}(H)^{\vee,-}) = \Theta_{S_\infty} \prod_{v \in S_{ram}} (\mathrm{N}I_v,\ 1 - \sigma_v^{-1} e_v)$$

Theorem. For odd primes p, we have

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(\mathrm{Sel}_S^{\mathfrak{q}}(H)_p^-) = (\Theta_S)$$

RIBET'S METHOD

(DIAGRAM H/T BARRY MAZUR)



GROUP RING VALUED MODULAR FORMS

$M_k(G)$ = Hilbert modular forms over F of weight k with Fourier coefficients in $\mathbf{Z}_p[G]$ such that for every character χ of G, applying χ yields a form of nebentype χ.

Example: Eisenstein Series.

$$E_1(G) = \frac{1}{2^d}\Theta + \sum_{\mathfrak{m}\subset\mathcal{O}}\left(\sum_{\mathfrak{a}\supset\mathfrak{m},(\mathfrak{a},S)=1}\sigma_{\mathfrak{a}}\right)q^{\mathfrak{m}}$$

This must be modified in level 1.

GROUP RING CUSP FORM

$$f = E_1(G)V_k - \frac{\Theta}{2^d}H_{k+1}(G)$$

is cuspidal at infinity, where V_k and $H_{k+1}(G)$ have constant term 1.

Choose $V_k \equiv 1 \pmod{p^N}$, where $\Theta \mid p^N$ away from trivial zeroes.

$$\boxed{f \equiv E_1(G) \pmod{\Theta}.}$$

The existence of V_k and $H_{k+1}(G)$ are non-trivial theorems of Silliman, generalizing results of Hida and Chai.

This can be modified to yield a cusp form f satisfying $\boxed{f \equiv E.}$

GALOIS REPRESENTATION

We hereafter assume that f is an eigenform.

The Galois representation associated to f can be chosen as:

$$\rho_f(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}_p[G])$$

where $a(\sigma) \equiv 1 \pmod{\Theta}, \quad d(\sigma) \equiv [\sigma] \pmod{\Theta}.$

This is because $f \equiv E_1(G) \pmod{\Theta}$ and

$$a_\ell(E_1(G)) = 1 + [\sigma_\ell]\,.$$

Let $B = \mathbf{Z}_p[G]\langle b(\sigma) \colon \sigma \in G_F \rangle$

COHOMOLOGY CLASS

Then $b(\sigma\tau) = a(\sigma)b(\tau) + b(\sigma)d(\tau)$ implies

$$b(\sigma\tau) \equiv b(\tau) + [\tau]b(\sigma) \pmod{\Theta}, \quad \text{hence}$$

$$\boxed{\kappa(\sigma) = [\sigma]^{-1}b(\sigma) \in H^1(G_F, B/\Theta B)\,.}$$

The class κ is unramified outside the level and p since ρ_f is.

Problem: In general, κ is not unramified at p.

To deal with this in the proof of IMC, Wiles invented "**horizontal Iwasawa theory**," which led to the **Taylor-Wiles method**.

Issue: In our context, this method meets with obstacles that appear insurmountable.

SPLITTING FIELD (CASE H/F UNRAMIFIED)

Pretend that κ is unramified at p. The splitting field of κ is an extension of H whose Galois group is a **quotient** of $\mathrm{Cl}_{\mathfrak{q}}(H)$:

$$\mathrm{Cl}_{\mathfrak{q}}(H)^{-} \twoheadrightarrow B/\Theta B$$

Hence

$$\mathrm{Fitt}(\mathrm{Cl}_{\mathfrak{q}}(H)^{-}) \subset \mathrm{Fitt}(B/\Theta B) \subset (\Theta)$$

since B is a faithful $\mathbf{Z}_p[G]$-module.

An analytic argument shows that this $\subset$ is an $=$.

GENERAL CASE

The previous slides works for H/F unramified, and can be modified when H/F is ramified only at primes not above p .

Key idea: move ramified primes to smoothing set.

When there is **ramification at p**, the situation is more complicated.

A **Selmer module** replaces $\mathrm{Cl}_{\mathfrak{q}}(H)^{-}$.

It is endowed with a surjective map to $\mathrm{Cl}_{\mathfrak{q}}(H)^{\vee,-}$.

GETTING A CLASS UNRAMIFIED AT P

Step 1: There is a non-zero divisor $x \in \mathbf{Z}_p[G]$ such that we can construct a "higher congruence":

$$f \equiv E_1(G) \pmod{x\Theta}$$

- x measures "**trivial zeroes** at p."
- Requires detailed construction of cusp form.
- Calculation of constant terms of Eisenstein series at **all cusps.**

GETTING A CLASS UNRAMIFIED AT P

Step 2: Define

$$B' = \langle b(\sigma) : \sigma \in I_{\mathfrak{p}},\ \mathfrak{p} \mid p \rangle \subset B$$

$$\overline{B} = B/(x\Theta B, B')$$

$$\kappa(\sigma) = [\sigma]^{-1} b(\sigma) \in H^1(G_F, \overline{B})$$

κ is now tautologically unramified at p.

$$\mathrm{Cl}_{\mathfrak{q}}(H)^- \twoheadrightarrow \overline{B}$$

$$\mathrm{Fitt}(\mathrm{Cl}_{\mathfrak{q}}(H)^-) \subset \mathrm{Fitt}(\overline{B})$$

FITTING IDEAL OF $\overline{B}$

Step 3: A miracle:

$$\mathrm{Fitt}(\overline{B}) \cdot (x) \subset \mathrm{Fitt}(B/x\Theta B) \subset (x\Theta)$$

so

$$\mathrm{Fitt}(\mathrm{Cl}_{\mathfrak{q}}(H)^{-}) \subset \mathrm{Fitt}(\overline{B}) \subset (\Theta)$$

as before.

EXACT FORMULA FOR THE UNITS

Our conjectural exact formula for u is given by a p-adic integral.

Suppose $\mathfrak{p} = (p)$:

Conjecture. We have

$$u = p^{\zeta(0)} \times\!\!\!\!\!\!\int_{\mathcal{O}_p^*} x \, d\mu(x)$$

where μ is a measure defined using the **Eisenstein cocycle.**

Shintani's method, topological polylogarithm (Beilinson-Kings-Levin), Sczech's method, …

COMPUTATIONAL EXAMPLE

This formula for Brumer-Stark units is explicitly computable.

Example. $F = \mathbf{Q}(\sqrt{305}), \quad \mathcal{O} = \mathbf{Z}\left[\frac{1+\sqrt{305}}{2}\right].$

$H =$ narrow Hilbert class field. $p = 3$.

Computing u and its conjugates to a high p-adic precision, we obtain a polynomial very close to:

$$81x^4 - \frac{9\sqrt{D}+345}{2}x^3 + \frac{15\sqrt{D}+419}{2}x^2 - \frac{9\sqrt{D}+345}{2}x + 81.$$

The splitting field of this polynomial is indeed H.

A LARGER EXAMPLE

$F = \mathbf{Q}(\sqrt{473}), \quad p = 5.$

To a high p-adic precision, u is a root of:

$$5^{10}x^6 + \frac{-253125\sqrt{D} - 4501875}{2}x^5$$
$$+\frac{496125\sqrt{D} + 5836125}{2}x^4 + \frac{-59535\sqrt{D} - 13546883}{2}x^3 +$$
$$\frac{496125\sqrt{D} + 5836125}{2}x^2 + \frac{-253125\sqrt{D} - 4501875}{2}x + 5^{10}.$$

Again, the splitting field of this polynomial is $H =$ narrow HCF.

HILBERT'S 12TH PROBLEM

If H is a cyclic CM extension of F in which $\mathfrak{p}$ splits completely, then the Brumer-Stark unit u for H can be shown to generate H.

It follows that if $S = \{u\}_{\mathfrak{p},H} \cup \{\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_{n-1}}\}$, where the α_i are elements of F^* whose signs in $\{\pm 1\}^n$ are a basis for this $\mathbf{Z}/2\mathbf{Z}$-vector space, then

$$F^{ab} = F(S).$$

PROOF OF CONJECTURAL EXACT FORMULA

Uses group ring valued modular forms, as in the proof of Brumer-Stark.

New features:

- An integral version of Gross-Stark due to Gross and Popescu, and its relationship to the p-adic integral formula.
- The Taylor-Wiles method of introducing auxiliary primes: "horizontal Iwasawa theory."

Thank you!