STARK'S CONJECTURES AND HILBERT'S 12TH PROBLEM

Samit Dasgupta
Duke University

University of Maryland Seminar, 4/14/2021

MOTIVATION

Today I will discuss two central related problems in Number Theory:

Explicit Class Field Theory

- Refinement of GL_1 case of Langlands Program
- Complex Multiplication
- Hilbert's 12th Problem

Special Values of *L*-functions

- Stark's Conjectures
- Birch-Swinnerton-Dyer Conjecture
- Beilinson's Conjecture and Bloch-Kato Conjecture

THE FIELD OF COMPLEX NUMBERS

A complex number $\alpha \in \mathbf{C}$ is called algebraic if it is the root of a nonzero polynomial $P(x) \in \mathbf{Q}[x]$.

The set of all algebraic numbers is a field $\overline{\mathbf{Q}}$.

We would like to understand the group $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of all automorphisms of $\overline{\mathbf{Q}}$.

The Langlands Program attempts to understand all n-dimensional representations of $G_{\mathbf{Q}}$.

More generally, we want to understand all n-dimensional representations of G_F for any finite extension $F/\mathbf{Q}$.

CLASS FIELD THEORY

Understanding the 1-dimensional representations of G_F is equivalent to understanding the abelianization G_F^{ab}.

This is the group of automorphisms of the maximal abelian extension F^{ab} over F.

Example: The field $\mathbf{Q}^{ab}$ is obtained from $\mathbf{Q}$ by adjoining all nth roots of unity for all positive integers n.

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

This is a theorem of Kronecker and Weber.

CLASS FIELD THEORY

For every positive integer n, there is a field extension F_n of F called the **narrow ray class field of conductor** n such that:

- $F_n \subset F_m$ if $n \mid m$
- $F^{ab} = \bigcup_{n \geq 1} F_n$
- $\mathrm{Gal}(F_1/F) \cong \mathrm{Pic}^+(\mathcal{O})$ and $\mathrm{Gal}(F_n/F_1) \cong (\mathcal{O}/n)^*/\mathcal{O}_+^*$

  where $\mathcal{O}$ is the **ring of integers** of F

Example: $\mathbf{Q}_n = \mathbf{Q}(e^{2\pi i/n})$ and $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \cong (\mathbf{Z}/n)^*$.

$$\mathcal{O} = \{x \in F : x \text{ is a root of a monic polynomial in } \mathbf{Z}[x]\}.$$

For $F = \mathbf{Q}$, we have $\mathcal{O} = \mathbf{Z}$.

EXPLICIT CLASS FIELD THEORY

Class field theory describes the automorphism group

$$\mathrm{Gal}(F^{ab}/F) = \varprojlim \mathrm{Gal}(F_n/F).$$

The goal of **explicit class field theory** is to construct the field F^{ab}, or equivalently, each of the fields F_n, using analytic functions depending only on the ground field F.

Example:

$$\mathbf{Q}^{ab} = \mathbf{Q}(S), \qquad S = \{e^{2\pi i x} : x \in \mathbf{Q}\}.$$

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 $j(q) = q^{-1} + 744 + 196884q + 2149360q^2 + \cdots$ 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 F_n 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. This means that every embedding $F \subset \mathbf{C}$ has image contained in $\mathbf{R}$.

- The **Brumer-Stark conjecture** predicts the existence of certain elements $u \in F_n$ 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

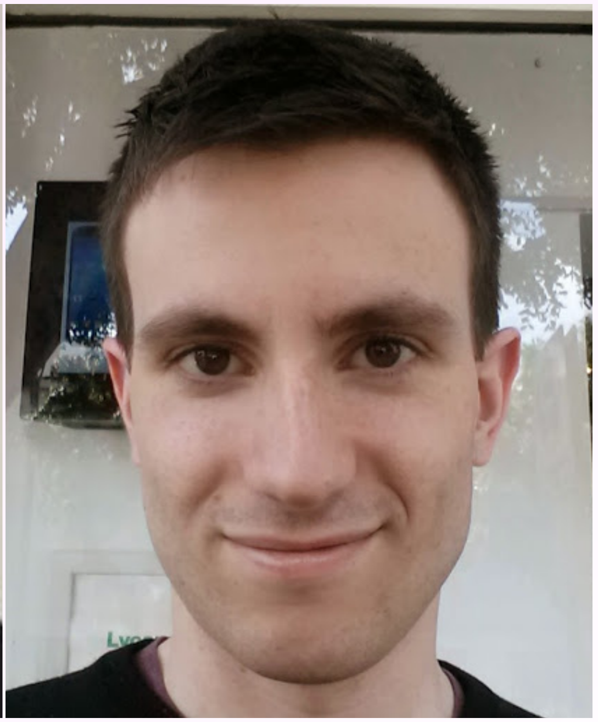
Benedict Gross

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.

ZETA FUNCTIONS

Let $\mathfrak{a} \subset \mathcal{O}$ be a nonzero ideal.

$$\mathrm{N}\mathfrak{a} = \#(\mathcal{O}/\mathfrak{a}) \text{ is finite.}$$

Define

$$\zeta_F(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s} = \prod_{\mathfrak{p} \text{ maximal}} \frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-s}}$$

Examples.

- $F = \mathbf{Q}$. $\quad \zeta_F(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$.
- $F = \mathbf{Q}(i)$. $\quad \zeta_F(s) = \frac{1}{4} \sum_{(m,n) \neq (0,0)} \frac{1}{(m^2 + n^2)^s}$.

DIRICHLET-DEDEKIND CLASS NUMBER FORMULA

Theorem (Dirichlet 1839, Dedekind 1894).

$$\frac{\zeta_F^{(r)}(0)}{r!} = -\frac{hR}{w}$$

where

$$\begin{aligned} r &= \text{rank of } \mathcal{O}^* \\ h &= \text{class number of } F = \#\operatorname{Pic}(\mathcal{O}_F) \\ R &= \text{regulator of } F \\ w &= \text{number of roots of unity in } F = \#\mu(F)\,. \end{aligned}$$

$$\mathcal{O}^* \cong \mathbf{Z}^r \times (\mathbf{Z}/w\mathbf{Z}).$$

EXAMPLE: $F = \mathbf{Q}(\sqrt{2})$

$\mathcal{O}_F = \mathbf{Z}[\sqrt{2}]\,.$

$$\mathcal{O}_F^* = \langle 1 + \sqrt{2}, -1 \rangle \cong \mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z}).$$

$h = 1,\ w = 2.$

$$R = \log(1 + \sqrt{2}).$$

$$\zeta_F'(0) = -\frac{\log(1+\sqrt{2})}{2}.$$

LOCAL TO GLOBAL

The class number formula relates the **locally** defined function

$$\zeta_F(s) = \prod_{\mathfrak{p}} \frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-s}}$$

to the **global** invariants $r, h, R,$ and w of the ring $\mathcal{O}_F$.

$$\frac{\zeta_F^{(r)}(0)}{r!} = -\frac{hR}{w}$$

L-FUNCTIONS

Artin map: for each maximal ideal $\mathfrak{p}$ not containing n, there is an associated element $\sigma_{\mathfrak{p}} \in G = \mathrm{Gal}(F_n/F)$.

Artin L-function:

If $\chi\colon G \to \mathbf{C}^*$ is a character, we define

$$L_n(\chi, s) = \prod_{\mathfrak{p} \not\supset (n)} \frac{1}{1 - \chi(\sigma_{\mathfrak{p}})(\mathrm{N}\mathfrak{p})^{-s}}.$$

For example, if χ is the trivial character, this is $\zeta_F(s)$ with the terms for $\mathfrak{p} \supset (n)$ missing.

STARK'S CONJECTURE

Fix an embedding $F_n \hookrightarrow \mathbf{C}$.

Assume that if F lands in $\mathbf{R}$ then F_n does too.

Conjecture (Stark 1971-80).

There exists $u \in \mathcal{O}_{F_n}^*$ such that for every character χ of G,

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

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 $F_n \hookrightarrow \mathbf{C}$.

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 F_n.

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

THE BRUMER-STARK CONJECTURE

Fix maximal ideals $\mathfrak{p}, \mathfrak{q} \subset \mathcal{O}_F$.

Fix a maximal ideal $\mathfrak{P} \subset \mathcal{O}_{F_n}$ above $\mathfrak{p}$.

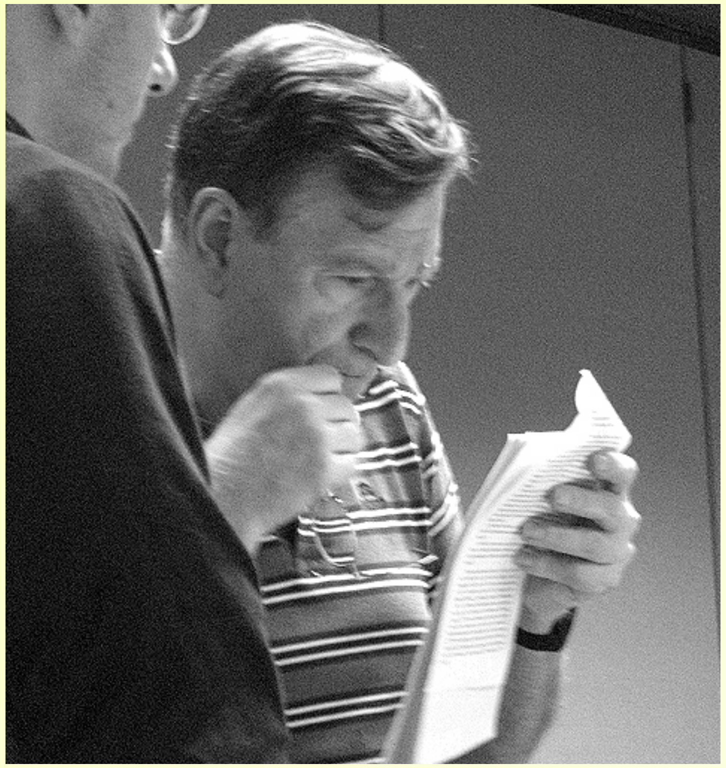
Conjecture (Tate-Brumer-Stark).

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

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

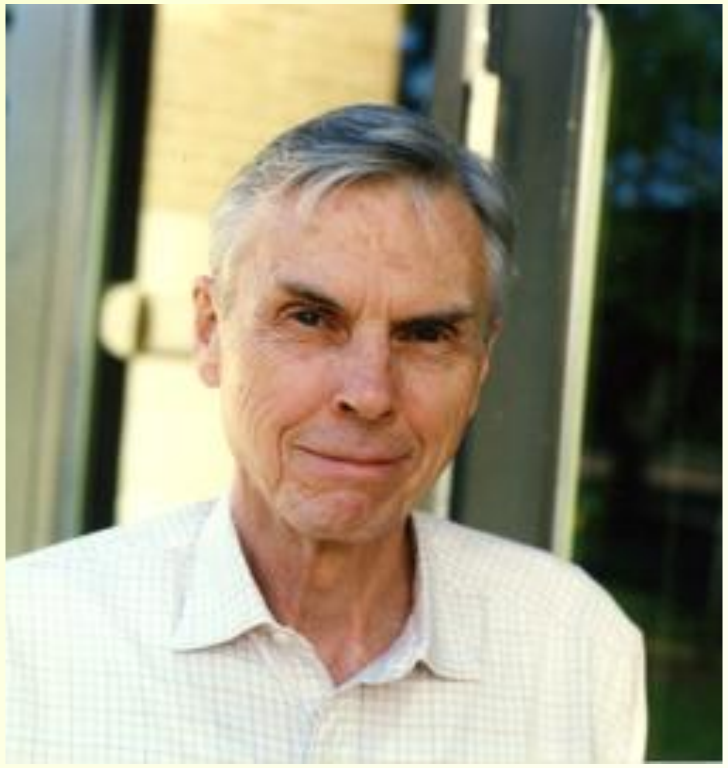
for all characters χ of G, and $u \equiv 1 \pmod{\mathfrak{q}\mathcal{O}_{F_n}}$.

Ludwig Stickelberger



Armand Brumer

Harold Stark



John Tate

RESULTS

Theorem (D-Kakde). There exists

$$u \in \mathscr{O}_{F_n}[1/\mathfrak{p}]^* \otimes \mathbf{Z}[1/2]$$

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

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

for all characters χ of G.

CLASS GROUP

Let $H = F_n$.

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

This is a G-module.

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

For this, it suffices to prove

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

for all primes p.

STRONG BRUMER-STARK

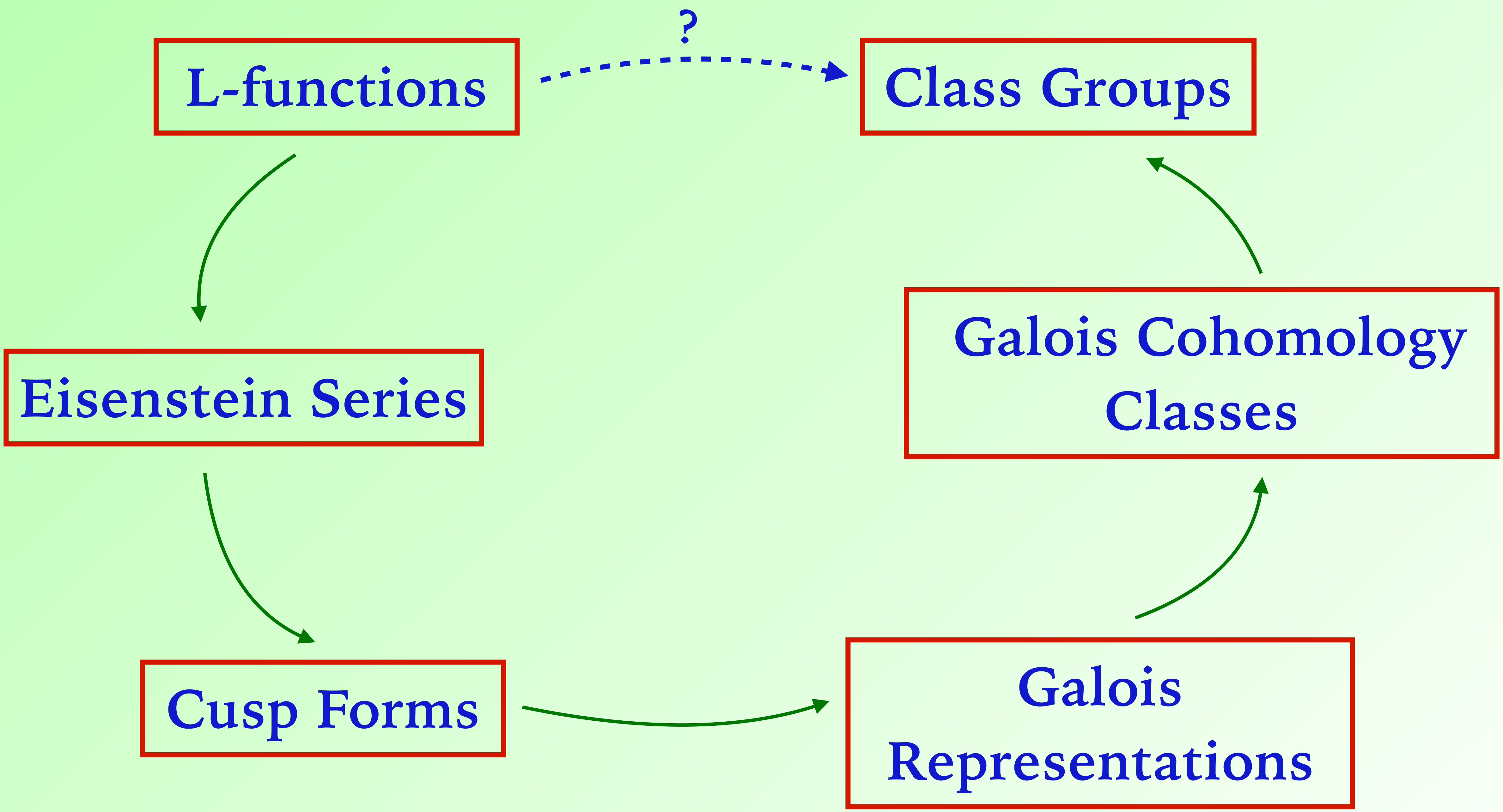
Theorem. For odd primes p, we have

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

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

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.

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

This must be modified if $n = 1$.

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 Jesse Silliman, generalizing results of Hida and Chai.

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

GALOIS REPRESENTATION

The splitting field of the associated cohomology class is then an extension of H whose Galois group is a **quotient** of $\mathrm{Cl}_{\mathfrak{q}}(H)$.

The fact that f is congruent to an Eisenstein series means that the Galois representation associated to f is **reducible**.

The fact that the congruence is modulo Θ implies that

$$\mathrm{Fitt}(\mathrm{Cl}_{\mathfrak{q}}(H)) \subset (\Theta).$$

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

Remark: This is for $n = 1$. For $n \geq 1$, a more complicated module than $\mathrm{Cl}_{\mathfrak{q}}(H)$ appears, and it is endowed with a surjective map to $\mathrm{Cl}_{\mathfrak{q}}(H)^{\vee}$.

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

Our formula for Brumer-Stark units is explicitly computable.

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

$n = 1$, $F_1 =$ 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 F_1.

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 F_1.

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

Using 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!