Explicit class field theory

Henri Darmon, McGill University

UCLA CHAT seminar

May 24, 2021

Explicit class field theory

This loosely formulated, somewhat ill-posed problem seeks to extend two prototypical results:

1. Kronecker-Weber: All abelian extensions of $\mathbb{Q}$ are generated by roots of unity, i.e., values of the function $e^{2\pi iz}$ at rational arguments.

2. Complex multiplication: All abelian extensions of imaginary quadratic fields can be generated by values of modular functions at imaginary quadratic arguments.

Hilbert's twelfth problem: to identify what class of functions might play the role of the exponential or modular functions, in generating all abelian extensions of a given number field.

The nature of this lecture

This lecture is a personal account of how my – still limited – understanding of this problem has evolved over the years;

The account I will give is chronological, rather than logical, focussing on the meandering, roundabout, often serendipitous nature of mathematical research.

Early influences: Harvard (1987-91)

It was a wonderful time and place to study elliptic curves!

These results were in the air:

- Karl Rubin's proof of finiteness of the Shafarevich-Tate group for CM elliptic curves, building on Coates-Wiles ($\sim$ 1986);

- The Gross-Zagier formula ($\sim$ 1985);

- Kolyvagin's descent, "Euler systems" ($\sim$ 1987)

- Tame refinements of the BSD conjecture (Mazur-Tate seminar in 1986), Stark and Gross-Stark conjectures;

- Kato's theorem (1991).

A formula of Rubin

$E/\mathbb{Q}$: a CM elliptic curve (by a quadratic imaginary field K).

$L(E,1) = L(\psi^{-1},0)$ for a Hecke character of infinity type $(1,0)$,
$\psi((\alpha)) = \alpha, \qquad \psi^*((\alpha)) = \bar{\alpha}.$

Let $\mathscr{L}_p{}^{\mathrm{Katz}}$ be the Katz p-adic L-function of K.

$$L(E,1) = L(\psi^{-1},0) \sim \mathscr{L}_p{}^{\mathrm{Katz}}(\psi).$$

Rubin's Formula (1991): If $L(E,1) = 0$, then there is a global point $P \in E(\mathbb{Q}) \otimes \mathbb{Q}$ for which

$$\boxed{\mathscr{L}_p{}^{\mathrm{Katz}}(\psi^*) = \Omega_p^{-1} \log_p^2(P).}$$

A similar formula of Perrin Riou

Shortly after, Bernadette Perrin Riou proposed a formula in the same spirit, for non CM curves.

The formulae of Rubin and Perrin-Riou suggest a tantalising approach to the construction of rational and algebraic points on elliptic curves, through the evaluation of leading terms of (p-adic) L-functions, just like Stark conjecturally constructs units in abelian extensions.

Problem: Extend Stark's conjecture to elliptic curves, in order to produce algebraic points on elliptic curves that could not be obtained otherwise.

From the sublime to the mundane

Let H be the Hilbert class field of an imaginary quadratic field K.

$E/\mathbb{Q}$ an elliptic curve satisfying a "Heegner hypothesis".

Theorem (Bertolini, D, 1989)

For all $\chi : \mathrm{Gal}(H/K) \longrightarrow \mathbb{C}^\times$,
$\mathrm{ord}_{s=1} L(E/K, \chi, s) = 1 \quad \Rightarrow \quad \dim_{\mathbb{C}}(E(H) \otimes \mathbb{C})^\chi = 1.$

This is a minor extension of the result of Kolyvagin.

It was nonetheless important on a personal level:

- it marked my first collaboration with Massimo Bertolini;
- it suggests an interesting open question.

An intriguing question

Let H be the Hilbert class field of a **real** quadratic field K;

$E/\mathbb{Q}$ an elliptic curve satisfying a "modified Heegner hypothesis".

$$\mathrm{ord}_{s=1} L(E/K, \chi, s) \text{ is odd}, \quad \text{for all } \chi : \mathrm{Gal}(H/K) \to \mathbb{C}^\times.$$

$$\mathrm{ord}_{s=1} L(E/H, s) \geq [H : K]$$

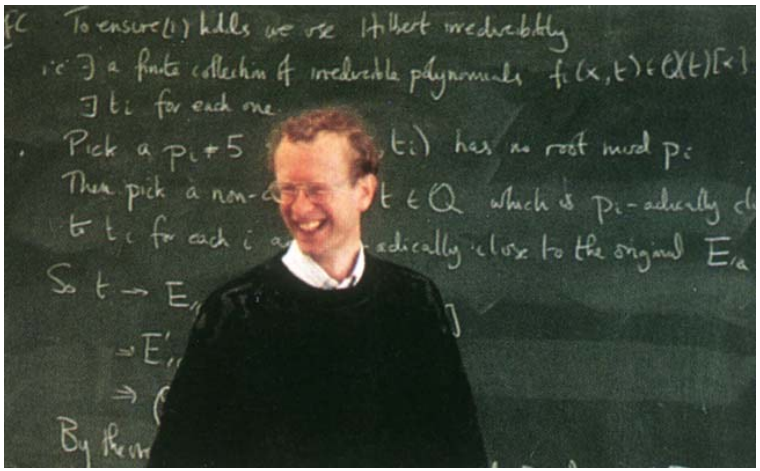
$$\mathrm{rank}(E(H)) \overset{?}{\geq} [H : K].$$

Question: How can one construct the systematic supply of points in $E(H)$ whose existence is predicted by the Birch and Swinnerton-Dyer conjecture?

Further influences: Princeton (1991-94)

My first years in Princeton were relatively tranquil.

Then, in June 1993:



I spent an exciting last year in Princeton absorbing these new ideas. Notably: the deformation theory of Galois representations and modular forms.

First years at McGill (1994-99)

The first serious steps towards an "elliptic Stark conjecture" began with a project with Massimo, whose aim was to transpose the p-adic Birch and Swinnerton-Dyer conjecture of Mazur, Tate, and Teitelbaum to the *anti-cyclotomic setting*.

A modest consequence:

Theorem (Bertolini, D, 1997)

For all $\chi : \mathrm{Gal}(H/K) \longrightarrow \mathbb{C}^\times$,
$L(E/K, \chi, 1) \neq 0 \quad \Rightarrow \quad \dim_{\mathbb{C}}(E(H) \otimes \mathbb{C})^\chi = 0.$

The proof rests crucially on congruences between modular forms.

It was vastly generalised by Matteo Longo, Ye Tian, Shouwu Zhang, and others.

A Rubin–Perrin-Riou style formula

The anti-cyclotomic p-adic L-function is in the Iwasawa algebra of $G_\infty := \mathrm{Gal}(K_\infty/K)$, $\quad K_\infty :=$ anticyclotomic $\mathbb{Z}_p$-extension of K.

$$L_p(E, K_\infty/K) \in \mathbb{Z}_p[[G_\infty]].$$

Theorem (Bertolini, D, 1998)

$L_p'(E, K_\infty/K) \sim \log(P)^2$, *where* $P \in E(\mathbb{Q})$.

The point P is obtained from *Heegner points*.

This result is both a p-adic analogue of Gross-Zagier, and an anticyclotomic analogue of Rubin-Perrin-Riou.

It seemed to extend formally to real quadratic fields!

Stark Heegner points: a first pass

Caveat: There is no "anticyclotomic $\mathbb{Z}_p$-extension" of a real quadratic K; and G_∞ is a finite group!

Auxiliary primes (à la Taylor-Wiles). Let $K_\infty^{(\ell)}$ be the maximal abelian p-extension unramified outside ℓ and p.
$\mathscr{L}_p(E, K_\infty^{(\ell)}/K) \in \mathbb{Z}_p[G_\infty^{(\ell)}]$. A "stub" of the p-adic L-function.

Conjecture (Inspired by the "tame refinements" of Mazur-Tate)

There is a global point $P \in E(K)$ for which

$$\lim_{\ell \to \infty} a_\ell(E)^{-1} \mathscr{L}_p{}'(E, K_\infty^{(\ell)}/K) = \log(P).$$

Stark-Heegner points over real quadratic fields Number theory (Tiruchirapalli, 1996) 41-69. Contemp. Math. **210**, AMS, Providence, RI, 1998.

A more convincing construction ($\sim$ 2000)

J. Milne: "Philosophically, one expects that, with the exception of $\mathbb{Q}$, one can not obtain abelian extensions of totally real fields by adjoining special values of automorphic functions."

Automorphic functions: $L^2(\Gamma\backslash G(\mathbb{R})) \subset H^0(\Gamma, \mathrm{Cont}(G(\mathbb{R}), \mathbb{R}))$.

Loose idea: the higher Γ- cohomology of suitable function spaces on $G(\mathbb{R})$, or $G(\mathbb{A}_{\mathbb{Q}})$, or $G(\mathbb{Q}_p)$, might supply the necessary extension of the notion of "automorphic function".

It seems more tractable, (but not indispensable!) to work with p-adic symmetric spaces.

The Drinfeld upper half-plane and the Ihara group

Let $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ be Drinfeld's upper half plane.

$\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p])$ acts on $\mathcal{H}_p$ by Mobius transformations.

It does not act discretely, and $H^1(\Gamma, \mathbb{Q}) = 0$.

The interesting cohomology occurs in degree 2.

Because $\Gamma = \mathrm{SL}_2(\mathbb{Z}) *_{\Gamma_0(p)} \mathrm{SL}_2(\mathbb{Z})$,

$$H^2(\Gamma, \mathbb{Q}) = H^1(\Gamma_0(p), \mathbb{Q}) \text{ as a Hecke module.}$$

Modularity: Let E be an elliptic curve over $\mathbb{Q}$ of conductor p. There is a Hecke eigenclass $\alpha_E \in H^2(\Gamma, \mathbb{Z})$ satisfying

$$T_\ell(\alpha_E) = a_\ell(E) \cdot \alpha_E, \qquad \text{for all} \qquad \ell \neq p.$$

Trivialising the two-cocyle α_E

Let $\mathcal{A}^\times$ be the multiplicative group of non-vanishing rigid analytic functions on $\mathcal{H}_p$. Let q_E be the Tate period of E.

Idea: Realise $q_E^{\alpha_E}$ as the periods of an $\mathcal{A}^\times$-valued one-cochain.

Theorem

The class $q_E^{\alpha_E}$ becomes trivial in $H^2(\Gamma, \mathcal{A}^\times)$. In other words, there is a one-cochain $J_E : \Gamma \longrightarrow \mathcal{A}^\times$ satisfying, for all $\gamma_1, \gamma_2 \in \Gamma$:

$$J_E(\gamma_1) \times J_E(\gamma_1\gamma_2)^{-1} \times \gamma_1(J_E(\gamma_2)) = q_E^{\alpha_E(\gamma_1,\gamma_2)}.$$

This theorem is a *formal consequence* of a 1986 conjecture of Mazur, Tate and Teitelbaum, proved by Greenberg-Stevens in 1990. Thus, it was proved 10 years before it was stated!

Rigid analytic cocycles

$$J_E(\gamma_1) \times J_E(\gamma_1\gamma_2)^{-1} \times \gamma_1(J_E(\gamma_2)) = q_E^{\alpha_E(\gamma_1,\gamma_2)}.$$

Definition. The class of J_E in $H^1(\Gamma, \mathcal{A}^\times/q_E^{\mathbb{Z}})$ is called the *rigid analytic cocycle* attached to E.

For $\tau \in \mathcal{H}_p$, there is an evaluation map $\mathrm{ev}_\tau : \mathcal{A}^\times \longrightarrow \mathbb{C}_p^\times$,

$$\mathrm{ev}_\tau : H^1(\Gamma, \mathcal{A}^\times/q_E^{\mathbb{Z}}) \longrightarrow H^1(\Gamma_\tau, \mathbb{C}_p^\times/q_E^{\mathbb{Z}}).$$

If $\Gamma_\tau = 1$, the target is trivial. It is non-trivial when $\Gamma_\tau \simeq \mathbb{Z}$, which occurs precisely when $\mathbb{Q}(\tau)$ is real quadratic.

$$J_E[\tau] := J_E(\gamma_\tau)(\tau), \qquad \langle\gamma_\tau\rangle = \mathrm{Stab}_\Gamma(\tau).$$

This quantity is called the *value* of J_E at the RM point τ.

Stark-Heegner points

General principle: The RM values of rigid analytic cocycles provide an appropriate — albeit, still poorly understood — substitute for the CM values of automorphic functions.

Conjecture (2000)

If τ is an RM point and $K = \mathbb{Q}(\tau)$, then $J_E[\tau]$ is a global point on E, defined over a ring class field of K.

These *Stark-Heegner points* should behave, in most key respects, *just like* Heegner points over ring class fields of imaginary quadratic fields.

Numerical example

$$E = 11A : y^2 + y = x^3 - x^2 - 10x - 20.$$

The field $\mathbb{Q}(\sqrt{101})$ has class number one.

$$J_E\left[\frac{1+\sqrt{101}}{2}\right] = (x/t^2, y/t^3) \pmod{11^{200}},$$

where

$$\begin{aligned} x &= 10816241366446925396670846851168 49 \\ y &= -19391462977749218369160989980706200472762157755 00 \\ &\quad -45034813271762519727132587561686024065704563549 3\sqrt{101} \\ t &= 1571135073196351 0 \end{aligned}$$

Second numerical example

$$E = 37A : y^2 + y = x^3 - x.$$

The field $\mathbb{Q}(\sqrt{1297})$ has class number 11.

$$J_E\left[\frac{1+\sqrt{1297}}{2}\right] = (x, y) \pmod{37^{50}},$$

where x satisfies the polynomial

$$961x^{11} - 4035x^{10} - 3868x^9 + 19376x^8 + 13229x^7 - 27966x^6 \\ -21675x^5 + 11403x^4 + 11859x^3 + 1391x^2 - 369x - 37.$$

It generates the Hilbert class field of $\mathbb{Q}(\sqrt{1297})$.

Relation with Stark's conjecture (2001-2006)

With Pierre Charollois and Samit Dasgupta, we explored the relation between Stark-Heegner points and (Gross-)Stark units.

I first met Samit in 2001, in Orlando, and Pierre in 2002 in Baltimore, at a conference on "Stark's conjecture: recent work and new directions". Both were at McGill in the period 2005-2006.

Samit's thesis (2004): The group $H^2(\Gamma, \mathbb{Z}) = H^1(\Gamma_0(p), \mathbb{Z})$ contains a class α_{DR} that is *Eisenstein*, the Dedekind Rademacher homomorphism encoding the periods of $\Delta(pz)/\Delta(z)$.

Theorem (Samit, 2003; Alice Pozzi, Jan Vonk, 2019)

There is a one-cochain $J_{\mathrm{DR}} : \Gamma \longrightarrow \mathcal{A}^\times$ *satisfying, for all* $\gamma_1, \gamma_2 \in \Gamma$: $J_{\mathrm{DR}}(\gamma_1) \times J_{\mathrm{DR}}(\gamma_1\gamma_2)^{-1} \times \gamma_1(J_{\mathrm{DR}}(\gamma_2)) = p^{\alpha_{\mathrm{DR}}(\gamma_1,\gamma_2)}$.

The RM values of the Dedekind-Rademacher cocycle

$J_{\mathrm{DR}} \in H^1(\Gamma, \mathcal{A}^\times/p^{\mathbb{Z}})$ is the *Dedekind-Rademacher cocycle*.

Conjecture (Dasgupta, D, 2003)

If τ is an RM point and $K = \mathbb{Q}(\tau)$, then $J_{\mathrm{DR}}[\tau]$ is a global p-unit in a ring class field of K.

A "Kronecker limit formula" relating $J_{\mathrm{DR}}[\tau]$ to p-adic L-series.

$L_p(K, \mathcal{C}, s) :=$ Deligne-Ribet p-adic L-function.

$J^+_{\mathrm{DR}}[\tau] := J_{\mathrm{DR}}[\tau] \times J_{\mathrm{DR}}[\tau'] = \mathrm{Norm}_{\mathbb{Q}_p(\tau)/\mathbb{Q}_p} J_{\mathrm{DR}}[\tau]$.

Theorem (Dasgupta, D, 2003)

The quantity $\log_p(J^+_{\mathrm{DR}}[\tau])$ is equal to $L'_p(K, \mathcal{C}_\tau, 0)$, and hence its algebraicity follows from the p-adic Gross-Stark conjecture.

Proof of the Gross-Stark conjecture

Theorem (Dasupta, Pollack, D, $\sim$ 2011)

The p-adic Gross-Stark conjecture is true (for totally odd characters of totally real fields).

Key ingredient in the proof: deformation theory of Hilbert modular Eisenstein series, and of the associated Galois representations.

This direction has been taken much further by Pierre and Samit, and Samit and Mahesh Kakde (extensions to $\mathrm{GL}(n)$, tame refinements of the Gross-Stark conjecture, etc.)

Their successes continue to place Stark's conjecture and (p-adic) L-functions at the center of an important approach to explicit class field theory.

What geometry underlies rigid analytic cocycles?

In the period 2006-2015, collaborations with Kartik Prasanna and Victor Rotger nudged me towards a more "geometric" approach to Stark-Heegner points.

• Analogy between Stark-Heegner points and Abel-Jacobi images of (algebraic) cycles.

• Arithmetic of triple products of modular forms, $L(f \otimes g \otimes h, s)$ led to theoretical progress on Stark-Heegner points.

• This was far from clear to me at the outset, and I owe much to Victor's insistence (in the summer of 2010, in Barcelona) that this was a worthwhile direction to pursue.
weight $(2, 2, 2) \rightsquigarrow$ weight $(2, 1, 1)$.

p-adic families of diagonal cycles

Let K be a **real** quadratic field.

Theorem (Victor Rotger, D, 2011)

For all $\chi : \mathrm{Gal}(H/K) \longrightarrow \mathbb{C}^\times$,
$L(E/K, \chi, 1) \neq 0 \quad \Rightarrow \quad \dim_{\mathbb{C}}(E(H) \otimes \mathbb{C})^\chi = 0.$

Proof. Kato method 's with "Beilinson-Kato elements" replaced by "diagonal cycle classes in p-adic families".

- K imaginary quadratic, analytic rank 1: Bertolini, D (1987).
- K imaginary quadratic, analytic rank 0: Bertolini, D (1997).
- K real quadratic, analytic rank 0: Rotger, D, (2011).
- K real quadratic, analytic rank 1: **completely open**.

Rigid meromorphic cocycles (2017-)

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p])$ and $\mathcal{M}^\times$ be the multiplicative group of *rigid meromorphic functions* on $\mathcal{H}_p$.

Definition (Jan Vonk, D)

A rigid meromorphic cocycle is a class in $H^1(\Gamma, \mathcal{M}^\times)$.

Clues that this notion might be fruitful:

• A conjecture of Bill Duke and Yingkun Li on the fourier coefficients of weak harmonic Maass forms.

• A p-adic analogue, with Alan Lauder and Victor Rotger, relating fourier coefficients of p-adic deformations of RM theta series of weight one, to the p-adic logarithms of q-units in H, with $q \neq p$. The p-adic L-functions only know about p-adic logarithms of p-units! Fourier coefficients seem to carry richer information.

Construction of rigid meromorphic cocycles

Theorem (Jan Vonk, D)

Suppose $p = 2, 3, 5, 7,$ or 13. Then for all $\tau \in \mathcal{H}_p^{\mathrm{RM}}$, there is an essentially unique $J_\tau \in H^1(\Gamma, \mathcal{M}^\times)$ for which the divisor of $J_\tau(\gamma)$ is supported on $\Gamma\tau$, for all $\gamma \in \Gamma$.

- The construction and classification is based on ideas of Marvin Knopp, Youngju Choie, Don Zagier, ... on "rational period functions".

- Jan and I were strongly inspired article of Duke, Ozlem Imamoglu and Arpad Toth on "modular cocycles and linking numbers".

Real quadratic singular moduli

Conjecture (Vonk, D, 2017)

If τ_1, τ_2 are two RM points in $\mathcal{H}_p$, then

$$J_p(\tau_1, \tau_2) := J_{\tau_1}[\tau_2] \qquad (= J_{\tau_2}[\tau_1]^{-1})$$

behaves "in all key respects" just like the difference

$$J_\infty(\tau_1, \tau_2) := j(\tau_1) - j(\tau_2)$$

where τ_1 and τ_2 are CM points of $\mathcal{H}$.

- *They belong to the expected compositum of narrow ring class fields of real quadratic fields;*
- *They admit explicit factorisations, as in the work of Gross and Zagier.*

Evidence for RM singular moduli

• There is ample experimental evidence for the conjectures on RM singular moduli.

• There is also a growing body of *theoretical evidence*, based on the study of p-adic deformations of modular forms and their associated Galois representations: (joint works with Yingkun Li, Alice Pozzi, and Jan Vonk).

• Whereas the algebraicity of Stark-Heegner points remains shrouded in mystery, the prospects for establishing the predicted algebraicity of "differences of RM singular moduli" are vastly better.

Closing remarks

The path leading up to a "theory of RM singular moduli" has been slow and tortuous, filled with misconceptions, false leads, dead ends, and long periods of just being stuck;

It has been an enjoyable and far from solitary trek! I owe a tremendous debt to

- The mentors whose ideas launched me in a fruitful direction; (Dick Gross, Andrew Wiles, John Tate, Barry Mazur, Karl Rubin, Bernadette Perrin-Riou, Ralph Greenberg, Glenn Stevens, ...)

- The collaborators who frequently lifted me out of a rut, (Massimo Bertolini, Adrian Iovita, Samit Dasgupta, Pierre Charollois, Adam Logan, Kartik Prasanna, Victor Rotger, Alan Lauder, Jan Vonk, Alice Pozzi, ...)

Thank you for your attention!