Modular algorithms for Gross–Stark units and Stark–Heegner points

Håvard Damm-Johnsen

Mathematical Institute
University of Oxford

LMFDB, Computation, and Number Theory (LuCaNT)

UNIVERSITY OF OXFORD
Mathematical Institute

Oxford Mathematics

Hilbert's 12^{th} problem

Can we generate all abelian extensions of a given number field with values of analytic functions?

$$\mathbb{Q}$$

Kronecker–Weber:

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{N \in \mathbb{N}} \mathbb{Q}(e^{2\pi i/N})$$

$$K = \mathbb{Q}(\sqrt{-D})$$

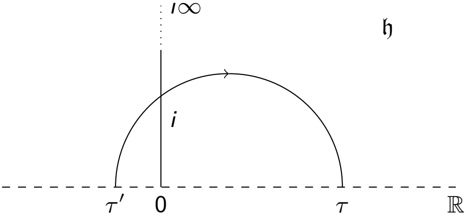
CM theory:

$$K^{\mathrm{ab}} \approx \mathbb{Q}^{\mathrm{ab}} \cdot \bigcup_{\tau \in K \cap \mathfrak{h}} K(j(\tau))$$

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

- Stark conjectures – based on L-functions
- Real quadratic fields?

RM points

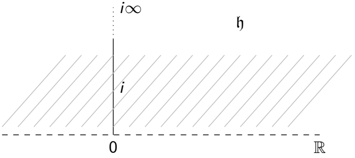


- Hermite: RM point τ with discriminant $D > 0$ gives geodesic in $\mathfrak{h}$
- $\rightsquigarrow$ Oriented intersection number $(0, i\infty) \frown (\tau', \tau)$
- $\rightsquigarrow$ Knopp cocycle:

$$\gamma \mapsto \sum_{\delta \in \mathrm{SL}_2(\mathbb{Z})} \frac{(\infty, \gamma\infty) \frown (\delta\tau', \delta\tau)}{z - \delta\tau} \in H^1(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C}(z))$$

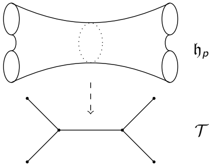
Archimedean and non-archimedean analysis

$\mathbb{R}$



$\mathbb{C}(z)$
$\mathrm{SL}_2(\mathbb{Z})$

$\mathbb{Q}_p$



$\mathcal{M}$ (*rigid meromorphic functions on* $\mathfrak{h}_p$)
$\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p])$ (*the Ihara group*)

p-adic Knopp cocycle: $$\gamma \mapsto \sum_{\delta \in \Gamma} \frac{(\infty, \gamma\infty) \frown (\delta\tau', \delta\tau)}{z - \delta\tau} \in H^1(\Gamma, \mathcal{M})$$

Rigid meromorphic cocycles

- [Darmon–Vonk '16?]: General theory of rigid meromorphic cocycles
- Evaluate at points in $\mathfrak{h}_p \rightsquigarrow$ algebraicity conjectures
- [Darmon–Pozzi–Vonk '20] *Winding cocycle:* $J_w \in H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$
- Decomposes under Hecke action on $H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$:

$$T_p J_w = a_p(E_2^{(p)}) J_{\mathrm{DR}} + \sum_{g \in S_2(\Gamma_0(p))} a_p(g) J_g$$

Why care?

- $J_{DR}[\tau]$ = *Gross–Stark unit*, generates the maximal unramified abelian extension H^+ of $\mathbb{Q}(\tau)$
- $J_g[\tau]$ = *Stark–Heegner point* on elliptic curve E_g (conjecturally) over H^+

This "solves" Hilbert's 12th problem in a similar way to CM theory!

Example

Let $\tau = 1 + 2\sqrt{3}$ and $p = 11$. There is a unique eigenform $g \in S_2(\Gamma_0(p))$, and we compute

- $J_{\mathrm{DR}}[\tau] = \frac{7+6\sqrt{-2}}{11}$ generates

$$H^+ = \mathbb{Q}(\sqrt{3}, \sqrt{-2}) = \texttt{lmfdb.4.0.576.1},$$

- $J_g[\tau] = (2\sqrt{2}, 5 + 4\sqrt{2})$ is a point defined over H^+ on

$$y^2 + y = x^3 - x^2 - 10x - 20 = \texttt{lmfdb.11.a2}$$

The diagonal restriction derivative

Theorem (Darmon–Pozzi–Vonk '23)

For any RM point τ with fundamental discriminant D and p inert in $\mathbb{Q}(\tau)$, there exists a modular form $G_\tau \in M_2(\Gamma_0(p))$ with q-expansion

$$G_\tau = \textit{constant term} + \sum_{n=1}^{\infty} \log_p(T_n J_w[\tau]) q^n.$$

Construction:

- Take linear combo. of two p-adic families of HMFs specialising to $E_\tau^{(p)}$,
- Take formal derivative in weight space, and restrict argument to diagonal,
- Prove that this gives a p-adic modular form,
- Apply Hida's *ordinary projection operator* $\rightsquigarrow$ classical modular form G_τ.

Explicit computation (D-J. '23)

- The proof can be made explicit!
- Slogan: higher Fourier coefficients of Eisenstein series are easy to compute.
- Basis for p-adic modular form space using Lauder's algorithms $\rightsquigarrow$ solve for constant term
- Compute ordinary projection as matrix on basis to get G_τ.
- Now write in terms of eigenbasis of $M_2(\Gamma_0(p))$:

$$G_\tau = \log_p J_{\mathrm{DR}}[\tau] \cdot E_2^{(p)} + \sum_{g \in S_2(\Gamma_0(p))} g \cdot \frac{L(0,g)}{\Omega^+_{E_g}} \log_p J_g[\tau]$$

- Key difficulty: recovering invariants from their p-adic logarithms: $\log_p(p) = \log_p(\zeta) = 0$.

Resulting data

Tables of Gross–Stark units and Stark–Heegner points on $X_0(p)$ for $p < 20$:

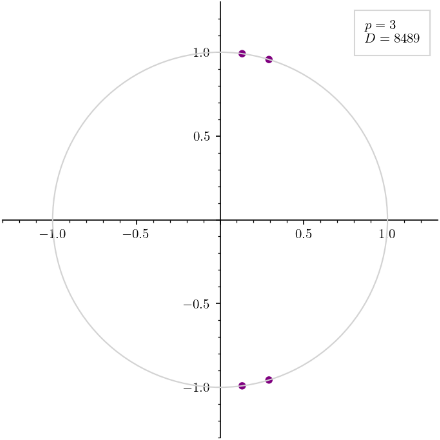
TABLE 4. Minimal polynomials of Brumer–Stark units for $p = 2$, $2000 \le D \le 2101$.

D	P_D
2005	$2^{12}x^8 + 2^4 \cdot 1055x^7 + 2^2 \cdot 9419x^6 + 57995x^5 + 66831x^4 + 57995x^3 + 2^2 \cdot 9419x^2 + 2^4 \cdot 1055x + 2^{12}$
2013	$2^{30}x^4 - 2^3 \cdot 57677665x^3 - 1118365527x^2 - 2^3 \cdot 57677665x + 2^{30}$
2021	$2^9x^6 + 2^2 \cdot 111x^5 + 2^1 \cdot 123x^4 - 101x^3 + 2^1 \cdot 123x^2 + 2^2 \cdot 111x + 2^9$
2037	$2^{18}x^4 + 2^3 \cdot 16215x^3 - 263887x^2 + 2^3 \cdot 16215x + 2^{18}$
2045	$2^6x^4 - 9x^3 - 65x^2 - 9x + 2^6$
2077	$2^3x^2 + 15x + 2^3$
2085	$2^{24}x^4 - 2^3 \cdot 6289393x^3 + 70333881x^2 - 2^3 \cdot 6289393x + 2^{24}$
2093	$2^8x^4 - 2^1 \cdot 217x^3 + 645x^2 - 2^1 \cdot 217x + 2^8$
2101	$2^{13}x^6 + 2^6 \cdot 79x^5 - 2^3 \cdot 1009x^4 - 10161x^3 - 2^3 \cdot 1009x^2 + 2^6 \cdot 79x + 2^{13}$

TABLE 2. Table of Stark–Heegner points on $E : y^2 + xy + y = x^3 - x^2 - x - 14$, for $D < 100$.

D	X	Y
12	$x^2 - 6x + 10$	$x^2 - 2x + 10$
24	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 + \frac{230}{27}x + 25$
28	$x^2 - 6x + 10$	$x^2 + 10x + 41$
44	$x^2 - 14x + 338$	$x^2 - 26x + 7394$
56	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 + \frac{230}{27}x + 25$
57	$x^2 + \frac{2306}{1225}x + \frac{6521}{1225}$	$x^2 + \frac{111042}{42875}x + \frac{15319}{8575}$
88	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 - \frac{182}{27}x + \frac{401}{9}$
92	$x^2 - 6x + 10$	$x^2 - 2x + 10$

Visualising Galois orbits of Gross–Stark units



Extending DPV to non-fundamental discriminants

Fundamental assumption in DPV: $E_\tau^{(p)}(z,z) = 0$ for p inert in $\mathbb{Q}(\sqrt{D})$. Not true when τ is non-fundamental.

Two options:

- consider $\mathrm{Tr}_1^N E_\tau^{(p)}(z,z)$,
- consider Eisenstein series $E_\tau^{(p)}(z,z)$ on congruence subgroup $\mathrm{SL}_2(\mathcal{O}_\tau)$.

I computed an explicit formula for the trace, and it does not look great.
Once we find the right formula, we can compute *ring class fields* of real quadratic fields!

Where to learn more

Paper in the LuCaNt proceedings

Modular algorithms for Gross–Stark units and Stark–Heegner points

Håvard Damm-Johnsen

Jan Vonk's PCMI notes

Rigid cocycles and singular moduli for real quadratic fields

J. B. Vonk

Abstract. These lectures give an introduction to the theory of rigid cocycles, and discuss their role in the analytic construction of singular moduli for real quadratic fields. Special emphasis will lie on the computational techniques and experiments that informed the development of this theory.

Talk to me!

More visuals