Hilbert modular forms from orthogonal modular forms on binary lattices

Haochen Wu

Dartmouth College

joint work with John Voight (University of Sydney)

July 8, LuCaNT 2025

Orthogonal modular forms

Let $Q\colon V \to F$ be a nondegenerate quadratic form over a totally real number field F with $R = \mathbb{Z}_F$ and Λ be a R-lattice in V.

$$\begin{aligned}
\mathrm{O}(V) &\coloneqq \{f \in \mathrm{GL}(V)\colon Q(f(x)) = Q(x)\ \forall x \in V\} \\
\mathrm{GSO}(V) &\coloneqq \{(f,u) \in \mathrm{SL}(V) \times F^{\times}\colon Q(f(x)) = uQ(x)\ \forall x \in V\} \\
\mathrm{GSO}(\Lambda) &\coloneqq \text{ the subgroup of } \mathrm{GSO}(V) \text{ that preserves } \Lambda \\
\mathrm{Gen}_{\mathrm{GSO}}(\Lambda) &\coloneqq \{\Lambda' \subset V\colon \Lambda_{\mathfrak{p}} \simeq_{\mathrm{GSO}} \Lambda'_{\mathfrak{p}} \text{ for all prime } \mathfrak{p} \text{ of } R\} \\
\mathrm{Cls}_{\mathrm{GSO}}(\Lambda) &\coloneqq \mathrm{Gen}_{\mathrm{GSO}}(\Lambda)/{\simeq_{\mathrm{GSO}}}
\end{aligned}$$

The space of **orthogonal modular forms** for Λ (with trivial weight) is

$$M(\Lambda) \coloneqq \mathrm{Map}(\mathrm{Cls}_{\mathrm{GSO}}(\Lambda), \mathbb{C}).$$

Theorem

Suppose that $\dim_F V = 2$. Then $\mathrm{Cls}_{\mathrm{GSO}}(\Lambda) \simeq \mathrm{Cl}(S)$ where $S = \mathrm{Clf}^0(Q_\Lambda)$ is the even Clifford algebra of Λ.

Hecke operators

For $\mathfrak{p} \nmid \operatorname{sgndisc}(\Lambda)$ with $\mathfrak{p} = \mathfrak{P}\mathfrak{P}'$, define the **Hecke operator**

$$\begin{aligned} T_{\mathfrak{P}} \colon M(\mathrm{Cl}(S)) &\to M(\mathrm{Cl}(S)) \\ f &\mapsto \Big([\mathfrak{A}] \mapsto f([\mathfrak{A}\mathfrak{P}])\Big). \end{aligned}$$

The eigenforms are multiplicative characters on $\mathrm{Cl}(S) \Rightarrow$ algebraic Grössencharacters Ψ.

Given a nonzero ideal class $[\mathfrak{B}] \in \mathrm{Cl}(S)$, define the **theta series** with respect to $[\mathfrak{B}]$ to be

$$\theta_{\mathfrak{B}}(z) := \sum_{\nu \in (\mathfrak{B}^{-1})_{>0}} e^{2\pi i \operatorname{Tr}(\mathrm{Nm}_{K/F}(\nu) z)}.$$

Hilbert modular forms

Theorem (Eichler, Walling, Voight–Wu)

Suppose that $\# \mathrm{Cl}^{+}(F) = 1$ and Λ has squarefree discriminant $\mathfrak{N}$. Then

$$M(\Lambda) \hookrightarrow M_1(\Gamma_0(\mathfrak{N}), \chi)$$

where $\chi(\gamma) = \left(\frac{\mathrm{sgndisc}(Q)}{d}\right)$ for each $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{N})$.

Example

Let $F = \mathbb{Q}(\sqrt{5})$ and $Q \colon F^2 \to F$ be defined by $Q(x, y) = x^2 + xy + 6y^2$. Let $\Lambda = \mathbb{Z}^2$. Then $\# \operatorname{Cls}_{\mathrm{O}}(\Lambda) = 2$. We find eigenvectors $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $f = \begin{pmatrix} 1 \\ -\frac{1}{2} \end{pmatrix} \in M(\Lambda)$. We have $T_2(f) = -f$.

Let $K = F(\sqrt{-23})$ and Ψ be a Hecke character on $\mathbb{Z}_K$. Now $2 = \mathfrak{P}_1\mathfrak{P}_2$ in K. We compute that $\Psi(\mathfrak{P}_1) + \Psi(\mathfrak{P}_2) = -1$.

Computing genus 2 curves over $\mathbb{Q}$ whose Jacobians have good reduction away from 2

LMFDB, Computation, and Number Theory (LuCaNT) 2025, ICERM

Robin Visser
Faculty of Mathematics and Physics
Charles University

8 July 2025

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Some examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.
- $C : y^2 = x^5 + 478x^3 + 57122x$ has bad reduction at $\{2, 13\}$.
- $C : y^2 = x^5 + 28x^4 - 868x^3 - 6160x^2 + 43076x - 149072$ has bad reduction at $\{2, 3, 11\}$.

So far, we've found 512 examples of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Genus 2 curves good outside S

Easier Problem

Fix a small set of primes S. List all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobians have good reduction away from 2.

Smart's S-unit strategy:

- Let $C/\mathbb{Q} : y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ be such a curve, where $\alpha_i \in \mathbb{Q}(J[2])$.
- Use Siegel's identity: $\dfrac{(\alpha_i-\alpha_j)(\alpha_k-\alpha_\ell)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} + \dfrac{(\alpha_i-\alpha_\ell)(\alpha_j-\alpha_k)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} = 1$
- Compute all possible 2-torsion fields $\mathbb{Q}(J[2])$.
- Solve the T-unit equations $x+y=1$ for $x, y \in O_T^\times$ over $\mathbb{Q}(J[2])$, where T is the primes in $\mathbb{Q}(J[2])$ lying above S.

Solving a linear system

Let $\psi_1, \psi_2, \ldots, \psi_t$ be a set of T-unit generators over $\mathbb{Q}(J[2])$. Let $a_{k,i,j} \in \mathbb{Z}$ be given by

$$\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \cdots \psi_t^{a_{t,i,j}}.$$

We can compute the integers $a_{k,i,j}$ as solutions to a big linear system of equations!

Examples of linear constraints on $a_{k,i,j}$:

- Galois constraints: For all $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$, $a_{f_\sigma(k), g_\sigma(i), g_\sigma(j)} = a_{k,i,j}$.
- Cluster pictures (using that J has good reduction at all odd primes).
- Solving simple T-unit equations (i.e. $\tau + \sigma(\tau) = 1$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$).

How to solve the linear system:

- Brute force.
- Closest vector problem (CVP).
- Integer linear programming (ILP).

Summary - bit.ly/genus2

Theorem (V. 2025)

There are at least 512 $\mathbb{Q}$-isomorphism classes of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2. This list includes all such curves $C/\mathbb{Q}$ which have good reduction away from S and where $\mathbb{Q}(J[2]) \subseteq M$, where (S, M) can be any of the following 18 pairs:

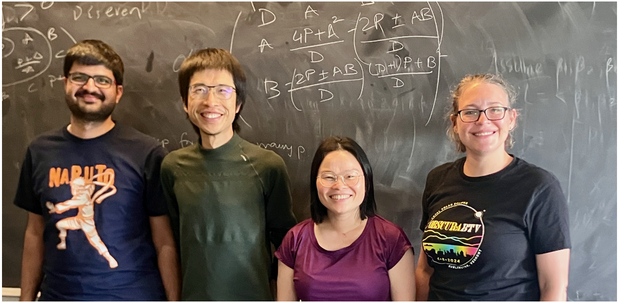
$$\big(\{2,3\},\mathbb{Q}(\zeta_{16})\big),\ \big(\{2,3\},\mathbb{Q}(\zeta_8,\sqrt[4]{2})\big),\ \big(\{2,3\},\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})\big),\ \big(\{2,5\},\mathbb{Q}(\zeta_{16})\big),$$
$$\big(\{2,5\},\mathbb{Q}(\zeta_8,\sqrt[4]{2})\big),\ \big(\{2,5\},\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})\big),\big(\{2,7\},\mathbb{Q}(\zeta_{16})\big),\ \big(\{2,7\},\mathbb{Q}(\zeta_8,\sqrt[4]{2})\big),$$
$$\big(\{2,7\},\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})\big),\ \big(\{2,3,5\},\mathbb{Q}(\zeta_{16})\big),\ \big(\{2,3,7\},\mathbb{Q}(\zeta_{16})\big),\ \big(\{2,3,7\},\mathbb{Q}(\sqrt[4]{2\sqrt{2}-3})\big),$$
$$\big(\{2,5,7\},\mathbb{Q}(\zeta_{16})\big),\ \big(\{2,5,7\},\mathbb{Q}(\zeta_8,\sqrt[4]{2})\big),\ \big(\{2,3,5,7\},\mathbb{Q}(\zeta_4)\big),\ \big(\{2,3,5,7\},\mathbb{Q}(\sqrt{-2})\big),$$
$$\big(\{2,3,5,7\},\mathbb{Q}(\sqrt{2})\big),\ \big(\{2,3,5,7,11,13\},\mathbb{Q}\big).$$

- If you can find any more curves, you'll win ~~£100~~ \$300. (T&Cs apply)

Gross lattices of supersingular elliptic curves

Ha Tran

University of Alberta, Augustana Faculty
joint work with Chenfeng He, Gaurish Korpal, and Christelle Vincent



Gross lattices

Let $B_{p,\infty}$ be the quaternion algebra over $\mathbb{Q}$ that ramifies exactly at p & ∞.

- The **Gross lattice** of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ is the rank 3 lattice

$$\mathcal{O}^T = \{2x - \mathrm{Tr}(x) : x \in \mathcal{O}\}.$$

- In case E is supersingular, $\mathrm{End}(E) \cong \mathcal{O}$ for some maximal order $\mathcal{O}$. We also say $\mathcal{O}^T$ **is the Gross lattice of** E.
- Define the **inner product** in $B_{p,\infty}$ as $(x, y) = \frac{1}{2}\mathrm{Tr}(x\bar{y})$.
- $\mathcal{O}^T$ always admits a basis that attains its successive minima, i.e., there exist $\beta_i \in \mathcal{O}^T$ such that $\|\beta_i\|^2 = \mathrm{N}(\beta_i) = D_i$, here D_i is the smallest value D_i such that the rank $\langle x \in \Lambda : \mathrm{N}(x) \leq D_i \rangle_{\mathbb{Z}} \geq i$ for $i \in \{1, 2, 3\}$

Why Gross lattices?

Theorem (Chevyrev-Galbraith (2014) and Goren-Love (2024))

Let $\mathcal{O}$ and $\mathcal{O}'$ be two maximal orders of $B_{p,\infty}$.
Suppose that $\mathcal{O}^T$ and $\mathcal{O}'^T$ have the same successive minima.
Then $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic.

Lemma (Chevyrev-Galbraith 2014)

Let $\mathcal{O} \cong \mathrm{End}(E)$ be a maximal order in $B_{p,\infty}$ and D_1 and D_2 the first two successive minima of $\mathcal{O}^T$.
If $j(E) \in \mathbb{F}_p$, then $D_1 D_2 \leq \frac{16p}{3}$.

Our main results

Theorem (HKTV 2025)

Let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$.
Then $j(E) \in F_p$ if and only if one of the following conditions holds.

1. *Its Gross lattice $\mathcal{O}^T$ has a rank 2 sublattice of determinant $4p$.*
2. *A rank 2 sublattice of $\mathcal{O}^T$ with a basis consisting of two elements that attain the first two successive minima of $\mathcal{O}^T$ is of determinant $4p$.*
3. *The third successive minimum of its Gross lattice $\mathcal{O}^T$ is bounded by $p \leq D_3 \leq \frac{8p}{7} + \frac{7}{4}$.*

Our main results (cont.)

Theorem (HKTV 2025)

Let E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$.
Then $j(E) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ if and only if one of the following conditions holds.

1. *Any rank 2 sublattice of its Gross lattice $\mathcal{O}^T$ has determinant $4np$ where $n \geq 2$ is an integer.*
2. *The third successive minimum of its Gross lattice $\mathcal{O}^T$ is $D_3 \leq \frac{3}{5}p + 5$.*

Homomorphisms from Rational Points on Elliptic Curves to Ideal Class Groups

Colin Jackson

Department of Mathematics
University of Colorado Boulder

LuCaNT 2025
Tuesday, July 8th, 2025

Past Work

In the past, people have found homomorphisms

Rational Points on EC's $\to$ Ideal Class Groups of Quadratic Fields

Buell, 1977: $$\left\{ \begin{array}{c} \text{Rational Points on} \\ y^2 = 4(x+a)(x^2+bx+c)+\mathcal{D} \end{array} \right\} \to \mathrm{Cl}(\mathbb{Q}(\sqrt{\mathcal{D}}))$$

- Noticed when finding quadratic class groups with large 3-rank
- Later found (2016) to correspond to the *ideal class pairing*.

Soleng, 1992: $$\left\{ \begin{array}{c} \text{Subgroup of the Rational Points on} \\ y^2 = x^3 + a_2x^2 + a_4x + a_6 \end{array} \right\} \to \mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$$

- Used to proved that ideals in class groups of quadratic fields can have arbitrarily large order
- Find infinitely many quadratic class groups with certain subgroups.

Quadratic Orders

Using E given by $y^2 = \overbrace{x^3 + a_2x^2 + a_4x + a_6}^{f(x)}$:

Integral Points (x_0, y_0) on E

$$\xrightarrow{x=n} (n - x_0, y - y_0) \text{ in } \frac{\mathbb{Z}[y]}{(y^2 - f(n))}$$
$$\longrightarrow (n - x_0, \sqrt{f(n)} - y_0) \text{ in } \mathbb{Z}[\sqrt{f(n)}]$$

and this corresponds to the ideal classes that Buell and Soleng found.

This is an invertible ideal in $\mathbb{Z}[\sqrt{f(n)}]$ if and only if

$$\gcd\left(n - x_0, 2y_0, n^2 + nx_0 + x_0^2 + a_2(n + x_0) + a_4\right) = 1$$

Fix $n = 0$ and extend to rational points to obtain a homomorphism

$$E(\mathbb{Q})_{\text{quadratic primitive}} \to \text{Cl}(\mathbb{Z}[\sqrt{a_6}])$$
$$\left(\frac{a}{c^2}, \frac{b}{c^3}\right) \mapsto [(a, -kb + \sqrt{a_6})], \text{ with } kc^3 = 1 \mod a.$$

Cubic Orders

Using E given by $x^3 = \overbrace{y^2 + a_3 y - a_6}^{g(y)}$:
Integral Points (x_0, y_0) on E

$$\xrightarrow{y=m} (x - x_0, m - y_0) \text{ in } \frac{\mathbb{Z}[x]}{(x^3 - g(m)))}$$

$$\longrightarrow (\sqrt[3]{g(m)} - x_0, m - y_0) \text{ in } \mathbb{Z}[\sqrt[3]{g(m)}]$$

This is an invertible ideal in $\mathbb{Z}[\sqrt[3]{g(m)}]$ if and only if

$$\gcd\left(m - y_0, 3x_0^2, m + y_0 + a_3\right) = 1$$

Fix $m = 0$ and extend to rational points to obtain

$$E(\mathbb{Q})_{\text{cubic primitive}} \to \mathrm{Cl}(\mathbb{Z}[\sqrt[3]{a_6}])$$

$$\left(\frac{a}{c^2}, \frac{b}{c^3}\right) \mapsto [(b, -ka + \sqrt[3]{a_6})], \text{ with } kc^2 = 1 \mod b.$$

Thank You!

Colin Jackson
University of Colorado Boulder
colin.jackson@colorado.edu

- Duncan A. Buell, *Class groups of quadratic fields*, Math. Comp. **30** (1976), no. 135, 610–623. MR 404205
- ______, *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. (2) **15** (1977), no. 1, 19–25. MR 434949
- Duncan A. Buell and Gregory S. Call, *Class pairings and isogenies on elliptic curves*, J. Number Theory **167** (2016), 31–73. MR 3504033
- Ragnar Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Number Theory **46** (1994), no. 2, 214–229. MR 1269253

Wild Conductor Exponents of Plane Quartics

James Rawson

University of Warwick

LuCaNT: 08/07/25

Joint work with Elvira Lupoian (University College London)

Conductors of Abelian Varieties

Definition

The *conductor* of an abelian variety, $A/\mathbb{Q}$, is $\prod_p p^{n_p}$, where $n_p = n_{p,tame} + n_{p,wild}$.
For any $\ell \neq p$, the tame part is given by $n_{p,tame} = V_\ell(A)^{I_p}$.
Let $G = \mathrm{Gal}(\mathbb{Q}_p(A[\ell])/\mathbb{Q}_p)$, then $n_{p,wild} = \sum_{i=1}^{\infty} \frac{\mathrm{codim}\, A[\ell]^{G_i}}{[G_0 : G_i]}$

Wild conductor exponents at odd primes	$\leftrightsquigarrow$	2-torsion
Wild conductor exponent at 2	$\leftrightsquigarrow$	3-torsion

Notation

The conductor of a curve is the conductor of its Jacobian.

Odd Conductor Exponents

For hyperelliptic curves, $y^2 = f(x)$, 2-torsion is generated by differences of roots of f. This gives an explicit formula for the conductor, see Dokchitser-Dokchitser-Maistret-Morgan 2018.

Theorem

The two-torsion of a plane quartic is generated by differences of bitangents

Algorithm for computing wild exponents at $p \neq 2$:

1. Determine equations for bitangents from a choice of model [Gröbner basis]
2. Find field of definition of all bitangents over $\mathbb{Q}_p$ and its Galois group
3. Compute a basis for 2-torsion from the bitangents [linear algebra]
4. Calculate Galois representation on 2-torsion
5. Evaluate conductor formula

Even Conductor Exponents

Is there an analogue for bitangents for 3-torsion? No! Even hard for hyperelliptic curves (for $g = 2$, see Dokchitser-Doris 2017, and $g = 3$, see Lupoian 2022).

Theorem (Lupoian-Rawson 2024/5)

Let C be a plane quartic with $P \in C(\mathbb{Q})$, then 3-torsion corresponds to plane cubics through P, meeting the curve with multiplicity (a multiple of) 3 at every intersection point.

Algorithm for computing wild exponents at 2:

1. Compute scheme of such cubics
2. Calculate complex approximations to the roots [homotopy continuation]
3. Recover the defining polynomials [continued fractions or LLL]
4. Find the field of definition its Galois group over $\mathbb{Q}_2$
5. Determine the Galois action and associated representation

Numerical Results

For the first 100 curves in Drew Sutherland's database of genus 3 curves, we computed the wild conductor exponents at odd primes. There were 7 curves with non-zero wild exponent, all at 3.

Discriminant	Conductor
$15957 = 3^4 \times 197$	$3^{2+2} \times 197^{1+0}$
$15957 = 3^4 \times 197$	$3^{2+2} \times 197^{1+0}$
$17307 = 3^3 \times 641$	$3^{2+1} \times 641^{1+0}$
$20331 = 3^4 \times 251$	$3^{2+2} \times 251^{1+0}$
$22707 = 3^3 \times 29^2$	$3^{2+1} \times 292 + 0?$
$25029 = 3^5 \times 103$	$3^{2+3} \times 103^{1+0}$
$27702 = 2 \times 3^6 \times 19$	$2^{1+0} \times 3^{4+2} \times 19^{1+0}$

We also computed two examples at 2. These had discriminant $7376 = 2^4 \times 461$ and $12368 = 2^4 \times 773$, and both had wild conductor 2 at 2.

Wild conductor exponents of curves

Harry Spencer

University College, London

8 July 2025

Wild conductor exponents

We can provably (and practically) compute $n_{C,p,\text{wild}}$ in the following cases:

- C an elliptic curve.
- C hyperelliptic, $p > 2$ or low genus.
- C superelliptic, p prime to exponent.
- C non-hyperelliptic of genus $3, 4$ or 5, $p > 2$.
- C plane quartic with a rational point.

Theorem (M^{2}D^2)

Let $C/\mathbb{Q} : y^2 = f(x)$ be a hyperelliptic curve, $p > 2$:

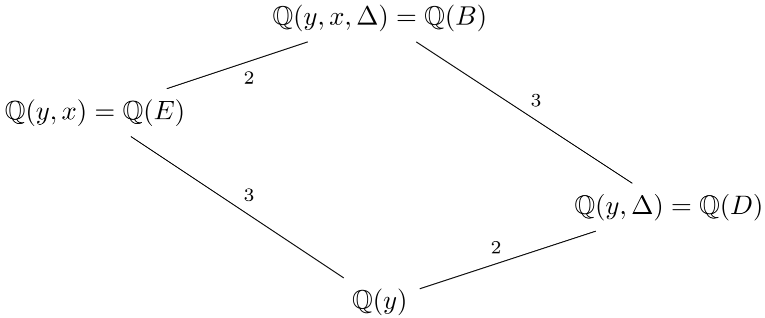
$$n_{C,p,\text{wild}} = \sum_{r \in R/G_{\mathbb{Q}_p}} v_p(\Delta(\mathbb{Q}_p(r)/\mathbb{Q}_p)) - [\mathbb{Q}_p(r) : \mathbb{Q}_p] + f_{\mathbb{Q}_p(r)/\mathbb{Q}_p},$$

where R is the set of roots of f over $\bar{\mathbb{Q}}_p$.

Idea: generalise this formula to degree d covers of $\mathbb{P}^1$, $p > d$.

Toy example

Consider an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ with $a \neq 0$. We consider the degree 3 cover to $\mathbb{P}^1$ and fill in the Galois diagram:



where $\Delta^2 = \text{disc}_x(x^3 + ax + (b - y^2))$. It turns out $E[3] \cong \text{Jac}(D)[3]$ and E and D have the same wild conductor exponents at $p \neq 3$.

Replacing $E \to \mathbb{P}^1$ by a degree 3 simply branched cover $C \to \mathbb{P}^1$, $\text{Jac}(D)[3] \cong \text{Jac}(C)[3] \oplus$ stuff as wild inertia reps for $p \neq 3$.

Main theorem

Theorem

Let $C \to \mathbb{P}^1$ be a degree d simply branched cover. For $p > d$,

$$n_{C,p,\text{wild}} = \sum_{r \in R/G_{\mathbb{Q}_p}} v_p(\Delta(\mathbb{Q}_p(r)/\mathbb{Q}_p)) - [\mathbb{Q}_p(r) : \mathbb{Q}_p] + f_{\mathbb{Q}_p(r)/\mathbb{Q}_p},$$

where R is the set of $\bar{\mathbb{Q}}_p$-branch points.

Idea of proof

Unramified cyclic covers + Galois theory + representation theory

Perturbations

For $g \in \mathbb{Q}_p[t]$, write

$$w_p(g) = \sum_{r \in R/G_{\mathbb{Q}_p}} m(r) \cdot (v_p(\Delta(\mathbb{Q}_p(r)/\mathbb{Q}_p)) - [\mathbb{Q}_p(r) : \mathbb{Q}_p] + f_{\mathbb{Q}_p(r)/\mathbb{Q}_p}),$$

where R is the set of $\bar{\mathbb{Q}}_p$-roots of g and r is a root with multiplicity $m(r)$.

Lemma

For p^{th}-power free g, the quantity $w_p(g)$ is locally constant.

Likewise, wild conductor exponents are locally constant. If we can perturb a degree d cover $\pi : C \to \mathbb{P}^1$ to obtain $\tilde{C} \to \mathbb{P}^1$ simply branched, then we can read off wild conductor exponents from the branch locus of π.

Example

Suppose $C : f(x, y) = 0$ is a smooth affine model for a curve and $\deg_x f = d$. Then, for $p > d$, we have $n_{C,p,\text{wild}} = w_p(\text{disc}_x f)$.

Learning Fricke signs from Maass Form Coefficients

Joanna Bieri, Giorgi Butbaia, Edgar Costa, **Aly Deines**, Kyu-Hwan Lee, David Lowry-Duda, Tom Oliver, Yidi Qi, and **Tamara Veenstra** [1]

LuCaNT 2025 Lightning Talk

[1] Special thanks to the Mathematics and Machine Learning Program at Harvard University's Center of Mathematical Sciences and Applications. Paper to appear in the Proceedings from this program in *Advances in Theoretical and Mathematical Physics*.

What's up with Maass forms?

- $\approx$ 35K Maass forms recently added to LMFDB. (see David Lowry-Duda's talk).
- but with Fricke'n sign problems
- For about half of the Maass forms in the dataset the Fricke sign is unknown.
- Its complicated to compute. In general, need trace formula, Hejhal's algorithm, and modularity properties.

Can we predict it with machine learning techniques instead?

Experiments on training and validation data

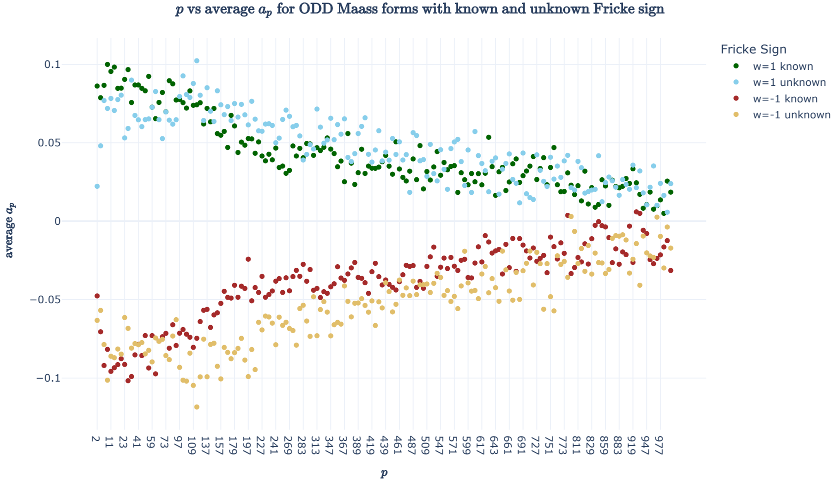
- Performed LDA on all the training data (12,795 observations) normalized by symmetry. Tested accuracy on validation data (3199 observations).
- Compared to heuristic Hejhal's algorithm for computing Fricke sign (try all possible combinations and see if consistent with other information: requires precision in Fourier coefficients.)

LDA method	all symmetry (normalized)	even symmetry	odd symmetry
LDA using all a_n	0.9612	0.9488	0.9633
LDA using only a_p	0.8625	0.8261	0.8800
LDA vs Heuristic Hejhal	0.9545	0.9461	0.9609

Notes:

- Surprisingly, a_n is better than a_p.
- Interestingly, unsupervised clustering algorithms such as K-means and PCA were not successful at distinguishing the Fricke sign.

Examined average value of $(-1)^{\sigma} a_p$ for known and unknown Fricke signs separated by known and predicted Fricke sign. First for ODD Maass forms.



Many more experiments

- How many a_n do we need?
- Is LDA using information about the Fricke sign embedded in the Fourier coefficients (when the prime divides the level)?