Lightning Talks
Thursday July 13, 2023

Presenters -

Lewis Combes (University of Sheffield

Pascal Molin (Université Paris Cité)

Eric Moss (Boston College)

Tung Nguyen (Western University

Alexey Pozdnyakov (University of Connecticut

Brandon Williams

Ajmain Yamin (CUNY Graduate Center

Mingjie Chen (University of Birmingham)

Travis Morrison (Virginia Tech)

James Boyd (Wolfram Institute)

Daniel Gordon (IDA Center for Communications Research- La Jolla)

Maria Sabitova (CUNY Queens College)

Period polynomials of Bianchi modular forms
LuCANT

Lewis Combes

University of Sheffield

Classical period polynomials

Let $\Delta \in S_{12}(\mathrm{PSL}_2(\mathbb{Z}))$.

Classical period polynomials

Let $\Delta \in S_{12}(\mathrm{PSL}_2(\mathbb{Z}))$.

$$\begin{aligned} r_\Delta(X,Y) &= \int_0^{\infty \mathrm{i}} \Delta(z)(Xz+Y)^{10} dz \\ &= \omega_+ \left(\tfrac{36}{691}X^{10} - X^8Y^2 + 3X^6Y^4 - 3X^4Y^6 + X^2Y^8 - \tfrac{36}{691}Y^{10}\right) \\ &+ \omega_- \left(4X^9Y - 25X^7Y^3 + 42X^5Y^5 - 25X^3Y^7 + 4XY^9\right), \end{aligned}$$

where $\omega_+ \approx 0.11437902$ and $\omega_- \approx 0.00926927$.

Classical period polynomials

Let $\Delta \in S_{12}(\mathrm{PSL}_2(\mathbb{Z}))$.

$$
\begin{aligned}
r_\Delta(X,Y) &= \int_0^{\infty \mathrm{i}} \Delta(z)(Xz+Y)^{10}dz \\
&= \omega_+\left(\tfrac{36}{691}X^{10} - X^8Y^2 + 3X^6Y^4 - 3X^4Y^6 + X^2Y^8 - \tfrac{36}{691}Y^{10}\right) \\
&+ \omega_-\left(4X^9Y - 25X^7Y^3 + 42X^5Y^5 - 25X^3Y^7 + 4XY^9\right),
\end{aligned}
$$

where $\omega_+ \approx 0.11437902$ and $\omega_- \approx 0.00926927$.

Recall Ramanujan's famous congruence

$$\Delta \equiv E_{12} \pmod{691}.$$

Bianchi period polynomials

Base-change Δ to $K = \mathbb{Q}(\sqrt{-11})$, and compute in Magma the space of period polynomials using cohomology.

Bianchi period polynomials

Base-change Δ to $K = \mathbb{Q}(\sqrt{-11})$, and compute in Magma the space of period polynomials using cohomology. Bianchi period polynomials come in four variables, X, Y, $\overline{X}$ and $\overline{Y}$.

Bianchi period polynomials

Base-change Δ to $K = \mathbb{Q}(\sqrt{-11})$, and compute in Magma the space of period polynomials using cohomology. Bianchi period polynomials come in four variables, X, Y, $\overline{X}$ and $\overline{Y}$.

$$r_\Delta(X, Y, \overline{X}, \overline{Y}) = \tfrac{31452624}{691} X^{10}\overline{X}^{10} + \text{(integral terms)} - \tfrac{31452624}{691} Y^{10}\overline{Y}^{10}$$

and $\Delta \equiv E_{12} \pmod{691}$ still holds.

Bianchi period polynomials

Base-change Δ to $K = \mathbb{Q}(\sqrt{-11})$, and compute in Magma the space of period polynomials using cohomology. Bianchi period polynomials come in four variables, X, Y, $\overline{X}$ and $\overline{Y}$.

$$r_{\Delta}(X, Y, \overline{X}, \overline{Y}) = \tfrac{31452624}{691} X^{10}\overline{X}^{10} + (\text{integral terms}) - \tfrac{31452624}{691} Y^{10}\overline{Y}^{10}$$

and $\Delta \equiv E_{12} \pmod{691}$ still holds. Two genuine cusp forms F_1, F_2 also in the space. This is **rare** for level 1 Bianchi forms.

$$r_{F_1}(X, Y, \overline{X}, \overline{Y}) = \tfrac{40656}{173} X^{10}\overline{X}^{10} + (\text{integral terms}) - \tfrac{40656}{173} Y^{10}\overline{Y}^{10}.$$

and $F_1, F_2 \equiv E_{12} \pmod{173}$.

Bianchi period polynomials

Base-change Δ to $K = \mathbb{Q}(\sqrt{-11})$, and compute in Magma the space of period polynomials using cohomology. Bianchi period polynomials come in four variables, X, Y, $\overline{X}$ and $\overline{Y}$.

$$r_\Delta(X, Y, \overline{X}, \overline{Y}) = \tfrac{31452624}{691} X^{10}\overline{X}^{10} + \text{(integral terms)} - \tfrac{31452624}{691} Y^{10}\overline{Y}^{10}$$

and $\Delta \equiv E_{12} \pmod{691}$ still holds. Two genuine cusp forms F_1, F_2 also in the space. This is **rare** for level 1 Bianchi forms.

$$r_{F_1}(X, Y, \overline{X}, \overline{Y}) = \tfrac{40656}{173} X^{10}\overline{X}^{10} + \text{(integral terms)} - \tfrac{40656}{173} Y^{10}\overline{Y}^{10}.$$

and $F_1, F_2 \equiv E_{12} \pmod{173}$.

$\rightsquigarrow$ congruences can be detected with period polynomials.

Congruences between cusp forms

Haberland's formula for $\mathbb{Q}$:

$$\text{Period polynomials} \rightsquigarrow \text{Petersson product}$$

Congruences between cusp forms

Haberland's formula for $\mathbb{Q}$:

$$\text{Period polynomials} \rightsquigarrow \text{Petersson product}$$

In `https://arxiv.org/abs/2306.10877`, we compute a (conjectural) analogue to find another congruence

$$\Delta \equiv F_1, F_2 \pmod{43}.$$

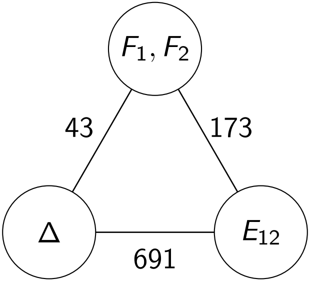
Congruences between cusp forms

Haberland's formula for $\mathbb{Q}$:

$$\text{Period polynomials} \rightsquigarrow \text{Petersson product}$$

In https://arxiv.org/abs/2306.10877, we compute a (conjectural) analogue to find another congruence

$$\Delta \equiv F_1, F_2 \pmod{43}.$$



Computing S5 modular forms with the « Abstract Groups » section

Pascal MOLIN - Université Paris-Cité

$$\rho : G_{\mathbb{Q}} \to GL_2(F) \quad \longleftrightarrow \quad g \in S_1(N, \chi, F)$$

odd, irred, cond N, det χ — Serre, Deligne, Khare, Wintenberger — eigen newform

$\rho(\mathrm{Frob}_p)$ $\xrightarrow{\text{today}}$ a_p

S5 forms?

$$\mathrm{Gal}(L/\mathbb{Q}) = S_5 \xrightarrow[\bar{\rho}]{\sim} PGL_2(\mathbb{F}_5) \qquad \text{(Galois)}$$

proj image too big, g does not come from char 0
(aka "ethereal form")

S5 forms?

$$\tilde{L} \qquad \mathrm{Gal}(\tilde{L}/\mathbb{Q}) \overset{\rho}{\hookrightarrow} GL_2(\mathbb{F}_{25})$$

$$\big| \qquad\qquad\qquad\qquad \downarrow$$

$$L \qquad \mathrm{Gal}(L/\mathbb{Q}) = S_5 \underset{\bar{\rho}}{\overset{\sim}{\longrightarrow}} PGL_2(\mathbb{F}_5) \qquad \text{(Galois)}$$

$$\big|$$

$$\mathbb{Q}$$

$$+ \text{ today } F = \mathbb{F}_{25}, \ \chi^2 = 1, \ \tilde{L}^{\ker \chi} = L^{\ker \mathrm{sign}}$$

Lifting 1: group theory

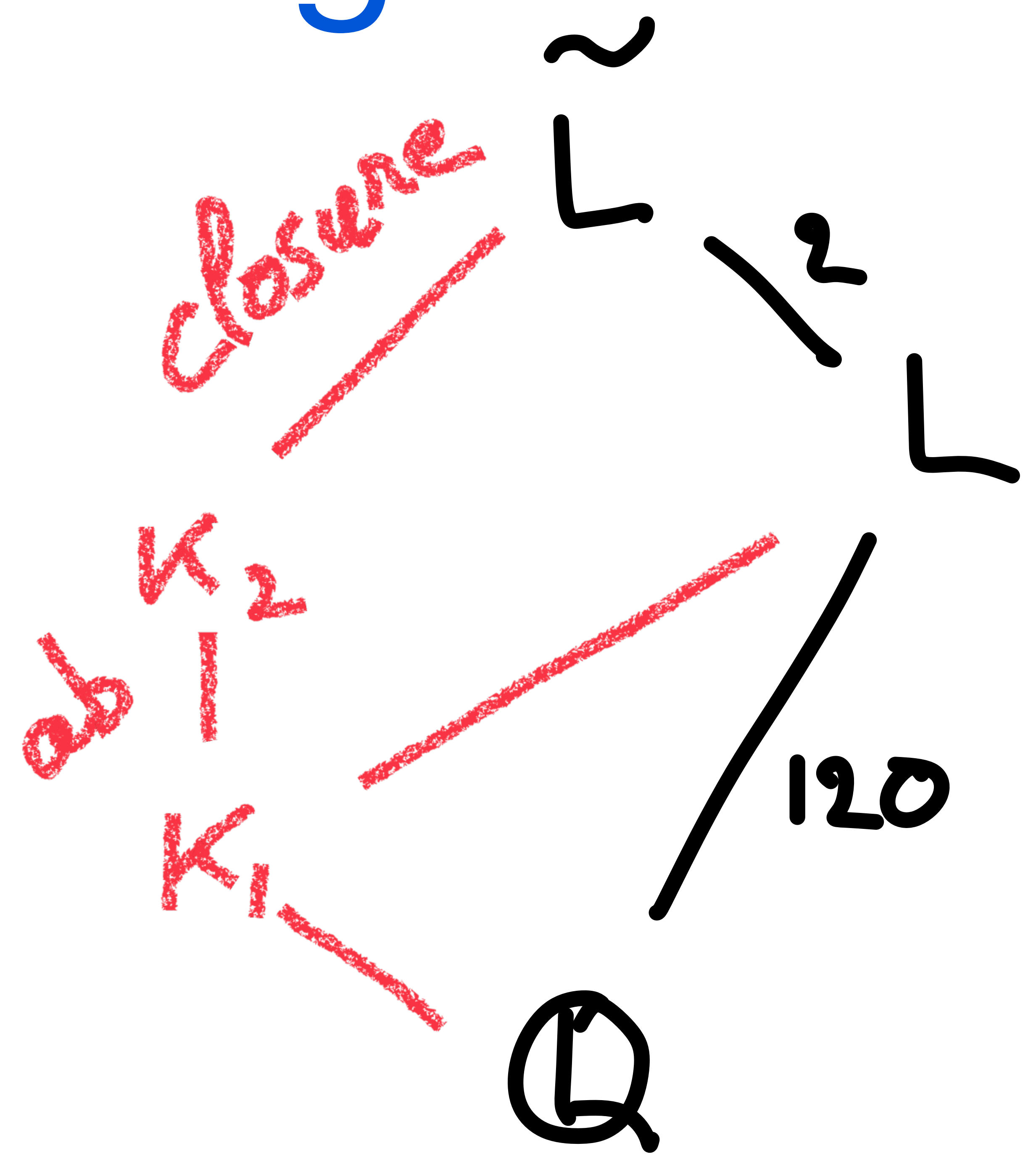
$$\begin{array}{ccccc}
\tilde{L} & & C & \hookrightarrow & \mathbb{F}_{25}^{\times} \\
| & & \downarrow & & \downarrow \\
| & & \tilde{G} & \overset{\rho}{\hookrightarrow} & GL_2(\mathbb{F}_{25}) \\
| & & \downarrow & & \downarrow \\
L & & S_5 & \overset{\bar{\rho}}{\hookrightarrow} & PGL_2(\mathbb{F}_{25})
\end{array}$$

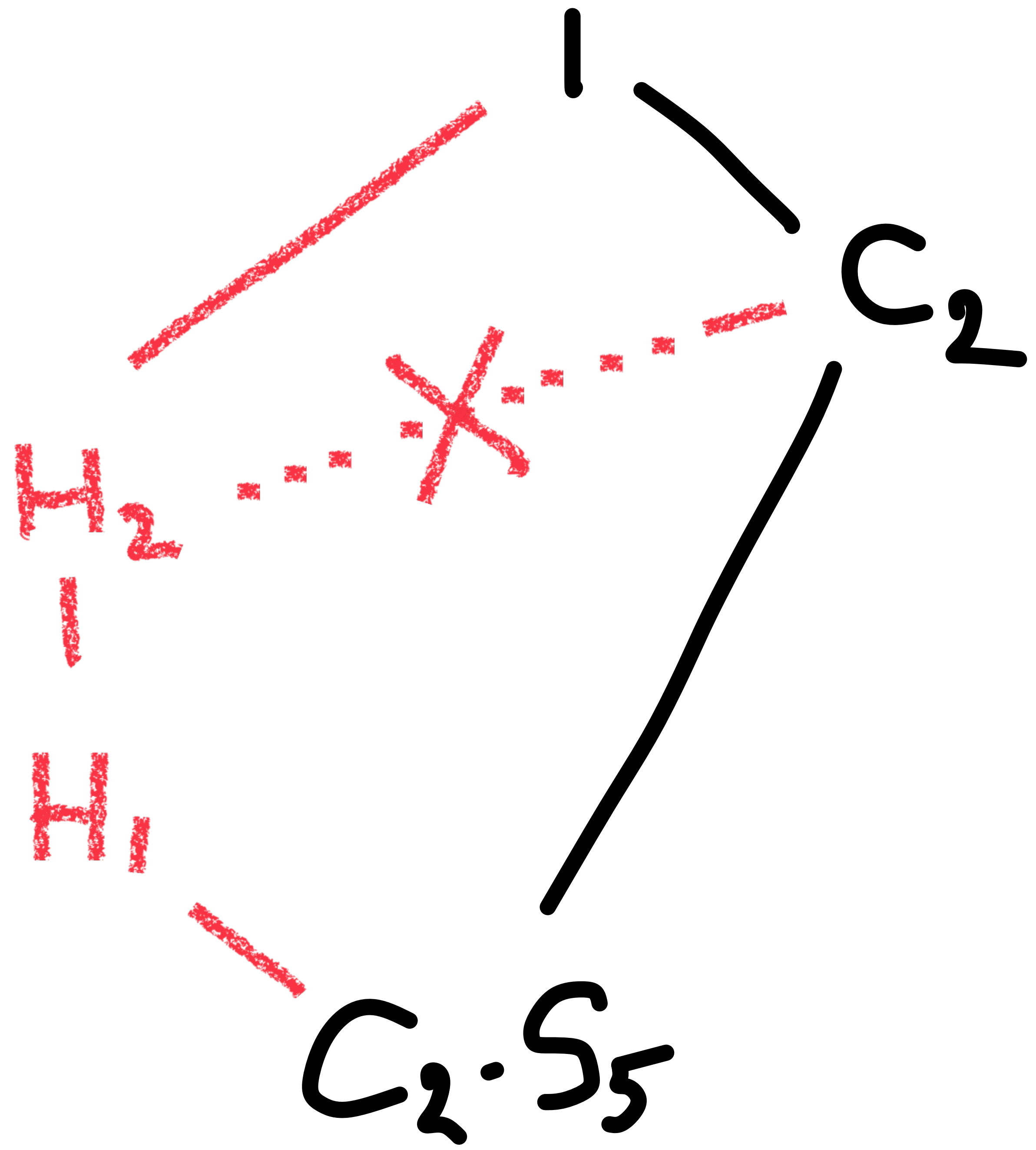
Extension of S_5
- \+ central
- \+ non split
- \+ cyclic
- \+ $\#C = 2$ if χ quadratic and $\ker \chi = \ker \mathrm{sign}$

LMFDB: $\tilde{G} = C_2 \cdot S_5 = \left\langle SL_2(\mathbb{F}_5), \begin{pmatrix} \alpha & \\ & 2\alpha \end{pmatrix} \right\rangle$

$\alpha^2 = 2\,[5]$

Lifting 2: Galois theory





$1 \subset H_2 \triangleleft H_1 \subset C_2 \cdot S_5$

H_1/H_2 abelian

LMFDB : $\underset{H_2}{C_5}$ — $\underset{H_1}{C_5 : C_4}$ — $C_2 \cdot S_5$

Algo $\underset{\text{LMFDB}}{S_5 \text{ field}} \longrightarrow L \xrightarrow[\text{Galois}]{} K_1 \xrightarrow[\text{CFT}]{} K_2 \longrightarrow \tilde{L} \rightsquigarrow g$

+ other cases

Computing Bianchi-Maass Forms

Eric Moss

Boston College

2023 LuCaNT Lightning Talks

July 13, 2023

Bianchi groups Γ_d act discretely on hyperbolic 3-space. Let $d > 0$ and let $\mathcal{O}_d = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.

$$\mathcal{H}^3 = \{x + jy \mid x \in \mathbb{C},\ y > 0\}$$

$$\Gamma_d = \mathrm{PSL}_2(\mathcal{O}_d) \circlearrowright \mathcal{H}^3$$

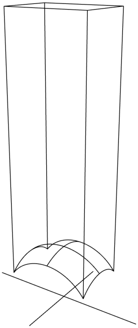
Definition

Bianchi-Maass form of weight 0 for Γ_d

- $f : \Gamma_d \backslash \mathcal{H}^3 \to \mathbb{C}$, smooth, L^2
- $\Delta f = \lambda f$

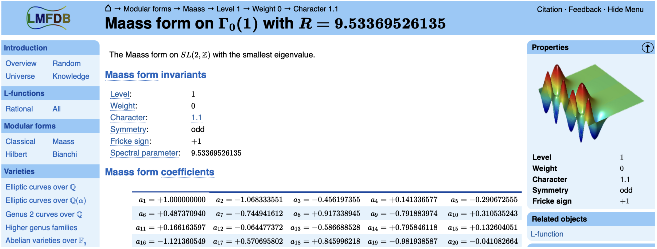
Our interest is in cusp forms. They have a Fourier expansion ($\lambda = 1 - (ir)^2$),

$$f(x+jy) = \sum_{n \in \mathcal{O}_d} a_n y K_{ir}\left(\frac{2\pi}{A}|n|y\right) \exp\left(\frac{\pi i}{A}\langle in, x\rangle\right).$$



$d = 2$

- It is expected that level 1 Maass cusp forms are "transcendental"; coefficients and eigenvalues conjectured to be transcendental numbers.
- We use **Hejhal's algorithm**. Produces a well-conditioned linear system with the coefficients a_n as the unknowns. Is heuristic, not rigorous.
- Dennis Hejhal (1992) over $\mathbb{Q}$
- Gunther Steil (1997) nonlinear methods for $d = 1, 2, 3, 7, 11$ ($h(\mathcal{O}_d) = 1$, euclidean)
- Holger Then (2004) extended Hejhal to $\mathrm{PSL}_2(\mathbb{Z}[i])$ (i.e. $d = 1$).


LMFDB

⌂ → Modular forms → Maass → Level 1 → Weight 0 → Character 1.1

Citation · Feedback · Hide Menu

Maass form on $\Gamma_0(1)$ with $R = 9.53369526135$

Introduction: Overview, Random, Universe, Knowledge
L-functions: Rational, All
Modular forms: Classical, Maass, Hilbert, Bianchi
Varieties: Elliptic curves over $\mathbb{Q}$, Elliptic curves over $\mathbb{Q}(\alpha)$, Genus 2 curves over $\mathbb{Q}$, Higher genus families, Abelian varieties over $\mathbb{F}_q$

The Maass form on $SL(2, \mathbb{Z})$ with the smallest eigenvalue.

Maass form invariants

Level:	1
Weight:	0
Character:	1.1
Symmetry:	odd
Fricke sign:	+1
Spectral parameter:	9.53369526135

Maass form coefficients

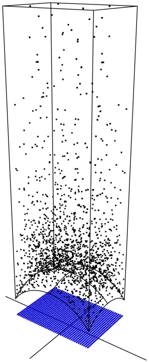
$a_1 = +1.000000000$	$a_2 = -1.068333551$	$a_3 = -0.456197355$	$a_4 = +0.141336577$	$a_5 = -0.290672555$
$a_6 = +0.487370940$	$a_7 = -0.744941612$	$a_8 = +0.917338945$	$a_9 = -0.791883974$	$a_{10} = +0.310535243$
$a_{11} = +0.166163597$	$a_{12} = -0.064477372$	$a_{13} = -0.586688528$	$a_{14} = +0.795846118$	$a_{15} = +0.132604051$
$a_{16} = -1.121360549$	$a_{17} = +0.570695802$	$a_{18} = +0.845996218$	$a_{19} = -0.981938587$	$a_{20} = -0.041082664$

Properties

Level	1
Weight	0
Character	1.1
Symmetry	odd
Fricke sign	+1

Related objects
L-function

- I have implemented an extension of Hejhal's algorithm to the remaining Euclidean fields ($d = 1, 2, 3, 7, 11$). In `C++` using `Arb`.
- Must search for eigenvalues and coefficients simultaneously.
- Extending Hejhal to $\mathcal{O}_d$ comes with an increase in computational complexity which increases as d increases.
- Coming soon: Extending to noneuclidean $\mathcal{O}_d$ with $h(\mathcal{O}_d) = 1$. Key tool: reduction algorithm for points in $\mathcal{H}^3$



≈1800 points

Fekete polynomials of principal Dirichlet characters

Shiva Chidambaram, Ján Mináč
Duy Tan Nguyen, Tung T. Nguyen (*)

Western University

LMFDB, Computation, and Number Theory
ICERM, July 2023

- Let χ be a Dirichlet character of modulus n. The L-function of χ is defined as

$$L(\chi, s) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}.$$

- $L(\chi, s)$ has the following integral representation

$$\Gamma(s)L(\chi, s) = \int_0^1 \frac{(-\log(t))^{s-1}}{t} \frac{F_\chi(t)}{1 - t^n} dt$$

where $\Gamma(s)$ is the Gamma function and

$$F_\chi(x) = \sum_{a=0}^{n-1} \chi(a) x^a.$$

- Fekete observed that if χ is a quadratic character such that $F_\chi(x)$ has no real roots on $(0, 1)$, then $L(\chi, s)$ has no real zeros near 1.

- Let χ_n be the principal Dirichlet character of modulus n

$$\chi_n(a) = \begin{cases} 0 & \text{if} \quad \gcd(a,n) > 1 \\ 1 & \text{if} \quad \gcd(a,n) = 1. \end{cases}$$

- Let

$$F_n(x) = F_{\chi_n}(x) = \sum_{\substack{0 \le a \le n-1 \\ \gcd(a,n)=1}} x^a.$$

- Our numerical data suggests that F_n has exactly one irreducible non-cyclotomic factor, which we denote by f_n. Furthermore, the Galois group of f_n is as large as possible.
- For example

$$F_{15}(x) = x\Phi_2\Phi_4\Phi_8 f_{15}(x),$$

where $f_{15}(x) = x^6 - x^4 + x^3 - x^2 + 1$.

- If $d|n$, then by the theory of Ramanujan sums

$$F_n(\zeta_d) = \frac{\mu(d)\varphi(n)}{\varphi(d)}.$$

- Let p be a prime number such that $\gcd(p, n) = 1$. Then we have the following recursive formula

$$F_{np}(x) = \frac{1 - x^{np}}{1 - x^n} F_n(x) - F_n(x^p).$$

- If $d \nmid np$ and $d|p - 1$ then Φ_d is a factor of F_{np}.
- By induction

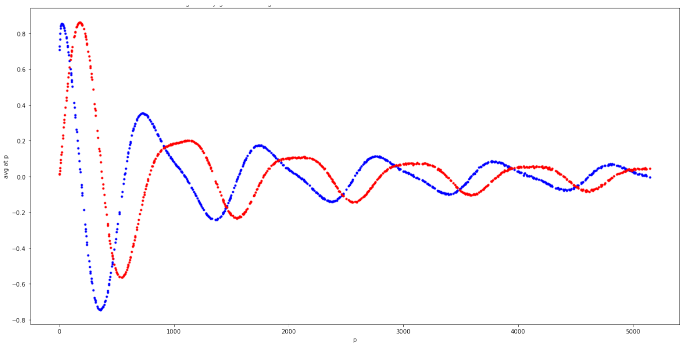
$$F_n(x) = (1 - x^n) \sum_{m|n} \mu(m) \frac{x^m}{1 - x^m}.$$

- Using this formula, we can derive various combinatorial conditions on d such that Φ_d is a factor of F_n. We can also determine precisely the multiplicity of Φ_d.

Thank you!

Murmurations in Arithmetic

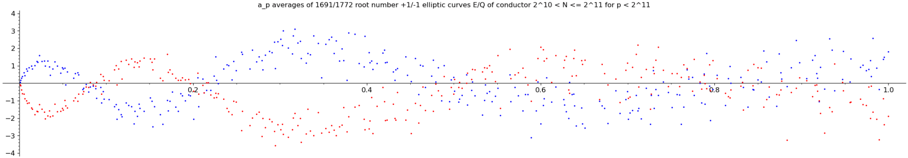
Alexey Pozdnyakov
University of Connecticut

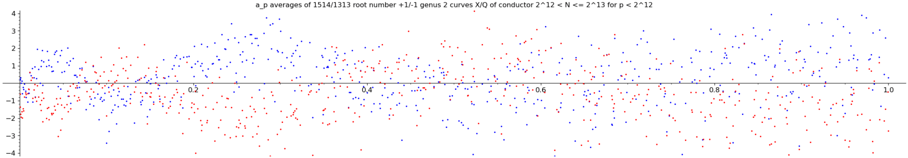


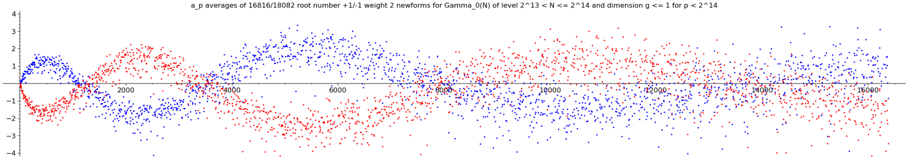
A Murmuration of Dirichlet Characters.

Paper: arXiv.2307.00256

Murmurations of L-functions







Much more at math.mit.edu/∼drew/murmurations

Theorem for Dirichlet Characters

Theorem

For $c \in \mathbb{R}_{>1}$ and $y \in \mathbb{R}_{>0}$ we have,

$$\lim_{X\to\infty} \frac{\log X}{X} \sum_{\substack{N\in[X,cX] \\ N \text{ prime}}} \sum_{\chi\in\mathcal{D}_\pm(N)} \frac{\chi(\lceil yX\rceil^{\mathfrak{p}})}{G(\chi)} = \begin{cases} \int_1^c \cos\left(\frac{2\pi y}{x}\right)dx, & \text{if } +, \\ -i\int_1^c \sin\left(\frac{2\pi y}{x}\right)dx, & \text{if } -, \end{cases}$$

where $\mathcal{D}_\pm(N) = \{\chi \bmod N : \chi \text{ primitive}, \chi(-1) = \pm 1\}$.

- Similar results for weight 2, 4, 6 modular newforms (Nina Zubrilina).
- Universal density function for any *suitable* family of L-functions.
- Connections to L-function zeros and one-level density.
- See Murmurations in Arithmetic on ICERM website for related talks.

Computation of vector-valued modular forms

Brandon Williams

RWTH Aachen University

July 13, 2023

Weil representation ρ_L of $\mathrm{Mp}_2(\mathbb{Z})$ attached to an even lattice L. Applications: Jacobi forms (lattice index); Saito–Kurokawa lift / Gritsenko lift; Borcherds products.

"Computation" of modular forms $M_*(\rho_L)$:
(1) Each space $M_k(\rho_L)$ is finite dim'l and defined over $\mathbb{Q} \Rightarrow$ compute coefficients of a $\mathbb{Q}$-basis;
(2) $M_*(\rho_L)$ is a free $\mathbb{Q}[E_4, E_6]$-module of rank $\det(L) \Rightarrow$ compute coefficients of a basis.

Elements of $M_*(\rho_L)$:
(1) Theta series (if L is positive definite)
(2) Eisenstein series (easy Fourier coefficients)

Algorithm. Certain lattice embeddings $i : L \to M$ lead to "pullback" morphisms $i^* : M_*(\rho_M) \to M_*(\rho_L)$. Here $\det(M)$ can be smaller than $\det(L)$.

(1) Find $\dim S_k$ using Riemann–Roch formula.

(2) Compute a lattice embedding $i : L \to M$ with $\mathrm{rk}(M) = \mathrm{rk}(L) + 1$ and $\det(M)$ small.

(3) Pull back Eisenstein series $E_{k-1/2}$ and related forms (Serre derivative, multiples by $\mathbb{Q}[E_4, E_6]$) along i^*.

Lemma. If $k \geq 3$ then as i runs through all (appropriate) embeddings $E_k - i^*(E_{k-1/2})$ spans S_k! So repeat (1)-(3) to get a basis.

(4) If k is small then use

$$S_k(\rho) = \{F/E_4 : \; F \in S_{k+4}(\rho) \text{ such that } \vartheta\vartheta(F/E_k) \in S_{k+4}(\rho)\}$$

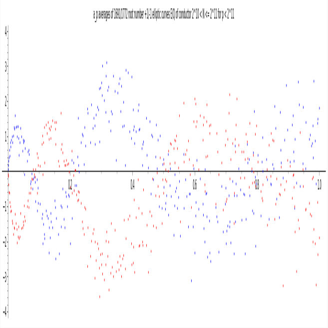
where ϑ is the Serre derivative $\vartheta(f) = \eta^{2k}(f/\eta^{2k})'$.

Implementation in Sage.

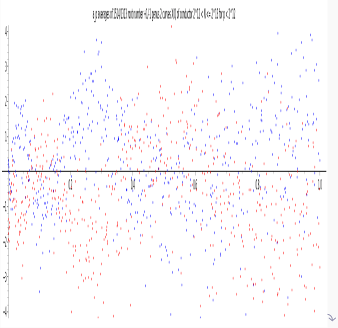
Belyi Pairs of Complete Regular Dessins

Ajmain Yamin
ayamin@gradcenter.cuny.edu

CUNY Graduate Center



LuCaNT
July 13, 2023



Problem + Previous Works

Problem Statement + Definitions

Compute Belyi pairs (affine models) of *complete regular dessins*.
Complete regular dessin a.k.a. *K_n-dessin*: bipart. dessin of a *CRM*.
Compl. reg. map (CRM): reg. map w/ underlying graph K_n.

Theorem (Biggs (1985) + James & Jones (1971))

Classification of CRMs: Cayley maps associated to $\mathbb{F}_n$.

Theorem (Jones, Streit & Wolfart (2009))

Min. field of def. of K_n-dessin: spl. field of p in $\mathbb{Q}(\zeta_{n-1})$, $n = p^f$.

Theorem (Hidalgo (2015))

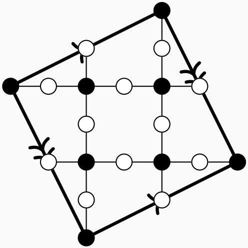
Explicit affine models of K_8-dessins defined over $\mathbb{Q}(\sqrt{-7})$.

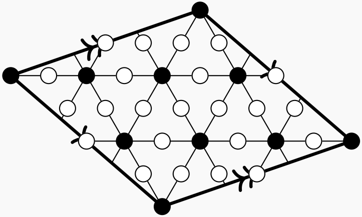
Solution + Future Work

Theorem (Y. (2023))

Explicit affine models of K_5 & K_7-dessins def. / $\mathbb{Q}(i)$ & $\mathbb{Q}(\omega)$ resp.

Method: Cyclotomic construction + manipulate $\wp$-functions.





Future work: Generalize cycl. constr. + higher genus arithmetic.

Hidden Stabilizers, the Isogeny To Endomorphism Ring Problem and the Cryptanalysis of pSIDH

joint with Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, Christophe Petit

LuCaNT 2023

Mingjie Chen

University of Birmingham

July 2023

Isogeny-based Cryptography

After the death of SIDH in July 2022 ……

SQISign
SQISignHD
Scallop
pSIDH ……

Endomorphism Ring Problem
Given a supersingular elliptic curve E, compute its endomorphism ring End(E).

Path-finding Problem
Given a supersingular elliptic curve E, find a path on the supersingular ℓ-isogeny graph from E to a fixed curve E_0

?

Can we find End(E) if we know an isogeny from E_0 of arbitrary degree D?

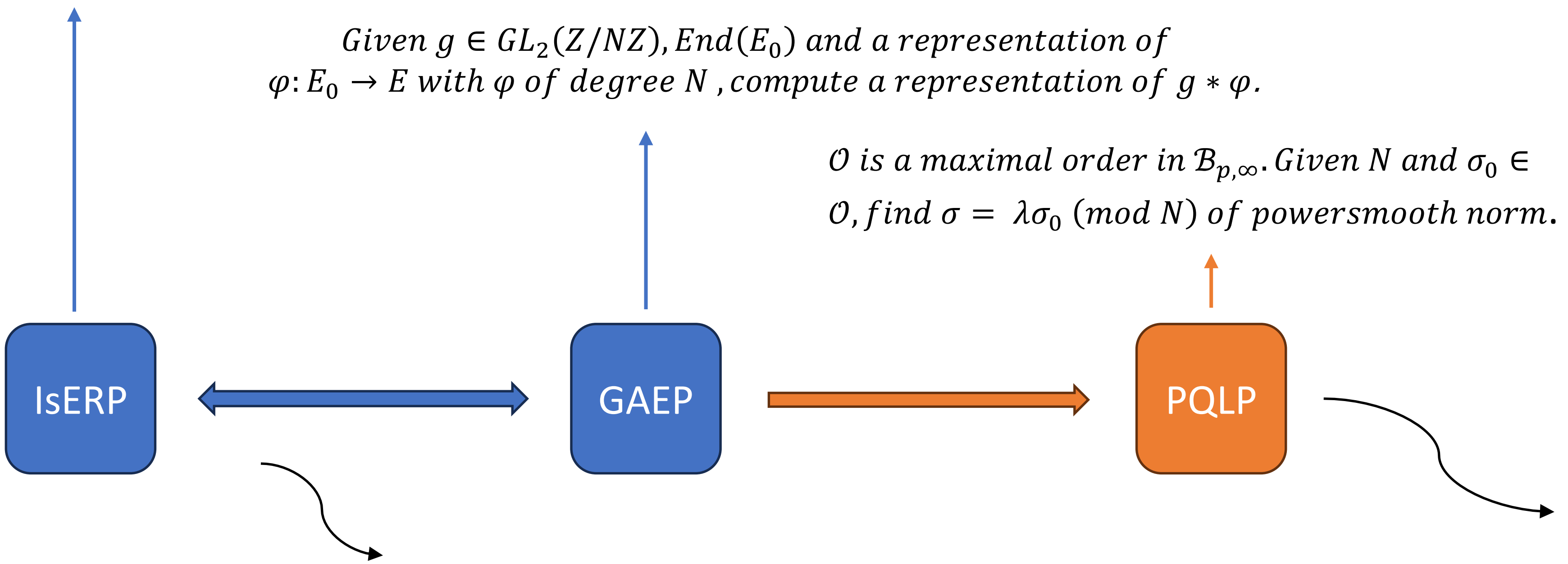
IsERP

Resolution of the IsERP

Given $End(E_0)$, *a representation of* $\varphi: E_0 \to E$, *compute* $End(E)$.

Given $g \in GL_2(Z/NZ), End(E_0)$ *and a representation of* $\varphi: E_0 \to E$ *with* φ *of degree* N, *compute a representation of* $g * \varphi$.

$\mathcal{O}$ *is a maximal order in* $\mathcal{B}_{p,\infty}$. *Given* N *and* $\sigma_0 \in \mathcal{O}$, *find* $\sigma = \lambda\sigma_0 \pmod N$ *of powersmooth norm*.



Reducing IsERP to GAEP, we have a polynomial time quantum algorithm that solves the Borel Hidden Subgroup Problem.

We design a polynomial time algorithm that resolves it.

Beyond the SEA (algorithm): Computing the trace of a supersingular endomorphism

Travis Morrison

Virginia Tech

joint work with: Lorenz Panny, Jana Sotáková, Michael Wills

Computing the trace of an endomorphism

Problem: given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha \in \mathbb{Z}$.

Why?

Computing $\mathrm{Tr}\,\pi_E$ reveals the *ring structure* of $\mathbb{Z}[\pi_E]$, i.e. a multiplication table for the basis $1, \pi_E$.
If E is supersingular: computing traces lets us determine a multiplication table for basis elements of $\mathrm{End}(E)$ (or a suborder)

How? Schoof's algorithm

For small primes ℓ, compute the characteristic polynomial of $\pi_E\big|_{E[\ell]} \in \mathrm{End}(E[\ell])$ to get $t_\ell \equiv \mathrm{Tr}\,\pi_E \pmod{\ell}$. Recover $\mathrm{Tr}\,\pi_E$ from the t_ℓ's with CRT.

Elkies' method for computing t_ℓ

If E admits a rational ℓ-isogeny ϕ, compute characteristic polynomial of $\pi_E\big|_{\ker\phi} \in \mathrm{End}(\ker\phi)$ to get t_ℓ.

The SEA algorithm for supersingular endomorphisms

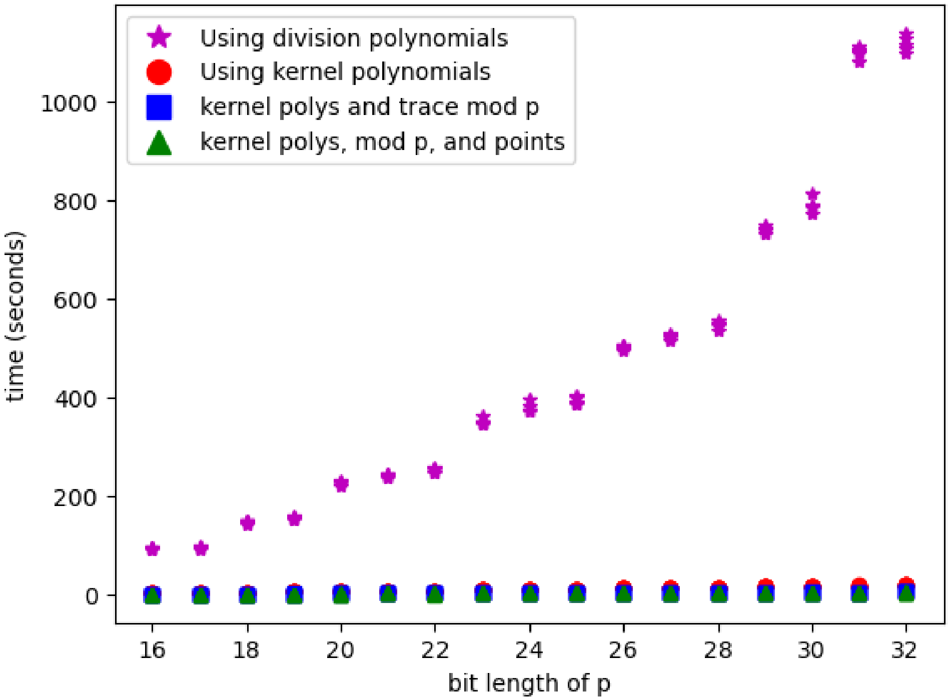
When $E/\mathbb{F}_{p^2}$ is supersingular: $E/\mathbb{F}_{p^2}$ has **all** of its ℓ-isogenies defined over $\mathbb{F}_{p^2}$ (every prime is an Elkies prime!)

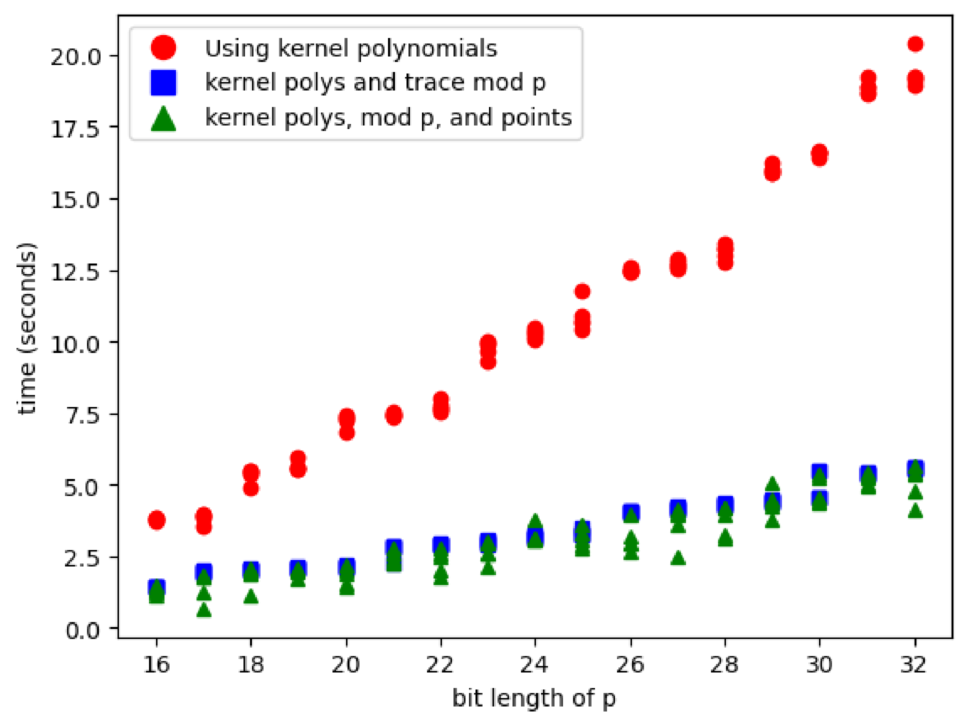
Theorem (M.-Panny-Sotáková-Wills)

There is an algorithm for computing the trace of an endomorphism α of a supersingular $E/\mathbb{F}_{p^2}$. Assuming GRH and that $\deg \alpha = d^e$ with $e = O(\log p)$ and $d = O(1)$, the algorithm terminates in expected $\tilde{O}((\log p)^4)$ bit operations.

Beyond the SEA (algorithm)

1. Compute $a \in \mathbb{F}_{p^2}$ such that $\alpha^*\omega_E = a\omega_E$, we get $\operatorname{Tr} \alpha \equiv \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} a \pmod{p}$
2. Since E is supersingular we know $\#E(\mathbb{F}_{p^2})$. If $\ell | \#E(\mathbb{F}_{p^2})$ then find P of order ℓ and solve $(\alpha + \widehat{\alpha})(P) = t_\ell P$.


Using division polynomials
Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
time (seconds)
0
200
400
600
800
1000
16
18
20
22
24
26
28
30
32
bit length of p


Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
time (seconds)
bit length of p
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
16
18
20
22
24
26
28
30
32

Online Math Databases on the Cheap

Dan Gordon

Center for Communications Research - La Jolla

gordon@ccr-lajolla.org

July 13, 2023

The La Jolla Combinatorics Repository

A quick history

- Started in 1996 as a database of covering designs, one per HTML page
- Grew, rewrote as a MySQL database
- Hundreds of contributors of covering designs from all over
- Over the years added difference sets, circulant weighing matrices, Steiner systems

Issues

- I had to learn HTML, PHP, SQL, and AWS system administration
- Location changed from `http://sdcc12.ucsd.edu/~xm3dg/cover.html` to `http://www.ccrwest.org/cover.html` to `https://dmgordon.org`.
- How to make sure the data will always be available?

Many mathematicians face this issue

October 2021 Email from Robert Craigen

- Sent to 10 researchers interested in “Hadamardish” materal
- Led to a zoom discussion of how to make data available online
- Wanted systematic, permanent, comprehensive databases
- No consensus about how to achieve that

First Try

For a paper published in DCC this year:

- `github` repo with data, basic code to use it
- jupyter notebook to run the code in
- `zenodo.org` gave it a permanent home with a DOI
- `mybinder.org` lets you run it without installing anything

Issues

- binder is slow
- can this scale up to larger (several GB) databases?
- Are there better solutions?

Links

- The La Jolla Combinatorics Repository
- Signed Difference Sets
  - https://doi.org/10.5281/zenodo.7473882
  - github repo

A number theoretic classification of toroidal solenoids

Maria Sabitova

CUNY