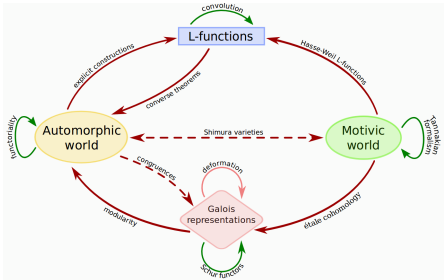
Number Theory and the LMFDB

Andrew V. Sutherland

Massachusetts Institute of Technology



The Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation

The Riemann zeta function

The Riemann zeta function is defined by a Dirichlet series with an Euler product

$$\zeta(s) := \sum_{n\geq 1} n^{-s} = \prod_p (1 + p^{-s} + p^{-2s} + \cdots) = \prod_p (1 - p^{-s})^{-1}$$

that converges for $s \in \mathbb{C}$ with real part greater than 1. Adding the "missing" Euler factor $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(\frac{s}{2})$ for the "infinite prime" yields the completed zeta function

$$\xi(s) := \Gamma_{\mathbb{R}}(s)\zeta(s) = \xi(1 - s)$$

which satisfies a functional equation and is defined for $s \neq 0, 1$.

The Riemann zeta function has "trivial zeros" coming from zeros of $\Gamma_{\mathbb{R}}(s)$, as well as infinitely many at complex values of s that are all believed to have real part $1/2$.

Counting prime numbers

As meticulously observed by Gauss, for large x the density of primes near x is $\frac{1}{\log x}$. This suggests that if $\pi(x)$ counts the number of primes $p \le x$ then we should have

$$\pi(x) \approx \frac{1}{\log 2} + \frac{1}{\log 3} + \frac{1}{\log 4} + \cdots + \frac{1}{\log x} \approx \int_2^x \frac{dt}{\log t} =: \mathrm{Li}(x)$$

The Prime Number Theorem (proved in 1896) states that $\frac{\pi(x)}{\mathrm{Li}(x)} \to 1$ as $x \to \infty$, but $\pi(x) - \mathrm{Li}(x)$ does not converge, it oscillates infinitely and without bound.

Remarkably, 40 years early Riemann suggested that one could get a better estimate via

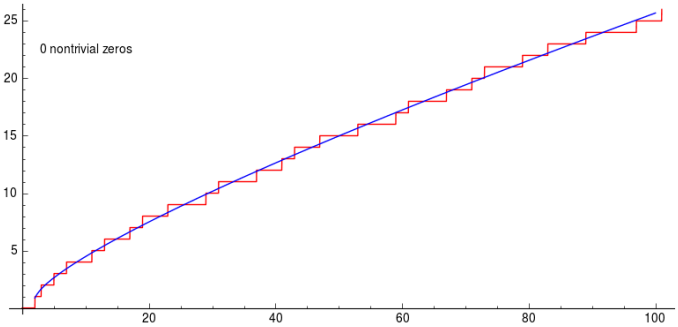
$$\mathrm{Li}(x) \approx \sum_{n \ge 1} \frac{\pi(x^{1/n})}{n} \qquad \overset{\mu\text{-inversion}}{\Longrightarrow} \qquad \pi(x) \approx \sum_{n \ge 1} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}) =: R(x),$$

where $\mu(n) = (-1)^k$ for squarefree n with k prime factors and $\mu(n) = 0$ otherwise.

Counting prime numbers

We can use Riemann's explicit formula to count primes using nontrivial zeros ρ of $\zeta(s)$:

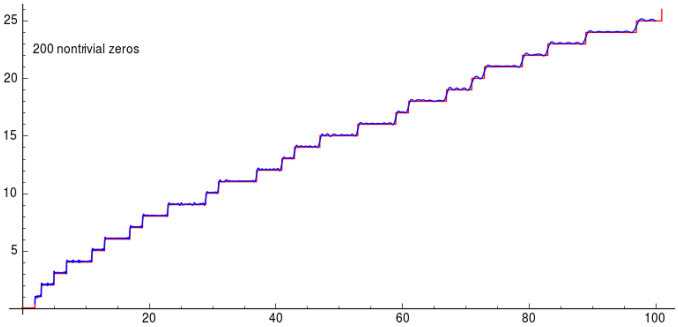
$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$



Counting prime numbers

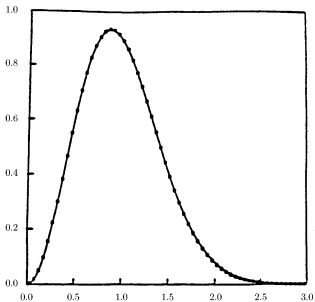
We can use Riemann's explicit formula to count primes using nontrivial zeros ρ of $\zeta(s)$:

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$



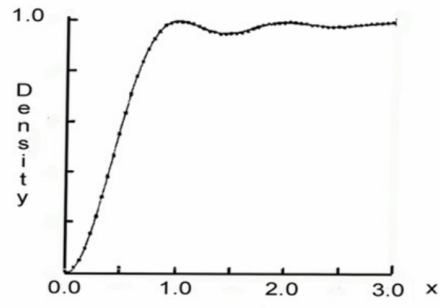
Random matrix models

The Hilbert-Pólya conjecture suggests that the zeros of $\zeta(s)$ should correspond to the eigenvalues of a self-adjoint operator. This was first explored by Montgomery and then numerically investigated by Odlyzko, who collected evidence for it by comparing the spacing of zeroes and eigenvalues of random $n \times n$ Hermitian matrices as $n \to \infty$.



Normalized spacing of 70 million consecutive zeros versus normalized eigenvalue spacing for Hermitian matrices in the Gaussian Unitary Ensemble (GUE).

zeros of $\zeta(s)$
in the LMFDB



Pair correlations for 80 million consecutive zeros near the 10^{20}th versus conjectured density for GUE.

Number fields

An algebraic integer is a complex number α that is the root of a monic irreducible polynomial $f \in \mathbb{Z}[x]$. The set of all algebraic integers forms a ring $\overline{\mathbb{Z}}$ that contains $\mathbb{Z}$.

Number fields $K := \mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(f(x))$ are defined by adjoining some $\alpha \in \mathbb{Z}[x]$ to $\mathbb{Q}$. They are $\mathbb{Q}$-vector spaces of degree $d := \deg f$ with $\mathbb{Q}$-basis $1, \alpha, \ldots \alpha^{d-1}$.

The ring of integers $\mathcal{O}_K := K \cap \overline{\mathbb{Z}}$ is a lattice isomorphic to $\mathbb{Z}^d$, but $1, \alpha, \ldots, \alpha^{d-1}$ is not necessarily a $\mathbb{Z}$-basis for $\mathcal{O}_K$ (when this holds we say that K is monogenic).

The fundamental theorem of arithmetic typically fails in rings of integers $\mathcal{O}_K$ because prime factorizations need not be unique, e.g. $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

If we instead work with ideals (finitely generated sub-modules of $\mathcal{O}_K$), the fundamental theorem of arithmetic is restored: $(6) = (2, 1 + \sqrt{-5})^2 \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$. It then makes sense to talk about (and to count) "primes" in number fields.

The Cohen-Lenstra heuristics

Every number field has an ideal class group $\mathrm{cl}(\mathcal{O}_K)$, the finite abelian group of equivalence classes of nonzero $\mathcal{O}_K$-ideals where $\mathfrak{a} \sim \mathfrak{b}$ if $\alpha\mathfrak{a} = \mathfrak{b}$ for some $\alpha \in K$. For example, $(2, 1+\sqrt{-5}) \sim (3, 1+\sqrt{-5})$, since we can take $\alpha = \frac{1+\sqrt{-5}}{2}$.

The ideal class group is trivial if and only if unique factorization holds in $\mathcal{O}_K$.

The Cohen-Lenstra heuristics for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ predict that the odd part of $\mathrm{cl}(D) := \mathrm{cl}(O_K)$ has the distribution of a random finite abelian group of odd order. More precisely, for every odd prime ℓ and finite group H of ℓ-power order:

$$\lim_{x\to\infty} \frac{\#\{\mathbb{Q}(\sqrt{D}) : \mathrm{cl}(D)[\ell^\infty] \simeq H \text{ and } 0 < -D \le x\}}{\#\{\mathbb{Q}(\sqrt{D}) : 0 < -D \le x\}} = \frac{1}{\#\operatorname{Aut}(G)} \prod_{n\ge 1}(1-\ell^{-n}).$$

Example: we should expect $\#\,\mathrm{cl}(D)$ to be divisible by 3 with probability $0.439873\ldots$, and expect to see $\mathrm{cl}(D) \simeq \mathbb{Z}/9\mathbb{Z}$ eight times as often as $\mathrm{cl}(D) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Counting roots modulo p

Fix a monic irreducible $f \in \mathbb{Z}[x]$ of degree d and for each prime p let us define

$$N_f(p) := \#\{a \in [0, p-1] : f(a) \equiv 0 \bmod p\} \in [0, d].$$

We would like to understand how $N_f(p)$ varies with p. For $f(x) = x^3 - x + 1$ we have

p:	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
$N_f(p)$	0	0	1	1	1	0	1	1	2	0	0	1	0	1	0	1	3

Let $c_i(B)$ count the primes $p \leq B$ with $N_f(p) = i$. We have the following statistics:

B	$c_0(B)$	$c_1(B)$	$c_2(B)$	$c_3(B)$
10^3	0.323353	0.520958	0.005988	0.155689
10^4	0.331433	0.510586	0.000814	0.157980
10^5	0.333646	0.502867	0.000104	0.163487
10^6	0.333185	0.500783	0.000013	0.166032
10^9	0.333328	0.500016	0.000000	0.166656
10^{12}	0.333333	0.500000	0.000000	0.166666

The Chebotarev density theorem

These statistics are explained by the Chebotarev density theorem. The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the roots of $f(x)$ by permuting them. The Galois group G of f, and of the number field $\mathbb{Q}[x]/(f(x))$, is the corresponding permutation group, a subgroup of S_d.

One can define, for primes $p \nmid \mathrm{disc}(f)$ a Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which acts on the roots of $f(x)$ via an element of G. The number of roots of $f(x)$ mod p is the number of fixed points of this permutation.

The Chebotarev density theorem states that the Frob_p are equidistributed over G.

In our example with $f = x^3 - x + 1$ the group $G = S_3$ has $2/6$ elements that fix 0 roots, $3/6 = 1/2$ elements that fix 1 root, and $1/6$ elements that fix 3 roots.

If we had instead chosen $f = x^3 - x^2 - 2x + 1$ we would have $G = C_3$, which has $2/3$ elements that fix 0 roots and $1/3$ elements that fix 3 roots.

The Dedekind zeta function of a number field

Each number field K has a zeta function defined by a Dirichlet series and Euler product

$$\zeta_K(s) := \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

where $N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}]$. For $K = \mathbb{Q}$ we have $N(n\mathbb{Z}) = [\mathbb{Z} : n\mathbb{Z}] = n$ and $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.

$\zeta_K(s)$ has a pole at $s = 1$ whose residue is given by the analytic class number formula:

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |D_K|^{1/2}},$$

where r_1 and $2r_2$ count real and complex embeddings of K, $h_K := \#\,\mathrm{cl}(\mathcal{O}_K)$ is the class number, R_K is the regulator, $w_K := \#\mu_K$ counts roots of unity, and $D_K := \operatorname{disc} \mathcal{O}_K$.

Number fields in the LMFDB

Elliptic curves

Let E be an elliptic curve, which can be defined by an equation

$$E\colon y^2 = x^3 + Ax + B,$$

where A and B are integers; it is a curve of genus 1.

Elliptic curves over finite fields (where arithmetic is performed modulo p) are a key component of our communications security infrastructure — you use them every day.

The number of solutions to E modulo p can be written as

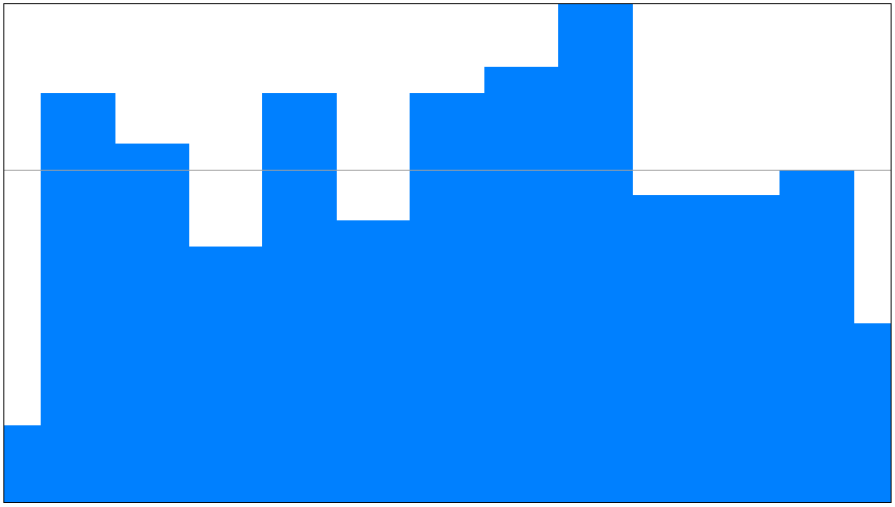
$$p + 1 - a_p,$$

Hasse

where a_p is an integer bounded by $|a_p| \leq 2\sqrt{p}$.

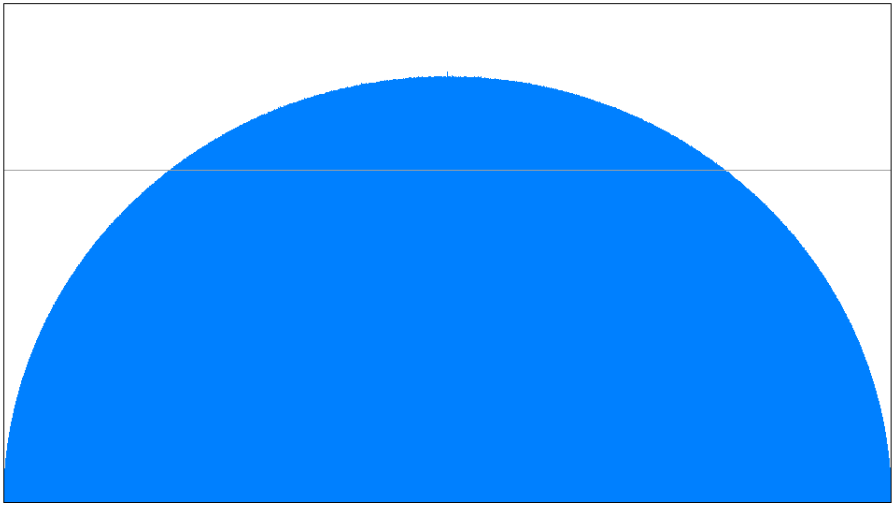
Let us now consider the sequence $x_p := -a_p/\sqrt{p} \in [-2, 2]$ indexed by primes p.

a1 histogram of y^2 = x^3 + x + 1 for p <= 2^10
170 data points in 13 buckets, z1 = 0.029, out of range data has area 0.018



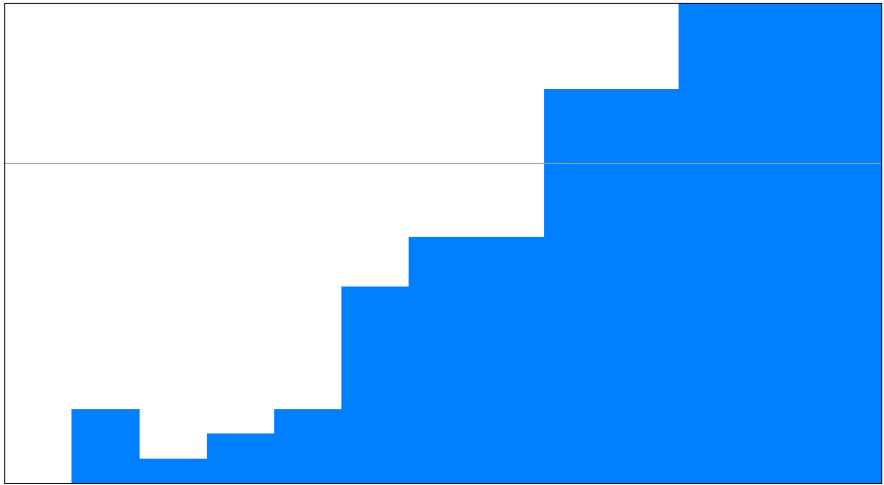
Moments: 1 0.051 1.039 0.081 2.060 0.294 4.971 1.134 13.278 4.308 37.954

a1 histogram of y^2 = x^3 + x + 1 for p <= 2^40
41203088794 data points in 202985 buckets



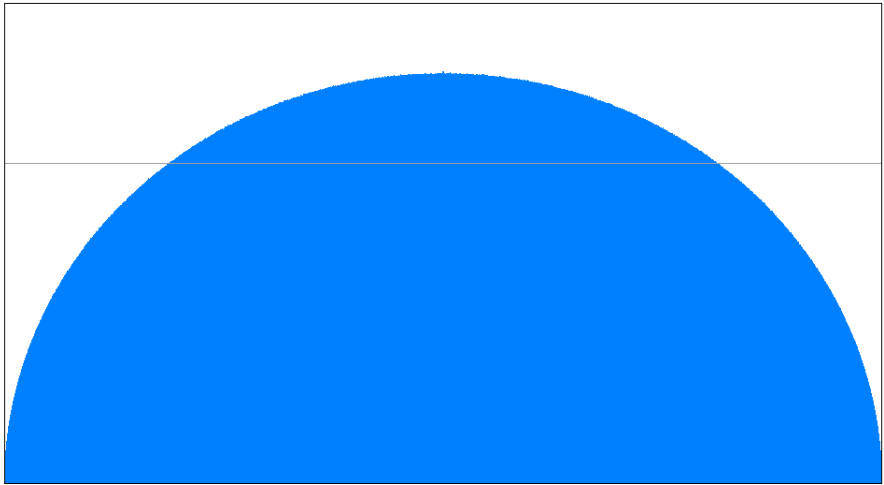
Moments: 1 0.000 1.000 0.000 2.000 0.000 5.000 0.000 14.000 0.000 41.999

a1 histogram of y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x
+ 34481611795030556467032985690390720374855944359319180361266008296291939448732243429 for p <= 2^10
172 data points in 13 buckets, z1 = 0.023, out of range data has area 0.250



Moments: 1 1.034 1.716 2.532 4.446 7.203 13.024 22.220 40.854 72.100 133.961

a1 histogram of y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x
+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9 for p <= 2^40
41203088796 data points in 202985 buckets



Moments: 1 0.000 1.000 0.000 2.000 0.000 5.000 0.001 14.000 0.003 42.000

The Sato-Tate conjecture

The Sato-Tate conjecture states that, except for certain families of well understood exceptions we will always see the same semicircular limiting distribution.

Mikio Sato

John Tate

Theorem (Taylor et al. 2008)

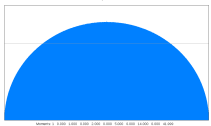
For every unexceptional elliptic curve $E/\mathbb{Q}$,
the sequence x_p converges to the semicircular distribution.

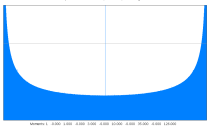
Richard Taylor

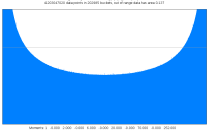
Richard Taylor received the 2014 Breakthrough Prize in Mathematics for this work.

Sato-Tate groups and their distributions

There are two Sato-Tate distributions that arise for elliptic curves $E/\mathbb{Q}$, depending on whether E is exceptional or not, but over general number fields there are three:





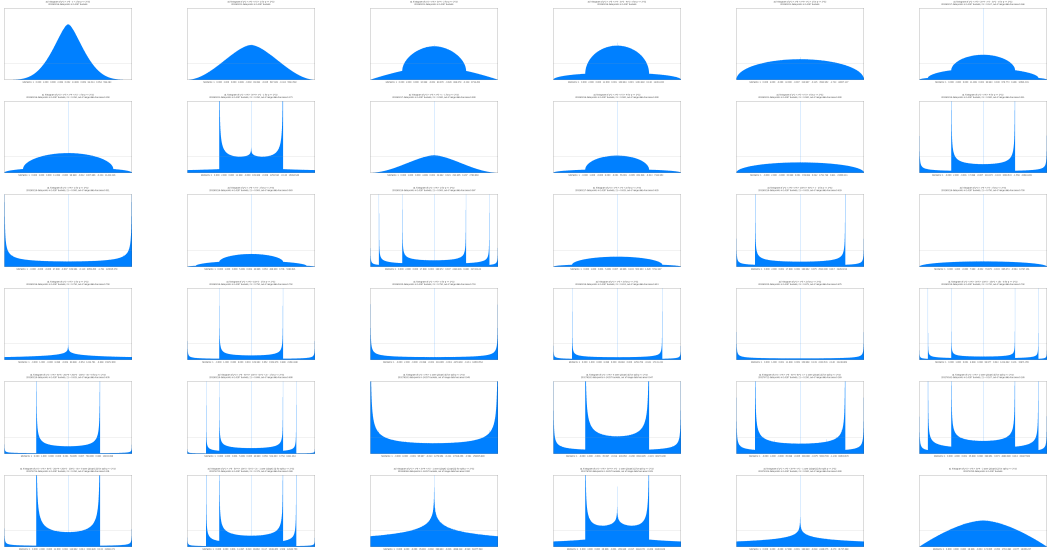


Each corresponds to the distributions of traces in a compact subgroup of SU(2), the Sato–Tate group of E. Katz–Sarnak and Serre extended this random matrix model to curves of genus g and abelian varieties of dimension g using subgroups of USp($2g$).

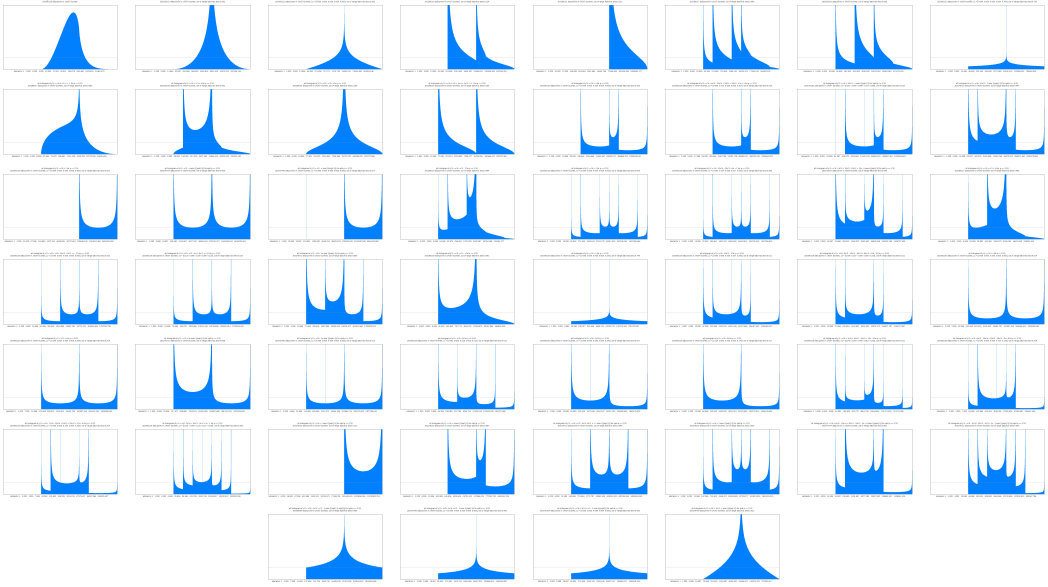
The Sato-Tate conjecture is open for genus $g > 1$, but Sato-Tate groups have been completely classified for for $g \leq 3$. There are 52 in genus 2 and 410 in genus 3 [Fité-Kedlaya-Rotger-S 2012, Fité-Kedlaya-S 2019].

These classifications involved more than a thousand CPU-years of computation.

Sato-Tate trace distributions of genus 2 curves:



Sato-Tate a_{p^2}-distributions of genus 2 curves:



Sato-Tate group $J_2(E_4)$ of weight 1 and degree 6

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 $\mathbb{F}_q$

Fields
Number fields
p-adic fields

Representations
Dirichlet characters
Artin representations

Groups
Galois groups
Sato-Tate groups

Database

Invariants

Weight: 1
Degree: 6
$\mathbb{R}$-dimension: 4
Components: 8
Contained in: USp(6)
Rational: yes

Identity component

Name: $\mathrm{U}(1) \times \mathrm{SU}(2)_2$
$\mathbb{R}$-dimension: 4
Description: $\left\{ \begin{bmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & \overline{B} \end{bmatrix} : A \in \mathrm{U}(1) \subseteq \mathrm{SU}(2), B \in \mathrm{SU}(2) \right\}$ Symplectic form: $\begin{bmatrix} J_2 & 0 & 0 \\ 0 & 0 & J_2 \\ 0 & -J_2 & 0 \end{bmatrix}$, $J_2 := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
Hodge circle: $\mathrm{diag}(u, \bar{u}, u, u, \bar{u}, u)$

Component group

Name: $C_2 \times C_4$
Order: 8
Abelian: yes
Generators: $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_8^3 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_8^1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_8^7 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_8^7 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Subgroups and supergroups

Maximal subgroups: $J(E_4, E_2)$, $J_1(E_4)$, $J_2(E_2)$
Minimal supergroups: $J_2(J(E_4))$

Moment sequences

x	$\mathrm{E}[x^0]$	$\mathrm{E}[x^1]$	$\mathrm{E}[x^2]$	$\mathrm{E}[x^3]$	$\mathrm{E}[x^4]$	$\mathrm{E}[x^5]$	$\mathrm{E}[x^6]$	$\mathrm{E}[x^7]$	$\mathrm{E}[x^8]$	$\mathrm{E}[x^9]$	$\mathrm{E}[x^{10}]$	$\mathrm{E}[x^{11}]$	$\mathrm{E}[x^{12}]$
a_1	1	0	3	0	27	0	380	0	6923	0	148260	0	3539250
a_2	1	2	9	51	371	3198	31103	328772	3684451	43072206	519669707	6424161175	80957964029
a_3	1	0	12	0	858	0	132960	0	28778050	0	7315716384	0	2039189137128

Properties

Label 1.6.J.8.2a

Name	$J_2(E_4)$
Weight	1
Degree	6
Real dimension	4
Components	8
Contained in	USp(6)
Identity component	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$
Component group	$C_2 \times C_4$

Downloads

Underlying data

Learn more

Source and acknowledgments
Completeness of the data
Reliability of the data
Sato-Tate group labels

Elliptic curves and their L-functions

The L-function of an elliptic curve $E/\mathbb{Q}$ is defined by the Euler product

$$L(E,s) = \prod_p L_p(p^{-s})^{-1} = \prod_p \left(1 - a_p p^{-s} + \chi(p) p^{1-2s}\right)^{-1}$$

where $\chi(p)$ is 0 at bad primes and 1 otherwise and $a_p \in \{0, \pm 1\}$ when $\chi(p) = 0$.

As shown by Mordell, the set of rational points $E(\mathbb{Q})$ on an elliptic curve is a finitely generated abelian group, hence isomorphic to $\mathbb{Z}^r \times T$ with $T \simeq E(\mathbb{Q})_{\mathrm{tor}}$ finite.

The Birch and Swinnerton-Dyer (BSD) conjecture states that

$$\frac{1}{r!} L^{(r)}(E,1) = \frac{\#Ш(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p C_p}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}.$$

In particular, r is the order of vanishing of $L(E,s)$ at $s = 1$ (the analytic rank).

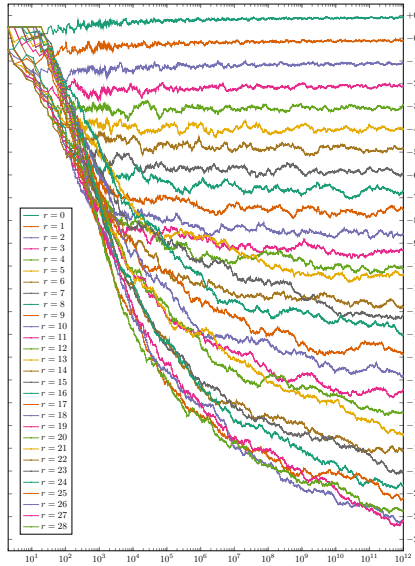
Detecting the rank

The BSD conjecture implies

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{\substack{p\le x \\ p\nmid \Delta_E}} \frac{a_p \log p}{p} = -r + \frac{1}{2}.$$

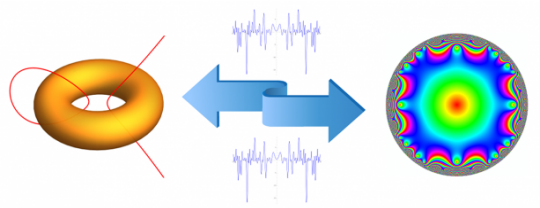
This agrees well with the data when the conductor N_E is small, but for large r the conductor cannot be small and it becomes infeasible to make $x \gg \sqrt{N_E}$, which one expects to need to get convergence.

Elliptic curves in the LMFDB



Elliptic curves and their L-functions

Taylor's proof of the Sato-Tate conjecture extends the Modularity Theorem that connects elliptic curves and modular forms through their L-functions.



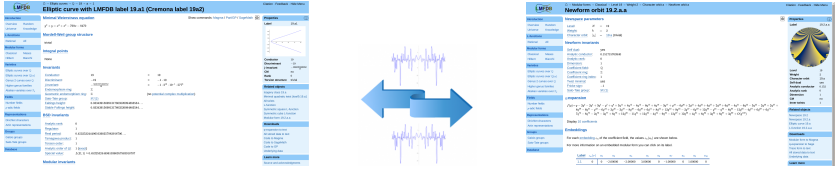
Theorem (Eichler, Taniyama, Shimura, Weil, Langlands-Tunnel, Serre, Ribet, Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor)

For each $N \geq 1$, the set of L-functions $L(E,s) := \prod(1 - a_p p^{-s} + p^{1-2s})^{-1}$ of elliptic curves $E/\mathbb{Q}$ of conductor N is equal to the set of L-functions $L(f,s) = \sum a_n n^{-s}$ of newforms $f \in S_2^{\text{new}}(\Gamma_0(N))$ of level N with rational q-expansions: $\sum a_n q^n$.

The *L*-functions and Modular Forms Database (LMFDB)

The relationship between elliptic curves and modular forms established by the Modularity Theorem is just a small part of the Langlands Program, a vast web of conjectures that connects arithmetic and automorphic objects via their *L*-functions.

The *L*-functions and Modular Forms Database is devoted to making these connections explicit. It provides compelling evidence for many aspects of the Langlands Program, including generalizations of BSD and RH, as well as datasets that can be used to formulate and test new conjectures, and to prove theorems.



Modular forms in the LMFDB

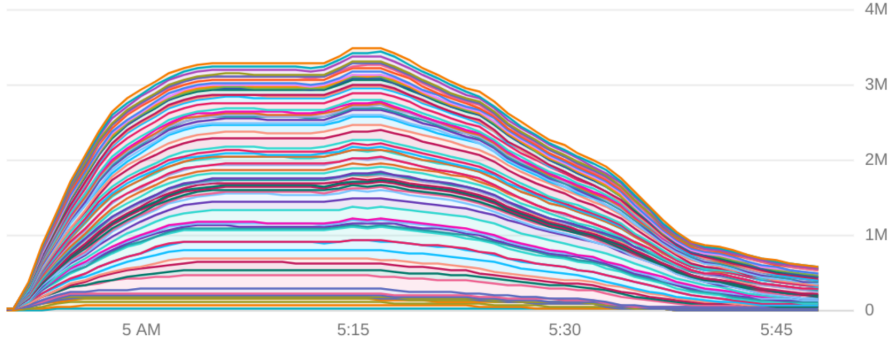
Automorphic forms associated to genus 2 curves

Type	Conductor	Curve Equation	Motive	Modular form
$\mathbf{A}[C_1]_{(s)}$	$277 = 277^1$	$y^2+(x^3+x^2+x+1)y = -x^2-x$	typical abelian surface	paramodular form
$\mathbf{B}[C_1]_s$	$529 = 23^2$	$y^2+(x^3+x+1)y = -x^5$	surface with RM by $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$	CMF 23.2.1.a
$\mathbf{B}[C_1]_{ns}$	$294 = 2^1 3^1 7^2$	$y^2+(x^3+1) = x^4+x^2$	product of ECs 14a4 and 21a4 over $\mathbb{Q}$	CMFs 14.2.1.a and 21.2.1.a
$\mathbf{B}[C_2]_s$	$10368 = 2^7 3^4$	$y^2+x^2y = 3x^5-4x^4+6x^3-3x^2+1$	surface with RM by $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$	HMF 162.1-a over $\mathbb{Q}(\sqrt{2})$
$\mathbf{B}[C_2]_{ngs}$	$1088 = 2^6 17^1$	$y^2+(x^3+x^2+x+1)y = x^4+x^3+2x^2+x+1$	Weil restriction of 17.1-a1 over $\mathbb{Q}(\sqrt{2})$	HMF 17.1-a over $\mathbb{Q}(\sqrt{2})$
$\mathbf{C}[C_2]_{(ns)}$	$448 = 2^6 7^1$	$y^2+(x^3+x)y = x^4-7$	product of PCM EC 32a3 and EC 14a6 over $\mathbb{Q}$	CMFs 32.2.1.a and 14.2.1.a
$\mathbf{D}[C_4]_{(s)}$	$3125 = 5^5$	$y^2+y = x^5$	surface with CM by $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}(\zeta_5)$	CM HMF 125.1-a over $\mathbb{Q}(\sqrt{5})$
$\mathbf{D}[D_2]_{(ns)}$	$8192 = 2^{13}$	$y^2 = x^6-9x^4+16x^2-8$	product of PCM ECs 32a3 and 256d1 over $\mathbb{Q}$	CMFs 32.2.1.a and 256.2.1.d
$\mathbf{E}[C_1]_{(ns)}$	$196 = 2^2 7^2$	$y^2+(x^2+x)y = x^6+3x^5+6x^4+7x^3+6x^2+3x+1$	square of EC 14a1 over $\mathbb{Q}$	CMF 14.2.1.a
$\mathbf{E}[C_2, \mathbb{C}]_{(ngs)}$	$576 = 2^6 3^2$	$y^2+(x^3+x^2+x+1)y = -x^3-x$	square of EC 9.1-a3 over $\mathbb{Q}(\sqrt{2})$	CMF 24.2.13.a
$\mathbf{E}[C_3]_{(ngs)}$	$324 = 2^2 3^4$	$y^2+(x^3+x+1)y = x^5+2x^4+2x^3+x^2$	square of EC 8.1-a1 over 3.3.81.1	CMF 18.2.13.a
$\mathbf{E}[C_4]_{(ngs)}$	$256 = 2^8$	$y^2+y = 2x^5-3x^4+x^3+x^2-x$	square of EC 1.1-a5 over 4.4.2048.1	CMF 16.2.5.a
$\mathbf{E}[C_6]_{(ngs)}$	$169 = 13^2$	$y^2+(x^3+x+1)y = x^5+x^4$	square of EC 1.1-a3 over 6.6.371293.1	CMF 13.2.4.a
$\mathbf{E}[C_2, \mathbb{R}\times\mathbb{R}]_s$	$455625 = 3^6 5^4$	$y^2+(x^3+x^2+x+1)y = x^5-3x^4-2x-1$	surface with QM ($D=6$) over 2.0.3.1	BMF over 2.0.3.1 of level 50625
$\mathbf{E}[C_2, \mathbb{R}\times\mathbb{R}]_{ngs}$	$3969 = 3^4 7^2$	$y^2+(x^2+x+1)y = -3x^5+5x^4-4x^3+x$	Weil restriction of 441.2-a over 2.0.3.1	BMF 2.0.3.1-441.2-a
$\mathbf{E}[C_2, \mathbb{R}\times\mathbb{R}]_{ns}$	$675 = 3^3 5^2$	$y^2 = -x^6-14x^5-44x^4+28x^3-44x^2-14x-1$	product of ECs 15a2 and 45a2 over $\mathbb{Q}$	CMFs 15.2.1.a and 45.2.1.a
$\mathbf{E}[D_2]_s$	$20736 = 2^8 3^4$	$y^2 = -27x^6-54x^5-27x^4+18x^3+18x^2-2$	surface with QM ($D=6$) over 4.0.576.2	HMF 324.1-b over $\mathbb{Q}(\sqrt{2})$
$\mathbf{E}[D_3]_s$	$34992 = 2^4 3^7$	$y^2 = -2x^6-6x^5+10x^3+9x^2-18x+6$	surface with QM ($D=6$) over 6.0.2834352.2	BMF over 2.0.3.1 of level 3888
$\mathbf{E}[D_4]_s$	$20736 = 2^8 3^4$	$y^2+y = 6x^5+9x^4-x^3-3x^2$	surface with QM ($D=6$) over 8.0.339738624.10	BMF over 2.0.3.1 of level 2304
$\mathbf{E}[D_6]_s$	$8100 = 2^2 3^4 5^2$	$y^2+x^3y = x^6+3x^5-42x^4+43x^3+21x^2-60x-28$	surface with QM ($D=6$) over degree 12 field	BMF over 2.0.3.1 of level 900
$\mathbf{E}[D_2]_{ngs}$	$6400 = 2^8 5^2$	$y^2 = 2x^5+5x^4+8x^3+7x^2+6x+2$	square of EC 256.1-a1 over $\mathbb{Q}(\sqrt{5})$	HMF 2.2.5.1-256.1-a
$\mathbf{E}[D_3]_{ngs}$	$2187 = 3^7$	$y^2+(x^3+1)y = -1$	square of EC over 6.0.177147.2	BMF over 2..0.3.1 of level 243
$\mathbf{E}[D_4]_{ngs}$	$3600 = 2^4 3^2 5^2$	$y^2+x^2y = x^5-3x^4+11x^2-16x$	square of EC over 4.0.13500.2	BMF over $\mathbb{Q}(i)$ of level 225
$\mathbf{E}[D_6]_{ngs}$	$3600 = 2^4 3^2 5^2$	$y^2+x^3y = 14x^3-20$	square of EC over 6.0.7200000.1	BMF over 2.0.3.1 of level 400
$\mathbf{F}[D_2, C_2, \mathfrak{C}]_{ngs}$	$576 = 2^6 3^2$	$y^2+x^3y = 5x^3-2$	square of PCM EC 1.1-a2 over $\mathbb{Q}(\sqrt{6})$	CM HMF 1.1-a over $\mathbb{Q}(\sqrt{6})$
$\mathbf{F}[C_2, C_1, \mathrm{M}_2(\mathbb{R})]_{ns}$	$729 = 3^6$	$y^2+y = -48x^6+15x^3-1$	square of PCM EC 27.a4 over $\mathbb{Q}$	CM CMF 27.2.1.a

One page of the "giant table" [Booker-Sijsling-S-Voight-Yasaki 2022?]

Exploring the Langlands landscape in genus 2

On January 9, 2022 we launched the last in a series of three computations exploring the Langlands correspondence in genus 2. We enumerated more than 10^{19} genus 2 curves looking for those with small conductor with the goal of expanding the LMFDB and matching their L-functions to those of known automorphic forms of small level.



We used a total of 4,034,560 Intel/AMD cores in 73 data centers across the globe.

Exploring the Langlands landscape in genus 2

We found millions of genus 2 curves of small conductor, including the curve

$$C_{903} : y^2 + (x^2 + 1)y = x^5 + 3x^4 - 13x^3 - 25x^2 + 61x - 28$$

of conductor 903 and whose L-function coefficients match those of the paramodular form of level 903 computed by Poor–Yuen. This was the last explicitly known paramodular form that had not been matched to a genus 2 curve or abelian surface.

We also found curves of conductor 657, 760, 775, 924 not previously known to occur, and many new genus 2 L-functions of small conductor:

conductor bound	1000	10000	100000	1000000
curves in LMFDB	159	3069	20265	66158
curves found	807	25438	447507	5151208
L-functions in LMFDB	109	2807	19775	65534
L-functions found	200	9409	212890	2426708

The L-function of a curve

Let X be a nice (smooth, projective, geometrically integral) curve of genus g over $\mathbb{Q}$. The L-function of X is defined by

$$L(X,s) = L(\mathrm{Jac}(X),s) := \sum_{n\geq 1} a_n n^{-s} := \prod_p L_p(p^{-s})^{-1}.$$

For primes p of good reduction for X we have the zeta function of $X_p := X \bmod p$:

$$Z(X_p;s) := \exp\left(\sum_{r\geq 1} \#X(\mathbb{F}_{p^r})\frac{T^r}{r}\right) = \frac{L_p(T)}{(1-T)(1-pT)}.$$

The L-polynomial $L_p \in \mathbb{Z}[T]$ in the numerator satisfies

$$L_p(T) = T^{2g}\chi_p(1/T) = 1 - a_p T + \cdots + p^g T^{2g}$$

where $\chi_p(T)$ is the charpoly of the Frobenius endomorphism of $\mathrm{Jac}(X_p)$.

The Selberg class with polynomial Euler factors

The Selberg class S^{poly} consists of Dirichlet series $L(s) = \sum_{n \geq 1} a_n n^{-s}$ for which

1. $L(s)$ has an analytic continuation that is holomorphic at $s \neq 1$;
2. For some $\gamma(s) = Q^s \prod_{i=1}^r \Gamma(\lambda_i s + \mu_i)$ and ε, the completed L-function $\Lambda(s) := \gamma(s) L(s)$ satisfies the functional equation
$$\Lambda(s) = \varepsilon \overline{\Lambda(1 - \bar{s})},$$
where $Q > 0$, $\lambda_i > 0$, $\mathrm{Re}(\mu_i) \geq 0$, $|\varepsilon| = 1$. Define $\deg L := 2 \sum_i^r \lambda_i$.
3. $a_1 = 1$ and $a_n = O(n^{\varepsilon})$ for all $\varepsilon > 0$ (Ramanujan conjecture).
4. $L(s) = \prod_p L_p(p^{-s})^{-1}$ for some $L_p \in \mathbb{Z}[T]$ with $\deg L_p \leq \deg L$ (has an Euler product).

The Dirichlet series $L_{\mathrm{an}}(s, X) := L(X, s + \frac{1}{2})$ satisfies (3) and (4), and conjecturally lies in S^{poly}; for $g = 1$ this is known (via modularity).

The approximate functional equation

Let $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^s\Gamma(s)$ and define $\Lambda(X,s) := \Gamma_{\mathbb{C}}(s)^g L(X,s)$. Then

$$\Lambda(X,s) = \varepsilon N^{1-s}\Lambda(X,2-s).$$

for some root number $\varepsilon = \pm 1$ and analytic conductor $N \in \mathbb{Z}_{\geq 1}$ determined by the a_p. Let $G(x)$ be the inverse Mellin transform of $\Gamma_{\mathbb{C}}(s)^g = \int_0^\infty G(x)x^{s-1}dx$, and define

$$S(x) := \frac{1}{x}\sum_{n\geq 1} a_n G(n/x),$$

so that $\Lambda(X,s) = \int_0^\infty S(x)x^{-s}dx$, and for all $x > 0$ we have $S(x) = \varepsilon S(N/x)$. The function $G(x)$ decays rapidly, and for sufficiently large c_0 we have

$$S(x) \approx S_0(x) := \frac{1}{x}\sum_{n\leq c_0 x} a_n G(n/x),$$

with an explicit bound on the tail $|S(x) - S_0(x)|$.

L-functions from nothing

As proposed by Booker and Farmer-Koutsoliotas-Lemurell, we can use the approximate functional equation to test for the existence of (and even enumerate) L-functions in S^{poly} with a given conductor N and root number ε.

Proof that there are no degree 2 rational L-functions of motivic weight 1 in S^{poly} for $N = 13$ and $\varepsilon = 1$:

```
[ 1 ], considering a_2 in { -2, -1, 0, 1, 2 }
[ 1 ], possible a_2: { -2, -1 }
    [ 1, -2 ], considering a_3 in { -3, -2, -1, 0, 1, 2, 3 }
    [ 1, -2 ], possible a_3: {}
    [ 1, -1 ], considering a_3 in { -3, -2, -1, 0, 1, 2, 3 }
    [ 1, -1 ], possible a_3: { -2 }
        [ 1, -1, -2, -1 ], considering a_5 in { -4, -3, -2, -1, 0, 1, 2, 3, 4 }
        [ 1, -1, -2, -1 ], possible a_5: {}

There are no degree 2 weight 1 rational L-functions in the Selberg class for N=13 and eps=1.
```