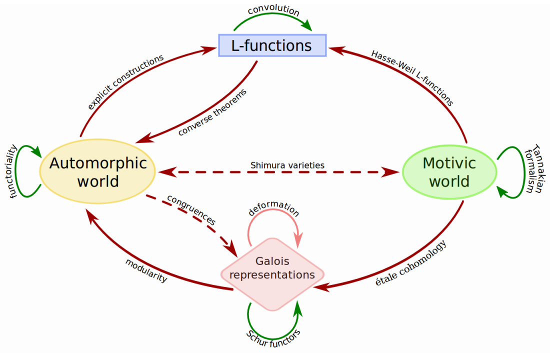
L-functions from nothing

Andrew V. Sutherland

Massachusetts Institute of Technology

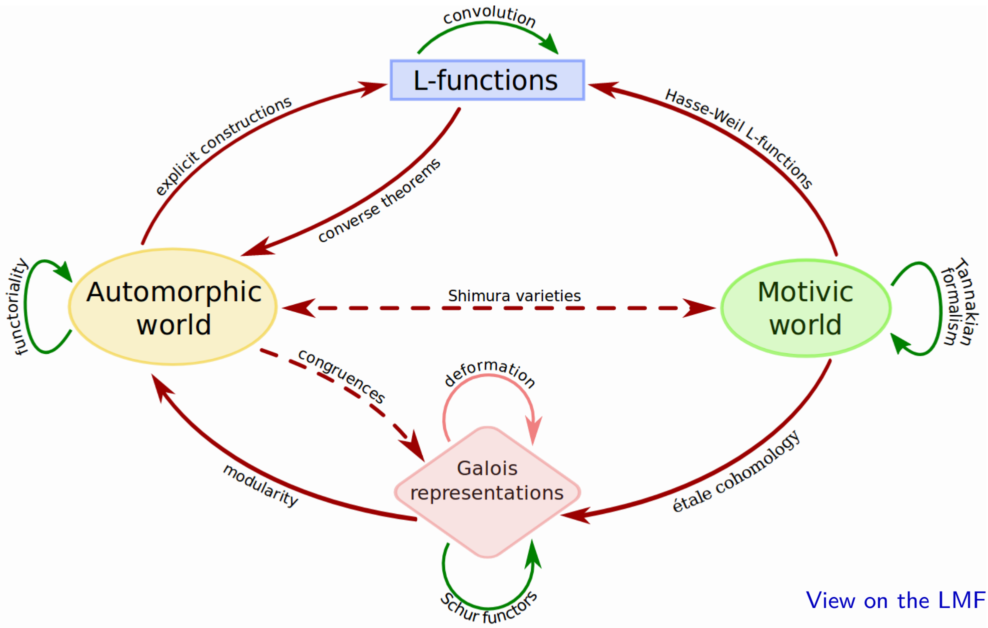


(joint work with Andrew R. Booker, University of Bristol)

Why L-functions?

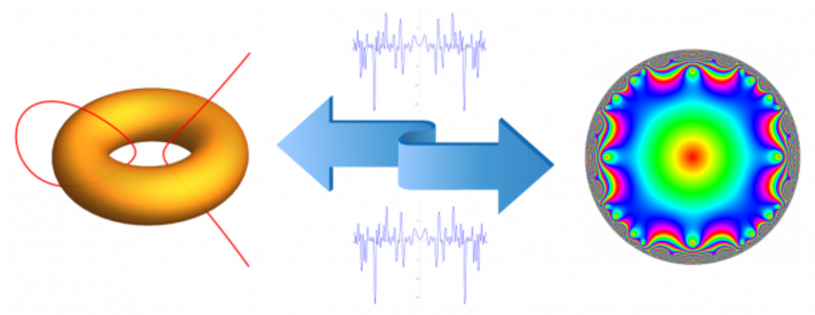
Many of the most important questions in number theory involve L-functions:

- Riemann hypothesis
- Artin conjecture
- Birch and Swinnerton-Dyer conjecture
- Tate conjecture
- Sato–Tate conjecture
- Lang–Trotter conjecture
- Murmurations
- Modularity and the Langlands program



View on the LMFDB

Elliptic curves and their L-functions



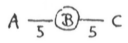
Theorem (Eichler, Shimura, Langlands–Tunnell, Frey, Serre, Ribet, Mazur, Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)

For each positive integer N, the set of L-functions $L(E,s)$ of elliptic curves $E/\mathbb{Q}$ of conductor N is equal to the set of L-functions $L(f,s)$ of newforms $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ of weight 2 and level N with rational q-expansions.

Antwerp IV tables (1972)

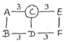
11 = 11

A	0	-1	1	0	0	-	1	I1	1	5	0
B	0	-1	1	-10	-20	-	5	I5	5	5	0
C	0	-1	1	-7820	-263580	-	1	I1	1	1	0



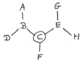
14 = 2.7

A	1	0	1	-1	0	-	2, 1	I2, I1	2, 1	6	0
B	1	0	1	-11	12	+	1, 2	I1, I2	1, 2	6	0
C	1	0	1	4	-6	-	6, 3	I6, I3	6, 3	6	0
D	1	0	1	-36	-70	+	3, 6	I3, I6	3, 6	6	0
E	1	0	1	-171	-874	-	18, 1	I18, I1	18, 1	2	0
F	1	0	1	-2731	-55146	+	9, 2	I9, I2	9, 2	2	0



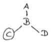
15 = 3.5

A	1	1	1	0	0	-	1, 1	I1, I1	1, 1	4	0
B	1	1	1	-5	2	+	2, 2	I2, I2	2, 2	8	0
C	1	1	1	-10	-10	+	4, 4	I4, I4	4, 4	8	0
D	1	1	1	-80	242	+	1, 1	I1, I1	1, 1	4	0
E	1	1	1	-135	-660	+	8, 2	I8, I2	8, 2	8	0
F	1	1	1	35	-28	-	2, 8	I2, I8	2, 8	4	0
G	1	1	1	-110	-880	-	16, 1	I16, I1	16, 1	2	0
H	1	1	1	-2160	-39540	+	4, 1	I4, I1	4, 1	2	0



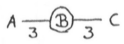
17 = 17

A	1	-1	1	-1	0	+	1	I1	1	4	0
B	1	-1	1	-6	-4	+	2	I2	2	4	0
C	1	-1	1	-1	-14	-	4	I4	4	4	0
D	1	-1	1	-91	-310	+	1	I1	1	2	0



19 = 19

A	0	1	1	1	0	-	1	I1	1	3	0
B	0	1	1	-9	-15	-	3	I3	3	3	0
C	0	1	1	-769	-8470	-	1	I1	1	1	0



20 = 2.2.5

A	0	1	0	-1	0	+	4, 1	IV, I1	0, 1	6	0
B	0	1	0	4	4	-	8, 2	IV*, I2	0, 2	6	0
C	0	1	0	-41	-116	+	4, 3	IV, I3	0, 3	2	0
D	0	1	0	-36	-140	-	8, 6	IV*, I6	0, 6	2	0

Elliptic curves computed by Swinnerton-Dyer

N	Factors	W-split of allforms	Complete split of newforms
11	11	0,1	0,1
14	2,7	0,1,0,0	0,1,0,0
15	3,5	0,1,0,0	0,1,0,0
17	17	0,1	0,1
19	19	0,1	0,1
20	2,5	0,0,1,0	0,0,1,0
21	3,7	0,0,1,0	0,0,1,0
22	2,11	0,1,0,1	0,0,0,0
23	23	0,2	0,2
24	2,3	0,0,1,0	0,0,1,0
26	2,13	0,1,1,0	0,1,1,0
27	3	0,1	0,1
28	2,7	0,1,0,1	0,0,0,0
29	29	0,2	0,2
30	2,3,5	0,1,1,0,0,1,0,0	0,0,1,0,0,0,0,0
31	31	0,2	0,2
32	2	0,1	0,1
33	3,11	0,2,0,1	0,1,0,0
34	2,17	0,1,1,1	0,0,1,0
35	5,7	0,1,2,0	0,1,2,0
36	2,3	0,0,1,0	0,0,1,0
37	37	1,1	1,1
38	2,19	0,2,1,1	0,1,1,0
39	3,13	0,1,2,0	0,1,2,0
40	2,5	1,1,1,0	0,1,0,0
41	41	0,3	0,3
42	2,3,7	0,1,1,1,1,0,1,0	0,0,0,0,1,0,0,0
43	43	1,2	1,2
44	2,11	0,2,1,1	0,0,1,0
45	3,5	0,1,1,1	0,0,1,0
46	2,23	0,3,0,2	0,1,0,0
47	47	0,4	0,4
48	2,3	1,1,1,0	0,1,0,0
49	7	0,1	0,1
50	2,5	0,1,1,0	0,1,1,0
51	3,17	0,3,1,1	0,2,1,0
52	2,13	1,1,2,1	0,0,1,0
53	53	1,3	1,3
54	2,3	0,2,1,1	0,1,1,0
55	5,11	0,3,1,1	0,2,1,0
56	2,7	0,3,1,1	0,1,1,0
57	3,19	1,1,2,1	1,0,1+1,0
58	2,29	1,2,1,2	1,0,1,0
59	59	0,5	0,5
60	2,3,5	0,2,1,0,1,1,2,0	0,0,0,0,0,0,0,0

Modular forms computed by Tingley

A more modern version of the same thing

Class	Conductor	Weierstrass equation
11.a	11	$y^2+y=x^3-x^2-7820x-263580$
14.a	$2\cdot 7$	$y^2+xy+y=x^3-2731x-55146$
15.a	$3\cdot 5$	$y^2+xy+y=x^3+x^2-2160x-39540$
17.a	17	$y^2+xy+y=x^3-x^2-91x-310$
19.a	19	$y^2+y=x^3+x^2-769x-8470$
20.a	$2^2\cdot 5$	$y^2=x^3+x^2-41x-116$
21.a	$3\cdot 7$	$y^2+xy=x^3-784x-8515$
24.a	$2^3\cdot 3$	$y^2=x^3-x^2-384x-2772$
26.a	$2\cdot 13$	$y^2+xy+y=x^3-460x-3830$
26.b	$2\cdot 13$	$y^2+xy+y=x^3-x^2-213x-1257$
27.a	3^3	$y^2+y=x^3-270x-1708$
30.a	$2\cdot 3\cdot 5$	$y^2+xy+y=x^3-5334x-150368$
32.a	2^5	$y^2=x^3-11x-14$
33.a	$3\cdot 11$	$y^2+xy=x^3+x^2-146x+621$
34.a	$2\cdot 17$	$y^2+xy=x^3-113x-329$
35.a	$5\cdot 7$	$y^2+y=x^3+x^2-131x-650$
36.a	$2^2\cdot 3^2$	$y^2=x^3-135x-594$
37.a	37	$y^2+y=x^3-x$
37.b	37	$y^2+y=x^3+x^2-1873x-31833$
38.a	$2\cdot 19$	$y^2+xy+y=x^3-86x-2456$
38.b	$2\cdot 19$	$y^2+xy+y=x^3+x^2-70x-279$
39.a	$3\cdot 13$	$y^2+xy=x^3+x^2-69x-252$

Label	Level	Weight	Dim	q-expansion
11.2.a.a	11	2	1	$q-2q^2-q^3+2q^4+q^5+2q^6-2q^7+\cdots$
14.2.a.a	14	2	1	$q-q^2-2q^3+q^4+2q^6+q^7-q^8+\cdots$
15.2.a.a	15	2	1	$q-q^2-q^3-q^4+q^5+q^6+3q^8+\cdots$
17.2.a.a	17	2	1	$q-q^2-q^4-2q^5+4q^7+3q^8-3q^9+\cdots$
19.2.a.a	19	2	1	$q-2q^3-2q^4+3q^5-q^7+q^9+3q^{11}+\cdots$
20.2.a.a	20	2	1	$q-2q^3-q^5+2q^7+q^9+2q^{13}+\cdots$
21.2.a.a	21	2	1	$q-q^2+q^3-q^4-2q^5-q^6-q^7+\cdots$
24.2.a.a	24	2	1	$q-q^3-2q^5+q^9+4q^{11}-2q^{13}+\cdots$
26.2.a.a	26	2	1	$q-q^2+q^3+q^4-3q^5-q^6-q^7+\cdots$
26.2.a.b	26	2	1	$q+q^2-3q^3+q^4-q^5-3q^6+q^7+\cdots$
27.2.a.a	27	2	1	$q-2q^4-q^7+5q^{13}+4q^{16}-7q^{19}+\cdots$
30.2.a.a	30	2	1	$q-q^2+q^3+q^4-q^5-q^6-4q^7+\cdots$
32.2.a.a	32	2	1	$q-2q^5-3q^9+6q^{13}+2q^{17}-q^{25}+\cdots$
33.2.a.a	33	2	1	$q+q^2-q^3-q^4-2q^5-q^6+4q^7+\cdots$
34.2.a.a	34	2	1	$q+q^2-2q^3+q^4-2q^6-4q^7+q^8+\cdots$
35.2.a.a	35	2	1	$q+q^3-2q^4-q^5+q^7-2q^9-3q^{11}+\cdots$
36.2.a.a	36	2	1	$q-4q^7+2q^{13}+8q^{19}-5q^{25}-4q^{31}+\cdots$
37.2.a.a	37	2	1	$q-2q^2-3q^3+2q^4-2q^5+6q^6+\cdots$
37.2.a.b	37	2	1	$q+q^3-2q^4-q^7-2q^9+3q^{11}+\cdots$
38.2.a.a	38	2	1	$q-q^2+q^3+q^4-q^6-q^7-q^8+\cdots$
38.2.a.b	38	2	1	$q+q^2-q^3+q^4-4q^5-q^6+3q^7+\cdots$
39.2.a.a	39	2	1	$q+q^2-q^3-q^4+2q^5-q^6-4q^7+\cdots$

Modularity for abelian varieties

An abelian variety is a smooth projective variety that is also an algebraic group (projective implies abelian). Elliptic curves are abelian varieties of dimension one.

Abelian varieties A of dimension g over a field k form a category whose morphisms are isogenies (surjective morphisms with finite kernel that preserve the group structure).

For $g \geq 1$ and k a number field, each A/k of dimension g has an L-function

$$L(A,s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(|\mathfrak{p}|^{-s})^{-1} = \sum_{n\geq 1} a_n n^{-s}$$

with L-polynomials $L_{\mathfrak{p}} \in \mathbb{Z}[T]$ and Dirichlet coefficients $a_n \in \mathbb{Z}$. For primes $\mathfrak{p}$ of good reduction, $L_{\mathfrak{p}}(T)$ is the numerator of the zeta function of $\bar{A}/\mathbb{F}_{\mathfrak{p}}$ of degree $2g$.
For A_1/k and A_2/k we have $L(A_1,s) = L(A_2,s)$ if and only if $A_1 \sim A_2$ (Faltings-Tate).

Conjecture

Every abelian variety over a number field is modular. For $k = \mathbb{Q}$ this means there is an isobaric automorphic representation π of $\mathrm{GL}_{2g}(\mathbb{A}_{\mathbb{Q}})$ for which $L(A,s) = L(s - 1/2, \pi)$.

Enumerating elliptic curves by conductor

To enumerate abelian varieties of dimension $g = 1$ over $\mathbb{Q}$ one may proceed as follows:

1. Prove the modularity conjecture for $g = 1$ and $k = \mathbb{Q}$.
2. Enumerate rational modular forms $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ for $N = 1, 2, 3, \ldots$
3. Use Eichler-Shimura to get an isogeny class representative E_f for each f.
4. Fill out isogeny classes by finding all the elliptic curves $E/\mathbb{Q}$ isogenous to E_f.

For $N \leq 500\,000$ this yields $3\,064\,705$ elliptic curves and $2\,164\,260$ L-functions.

Each of these steps is substantially more difficult for $g > 1$, even for $g = 2$.

There has been major recent progress on step 1 [Boxer-Calegari-Gee-Pilloni 2025], and on step 4 [van Bommel-Chidambaram-Costa-Kieffer 2023].

But step 2 is currently impractical, and even if this changes, step 3 is impossible, so we cannot apply this strategy for $g > 1$.

Challenges in dimension two

We have nothing close to a $g = 2$ version of the 1972 Antwerp tables. Current tables of rational weight-2 paramodular forms are provably complete only up to level 251 (Poor-Yuen 2025). This includes only one generic case (level 249), and we have yet to prove the existence of an abelian surface with the same L-function. Current tables of abelian surfaces over $\mathbb{Q}$ include only Jacobians and omit the very first case (level 121).

- Enumerating weight-2 paramodular forms is very difficult (no dimension formulas). Computing the L-function of a paramodular form is also very difficult.
- There is no analog of the Eichler-Shimura construction for paramodular forms (the converse of the modularity conjecture is false for $g = 2$ and $k = \mathbb{Q}$).
- Not all abelian surfaces over $\mathbb{Q}$ are Jacobians of genus 2 curves over $\mathbb{Q}$ (one can generically represent an abelian surface as a projective variety in $\mathbb{P}^{15}$ defined by 72 quadratic forms, but this is not a very pleasant thing to do).
- No algorithm is known to enumerate genus 2 curves over $\mathbb{Q}$ of a given conductor. Even computing the conductor of a given genus 2 curve can be very difficult.

Abelian surfaces over $\mathbb{Q}$

Abelian varieties of dimension $g = 2$ are abelian surfaces. Examples over $\mathbb{Q}$ include:

1. $A = E_1 \times E_2$ is a product of elliptic curves over $\mathbb{Q}$: $L(A,s) = L(E_1,s)L(E_2,s)$.
2. $A = A_f$ is the Eichler–Shimura image of a newform $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ with quadratic Hecke field: $L(A,s) = L(s - 1/2, f)L(s - 1/2, f^\sigma)$.
3. $A = \mathrm{Res}\, E$ is the Weil restriction of E/K with $[K:\mathbb{Q}] = 2$: $L(A,s) = L(E,s)$.
4. $A = \mathrm{Jac}\, C$ is the Jacobian of a genus 2 curve $C/\mathbb{Q}$: $L(A,s) = L(C,s)$.
5. $A = \mathrm{Prym}(C_1 \to C_2)$ is a Prym variety: $L(A,s) = L(C_1,s)/L(C_2,s)$.

These options are not mutually exclusive (especially at the level of isogeny classes).

A admits a principal polarization ($A \simeq A^\vee$) in cases 1,3,4, and usually in case 2, but usually not in case 5 (which is necessary; not all $A/\mathbb{Q}$ admit a principal polarization).

Modularity is known in cases 1 and 2, in case 3 when K is totally real (and for some imaginary K), and for a positive proportion of case 4 (when C are ordered by height).

Automorphic forms associated to abelian surfaces over $\mathbb{Q}$ (BSSVY)

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 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
$\mathbf{B}[C_1]_{ns}$	$294 = 2^1 3^1 7^2$	$y^2+(x^3+1)y = x^4+x^2$	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
$\mathbf{F}[D_2,C_2,\mathcal{H}]_{ngs}$	$576 = 2^6 3^2$	$y^2+x^3y = 5x^3-2$	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

Provisional result (proof in progress)

Theorem (Booker-S)

Assuming modularity of abelian surfaces and GRH for Rankin–Selberg L-functions, there are (at most) 1059 *(and at least 1057) isogeny classes of abelian surfaces over* $\mathbb{Q}$ *of conductor* ≤ 1500. *Among these*

- 818 *arise from products of elliptic curves over* $\mathbb{Q}$*;*
- 28 *arise from weight-2 newforms with quadratic Hecke field;*
- 7 *arise from the Weil restriction of an elliptic curve over a quadratic field;*
- *(at most)* 206 *(and at least 204) arise from generic abelian surfaces, of which at least* 193 *include a Jacobian.*

(Of the 13 generic abelian surfaces not known to arise as Jacobians, 11 arise as Prym varieties associated to a genus 3 cover of a genus 1 curve. We are currently searching for the other 2, which have conductors 969 and 1274. Finding them would allow us to remove everything in parentheses on this slide.)

Some non-provisional results

Theorem (Booker-S)

There are exactly two isogeny classes of modular abelian surfaces over $\mathbb{Q}$ with good reduction away from 7.

The set $S = \{7\}$ is the unique nonempty set of primes for which we currently know all isogeny classes of modular abelian surfaces over $\mathbb{Q}$ with good reduction away from S.

Theorem (Booker-S)

There are exactly three isogeny classes of modular abelian surfaces over $\mathbb{Q}$ with conductor dividing 2^{11}.

Conductor	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}	2^{18}	2^{19}	2^{20}
Num curves	2	0	4	10	33	62	65	72	68	64	38	40	54
Num isog classes	1	0	1	1	7	10	19	22	19	24	19	20	32

(Table 6.6 in Robin Visser's PhD thesis)

An axiomatic approach to L-functions of abelian varieties over $\mathbb{Q}$

Fix a positive integer g. We shall consider arithmetic L-functions of degree $2g$, motivic weight 1, field of coefficients $\mathbb{Q}$, and an Euler product

$$L(s) := \sum_n a_n n^{-s} = \prod_p L_p(p^{-s})^{-1},$$

with $a_n \in \mathbb{Z}$ and $L_p \in \mathbb{Z}[T]$ of degree $\leq 2g$. We further assume that $\Lambda(s) := \Gamma_{\mathbb{C}}(s)^g L(s)$ is holomorphic on $\mathbb{C}$ and satisfies the functional equation

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

with root number $\varepsilon = \pm 1$ and conductor N (with $\deg L_p = 2g$ iff $p \nmid N$), and that $|a_n| \leq d_{2g}(n)\sqrt{n}$, where $d_r(n) = \sum_{n_1 \cdots n_r = n} 1$.

Under the modularity conjecture, every abelian variety $A/\mathbb{Q}$ of dimension g has such an L-function (whose root number and conductor can be defined arithmetically).

Conversely, if we assume $L(s) = L(A,s)$ for some $A/\mathbb{Q}$ we can impose additional constraints on $L_p(s)$ for a particular choice of local root numbers ε_p for $p|N$.

Conductor bounds for abelian varieties over $\mathbb{Q}$

The formula of [Brumer–Kramer 94] gives explicit bounds on the p-adic valuation of the conductor N of an abelian variety $A/\mathbb{Q}$ of dimension g:

$$v_p(N) \le 2g + pd + (p-1)\lambda_p(d),$$

where $d = \lfloor \frac{2g}{p-1} \rfloor$ and $\lambda_p(d) = \sum i d_i p^i$, with $d = \sum d_i p^i$ and $0 \le d_i < p$.

g	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p > 7$
1	8	5	2	2	2
2	20	10	9	4	4
3	28	21	11	13	6

For $g \le 2$ these bounds are known to be tight (see `www.lmfdb.org` for examples).

A finite problem

Let $\mathcal{S}(g, N, \varepsilon)$ denote the set of L-functions $L(s)$ that satisfy our axioms for a particular choice of $g, N \in \mathbb{Z}_{>0}$ and $\varepsilon = \pm 1$.

The set $\mathcal{S}(g, N, \varepsilon)$ is conjectural finite. Moreover there is an effectively computable $n_0 = O(\sqrt{N})$ for which the coefficients $a_1, \ldots, a_{n_0}$ uniquely determine each $L \in \mathcal{S}(g, N, \varepsilon)$ (with $n_0 = O(\log^2 N)$ under GRH).

We seek an algorithm that takes inputs g, N, ε, determines a suitable n_0, and then outputs a list of distinct tuples $(a_1, \ldots, a_{n_0})$, one for each $L \in \mathcal{S}(g, N, \varepsilon)$.
See Booker and Farmer–Koutsoliotas–Lemurell for prior work in this direction.

Our plan: Compute $\mathcal{S}(g, N, \varepsilon)$ using linear algebra (and lattice reduction), then search for $A/\mathbb{Q}$ with $L(A, s) \in \mathcal{S}(g, N, \varepsilon)$.

Our plan depends crucially on being able to compute $\mathcal{S}(g, N, \varepsilon)$ explicitly.
This not only tells us when to stop searching, knowing $a_1, \ldots, a_{n_0}$ helps us search.

A brief digression

Conjecture (Shafarevich, proved by Faltings)

Let K be a number field and let S be a finite set of primes of K. The set of abelian varieties of dimension g over K with good reduction away from S is finite.

Conjecture (Mordell, proved by Faltings)

Let C be a nice curve of genus $g \geq 2$ over a number field K. The set $C(K)$ is finite.

Faltings' proofs are ineffective: they do not provide a way to enumerate (or even bound the size of) these sets and no such methods are currently known.

Alpöge and Lawrence recently proved under the Hodge, Tate, and Fontaine–Mazur conjectures, the existence of (hopelessly impractical) algorithms to do this.

Our results imply that under modularity and an integral converse theorem for GL_4 (with character twists), similar algorithms exist. They are also hopelessly impractical (but arguably less hopelessly impractical).

The approximate functional equation

Fix g, N, ε. For each nonnegative integer k we define $S_k(x) := \sum_n f_k(n/x) a_n/n$, where

$$f_k(x) := \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} (s-1)^k \Gamma_{\mathbb{C}}(s)^g x^{1-s}\, ds.$$

The functional equation then implies the identity

$$S_k(x) = \varepsilon(-1)^k S_k(N/x),$$

valid for all $x > 0$; this is an approximate functional equation. If we choose k so that $(-1)^k = -\varepsilon$ and put $x = \sqrt{N}$ we obtain a nontrivial linear constraint on the a_n:

$$\sum_n \frac{a_n}{n} f_k(n/\sqrt{N}) = 0. \tag{1}$$

The $O(\sqrt{n})$ bounds on a_n and rapid decay of $f_k(x)$ allow us to compute an interval $I_{k,m}$ containing the truncated sum in (1) for $n \le m$ that does not depend on the a_n.

A system of linear constraints

For each $k \geq 0$ of the correct parity (meaning $(-1)^k = -\varepsilon$), we have linear constraints

$$\sum_{n \leq m} f_k\left(n/\sqrt{N}\right)\frac{a_n}{n} \in I_{k,m}.$$

We restrict to $k = O(N^{1/4})$ and orthogonalize the f_k with respect to the inner product $\langle u, v\rangle = \int_0^\infty \frac{u(x)v(x)}{x}dx$. We also have the constraints $|a_n| \leq d_{2g}(n)\sqrt{n}$ for $n \geq 1$.

We now assume the $L \in \mathcal{S}(g, N, \varepsilon)$ are automorphic, and obtain additional constraints by twisting $L(s)$ by a Dirichlet character $\chi_q \colon \mathbb{Z} \to \mathbb{C}$.

This generally increases the conductor and widens the corresponding interval $I_{\chi,k,m}$, but for χ of small conductor q and small k we obtain useful constraints

$$\sum_{n \leq m} \Im\left(\chi_q(n)/\sqrt{(-1)^k \varepsilon_{A\times\chi_q}}\right) f_k\left(n/\sqrt{N_{A\times\chi_q}}\right)\frac{a_n}{n} \in I_{q,k,m}.$$

By fixing local root numbers at primes dividing N we can sharpen these constraints.

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1$, $m = 64$

We want to compute bounds on $a_2 \in \mathbb{Z}$ satisfying the constraints below.
We know *a priori* (via the Weil bounds) that $a_2 \in [-4, 4]$.

q	k	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\cdots$	a_{64}	$I_{q,k,64}$
1	1	1	0.446	0.216	0.112	0.0613	0.0349	0.0206	$\cdots$	3.10×10^{-9}	$-2.42 \pm 9.00 \times 10^{-6}$
1	3	-0.226	0.853	1	0.862	0.674	0.506	0.373	$\cdots$	8.56×10^{-7}	$+2.85 \pm 2.76 \times 10^{-3}$
1	5	0.854	-0.864	-1	-0.572	-0.112	0.223	0.421	$\cdots$	6.78×10^{-5}	-1.75 ± 0.212
1	7	-1	0.153	0.570	0.366	0.0354	0.202	0.308	$\cdots$	8.59×10^{-4}	-1.09 ± 3.70
3	1	-0.891	0	1	-0.866	0	0.618	-0.520	$\cdots$	9.62×10^{-4}	0.748 ± 5.88

- The solution dual to maximizing a_2 is $(0.969, -0.0859, 0.0124, -0.00332, 0.0027)$. **We don't care if this is slightly incorrect** (e.g. due to precision loss or bugs).
- Computing this linear combination of constraints using interval arithmetic and worst case bounds on $a_3, a_4, \ldots, a_{64}$ **we can prove** $a_2 \leq -0.929$.
- Rounding to integers, we deduce $a_2 \in [-4, -1]$, eliminating 5 of 9 possibilities. Minimizing a_2 may eliminate more possibilities (but not in this example).

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1$, $m = 64$

We now suppose $a_2 = -4$.
This forces $a_4 = 8, a_8 = -8, \ldots, a_{64} = -64$ which we move to the RHS.
For odd n we can express $a_{2n} = -4a_n$ in terms of a_n and remove it from the system.

q	k	a_3	a_4	a_5	a_6	a_7	a_8	a_9	$\cdots$	a_{63}	$I_{q,k,64}$
1	1	1	0	0.366	0	0.131	0	0.0499	$\cdots$	1.67×10^{-8}	$0.0853 \pm 3.99 \times 10^{-5}$
1	3	-1	0	0.146	0	0.279	0	0.198	$\cdots$	1.00×10^{-6}	$-2.91 \pm 2.71 \times 10^{-3}$
1	5	1	0	-0.590	0	-0.353	0	-0.0653	$\cdots$	2.36×10^{-5}	$4.76 \pm 7.38 \times 10^{-2}$
1	7	-0.675	0	1	0	0.111	0	-0.284	$\cdots$	3.57×10^{-4}	-4.90 ± 1.35
3	1	0	0	-1	0	0.540	0	0	$\cdots$	0	-4.45 ± 1.90

- The dual solutions for minimizing and maximizing a_3 are $(0.484, -0.352, 0.131, -0.0486, 0)$ and $(0.595, -0.27, 0.105, -0.0434, 0.0732)$.
- This allows us to prove $a_3 \in [0.264, 2.41]$ (given $a_2 = -4$).
- We deduce that $[1, -4, 1]$ and $[1, -4, 2]$ are the only possible extensions of $[1, -4]$ (for our fixed choice of conductor and local root numbers).

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1, m = 64$

We now suppose $a_2 = -3$ (this constrains but does not fix $a_4, a_8, \ldots, a_{64}$).
As above, for n odd we have $a_{2n} = -3a_n$ and remove a_{2n} from the system.

q	k	a_3	a_4	a_5	a_6	a_7	a_8	a_9	$\cdots$	a_{64}	$I_{q,k,64}$
1	1	1	0.827	0.340	0	0.118	0.0786	0.0441	$\cdots$	1.18×10^{-8}	$2.23 \pm 2.58 \times 10^{-5}$
1	3	-1	0.855	0.226	0	0.283	0.319	0.187	$\cdots$	7.32×10^{-7}	$1.86 \pm 1.77 \times 10^{-3}$
1	5	-0.243	-0.459	-1	0	-0.402	0.193	-0.0235	$\cdots$	2.66×10^{-5}	$0.373 \pm 7.30 \times 10^{-2}$
1	7	0.042	0.506	1	0	-0.367	-0.274	-0.788	$\cdots$	7.64×10^{-4}	-3.64 ± 2.47
3	1	0	0.506	-1	0	0.610	-0.263	0	$\cdots$	4.86×10^{-4}	-0.973 ± 2.22

- Using the dual solutions we are able to prove $a_3 \in [-1.55, 1.51]$ (given $a_2 = -3$).
- We find that $[1, -3, -1], [1, -3, 0], [1, -3, 1]$ are the possible extensions of $[1, -3]$.

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1, m = 64$

We now suppose $a_2 = -2$.

q	k	a_3	a_4	a_5	a_6	a_7	a_8	a_9	$\cdots$	a_{64}	$I_{q,k,64}$
1	1	1	0.670	0.300	0	0.0995	0.0637	0.0367	$\cdots$	9.60×10^{-9}	$-1.29 \pm 1.39 \times 10^{-5}$
1	3	-0.495	1	0.464	0	0.390	0.373	0.236	$\cdots$	8.56×10^{-7}	$2.40 \pm 1.38 \times 10^{-3}$
1	5	-0.390	-0.609	-1	0	-0.310	0.256	0.0834	$\cdots$	3.53×10^{-5}	$-0.0259 \pm 6.45 \times 10^{-2}$
1	7	0.0947	0.653	1	0	-0.393	-0.353	-0.797	$\cdots$	9.85×10^{-4}	-3.54 ± 2.12
3	1	0	0.622	-1	0	0.629	-0.324	0	$\cdots$	5.98×10^{-4}	-0.643 ± 1.82

- We find that $[1, -2, -2], [1, -2, -1]$ are the possible extensions of $[1, -2]$.

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1, m = 64$

We now suppose $a_2 = -1$.

q	k	a_3	a_4	a_5	a_6	a_7	a_8	a_9	$\cdots$	a_{64}	$I_{q,k,64}$
1	1	1	0.563	0.272	0	0.0873	0.0535	0.0316	$\cdots$	8.07×10^{-9}	$-3.69 \pm 1.17 \times 10^{-5}$
1	3	0.179	1	0.663	0	0.448	0.373	0.255	$\cdots$	8.56×10^{-7}	$2.63 \pm 1.38 \times 10^{-3}$
1	5	-0.679	-0.903	-1	0	-0.130	0.380	0.294	$\cdots$	5.24×10^{-5}	$-0.810 \pm 9.57 \times 10^{-2}$
1	7	0.191	0.920	1	0	-0.440	-0.498	-0.813	$\cdots$	1.39×10^{-3}	-3.38 ± 2.99
3	1	0	0.809	-1	0	0.659	-0.421	0	$\cdots$	7.78×10^{-4}	-0.115 ± 2.37

- Using the dual solutions we prove $a_3 \in [-7.14, -2.44]$ (given $a_2 = -1$).
- $v_3(N) = 1$ and $\varepsilon_3 = -1$ force $a_3 \geq -2$, so $[1, -1]$ cannot be extended.

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1, m = 64$

At this point we have determined that if $L(A, s) = \sum a_n n^{-s}$ is the L-function of a modular abelian surface of conductor 249 with $\varepsilon_3 = \varepsilon_{83} = -1$ we must have

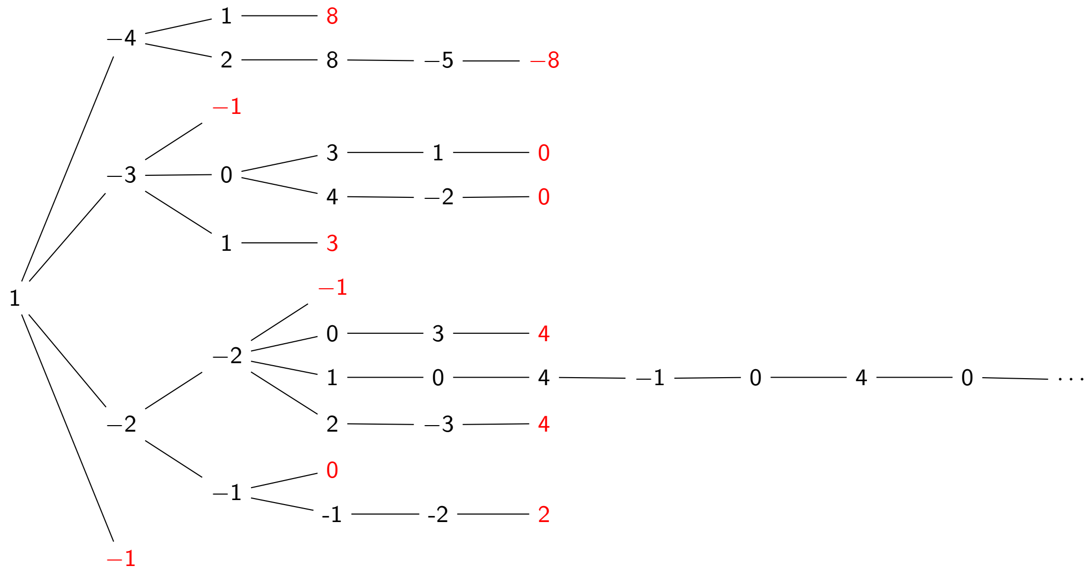
$$[a_1, a_2, a_3] \in \Big\{[1, -4, 1], [1, -4, 2], [1, -3, -1], [1, -3, 0], [1, -3, 1], [1, -2, -2], [1, -2, -1]\Big\}.$$

Continuing in this fashion we find

- 11 possibilities for $[a_1, a_2, a_3, a_4]$;
- 7 possibilities for $[a_1, a_2, a_3, a_4, a_5]$;
- 1 possibility for $[a_1, a_2, a_3, a_4, a_5, a_6, a_7]$, which determines $[a_8, a_9, a_{10}]$.

We now switch strategies and use LLL rather than linear programming.
We are searching for integer lattice points contained in a parallelepiped of small volume that we expect to contain at most one such point.

Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1$, $m = 64$



Example computation with $N = 249 = 3 \cdot 83$, $\varepsilon_3 = \varepsilon_{83} = -1, m = 64$

At this point we know that the L-function $L(A,s) = \sum a_n n^{-s}$ of every modular abelian surface $A/\mathbb{Q}$ with conductor 249 and local root numbers $\varepsilon_3 = \varepsilon_{83} = -1$ satisfies

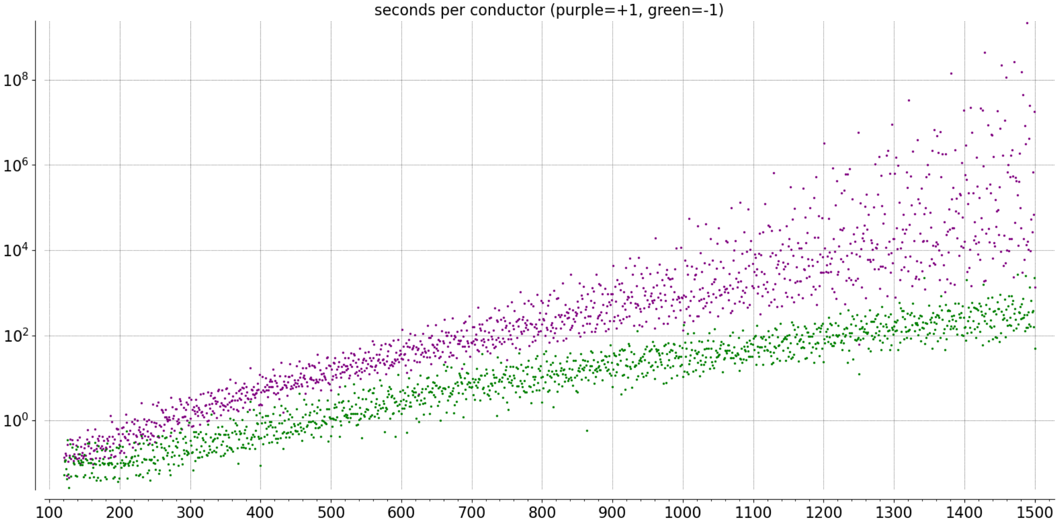
$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) = (1, -2, -2, 1, 0, 4, -1, 0, 4, 0).$$

Increasing m to 3000 yields a system with 738 unknown a_n and 219 constraints, with k ranging up to 77 and q up to 24. Using LLL (16 times) we are able to extend our unique prefix of length 10 to a unique prefix of length 1000.

This determines the L-polynomials $L_p(T)$ for $p \le 31$, which is more than enough to prove that any $A/\mathbb{Q}$ with this L-function prefix is generic (meaning $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$), and to prove (via the Rankin-Selberg inequality) that there is at most one isogeny class of abelian surfaces of conductor 249 (it is not hard to rule out other local root numbers).

The Jacobian of the genus 2 curve $y^2 + (x^3 + 1)y = x^2 + x$ is an obvious candidate (conductor and $a_1, \ldots, a_{1000}$ match), but it is (still) **not known to be modular**.

Timings



seconds per conductor (purple=+1, green=-1)
10^8
10^6
10^4
10^2
10^0
100
200
300
400
500
600
700
800
900
1000
1100
1200
1300
1400
1500

Proving completeness

If our algorithm outputs a nonempty list of feasible tuples $(a_1, \ldots, a_{n_0})$,
the next step is to show there is at most one L-function in $\mathcal{S}(g, N, \varepsilon)$ for each prefix.

For this step, we suppose that $(a_1, \ldots, a_{n_0})$ is the prefix of two distinct automorphic L-functions $L(s, \pi_1)$ and $L(s, \pi_2)$ in $\mathcal{S}(g, N, \varepsilon)$. The Rankin–Selberg convolution L-function $L(s, \pi_1 \boxtimes \pi_2)$ is entire unless $L(s, \pi_1)$ and $L(s, \pi_2)$ have a common factor.

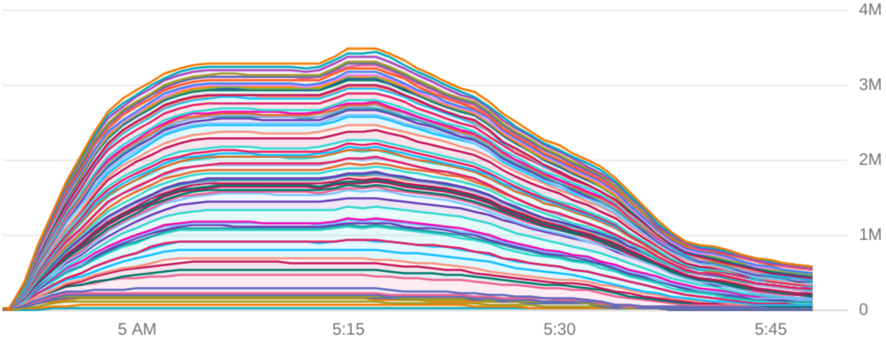
If they do, we reduce to the $g = 1$ case where everything is known. Otherwise, we construct an inequality the coefficients of $L(s, \pi_1 \boxtimes \pi_2)$ must satisfy and show that they do not (after increasing n_0 if necessary), proving that no such π_1 and π_2 exist.

We eventually obtain a list of distinct tuples $(a_1, \ldots, a_{n_0})$, each of which is the prefix of at most one automorphic L-function in $\mathcal{S}(g, N, \varepsilon)$.

This gives us an upper bound for our search that we expect to be tight.
Finding an abelian variety for each prefix proves completeness subject to modularity.

Searching for genus 2 curves

Over the past five years we have conducted several searches for genus 2 curves of small conductor. Below is a vCPU histogram from a computation we ran in 2022 that enumerated over 10^{19} genus 2 curves in a large parallel computation run in the cloud.



This computation used 4,034,560 vCPUs in 73 data centers across the globe, performing more than 300 vCPU years of computation in a few hours of real time.

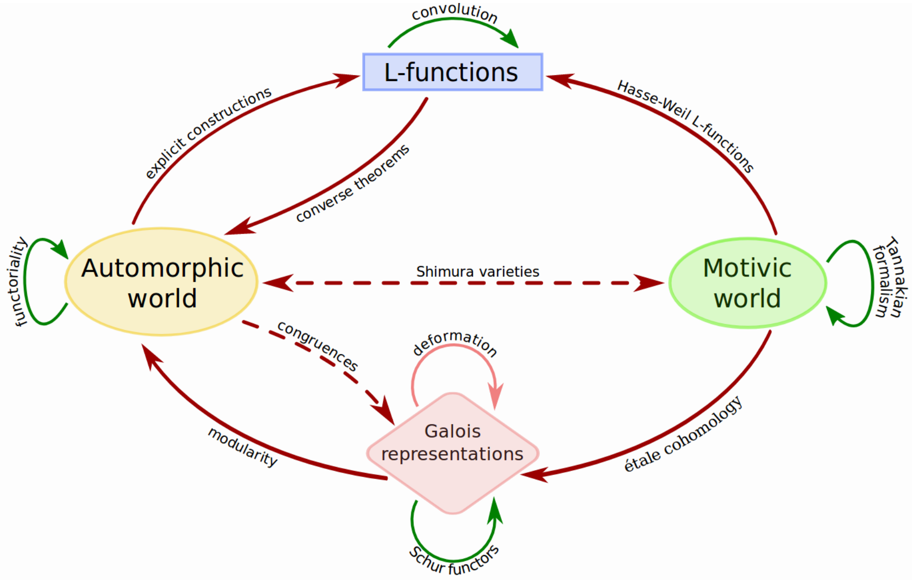
Searching for genus 2 curves

Our searches found 1927 Jacobians of conductor ≤ 1500 with 451 distinct L-functions, including many not previously known to arise for Jacobians (or even abelian surfaces).

We also found more than 6 million genus 2 curves of conductor $\leq 2^{20}$ with more than 2.5 million distinct L-functions, which will be added to the LMFDB later this summer.

conductor bound	1000	10 000	100 000	1 000 000
curves in LMFDB	159	3069	20 265	66 158
curves found	942	29 514	493 899	6 075 571
L-functions in LMFDB	109	2807	19 775	65 534
L-functions found	201	9534	194 612	2 559 187

Thank you!



convolution
L-functions
explicit constructions
converse theorems
Hasse-Weil L-functions
functoriality
Automorphic world
Shimura varieties
Motivic world
Tannakian formalism
congruences
deformation
Galois representations
modularity
étale cohomology
Schur functors

Bonus slide: Exploiting Galois representations

Let $A/\mathbb{Q}$ be an abelian surface of conductor N. For each $m \in \mathbb{Z}_{>1}$ we have a mod-m Galois representation

$$\rho_{A,m}\colon \operatorname{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{Z}/m\mathbb{Z}).$$

For $p \nmid mN$ the charpoly $\chi_p \in (\mathbb{Z}/m\mathbb{Z})[T]$ of $\rho_{A,m}(\mathrm{Frob}_p) \in \mathrm{GSp}_4(\mathbb{Z}/m\mathbb{Z})$ satisfies

$$\chi_p(T) \equiv T^{2g} L_p(T^{-1}) \bmod m.$$

The m-torsion field $\mathbb{Q}(A[m])$ is unramified away from $p|mN$ and of degree at most $\#\,\mathrm{GSp}_4(\mathbb{Z}/m\mathbb{Z})$. For small m and N it is feasible to enumerate all such fields K and their associated mod-m GSp_4-representations, especially $m = 2$ and N a prime power.

Each representation yields a mod-m congruence constraints on $L_p(T)$ for primes $p \nmid mN$. This dramatically reduces the amount of branching in our algorithm.