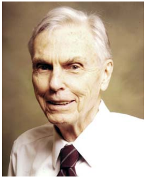
Sato-Tate distributions

Andrew V. Sutherland

Massachusetts Institute of Technology

February 4, 2016

Mikio Sato



John Tate

Joint work with F. Fité, K.S. Kedlaya, and V. Rotger (part 1), and D. Harvey (part 2).

Sato-Tate in dimension 1

Let $E/\mathbb{Q}$ be an elliptic curve, which we can write in the form

$$y^2 = x^3 + ax + b,$$

and let p be a prime of good reduction ($4a^3 + 27b^2 \not\equiv 0 \bmod p$).

The number of $\mathbb{F}_p$-points on the reduction E_p of E modulo p is

$$\#E_p(\mathbb{F}_p) = p + 1 - t_p,$$

where the trace of Frobenius $t_p \in \mathbb{Z}$ lies in the interval $[-2\sqrt{p}, 2\sqrt{p}]$.

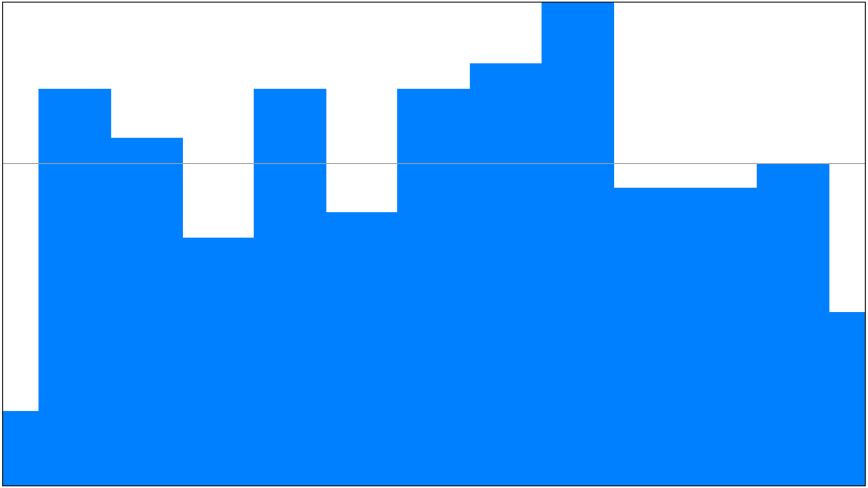
We are interested in the limiting distribution of $x_p = -t_p/\sqrt{p} \in [-2, 2]$, as p varies over primes of good reduction up to N, as $N \to \infty$.

Example: $y^2 = x^3 + x + 1$

p	t_p	x_p	p	t_p	x_p	p	t_p	x_p
3	0	**0.000000**	71	13	**−1.542816**	157	−13	**1.037513**
5	−3	**1.341641**	73	2	**−0.234082**	163	−25	**1.958151**
7	3	**−1.133893**	79	−6	**0.675053**	167	24	**−1.857176**
11	−2	**0.603023**	83	−6	**0.658586**	173	2	**−0.152057**
13	−4	**1.109400**	89	−10	**1.059998**	179	0	**0.000000**
17	0	**0.000000**	97	1	**−0.101535**	181	−8	**0.594635**
19	−1	**0.229416**	101	−3	**0.298511**	191	−25	**1.808937**
23	−4	**0.834058**	103	17	**−1.675060**	193	−7	**0.503871**
29	−6	**1.114172**	107	3	**−0.290021**	197	−24	**1.709929**
37	−10	**1.643990**	109	−13	**1.245174**	199	−18	**1.275986**
41	7	**−1.093216**	113	−11	**1.034793**	211	−11	**0.757271**
43	10	**−1.524986**	127	2	**−0.177471**	223	−20	**1.339299**
47	−12	**1.750380**	131	4	**−0.349482**	227	0	**0.000000**
53	−4	**0.549442**	137	12	**−1.025229**	229	−2	**0.132164**
59	−3	**0.390567**	139	14	**−1.187465**	233	−3	**0.196537**
61	12	**−1.536443**	149	14	**−1.146925**	239	−22	**1.423062**
67	12	**−1.466033**	151	−2	**0.162758**	241	22	**−1.417145**

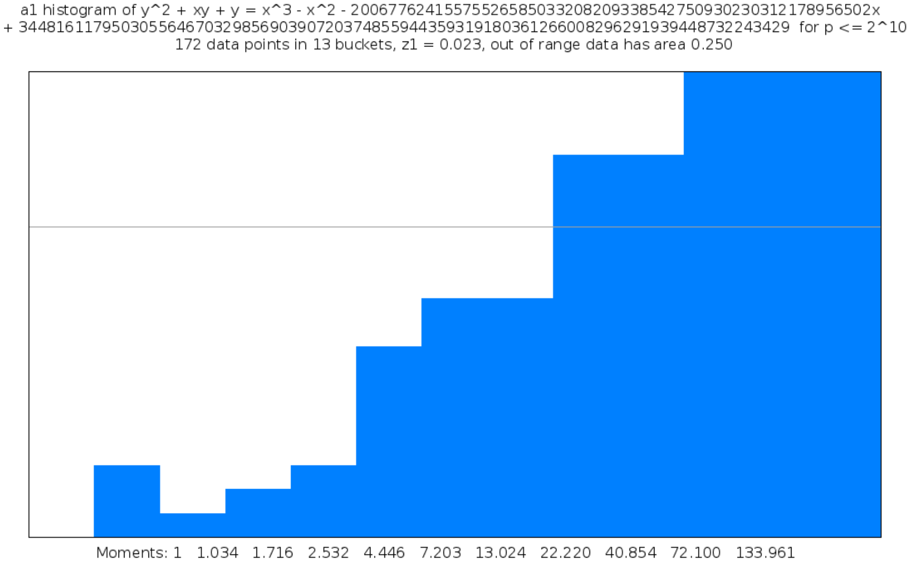
`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

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

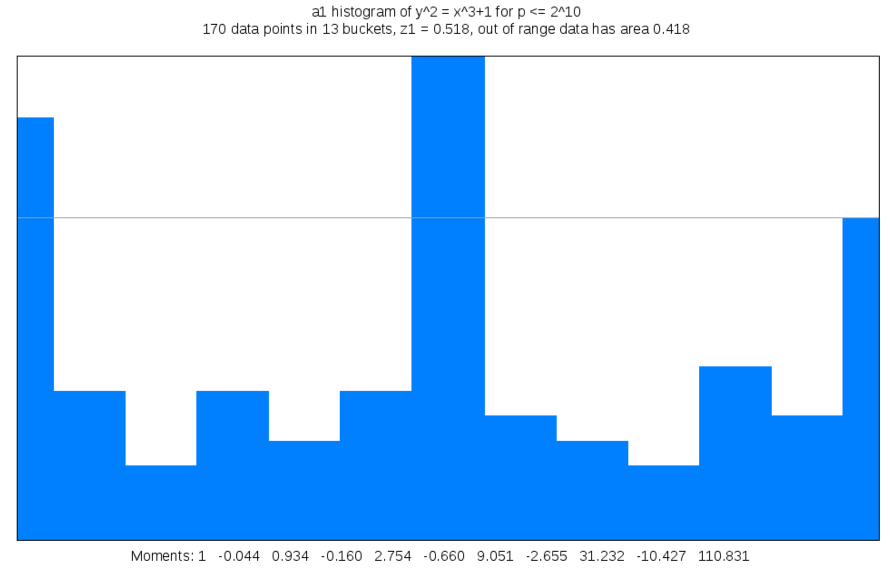


Moments: 1   0.051   1.039   0.081   2.060   0.294   4.971   1.134   13.278   4.308   37.954

click histogram to animate (requires adobe reader)

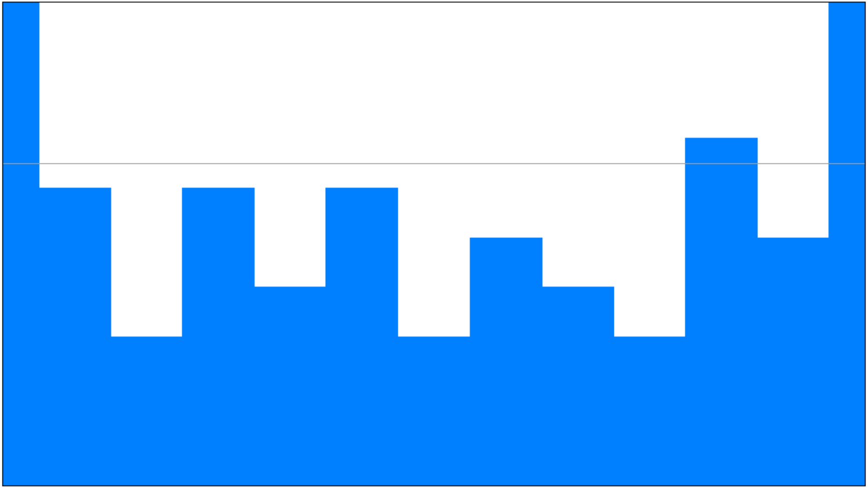


click histogram to animate (requires adobe reader)



click histogram to animate (requires adobe reader)

a1 histogram of y^2 = x^3+1 over Q(sqrt(-3)) for split p <= 2^10
164 data points in 13 buckets, out of range data has area 0.122



Moments: 1 -0.092 1.935 -0.331 5.710 -1.368 18.765 -5.504 64.750 -21.616 229.771

click histogram to animate (requires adobe reader)

Sato-Tate distributions in dimension 1

1. Typical case (no CM)

Elliptic curves $E/\mathbb{Q}$ without CM have the semicircular trace distribution. (This is also known for E/k, where k is a totally real number field).

[Barnet-Lamb, Clozel, Geraghty, Harris, Shepherd-Barron, Taylor]

2. Exceptional cases (CM)

Elliptic curves E/k with CM have one of two distinct trace distributions, depending on whether k contains the CM field or not.

[classical (Hecke, Deuring)]

Sato-Tate groups in dimension 1

The *Sato-Tate group* of E is a closed subgroup G of $\mathrm{SU}(2) = \mathrm{USp}(2)$ derived from the ℓ-adic Galois representation attached to E.

The refined Sato-Tate conjecture implies that the distribution of normalized traces of E_p converges to the distribution of traces in the Sato-Tate group of G, under the Haar measure.

G	G/G^0	E	k	$\mathrm{E}[a_1^0], \mathrm{E}[a_1^2], \mathrm{E}[a_1^4] \ldots$
$\mathrm{U}(1)$	C_1	$y^2 = x^3 + 1$	$\mathbb{Q}(\sqrt{-3})$	$1, 2, 6, 20, 70, 252, \ldots$
$N(\mathrm{U}(1))$	C_2	$y^2 = x^3 + 1$	$\mathbb{Q}$	$1, 1, 3, 10, 35, 126, \ldots$
$\mathrm{SU}(2)$	C_1	$y^2 = x^3 + x + 1$	$\mathbb{Q}$	$1, 1, 2, 5, 14, 42, \ldots$

In dimension 1 there are three possible Sato-Tate groups, two of which arise for elliptic curves defined over $\mathbb{Q}$.

Zeta functions and L-polynomials

Let $C/\mathbb{Q}$ be a nice curve of genus g and p a prime of good reduction. Define the *zeta function*

$$Z_p(T) := \exp\left(\sum_{r=1}^{\infty} N_r T^r / r\right),$$

where $N_r = \#C_p(\mathbb{F}_{p^r})$. This is a rational function of the form

$$Z_p(T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

where $L_p(T)$ is an integer polynomial of degree $2g$.

For $g = 1$ we have $L_p(t) = pT^2 + c_1 T + 1$, and for $g = 2$,

$$L_p(T) = p^2T^4 + c_1 pT^3 + c_2 T^2 + c_1 T + 1.$$

Normalized L-polynomials

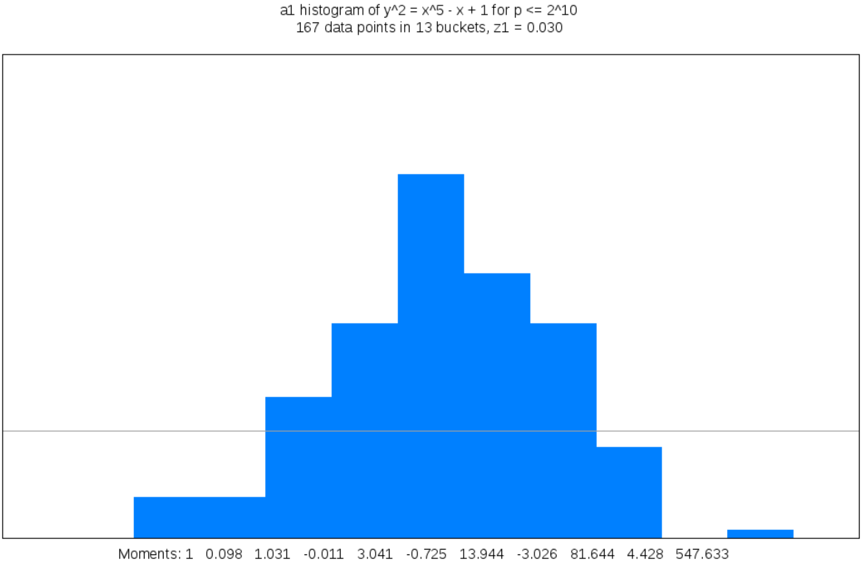
The normalized L-polynomial

$$\bar{L}_p(T) := L_p(T/\sqrt{p}) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{R}[T]$$

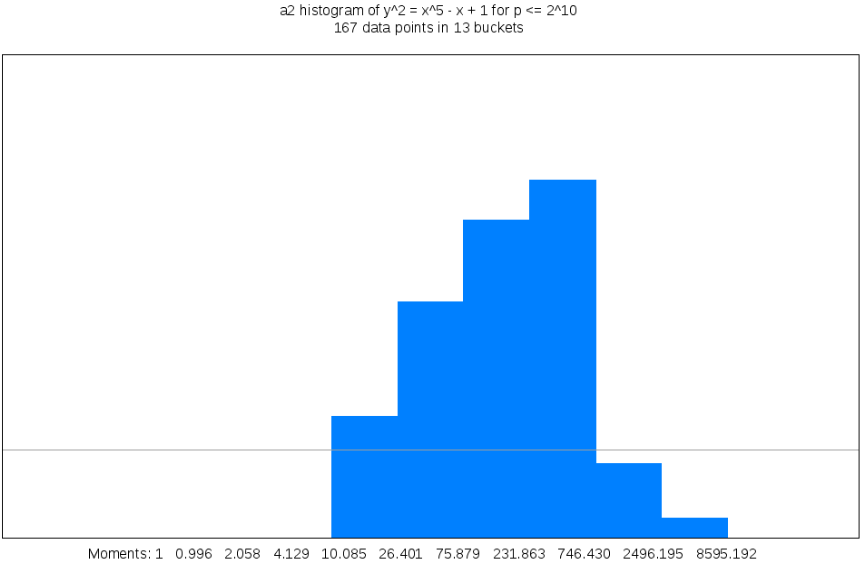
is monic, reciprocal ($a_i = a_{2g-i}$), and unitary (roots on the unit circle). The coefficients a_i satisfy the Weil bounds $|a_i| \le \binom{2g}{i}$.

We now consider the limiting distribution of $a_1, a_2, \ldots, a_g$ over all primes $p \le N$ of good reduction, as $N \to \infty$.

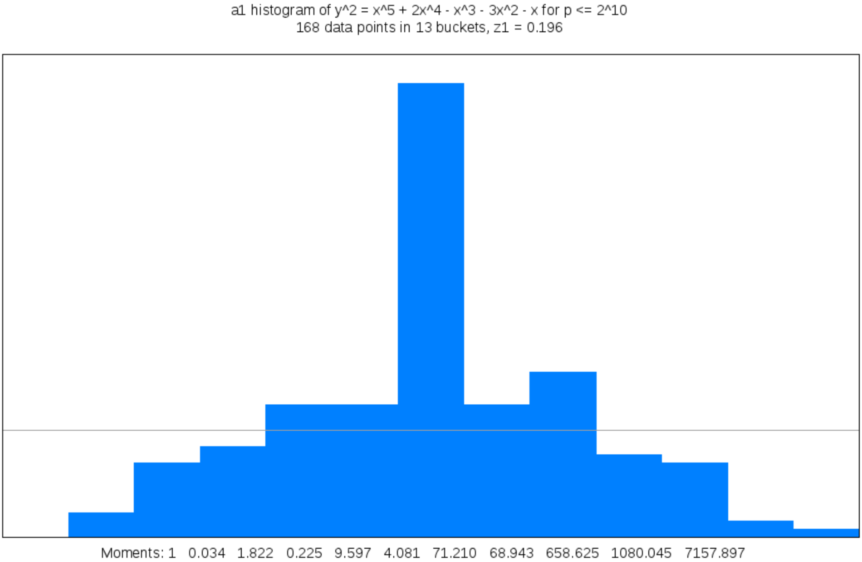
`http://math.mit.edu/~drew/g2SatoTateDistributions.html`



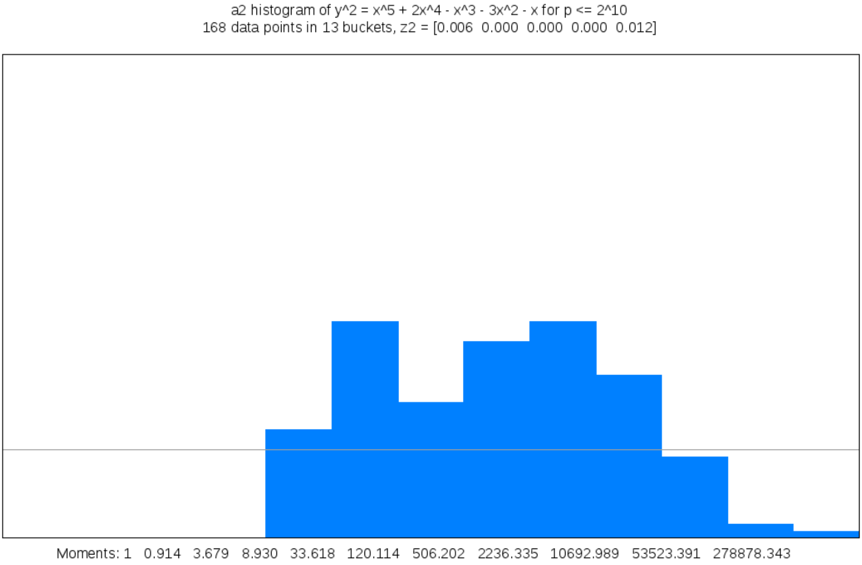
click histogram to animate (requires adobe reader)



click histogram to animate (requires adobe reader)

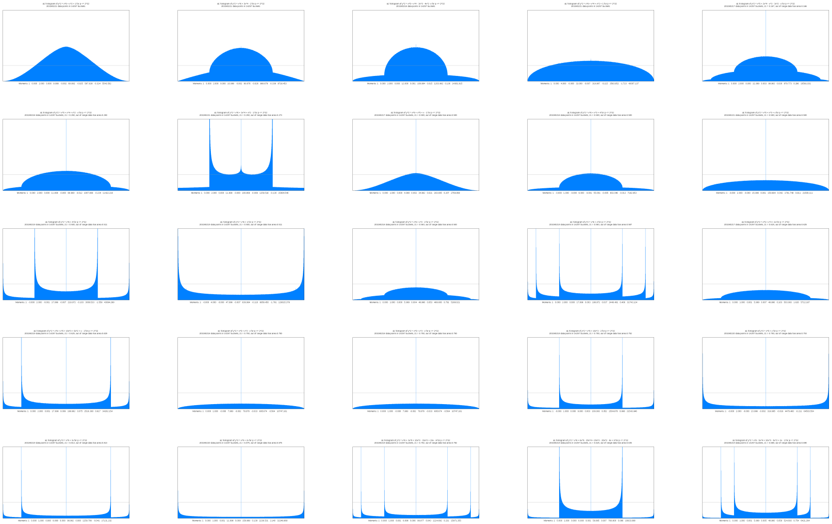


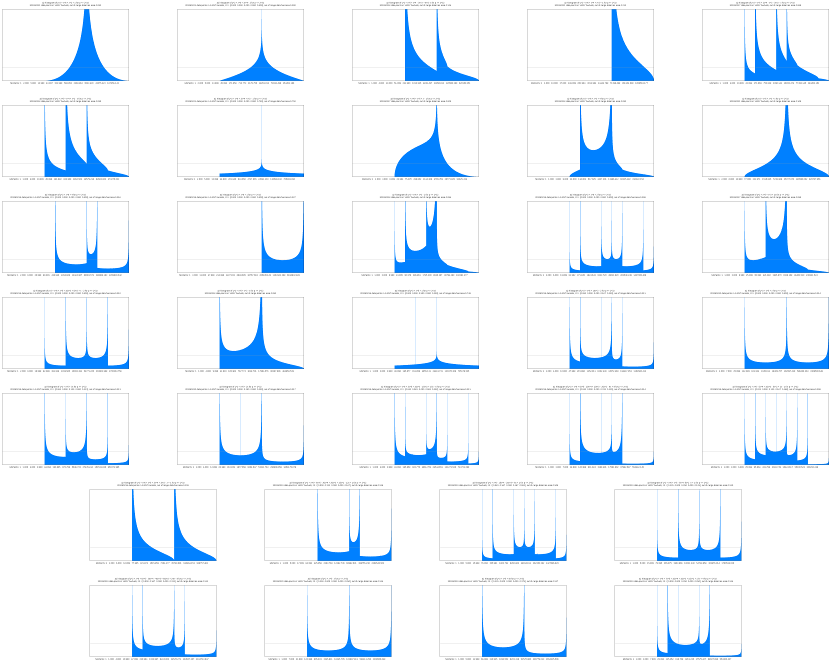
click histogram to animate (requires adobe reader)



click histogram to animate (requires adobe reader)

Exceptional distributions for abelian surfaces over $\mathbb{Q}$:





L-polynomials of Abelian varieties

Let A be an abelian variety of dimension $g \geq 1$ over a number field k, and let us fix a prime ℓ.

Let $\rho_\ell \colon G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ be the Galois representation arising from the action of $G_k := \mathrm{Gal}(\bar{k}/k)$ on the ℓ-adic Tate module

$$V_\ell(A) := \varprojlim A[\ell^n] \otimes \mathbb{Q}.$$

For each prime $\mathfrak{p}$ of good reduction for A we have the *L-polynomial*

$$L_\mathfrak{p}(T) := \det(1 - \rho_\ell(\mathrm{Frob}_\mathfrak{p})T),$$
$$\bar{L}_\mathfrak{p}(T) := L_\mathfrak{p}(T/\sqrt{\|\mathfrak{p}\|}) = \sum a_i T^i.$$

When A is the Jacobian of a genus g curve C, this agrees with our earlier definition of $L_\mathfrak{p}(T)$ as the numerator of the zeta function $Z_\mathfrak{p}(T)$.

The Sato-Tate problem for an abelian variety

The $\bar{L}_{\mathfrak{p}} \in \mathbb{R}[T]$ are monic, symmetric, unitary polynomials of degree $2g$.

Every such polynomial arises as the characteristic polynomial of a conjugacy class in the unitary symplectic group $\mathrm{USp}(2g)$.

Each probability measure on $\mathrm{USp}(2g)$ determines a distribution of conjugacy classes (hence a distribution of characteristic polynomials).

The *Sato-Tate problem*, in its simplest form, is to find a measure for which these classes are equidistributed.

Conjecturally, such a measure arises as the Haar measure of a compact subgroup ST_A of $\mathrm{USp}(2g)$.

The Sato-Tate group

Recall that the action of G_k on $V_\ell(A)$ induces the representation

$$\rho_\ell \colon G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}_\ell).$$

Let $G_\ell^{1,\mathsf{zar}}$ denote the kernel of the similitude character of $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ on the Zariski closure of $\rho_\ell(G_k)$. Now fix $\iota \colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, and define ST_A to be a maximal compact subgroup of the image $G_\ell^{1,\mathsf{zar}}$ under

$$\mathrm{Sp}_{2g}(\mathbb{Q}_\ell) \xrightarrow{\otimes_\iota \mathbb{C}} \mathrm{Sp}_{2g}(\mathbb{C}).$$

Conjecturally, ST_A does not depend on ℓ or ι; this is known for $g \leq 3$.

Definition [Serre]

$\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ is the *Sato-Tate group* of A.

The refined Sato-Tate conjecture

Let $s(\mathfrak{p})$ denote the conjugacy class of the image of $\mathrm{Frob}_{\mathfrak{p}}$ in ST_A.

Let μ_{ST_A} denote the image of the Haar measure on $\mathrm{Conj}(\mathrm{ST}_A)$, which does not depend on the choice of ℓ or ι.

Conjecture

The conjugacy classes $s(\mathfrak{p})$ are equidistributed with respect to μ_{ST_A}.

In particular, the distribution of $\bar{L}_{\mathfrak{p}}(T)$ matches the distribution of characteristic polynomials of random matrices in ST_A.

We can test this numerically by comparing statistics of the coefficients $a_1, \ldots, a_g$ of $\bar{L}_{\mathfrak{p}}(T)$ over $\|\mathfrak{p}\| \leq N$ to the predictions given by μ_{ST_A}.

`https://hensel.mit.edu:8000/home/pub/6`

The Sato-Tate axioms

The Sato-Tate axioms for abelian varieties (weight-1 motives):

1. G is closed subgroup of $\mathrm{USp}(2g)$.
2. **Hodge condition**: G contains a Hodge circle[1] whose conjugates generate a dense subset of G.
3. **Rationality condition**: for each component H of G and each irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$.

For any fixed g, the set of subgroups $G \subseteq \mathrm{USp}(2g)$ that satisfy the *Sato-Tate axioms* is **finite** up to conjugacy (3 for $g = 1$, 55 for $g = 2$).

[1] An embedding $\theta\colon \mathrm{U}(1) \to G^0$ where $\theta(u)$ has eigenvalues u, u^{-1} with multiplicity g.

The Sato-Tate axioms

The Sato-Tate axioms for abelian varieties (weight-1 motives):

1. G is closed subgroup of $\mathrm{USp}(2g)$.
2. **Hodge condition**: G contains a Hodge circle[1] whose conjugates generate a dense subset of G.
3. **Rationality condition**: for each component H of G and each irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$.

For any fixed g, the set of subgroups $G \subseteq \mathrm{USp}(2g)$ that satisfy the *Sato-Tate axioms* is **finite** up to conjugacy (3 for $g = 1$, 55 for $g = 2$).

Theorem

For $g \leq 3$, the group ST_A satisfies the Sato-Tate axioms.

This is expected to hold for all g.

[1] An embedding $\theta\colon \mathrm{U}(1) \to G^0$ where $\theta(u)$ has eigenvalues u, u^{-1} with multiplicity g.

Galois endomorphism modules

Let A be an abelian variety defined over a number field k.
Let K be the minimal extension of k in $\bar{k}$ for which $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$.
$\mathrm{Gal}(K/k)$ acts on the $\mathbb{R}$-algebra $\mathrm{End}(A_K)_{\mathbb{R}} := \mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

Definition

The *Galois (endomorphism module) type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$, where $[G, E] \simeq [G', E']$ iff there are isomorphisms $G \simeq G'$ and $E \simeq E'$ that are compatible with the Galois action.

Galois endomorphism modules

Let A be an abelian variety defined over a number field k.
Let K be the minimal extension of k in $\bar{k}$ for which $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$.
$\mathrm{Gal}(K/k)$ acts on the $\mathbb{R}$-algebra $\mathrm{End}(A_K)_{\mathbb{R}} := \mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

Definition

The *Galois (endomorphism module) type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$, where $[G, E] \simeq [G', E']$ iff there are isomorphisms $G \simeq G'$ and $E \simeq E'$ that are compatible with the Galois action.

Theorem [FKRS 2012]

For abelian varieties A/k of dimension $g \leq 3$ there is a one-to-one correspondence between Sato-Tate groups and Galois types.

More precisely, the identity component ST_A^0 is determined by $\mathrm{End}(A_K)_{\mathbb{R}}$, and there is a natural isomorphism $\mathrm{ST}_A/\mathrm{ST}_A^0 \simeq \mathrm{Gal}(K/k)$.

Real endomorphism algebras of abelian surfaces

abelian surface	$\mathbf{End}(A_K)_\mathbb{R}$	$\mathbf{ST}_A^0$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1)_2$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2)_2$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1)$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2)$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2)$
generic abelian surface	$\mathbb{R}$	$\mathrm{USp}(4)$

(factors in products are assumed to be non-isogenous)

Sato-Tate groups in dimension 2

Theorem [Fité-Kedlaya-Rotger-S 2012]

Up to conjugacy, 55 subgroups of $\mathrm{USp}(4)$ satisfy the Sato-Tate axioms:

$$\begin{array}{rl}
\mathrm{U}(1)_2\colon & C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, \\
& J(C_1), J(C_2), J(C_3), J(C_4), J(C_6), \\
& J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O), \\
& C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1 \\
\mathrm{SU}(2)_2\colon & E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6) \\
\mathrm{U}(1)\times\mathrm{U}(1)\colon & F, F_a, F_c, F_{a,b}, F_{ab}, F_{ac}, F_{ab,c}, F_{a,b,c} \\
\mathrm{U}(1)\times\mathrm{SU}(2)\colon & \mathrm{U}(1)\times\mathrm{SU}(2),\ N(\mathrm{U}(1)\times\mathrm{SU}(2)) \\
\mathrm{SU}(2)\times\mathrm{SU}(2)\colon & \mathrm{SU}(2)\times\mathrm{SU}(2),\ N(\mathrm{SU}(2)\times\mathrm{SU}(2)) \\
\mathrm{USp}(4)\colon & \mathrm{USp}(4)
\end{array}$$

Sato-Tate groups in dimension 2

Theorem [Fité-Kedlaya-Rotger-S 2012]

Up to conjugacy, 55 subgroups of $\mathrm{USp}(4)$ satisfy the Sato-Tate axioms:

$$\begin{array}{rl} \mathrm{U}(1)_2: & C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, \\ & J(C_1), J(C_2), J(C_3), J(C_4), J(C_6), \\ & J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O), \\ & C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1 \\ \mathrm{SU}(2)_2: & E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6) \\ \mathrm{U}(1)\times\mathrm{U}(1): & F, F_a, F_c, F_{a,b}, F_{ab}, F_{ac}, F_{ab,c}, F_{a,b,c} \\ \mathrm{U}(1)\times\mathrm{SU}(2): & \mathrm{U}(1)\times\mathrm{SU}(2),\ N(\mathrm{U}(1)\times\mathrm{SU}(2)) \\ \mathrm{SU}(2)\times\mathrm{SU}(2): & \mathrm{SU}(2)\times\mathrm{SU}(2),\ N(\mathrm{SU}(2)\times\mathrm{SU}(2)) \\ \mathrm{USp}(4): & \mathrm{USp}(4) \end{array}$$

Of these, exactly 52 arise as ST_A for an abelian surface A (34 over $\mathbb{Q}$).

Sato-Tate groups in dimension 2

Theorem [Fité-Kedlaya-Rotger-S 2012]

Up to conjugacy, 55 subgroups of $\mathrm{USp}(4)$ satisfy the Sato-Tate axioms:

$$\begin{array}{rl}
\mathrm{U}(1)_2: & C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, \\
& J(C_1), J(C_2), J(C_3), J(C_4), J(C_6), \\
& J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O), \\
& C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1 \\
\mathrm{SU}(2)_2: & E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6) \\
\mathrm{U}(1)\times\mathrm{U}(1): & F, F_a, F_c, F_{a,b}, F_{ab}, F_{ac}, F_{ab,c}, F_{a,b,c} \\
\mathrm{U}(1)\times\mathrm{SU}(2): & \mathrm{U}(1)\times\mathrm{SU}(2),\ N(\mathrm{U}(1)\times\mathrm{SU}(2)) \\
\mathrm{SU}(2)\times\mathrm{SU}(2): & \mathrm{SU}(2)\times\mathrm{SU}(2),\ N(\mathrm{SU}(2)\times\mathrm{SU}(2)) \\
\mathrm{USp}(4): & \mathrm{USp}(4)
\end{array}$$

Of these, exactly 52 arise as ST_A for an abelian surface A (34 over $\mathbb{Q}$).

This theorem says nothing about equidistribution, however this is now known in many special cases [FS 2012, Johansson 2013].

Sato-Tate groups in dimension 2 with $G^0 = \mathrm{U}(1)_2$.

d	c	G	G/G^0	z_1	z_2	$M[a_1^2]$	$M[a_2]$
1	1	C_1	C_1	0	$0, 0, 0, 0, 0$	$8, 96, 1280, 17920$	$4, 18, 88, 454$
1	2	C_2	C_2	1	$0, 0, 0, 0, 0$	$4, 48, 640, 8960$	$2, 10, 44, 230$
1	3	C_3	C_3	0	$0, 0, 0, 0, 0$	$4, 36, 440, 6020$	$2, 8, 34, 164$
1	4	C_4	C_4	1	$0, 0, 0, 0, 0$	$4, 36, 400, 5040$	$2, 8, 32, 150$
1	6	C_6	C_6	1	$0, 0, 0, 0, 0$	$4, 36, 400, 4900$	$2, 8, 32, 148$
1	4	D_2	D_2	3	$0, 0, 0, 0, 0$	$2, 24, 320, 4480$	$1, 6, 22, 118$
1	6	D_3	D_3	3	$0, 0, 0, 0, 0$	$2, 18, 220, 3010$	$1, 5, 17, 85$
1	8	D_4	D_4	5	$0, 0, 0, 0, 0$	$2, 18, 200, 2520$	$1, 5, 16, 78$
1	12	D_6	D_6	7	$0, 0, 0, 0, 0$	$2, 18, 200, 2450$	$1, 5, 16, 77$
1	2	$J(C_1)$	C_2	1	$1, 0, 0, 0, 0$	$4, 48, 640, 8960$	$1, 11, 40, 235$
1	4	$J(C_2)$	D_2	3	$1, 0, 0, 0, 1$	$2, 24, 320, 4480$	$1, 7, 22, 123$
1	6	$J(C_3)$	C_6	3	$1, 0, 0, 2, 0$	$2, 18, 220, 3010$	$1, 5, 16, 85$
1	8	$J(C_4)$	$\mathrm{C}_4 \times \mathrm{C}_2$	5	$1, 0, 2, 0, 1$	$2, 18, 200, 2520$	$1, 5, 16, 79$
1	12	$J(C_6)$	$\mathrm{C}_6 \times \mathrm{C}_2$	7	$1, 2, 0, 2, 1$	$2, 18, 200, 2450$	$1, 5, 16, 77$
1	8	$J(D_2)$	$\mathrm{D}_2 \times \mathrm{C}_2$	7	$1, 0, 0, 0, 3$	$1, 12, 160, 2240$	$1, 5, 13, 67$
1	12	$J(D_3)$	D_6	9	$1, 0, 0, 2, 3$	$1, 9, 110, 1505$	$1, 4, 10, 48$
1	16	$J(D_4)$	$\mathrm{D}_4 \times \mathrm{C}_2$	13	$1, 0, 2, 0, 5$	$1, 9, 100, 1260$	$1, 4, 10, 45$
1	24	$J(D_6)$	$\mathrm{D}_6 \times \mathrm{C}_2$	19	$1, 2, 0, 2, 7$	$1, 9, 100, 1225$	$1, 4, 10, 44$
1	2	$C_{2,1}$	C_2	1	$0, 0, 0, 0, 1$	$4, 48, 640, 8960$	$3, 11, 48, 235$
1	4	$C_{4,1}$	C_4	3	$0, 0, 2, 0, 0$	$2, 24, 320, 4480$	$1, 5, 22, 115$
1	6	$C_{6,1}$	C_6	3	$0, 2, 0, 0, 1$	$2, 18, 220, 3010$	$1, 5, 18, 85$
1	4	$D_{2,1}$	D_2	3	$0, 0, 0, 0, 2$	$2, 24, 320, 4480$	$2, 7, 26, 123$
1	8	$D_{4,1}$	D_4	7	$0, 0, 2, 0, 2$	$1, 12, 160, 2240$	$1, 4, 13, 63$
1	12	$D_{6,1}$	D_6	9	$0, 2, 0, 0, 4$	$1, 9, 110, 1505$	$1, 4, 11, 48$
1	6	$D_{3,2}$	D_3	3	$0, 0, 0, 0, 3$	$2, 18, 220, 3010$	$2, 6, 21, 90$
1	8	$D_{4,2}$	D_4	5	$0, 0, 0, 0, 4$	$2, 18, 200, 2520$	$2, 6, 20, 83$
1	12	$D_{6,2}$	D_6	7	$0, 0, 0, 0, 6$	$2, 18, 200, 2450$	$2, 6, 20, 82$
1	12	T	A_4	3	$0, 0, 0, 0, 0$	$2, 12, 120, 1540$	$1, 4, 12, 52$
1	24	O	S_4	9	$0, 0, 0, 0, 0$	$2, 12, 100, 1050$	$1, 4, 11, 45$
1	24	O_1	S_4	15	$0, 0, 6, 0, 6$	$1, 6, 60, 770$	$1, 3, 8, 30$
1	24	$J(T)$	$\mathrm{A}_4 \times \mathrm{C}_2$	15	$1, 0, 0, 8, 3$	$1, 6, 60, 770$	$1, 3, 7, 29$
1	48	$J(O)$	$\mathrm{S}_4 \times \mathrm{C}_2$	33	$1, 0, 6, 8, 9$	$1, 6, 50, 525$	$1, 3, 7, 26$

Sato-Tate groups in dimension 2 with $G^0 \neq \mathrm{U}(1)_2$.

d	c	G	G/G^0	z_1	z_2	$M[a_1^2]$	$M[a_2]$
3	1	E_1	C_1	0	$0, 0, 0, 0, 0$	$4, 32, 320, 3584$	$3, 10, 37, 150$
3	2	E_2	C_2	1	$0, 0, 0, 0, 0$	$2, 16, 160, 1792$	$1, 6, 17, 78$
3	3	E_3	C_3	0	$0, 0, 0, 0, 0$	$2, 12, 110, 1204$	$1, 4, 13, 52$
3	4	E_4	C_4	1	$0, 0, 0, 0, 0$	$2, 12, 100, 1008$	$1, 4, 11, 46$
3	6	E_6	C_6	1	$0, 0, 0, 0, 0$	$2, 12, 100, 980$	$1, 4, 11, 44$
3	2	$J(E_1)$	C_2	1	$0, 0, 0, 0, 0$	$2, 16, 160, 1792$	$2, 6, 20, 78$
3	4	$J(E_2)$	D_2	3	$0, 0, 0, 0, 0$	$1, 8, 80, 896$	$1, 4, 10, 42$
3	6	$J(E_3)$	D_3	3	$0, 0, 0, 0, 0$	$1, 6, 55, 602$	$1, 3, 8, 29$
3	8	$J(E_4)$	D_4	5	$0, 0, 0, 0, 0$	$1, 6, 50, 504$	$1, 3, 7, 26$
3	12	$J(E_6)$	D_6	7	$0, 0, 0, 0, 0$	$1, 6, 50, 490$	$1, 3, 7, 25$
2	1	F	C_1	0	$0, 0, 0, 0, 0$	$4, 36, 400, 4900$	$2, 8, 32, 148$
2	2	F_a	C_2	0	$0, 0, 0, 0, 1$	$3, 21, 210, 2485$	$2, 6, 20, 82$
2	2	F_c	C_2	1	$0, 0, 0, 0, 0$	$2, 18, 200, 2450$	$1, 5, 16, 77$
2	2	F_{ab}	C_2	1	$0, 0, 0, 0, 1$	$2, 18, 200, 2450$	$2, 6, 20, 82$
2	4	F_{ac}	C_4	3	$0, 0, 2, 0, 1$	$1, 9, 100, 1225$	$1, 3, 10, 41$
2	4	$F_{a,b}$	D_2	1	$0, 0, 0, 0, 3$	$2, 12, 110, 1260$	$2, 5, 14, 49$
2	4	$F_{ab,c}$	D_2	3	$0, 0, 0, 0, 1$	$1, 9, 100, 1225$	$1, 4, 10, 44$
2	8	$F_{a,b,c}$	D_4	5	$0, 0, 2, 0, 3$	$1, 6, 55, 630$	$1, 3, 7, 26$
4	1	G_4	C_1	0	$0, 0, 0, 0, 0$	$3, 20, 175, 1764$	$2, 6, 20, 76$
4	2	$N(G_4)$	C_2	0	$0, 0, 0, 0, 1$	$2, 11, 90, 889$	$2, 5, 14, 46$
6	1	G_6	C_1	0	$0, 0, 0, 0, 0$	$2, 10, 70, 588$	$2, 5, 14, 44$
6	2	$N(G_6)$	C_2	1	$0, 0, 0, 0, 0$	$1, 5, 35, 294$	$1, 3, 7, 23$
10	1	$\mathrm{USp}(4)$	C_1	0	$0, 0, 0, 0, 0$	$1, 3, 14, 84$	$1, 2, 4, 10$

Genus 2 curves realizing Sato-Tate groups with $G^0 = \mathrm{U}(1)_2$

Group	Curve $y^2 = f(x)$	k	K
C_1	$x^6 + 1$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-3})$
C_2	$x^5 - x$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(i, \sqrt{2})$
C_3	$x^6 + 4$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$
C_4	$x^6 + x^5 - 5x^4 - 5x^2 - x + 1$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-2}, a)$; $a^4 + 17a^2 + 68 = 0$
C_6	$x^6 + 2$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{2})$
D_2	$x^5 + 9x$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$
D_3	$x^6 + 10x^3 - 2$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{-2})$
D_4	$x^5 + 3x$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(i, \sqrt{2}, \sqrt[4]{3})$
D_6	$x^6 + 3x^5 + 10x^3 - 15x^2 + 15x - 6$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(i, \sqrt{2}, \sqrt{3}, a)$; $a^3 + 3a - 2 = 0$
T	$x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-2}, a, b)$;
			$a^3 - 7a + 7 = b^4 + 4b^2 + 8b + 8 = 0$
O	$x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-2}, \sqrt{-11}, a, b)$;
			$a^3 - 4a + 4 = b^4 + 22b + 22 = 0$
$J(C_1)$	$x^5 - x$	$\mathbb{Q}(i)$	$\mathbb{Q}(i, \sqrt{2})$
$J(C_2)$	$x^5 - x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2})$
$J(C_3)$	$x^6 + 10x^3 - 2$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{-2})$
$J(C_4)$	$x^6 + x^5 - 5x^4 - 5x^2 - x + 1$	$\mathbb{Q}$	see entry for C_4
$J(C_6)$	$x^6 - 15x^4 - 20x^3 + 6x + 1$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{3}, a)$; $a^3 + 3a^2 - 1 = 0$
$J(D_2)$	$x^5 + 9x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$
$J(D_3)$	$x^6 + 10x^3 - 2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{-2})$
$J(D_4)$	$x^5 + 3x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2}, \sqrt[4]{3})$
$J(D_6)$	$x^6 + 3x^5 + 10x^3 - 15x^2 + 15x - 6$	$\mathbb{Q}$	see entry for D_6
$J(T)$	$x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$	$\mathbb{Q}$	see entry for T
$J(O)$	$x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$	$\mathbb{Q}$	see entry for O
$C_{2,1}$	$x^6 + 1$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$
$C_{4,1}$	$x^5 + 2x$	$\mathbb{Q}(i)$	$\mathbb{Q}(i, \sqrt[4]{2})$
$C_{6,1}$	$x^6 + 6x^5 - 30x^4 + 20x^3 + 15x^2 - 12x + 1$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, a)$; $a^3 - 3a + 1 = 0$
$D_{2,1}$	$x^5 + x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2})$
$D_{4,1}$	$x^5 + 2x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt[4]{2})$
$D_{6,1}$	$x^6 + 6x^5 - 30x^4 - 40x^3 + 60x^2 + 24x - 8$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-2}, \sqrt{-3}, a)$; $a^3 - 9a + 6 = 0$
$D_{3,2}$	$x^6 + 4$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$
$D_{4,2}$	$x^6 + x^5 + 10x^3 + 5x^2 + x - 2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-2}, a)$; $a^4 - 14a^2 + 28a - 14 = 0$
$D_{6,2}$	$x^6 + 2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{2})$
O_1	$x^6 + 7x^5 + 10x^4 + 10x^3 + 15x^2 + 17x + 4$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-2}, a, b)$;
			$a^3 + 5a + 10 = b^4 + 4b^2 + 8b + 2 = 0$

Genus 2 curves realizing Sato-Tate groups with $G^0 \neq \mathrm{U}(1)_2$

Group	Curve $y^2 = f(x)$	k	K
F	$x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}(i, \sqrt{2})$	$\mathbb{Q}(i, \sqrt{2})$
F_a	$x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}(i)$	$\mathbb{Q}(i, \sqrt{2})$
F_{ab}	$x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(i, \sqrt{2})$
F_{ac}	$x^5 + 1$	$\mathbb{Q}$	$\mathbb{Q}(a)$; $a^4 + 5a^2 + 5 = 0$
$F_{a,b}$	$x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2})$
E_1	$x^6 + x^4 + x^2 + 1$	$\mathbb{Q}$	$\mathbb{Q}$
E_2	$x^6 + x^5 + 3x^4 + 3x^2 - x + 1$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{2})$
E_3	$x^5 + x^4 - 3x^3 - 4x^2 - x$	$\mathbb{Q}$	$\mathbb{Q}(a)$; $a^3 - 3a + 1 = 0$
E_4	$x^5 + x^4 + x^2 - x$	$\mathbb{Q}$	$\mathbb{Q}(a)$; $a^4 - 5a^2 + 5 = 0$
E_6	$x^5 + 2x^4 - x^3 - 3x^2 - x$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{7}, a)$; $a^3 - 7a - 7 = 0$
$J(E_1)$	$x^5 + x^3 + x$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$J(E_2)$	$x^5 + x^3 - x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2})$
$J(E_3)$	$x^6 + x^3 + 4$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$
$J(E_4)$	$x^5 + x^3 + 2x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt[4]{2})$
$J(E_6)$	$x^6 + x^3 - 2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{-2})$
$G_{1,3}$	$x^6 + 3x^4 - 2$	$\mathbb{Q}(i)$	$\mathbb{Q}(i)$
$N(G_{1,3})$	$x^6 + 3x^4 - 2$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$G_{3,3}$	$x^6 + x^2 + 1$	$\mathbb{Q}$	$\mathbb{Q}$
$N(G_{3,3})$	$x^6 + x^5 + x - 1$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$\mathrm{USp}(4)$	$x^5 - x + 1$	$\mathbb{Q}$	$\mathbb{Q}$

Part Two

Searching for curves

We surveyed the $\bar{L}$-polynomial distributions of genus 2 curves

$$y^2 = x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$$

$$y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$$

with integer coefficients $|c_i| \leq 128$. More than 2^{48} curves.

We found over 10 million non-isomorphic curves with exceptional distributions, including at least 3 apparent matches for each of the 34 Sato-Tate groups that can occur over $\mathbb{Q}$.

Representative examples were computed to high precision $N = 2^{30}$.

For each example, the field K was then determined, allowing the Galois type, and hence the Sato-Tate group, to be **provably** identified.

Exhibiting Sato-Tate groups of abelian surfaces

The 34 Sato-Tate groups that can arise for an abelian surface over $\mathbb{Q}$ are all realized by Jacobians of genus 2 curves.

By extending the base field from $\mathbb{Q}$ to a suitable subfield k of K, we can restrict $G/G^0 \simeq \mathrm{Gal}(K/k)$ to any normal subgroup of $\mathrm{Gal}(K/k)$ (base extension does not change the identity component G^0).

This allows us to realize all 52 Sato-Tate groups using base extensions of 34 curves defined over $\mathbb{Q}$ (in fact, 9 suffice).

Serre asks: can all 52 can be realized over a single base field k?

Exhibiting Sato-Tate groups of abelian surfaces

The 34 Sato-Tate groups that can arise for an abelian surface over $\mathbb{Q}$ are all realized by Jacobians of genus 2 curves.

By extending the base field from $\mathbb{Q}$ to a suitable subfield k of K, we can restrict $G/G^0 \simeq \mathrm{Gal}(K/k)$ to any normal subgroup of $\mathrm{Gal}(K/k)$ (base extension does not change the identity component G^0).

This allows us to realize all 52 Sato-Tate groups using base extensions of 34 curves defined over $\mathbb{Q}$ (in fact, 9 suffice).

Serre asks: can all 52 can be realized over a single base field k?

Theorem (Fité-Guitart 2015)

All 52 possible Sato-Tate groups arise for abelian surfaces defined over

$$k := \mathbb{Q}(\sqrt{-10}, \sqrt{-51}, \sqrt{-163}, \sqrt{-67}, \sqrt{817}, \sqrt{-57}).$$

Computing zeta functions

Algorithms to compute $L_p(T)$ for low genus hyperelliptic curves

	complexity (ignoring factors of $O(\log\log p)$)		
algorithm	$g=1$	$g=2$	$g=3$
point enumeration	$p\log p$	$p^2\log p$	$p^3\log p$
group computation	$p^{1/4}\log p$	$p^{3/4}\log p$	$p^{5/4}\log p$
p-adic cohomology	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$
CRT (Schoof-Pila)	$\log^5 p$	$\log^8 p$	$\log^{12} p$

Computing zeta functions

Algorithms to compute $L_p(T)$ for low genus hyperelliptic curves

	complexity (ignoring factors of $O(\log\log p)$)		
algorithm	$g = 1$	$g = 2$	$g = 3$
point enumeration	$p \log p$	$p^2 \log p$	$p^3 \log p$
group computation	$p^{1/4} \log p$	$p^{3/4} \log p$	$p^{5/4} \log p$
p-adic cohomology	$p^{1/2} \log^2 p$	$p^{1/2} \log^2 p$	$p^{1/2} \log^2 p$
CRT (Schoof-Pila)	$\log^5 p$	$\log^8 p$	$\log^{12} p$

(see [Kedlaya-S 2008]).

An average polynomial-time algorithm

All of these methods perform separate computations for each p.
But we want to compute $L_p(T)$ for all good $p \leq N$ using reductions of *the same curve* in each case. Can we take advantage of this?

An average polynomial-time algorithm

All of these methods perform separate computations for each p.
But we want to compute $L_p(T)$ for all good $p \le N$ using reductions of *the same curve* in each case. Can we take advantage of this?

Theorem (Harvey 2012)

There exists a deterministic algorithm that, given a hyperelliptic curve $y^2 = f(x)$ of genus g with a rational Weierstrass point and an integer N, computes $L_p(T)$ for all good primes $p \le N$ in time

$$O\big(g^{8+\epsilon} N \log^{3+\epsilon} N\big),$$

assuming the coefficients of $f \in \mathbb{Z}[x]$ have size bounded by $O(\log N)$.

Average time is $O\big(g^{8+\epsilon} \log^{4+\epsilon} N\big)$ per prime, polynomial in g and $\log p$.
Recently generalized to arithmetic schemes.

An average polynomial-time algorithm

	complexity (ignoring factors of $O(\log\log p)$)		
algorithm	$g=1$	$g=2$	$g=3$
point enumeration	$p\log p$	$p^2\log p$	$p^3\log p$
group computation	$p^{1/4}\log p$	$p^{3/4}\log p$	$p^{5/4}\log p$
p-adic cohomology	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$
CRT (Schoof-Pila)	$\log^5 p$	$\log^8 p$	$\log^{12} p$
Average polytime	$\log^4 p$	$\log^4 p$	$\log^4 p$

But is it practical?

The Hasse-Witt matrix of a hyperelliptic curve

The *Hasse-Witt* matrix of a hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_p$ of genus g is the $g \times g$ matrix $W_p = [w_{ij}]$ with entries

$$w_{ij} = f_{pi-j}^{(p-1)/2} \bmod p \qquad (1 \le i, j \le g).$$

The w_{ij} can each be computed using recurrence relations between the coefficients of f^n and those of f^{n-1}.

The congruence

$$L_P(T) \equiv \det(I - TW_p) \bmod p$$

allows us to determine the coefficients $a_1, \ldots, a_g$ of $L_p(T)$ modulo p. This is enough to compute $\#C_p(\mathbb{F}_p)$ for $p > 16g^2$.

The Hasse-Witt matrix of a hyperelliptic curve

The *Hasse-Witt* matrix of a hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_p$ of genus g is the $g \times g$ matrix $W_p = [w_{ij}]$ with entries

$$w_{ij} = f_{pi-j}^{(p-1)/2} \bmod p \qquad (1 \le i, j \le g).$$

The w_{ij} can each be computed using recurrence relations between the coefficients of f^n and those of f^{n-1}.

The congruence

$$L_P(T) \equiv \det(I - TW_p) \bmod p$$

allows us to determine the coefficients $a_1, \ldots, a_g$ of $L_p(T)$ modulo p. This is enough to compute $\#C_p(\mathbb{F}_p)$ for $p > 16g^2$.

The algorithm can be extended to compute $L_p(T)$ modulo higher powers of p (and thereby obtain $L_p \in \mathbb{Z}[T]$), but for $g \le 3$ it's easier to derive $L_p(T)$ from $L_p(T) \bmod p$ using computations in $\mathrm{Jac}(C)$.

Complexity

Theorem (Harvey-S 2014)

Given a hyperelliptic curve $y^2 = f(x)$ of genus g, and an integer N, one can compute the Hasse-Witt matrices W_p for all good primes $p \le N$ in

$$O\big(g^3 N \log^3 N \log\log N\big) \text{ time} \qquad \text{and} \qquad O(g^2 N) \text{ space},$$

assuming g and the bit-size of each coefficient of f are $O(\log N)$.

The complexity is close to optimal (nearly quasi-linear in output size).

Extends to computing $L_p \in \mathbb{Z}[T]$ in $O(g^{4+\epsilon} N \log^{3+\epsilon} N)$ time.

In progress: smooth plane quartics.

	genus 2		genus 3	
N	`smalljac`	`hwlpoly`	`hypellfrob`	`hwlpoly`
2^{14}	0.2	0.1	7.2	0.4
2^{15}	0.6	0.3	16.3	1.0
2^{16}	1.7	0.9	39.1	2.9
2^{17}	5.5	2.2	98.3	7.8
2^{18}	19.2	5.3	255	18.3
2^{19}	78.4	12.5	695	43.2
2^{20}	271	27.8	1950	98.8
2^{21}	1120	64.5	5600	229
2^{22}	2820	155	16700	537
2^{23}	9840	357	51200	1240
2^{24}	31900	823	158000	2800
2^{25}	105000	1890	501000	6280
2^{26}	349000	4250	1480000	13900
2^{27}	1210000	9590	4360000	31100
2^{28}	4010000	21200	12500000	69700
2^{29}	13200000	48300	39500000	155000
2^{30}	45500000	108000	120000000	344000

(Intel Xeon E5-2697v2 2.7 GHz CPU seconds).

Naïve approach

For each good prime $p < N$ we want to compute the entries

$$w_{ij} = f_{pi-j}^{(p-1)/2} \bmod p \qquad (1 \leq i,\ j \leq g).$$

of the Hasse-Witt matrix $W_p = [w_{ij}]$.

So we could iteratively compute $f, f^2, f^3, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$ and just reduce the x^{pi-j} coefficients of $f(x)^{(p-1)/2}$ mod p for each prime $p \leq N$.

Naïve approach

For each good prime $p < N$ we want to compute the entries

$$w_{ij} = f_{pi-j}^{(p-1)/2} \bmod p \qquad (1 \leq i,\ j \leq g).$$

of the Hasse-Witt matrix $W_p = [w_{ij}]$.

So we could iteratively compute $f, f^2, f^3, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$ and just reduce the x^{pi-j} coefficients of $f(x)^{(p-1)/2}$ mod p for each prime $p \leq N$.

But the polynomials f^n are huge, each has $\Omega(n^2)$ bits.
It would take $\Omega(N^3)$ time to compute $f, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$.

So this is a terrible idea...

Naïve approach

For each good prime $p < N$ we want to compute the entries

$$w_{ij} = f_{pi-j}^{(p-1)/2} \bmod p \qquad (1 \le i,\ j \le g).$$

of the Hasse-Witt matrix $W_p = [w_{ij}]$.

So we could iteratively compute $f, f^2, f^3, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$ and just reduce the x^{pi-j} coefficients of $f(x)^{(p-1)/2}$ mod p for each prime $p \le N$.

But the polynomials f^n are huge, each has $\Omega(n^2)$ bits.
It would take $\Omega(N^3)$ time to compute $f, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$.

So this is a terrible idea...

But we don't need all the coefficients of f^n, we only need one,
and we only need to know its value modulo $p = 2n + 1$.

A better approach

For any integer $n \geq 0$ the equations

$$f^{n+1} = f \cdot f^n \qquad \text{and} \qquad (f^{n+1})' = (n+1) f' f^n$$

yield the relations

$$f_k^{n+1} = \sum_{j=0}^{d} f_j f_{k-j}^n \qquad \text{and} \qquad k f_k^{n+1} = (n+1) \sum_{j=0}^{d} j f_j f_{k-j}^n,$$

where f_k^n denotes the coefficient of x^k in f^n. Subtracting k times the first from the second and solving for f_k^n yields the identity

$$f_k^n = \frac{1}{k f_0} \sum_{j=1}^{d} (nj + j - k) f_j f_{k-j}^n, \tag{1}$$

which is valid for all positive integers k and n (assuming $f_0 \neq 0$).

If we now define

$$v_k^n := [f_{k-d+1}^n, \ldots, f_k^n] \in \mathbb{Z}^d,$$

then the last g entries of $v_{p-1}^{(p-1)/2} \bmod p$ form the first row of W_p, and

$$f_k^n \equiv \frac{1}{2kf_0} \sum_{j=1}^{d} (j-2k) f_j f_{k-j}^n \bmod p,$$

holds for $k \leq p-1 = 2n$. Starting from $v_0^n = [0, \ldots, 0, f_0^n]$, we compute

$$v_{p-1}^n \equiv \frac{v_0^n}{2^{p-1}(p-1)! f_0^{p-1}} \prod_{k=1}^{p-1} M_k \equiv -v_0^n \prod_{i=1}^{p-1} M_k \bmod p,$$

where the $d \times d$ matrices

$$M_k := \begin{bmatrix} 0 & \cdots & 0 & (d-2k)f_d \\ 2kf_0 & \cdots & 0 & (d-1-2k)f_{d-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 2kf_0 & (1-2k)f_1 \end{bmatrix}$$

do not depend on p!

Computing a sequence of reduced partial products

Computing the first row of W_p for all $p < N$ reduces to compute the sequence of reduced partial products

$$\begin{aligned} M_1 M_2 \bmod 3 \\ M_1 M_2 M_3 M_4 \bmod 5 \\ M_1 M_2 M_3 M_4 M_5 M_6 \bmod 7 \\ \vdots \\ M_1 M_2 M_3 M_4 M_5 M_6 \cdots M_{N-2} \bmod N-1 \end{aligned}$$

Doing this naïvely would take time quasi-quadratic in N.

But quasi-linear time is achieved with an *accumulating remainder tree*.

Accumulating remainder trees

Input: integer matrices $M_0, \ldots, M_{N-1}$ and moduli $m_0, \ldots, m_{N-1}$.

Output: $A_0, A_1, \ldots, A_{N-1}$, where $A_i := \prod_{j<i} M_j \bmod m_i$.

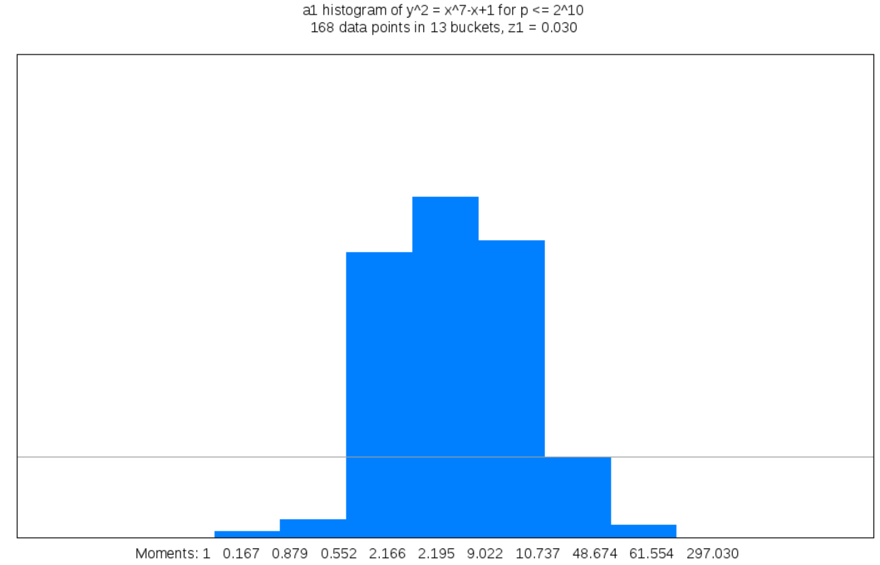
Algorithm:

1. If $N = 1$ then output $A_0 := 1$ and terminate (base case).
2. Use $M'_i := M_{2i} M_{2i+1}$ and $m'_i := m_{2i} m_{2i+1}$ to recursively compute $A'_1, \ldots, A'_{N/2}$.
3. Output

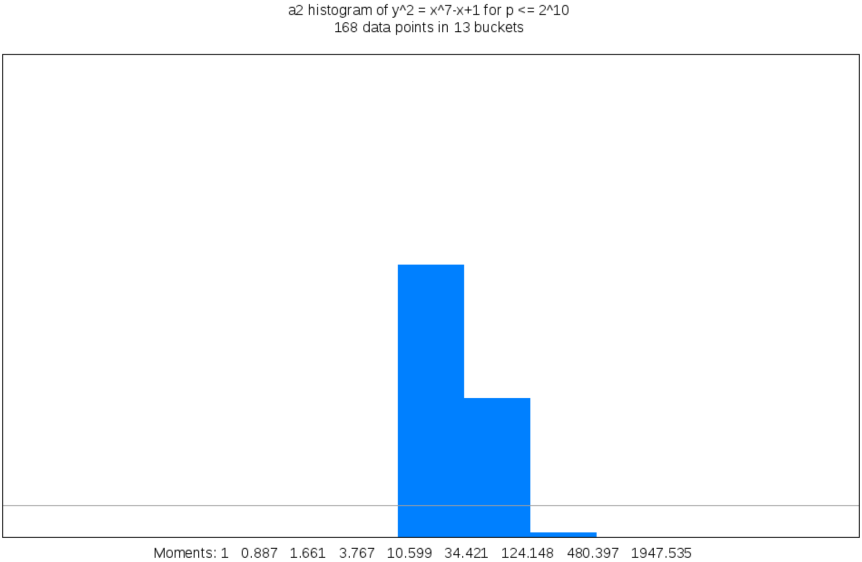
$$A_i := \begin{cases} A'_{i/2} \bmod m_i & i \text{ even;} \\ A'_{(i-1)/2} M_{i-1} \bmod m_i & i \text{ odd.} \end{cases}$$

Using FFT-multiplication, this runs in quasi-linear time.

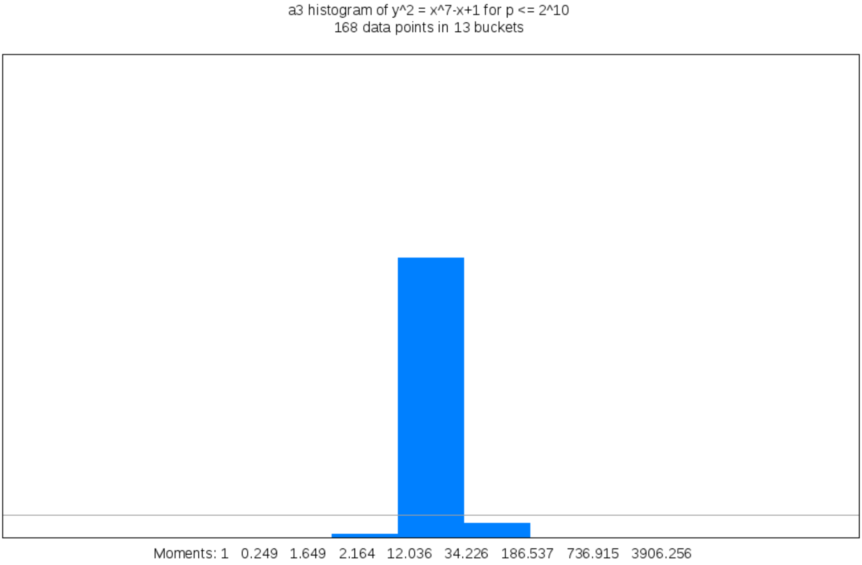
The space complexity can be improved using a *remainder forest*.



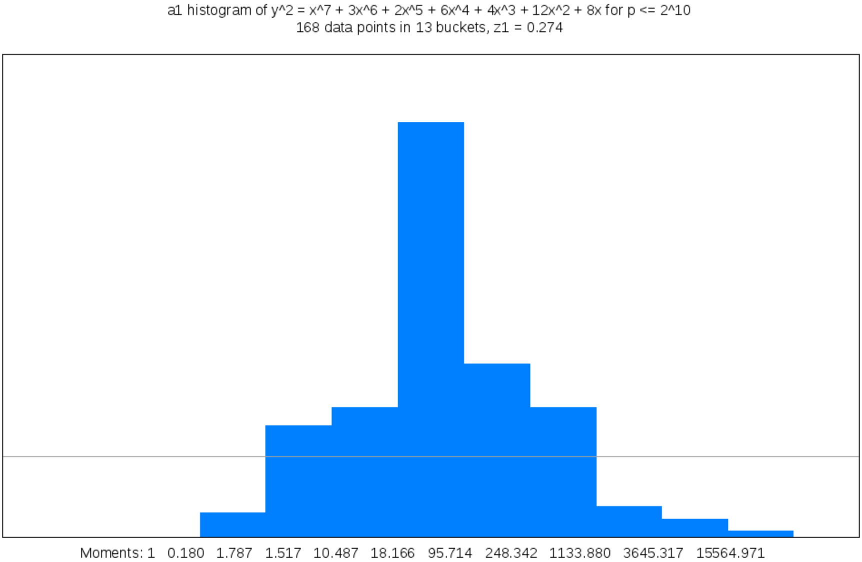
click histogram to animate (requires adobe reader)



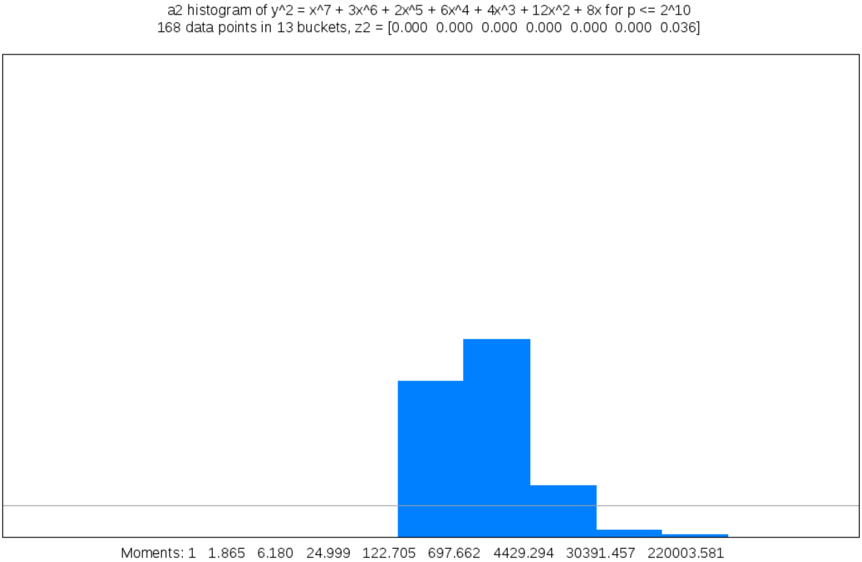
click histogram to animate (requires adobe reader)



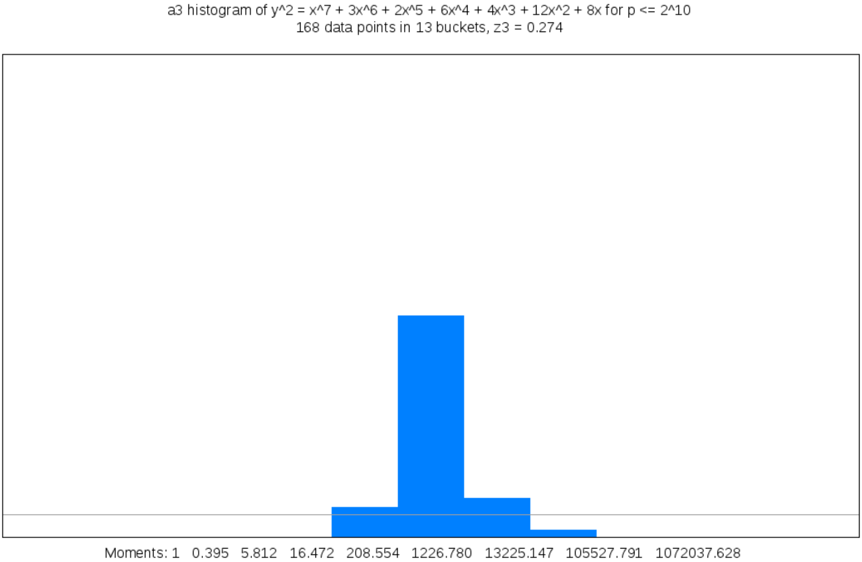
click histogram to animate (requires adobe reader)



click histogram to animate (requires adobe reader)



click histogram to animate (requires adobe reader)

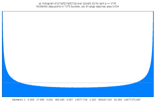


click histogram to animate (requires adobe reader)

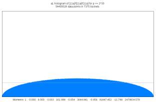
Real endomorphism algebras of abelian threefolds

abelian threefold	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}_A^0$
cube of a CM elliptic curve	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{U}(1)_3$
cube of a non-CM elliptic curve	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SU}(2)_3$
product of CM elliptic curve and square of CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1) \times \mathrm{U}(1)_2$
• product of CM elliptic curve and QM abelian surface • product of CM elliptic curve and square of non-CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$
product of non-CM elliptic curve and square of CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$
• product of non-CM elliptic curve and QM abelian surface • product of non-CM elliptic curve and square of non-CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$
• CM abelian threefold • product of CM elliptic curve and CM abelian surface • product of three CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$
• product of non-CM elliptic curve and CM abelian surface • product of non-CM elliptic curve and two CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$
• product of CM elliptic curve and RM abelian surface • product of CM elliptic curve and two non-CM elliptic curves	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
• RM abelian threefold • product of non-CM elliptic curve and RM abelian surface • product of 3 non-CM elliptic curves	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
product of CM elliptic curve and abelian surface	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{USp}(4)$
product of non-CM elliptic curve and abelian surface	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{USp}(4)$
quadratic CM abelian threefold	$\mathbb{C}$	$\mathrm{U}(3)$
generic abelian threefold	$\mathbb{R}$	$\mathrm{USp}(6)$

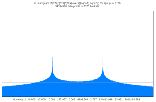
Connected Sato-Tate groups of abelian threefolds:



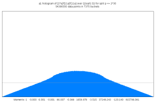
$\mathrm{U}(1)_3$



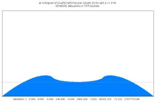
$\mathrm{SU}(2)_3$



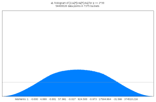
$\mathrm{U}(1) \times \mathrm{U}(1)_2$



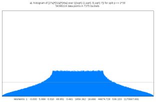
$\mathrm{U}(1) \times \mathrm{SU}(2)_2$



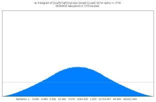
$\mathrm{SU}(2) \times \mathrm{U}(1)_2$



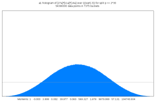
$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$



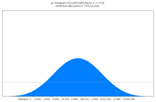
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$



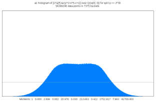
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$



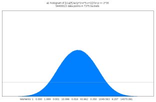
$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{U}(1)$



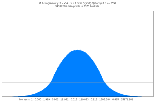
$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$



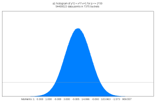
$\mathrm{U}(1) \times \mathrm{USp}(4)$



$\mathrm{SU}(2) \times \mathrm{USp}(4)$



$\mathrm{U}(3)$



$\mathrm{USp}(6)$

Partial classification of component groups

G_0	$G/G_0 \hookrightarrow$	$\lvert G/G_0 \rvert$ divides
$\mathrm{USp}(6)$	C_1	1
$\mathrm{U}(3)$	C_2	2
$\mathrm{SU}(2) \times \mathrm{USp}(4)$	C_1	1
$\mathrm{U}(1) \times \mathrm{USp}(4)$	C_2	2
$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	S_3	6
$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	D_2	4
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$	D_4	8
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathrm{C}_2 \wr \mathrm{S}_3$	48
$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$	$\mathrm{D}_4, \quad \mathrm{D}_6$	$8, \; 12$
$\mathrm{SU}(2) \times \mathrm{U}(1)_2$	$\mathrm{D}_6 \times \mathrm{C}_2, \quad \mathrm{S}_4 \times \mathrm{C}_2$	48
$\mathrm{U}(1) \times \mathrm{SU}(2)_2$	$\mathrm{D}_4 \times \mathrm{C}_2, \quad \mathrm{D}_6 \times \mathrm{C}_2$	$16, \; 24$
$\mathrm{U}(1) \times \mathrm{U}(1)_2$	$\mathrm{D}_6 \times \mathrm{C}_2 \times \mathrm{C}_2, \quad \mathrm{S}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$	96
$\mathrm{SU}(2)_3$	$\mathrm{D}_6, \quad \mathrm{S}_4$	24
$\mathrm{U}(1)_3$	$\cdots$	$336, \; 1728$

(disclaimer: this is work in progress subject to verification)