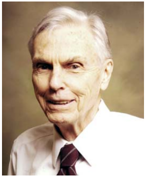
The Sato-Tate conjecture for abelian varieties

Andrew V. Sutherland

Massachusetts Institute of Technology

March 5, 2014

Mikio Sato



John Tate

Joint work with F. Fité, K.S. Kedlaya, and V. Rotger, and also with D. Harvey.

Sato-Tate in dimension 1

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

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

Let p be a prime of good reduction for E.
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 is an integer in $[-2\sqrt{p}, 2\sqrt{p}]$.

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.

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

Sato-Tate distributions in dimension 1

1. Typical case (no CM)

Elliptic curves $E/\mathbb{Q}$ w/o CM have the semi-circular trace distribution. (This is also known for E/k, where k is a totally real number field).

[Taylor et al.]

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]

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 normalized trace distribution of E converges to the distribution of traces in G given by Haar measure (the unique translation-invariant 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

For a smooth projective curve $C/\mathbb{Q}$ of genus g and each prime p of good redution for C we have the *zeta function*

$$Z(C_p/\mathbb{F}_p;T) := \exp\left(\sum_{k=1}^{\infty} N_k T^k/k\right),$$

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

$$Z(C_p/\mathbb{F}_p;T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

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

For $g=1$ we have $L_p(t) = pT^2 + c_1T + 1$, and for $g=2$,

$$L_p(T) = p^2T^4 + c_1pT^3 + c_2T^2 + c_1T + 1.$$

Normalized L-polynomials

The normalized polynomial

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

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

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

In this talk we will focus primarily on the case $g = 2$.

http://math.mit.edu/~drew

L-polynomials of Abelian varieties

Let A be an abelian variety of dimension $g \geq 1$ over a number field k.

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

$$V_\ell(A) := \varprojlim A[\ell^n].$$

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

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

In the case that 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 of C.

The Sato-Tate problem for an abelian variety

For each prime $\mathfrak{p}$ of k where A has good reduction, the polynomial $\bar{L}_{\mathfrak{p}} \in \mathbb{R}[T]$ is monic, symmetric, unitary, and 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 of an abelian variety

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

Let G_k^1 be the kernel of the cyclotomic character $\chi_\ell\colon G_k \to \mathbb{Q}_\ell^\times$.
Let $G_\ell^{1,\mathrm{Zar}}$ be the Zariski closure of $\rho_\ell(G_k^1)$ in $\mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$.
Choose $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, and let $G^1 = G_\ell^{1,\mathrm{Zar}} \otimes_\iota \mathbb{C} \subseteq \mathrm{Sp}_{2g}(\mathbb{C})$.

Definition [Serre]

$\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ is a maximal compact subgroup of $G^1 \subseteq \mathrm{Sp}_{2g}(\mathbb{C})$.
For each prime $\mathfrak{p}$ of good reduction for A, let $s(\mathfrak{p})$ denote the conjugacy class of $\rho_\ell(\mathrm{Frob}_\mathfrak{p})/\sqrt{\|\mathfrak{p}\|} \in G^1$ in ST_A.

Conjecturally, ST_A does not depend on ℓ or ι; this is known for $g \le 3$.
In any case, the characteristic polynomial of $s(\mathfrak{p})$ is always $\bar{L}_\mathfrak{p}(T)$.

Equidistribution

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 [Refined Sato-Tate]

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 $\|\mathfrak{p}\| \le N$ to the predictions given by μ_{ST_A}.

The Sato-Tate axioms for abelian varieties

1. G is closed.
2. G contains a subgroup H that is the image of a homomorphism $\theta\colon \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u and u^{-1} with multiplicity g, and H can be chosen so that its conjugates generate a dense subset of G^0 (such an H is called a *Hodge circle*).
3. For each component H of G and every irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$.

The Sato-Tate axioms for abelian varieties

1. G is closed.
2. G contains a subgroup H that is the image of a homomorphism $\theta\colon \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u and u^{-1} with multiplicity g, and H can be chosen so that its conjugates generate a dense subset of G^0 (such an H is called a *Hodge circle*).
3. For each component H of G and every 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).

Theorem

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

This follows from the Mumford-Tate and algebraic Sato-Tate conjectures, which are known for $g \leq 3$ (conjecturally true for all g).

Sato-Tate groups in dimension 2

Theorem 1 [FKRS 2012]

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

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

Sato-Tate groups in dimension 2

Theorem 1 [FKRS 2012]

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

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

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

Sato-Tate groups in dimension 2

Theorem 1 [FKRS 2012]

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

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

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

Note that our theorem says nothing about equidistribution; this is currently known in many special cases [FS 2012, Johansson 2013].

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

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 $G^0 \neq \mathrm{U}(1)$.

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

Galois types

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

Definition

The *Galois type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$, where $[G, E] \simeq [G', E']$ if there is an isomorphism $G \simeq G'$ and a compatible isomorphism $E \simeq E'$ of $\mathbb{R}$-algebras.

(NB: $G \simeq G'$ and $E \simeq E'$ does not necessarily imply $[G, E] \simeq [G', E']$).

Galois types and Sato-Tate groups in dimension 2

Theorem 2 [FKRS 2012]

Up to conjugacy, the Sato-Tate group G of an abelian surface A is uniquely determined by its Galois type, and vice versa.

We also have $G/G^0 \simeq \mathrm{Gal}(K/k)$, and G^0 is uniquely determined by the isomorphism class of $\mathrm{End}(A_K)_{\mathbb{R}}$, and vice versa:

$$\begin{array}{rlcrl}
\mathrm{U}(1) & \mathrm{M}_2(\mathbb{C}) & \qquad & \mathrm{U}(1)\times\mathrm{SU}(2) & \mathbb{C}\times\mathbb{R}\\
\mathrm{SU}(2) & \mathrm{M}_2(\mathbb{R}) & & \mathrm{SU}(2)\times\mathrm{SU}(2) & \mathbb{R}\times\mathbb{R}\\
\mathrm{U}(1)\times\mathrm{U}(1) & \mathbb{C}\times\mathbb{C} & & \mathrm{USp}(4) & \mathbb{R}
\end{array}$$

There are 52 distinct Galois types of abelian surfaces.

The proof uses the *algebraic Sato-Tate group* of Banaszak and Kedlaya, which, for $g \leq 3$, uniquely determines ST_A.

Exhibiting Sato-Tate groups of abelian surfaces

Remarkably, the 34 Sato-Tate groups that can arise over $\mathbb{Q}$ can all be realized as the Sato-Tate group of the Jacobian of a hyperelliptic curve.

The remaining 18 groups all arise as subgroups of these 34.

These subgroups can be obtained by extending the field of definition appropriately (in fact, one can realize all 52 groups using just 9 curves).

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

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 $G^0 \neq \mathrm{U}(1)$

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	$x^5 + 2x^4 - x^3 - 3x^2 - x$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{7}, a);\, a^3 - 7a - 7 = 0$
$J(E_1)$	$x^5 + x^3 + x$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$J(E_2)$	$x^5 + x^3 - x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt{2})$
$J(E_3)$	$x^6 + x^3 + 4$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$
$J(E_4)$	$x^5 + x^3 + 2x$	$\mathbb{Q}$	$\mathbb{Q}(i, \sqrt[4]{2})$
$J(E_6)$	$x^6 + x^3 - 2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3}, \sqrt[6]{-2})$
$G_{1,3}$	$x^6 + 3x^4 - 2$	$\mathbb{Q}(i)$	$\mathbb{Q}(i)$
$N(G_{1,3})$	$x^6 + 3x^4 - 2$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$G_{3,3}$	$x^6 + x^2 + 1$	$\mathbb{Q}$	$\mathbb{Q}$
$N(G_{3,3})$	$x^6 + x^5 + x - 1$	$\mathbb{Q}$	$\mathbb{Q}(i)$
$\mathrm{USp}(4)$	$x^5 - x + 1$	$\mathbb{Q}$	$\mathbb{Q}$

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 $|c_i| \leq 128$, over 2^{48} curves.

We specifically searched for cases not already addressed in [KS09].

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 $|c_i| \leq 128$, over 2^{48} curves.

We specifically searched for cases not already addressed in [KS09].

We found over 10 million non-isogenous curves with exceptional distributions, including at least 3 apparent matches for all of our target Sato-Tate groups.

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.

Existing algorithms for hyperelliptic curves

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

	complexity (ignoring factors of $O(\log\log p)$)		
algorithm	$g=1$	$g=2$	$g=3$

Existing algorithms for hyperelliptic curves

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	$p\log p$	$p^2\log p$	$p^3\log p$

Existing algorithms for hyperelliptic curves

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	$p^{1/4} \log p$	$p^{3/4} \log p$	$p^{5/4} \log p$

Existing algorithms for hyperelliptic curves

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	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$	$p^{1/2}\log^2 p$

Existing algorithms for hyperelliptic curves

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)	$\log^5 p$	$\log^8 p$	$\log^{12} p$ (?)

Existing algorithms for hyperelliptic curves

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

algorithm	$g = 1$	$g = 2$	$g = 3$
	complexity (ignoring factors of $O(\log\log p)$)		
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)	$\log^5 p$	$\log^8 p$	$\log^{12} p$ (?)

An average polynomial-time algorithm

All of the methods above 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.

An average polynomial-time algorithm

All of the methods above 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.

Theorem (H 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 $\log p$.

An average polynomial-time algorithm

All of the methods above 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.

Theorem (H 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 $p \leq N$ 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 (including curves over $\mathbb{Q}$).

An average polynomial-time algorithm

But is it practical?

An average polynomial-time algorithm

But is it practical? Yes!

	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	$\log^4 p$	$\log^4 p$	$\log^4 p$

For hyperelliptic curves of genus 2 and 3 the new algorithm is at least 30 times faster than current approaches, within the feasible range of N.