Sato-Tate distributions in genus 2

Andrew V. Sutherland

Massachusetts Institute of Technology

November 28, 2011

Joint work with Francesc Fité, Kiran S. Kedlaya, and Victor Rotger

http://arxiv.org/abs/1110.6638

Sato-Tate in genus 1

Let $E/\mathbb{Q}$ be an elliptic curve.
Let $t_p = p + 1 - \#E(\mathbb{F}_p)$ denote the trace of Frobenius.

Consider the distribution of

$$a_1 = -t_p/\sqrt{p} \in [-2, 2]$$

as $p \leq N$ varies over primes of good reduction.

What happens as $N \to \infty$?

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

Sato-Tate distributions in genus 1

1. Typical case (no CM)

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

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

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 genus 1

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

The generalized Sato-Tate conjecture implies that the normalized trace distribution of E converges to the distribution of the traces in G given by the Haar measure (the unique translation-invariant measure).

Each such distribution is uniquely determined by its *moment sequence*.

G	G/G^0	Example curve	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	$y^2 = x^3 + x + 1$	$\mathbb{Q}$	$1, 1, 2, 5, 14, 42, \ldots$

Three Sato-Tate groups, two of which arise for curves defined over $\mathbb{Q}$.

Normalized Euler factors (L-polynomials)

Let A be an abelian variety of dimension $g \geq 1$ over a number field k. Let $\rho_\ell \colon G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \cong \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ be the Galois representation arising from the action of G_k on the ℓ-adic Tate module $V_\ell(A)$.

For each prime $\mathfrak{p}$ of good reduction for A, let $q = \|\mathfrak{p}\|$ and define

$$L_\mathfrak{p}(T) = \det(1 - \rho_\ell(\mathrm{Frob}_\mathfrak{p})T),$$

$$\bar{L}_\mathfrak{p}(T) = L_\mathfrak{p}(T/\sqrt{q}) = \sum_{i=0}^{2g} a_i T^i.$$

The polynomial $\bar{L}_\mathfrak{p}(T)$ is real, monic, symmetric, and unitary.

Every such polynomial occurs as the characteristic polynomial of a unique conjugacy class in the compact Lie group $\mathrm{USp}(2g)$.

The Sato-Tate group ST_A

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 $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$.
Choose an embedding $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and let $G^1 = G_\ell^{1,\mathrm{Zar}} \otimes_\iota \mathbb{C}$.

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 $\|\mathfrak{p}\|^{-1/2}\rho_\ell(\mathrm{Frob}_\mathfrak{p}) \in G^1$ in ST_A.

The characteristic polynomial of $s(\mathfrak{p})$ is $\bar{L}_\mathfrak{p}(T)$.

The refined Sato-Tate conjecture

Let μ_{ST_A} denote the image on $\mathrm{Conj}(\mathrm{ST}_A)$ of the Haar measure on ST_A.

Conjecture [Serre]

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

In particular, the distribution of A's normalized Euler factors $\bar{L}_{\mathfrak{p}}(T)$ matches the distribution of characteristic polynomials of random matrices in ST_A.

The refined Sato-Tate conjecture

Let μ_{ST_A} denote the image on $\mathrm{Conj}(\mathrm{ST}_A)$ of the Haar measure on ST_A.

Conjecture [Serre]

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

In particular, the distribution of A's normalized Euler factors $\bar{L}_{\mathfrak{p}}(T)$ 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}.

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

The Sato-Tate axioms (weight 1 case)

A subgroup G of $\mathrm{USp}(2g)$ satisfies the *Sato-Tate axioms* if:

1. G is a closed.
2. (Hodge condition) There exists a homomorphism $\theta\colon \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u and u^{-1} with multiplicity g.
3. (Rationality condition) For each component H of G and each irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$.

Note: for any fixed g, the set of subgroups of $\mathrm{USp}(2g)$ that satisfy the Sato-Tate axioms is **finite** (up to conjugacy).

The Sato-Tate axioms (weight 1 case)

A subgroup G of $\mathrm{USp}(2g)$ satisfies the *Sato-Tate axioms* if:

1. G is a closed.
2. (Hodge condition) There exists a homomorphism $\theta\colon \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u and u^{-1} with multiplicity g.
3. (Rationality condition) For each component H of G and each irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$.

Note: for any fixed g, the set of subgroups of $\mathrm{USp}(2g)$ that satisfy the Sato-Tate axioms is **finite** (up to conjugacy).

Proposition

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

Conjecturally, this holds for all g.

Sato-Tate groups in genus 2

Theorem 1 [FKRS]

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

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

Sato-Tate groups in genus 2

Theorem 1 [FKRS]

Up to conjugacy, there are exactly 55 closed subgroups of $\mathrm{USp}(4)$ that 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, 52 can and do arise as ST_A for some abelian surface A, of which 34 can and do occur with A defined over $\mathbb{Q}$.

Sato-Tate groups in genus 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 genus 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 $\mathrm{End}(A_K)_{\mathbb{R}} = \mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

The *Galois type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$.

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 $\mathrm{End}(A_K)_{\mathbb{R}} = \mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

The *Galois type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$.

An isomorphism $[G, E] \cong [G', E']$ is an isomorphism $G \cong G'$ of groups and an equivariant isomorphism $E \cong E'$ of $\mathbb{R}$-algebras.

Note that one may have $G \cong G'$ and $E \cong E'$ but $[G, E] \not\cong [G', E']$.

Galois types and Sato-Tate groups

Theorem 2 [FKRS]

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

Moreover, G^0 is uniquely determined by the isomorphism class of $\mathrm{End}(A_K)_{\mathbb{R}}$, and vice versa:

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

We also have $G/G^0 \cong \mathrm{Gal}(K/k)$.

Twisted Lefschetz groups

The *Lefschetz group* L_A is defined as

$$\mathrm{L}_A = \{\gamma \in \mathrm{Sp}_{2g} : \gamma^{-1}\alpha\gamma = \alpha \text{ for all } \alpha \in \mathrm{End}(A_K)_{\mathbb{Q}}\}^0.$$

For each $\tau \in G_k$ define

$$\mathrm{L}_A(\tau) = \{\gamma \in \mathrm{Sp}_{2g} : \gamma^{-1}\alpha\gamma = \tau(\alpha) \text{ for all } \alpha \in \mathrm{End}(A_K)_{\mathbb{Q}}\}.$$

The *twisted Lefschetz group* is defined as $\mathrm{TL}_A = \cup_{\tau\in G_k}\mathrm{L}_A(\tau)$.

Theorem [Banaszak-Kedlaya]

Assume $g \leq 3$. Then ST_A is a maximal compact subgroup of $\mathrm{TL}_A \otimes_{\mathbb{Q}} \mathbb{C}$.

Exhibiting Sato-Tate groups in genus 2

For each Sato-Tate group G that can occur for an abelian surface defined over $\mathbb{Q}$, we can exhibit a curve $C/\mathbb{Q}$ for which $\mathrm{ST}_{\mathrm{Jac}(C)} = G$.

This accounts for 34 of the 52 Sato-Tate groups in genus 2.

Exhibiting Sato-Tate groups in genus 2

For each Sato-Tate group G that can occur for an abelian surface defined over $\mathbb{Q}$, we can exhibit a curve $C/\mathbb{Q}$ for which $\mathrm{ST}_{\mathrm{Jac}(C)} = G$.

This accounts for 34 of the 52 Sato-Tate groups in genus 2.
The remaining 18 groups all arise as subgroups of these 34.

Exhibiting Sato-Tate groups in genus 2

For each Sato-Tate group G that can occur for an abelian surface defined over $\mathbb{Q}$, we can exhibit a curve $C/\mathbb{Q}$ for which $\mathrm{ST}_{\mathrm{Jac}(C)} = G$.

This accounts for 34 of the 52 Sato-Tate groups in genus 2.
The remaining 18 groups all arise as subgroups of these 34.

By extending the field of definition of a suitable curve $C/\mathbb{Q}$, we can address the remaining 18 cases.

In fact, one can realize all 52 groups using just 9 curves.

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

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 curves with zero trace density $z_1 \geq 1/2$, which accounts for all 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 curves with zero trace density $z_1 \geq 1/2$, which accounts for all cases not already addressed in [KS09].

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

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

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 curves with zero trace density $z_1 \geq 1/2$, which accounts for all cases not already addressed in [KS09].

We found over 10 million non-isogenous curves with exceptional distributions, including at least 3 apparent matches for each 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 therefore the Sato-Tate group, to be **provably** identified.

Sato-Tate distributions in genus 2

Andrew V. Sutherland

Massachusetts Institute of Technology

November 28, 2011

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