Sato-Tate groups of abelian varieties

Kiran S. Kedlaya

Department of Mathematics, Massachusetts Institute of Technology
Department of Mathematics, University of California, San Diego
kedlaya@mit.edu, kedlaya@ucsd.edu
http://math.ucsd.edu/~kedlaya/slides/

Barcelona-Boston-Tokyo Number Theory Seminar
Barcelona, May 23, 2012

References:
An algebraic Sato-Tate group and Sato-Tate conjecture (with Grzegorz Banaszak), arXiv:1109.4449.
Sato-Tate distributions and Galois endomorphism modules in genus 2 (with Francesc Fité, Víctor Rotger, and Andrew V. Sutherland), arXiv:1110.6638; to appear in *Compositio Mathematica*.

Supported by NSF (CAREER grant DMS-0545904, grant DMS-1101343), DARPA (grant HR0011-09-1-0048), MIT (NEC Fund), UCSD (Warschawski chair).

Contents

1. Preface: the Chebotarev density theorem
2. The Sato-Tate conjecture for elliptic curves
3. The Sato-Tate group of an abelian variety
4. Sato-Tate groups of abelian surfaces

Contents

1. Preface: the Chebotarev density theorem
2. The Sato-Tate conjecture for elliptic curves
3. The Sato-Tate group of an abelian variety
4. Sato-Tate groups of abelian surfaces

The Chebotarev density theorem

Throughout this talk, let K denote a number field with ring of integers $\mathfrak{o}_K$, and let $\mathfrak{p}$ denote a generic maximal ideal of $\mathfrak{o}_K$ of norm q. Let $\mathbb{F}_{q^e}$ be the finite field of degree e over $\mathfrak{o}_K/\mathfrak{p}$.

Theorem

Let $f \in \mathfrak{o}_K[x]$ be a squarefree polynomial of degree $d > 0$ and put $X = \operatorname{Spec} \mathfrak{o}_K[x]/(f)$. For $i = 0, \dots, d$, for a certain explicit rational number c_i,

$$\lim_{N \to \infty} \frac{\#\{\mathfrak{p} : q \leq N, \#X(\mathbb{F}_q) = i\}}{\#\{\mathfrak{p} : q \leq N\}} = c_i.$$

In words, the left side computes the probability that for a random prime $\mathfrak{p}$, the reduction of f modulo $\mathfrak{p}$ has exactly i linear factors.

The Galois group

Theorem

Let $f \in \mathfrak{o}_K[x]$ be a squarefree polynomial of degree $d > 0$ and put $X = \operatorname{Spec} \mathfrak{o}_K[x]/(f)$. For $i = 0, \dots, d$, for a certain explicit rational number c_i,

$$\lim_{N \to \infty} \frac{\#\{\mathfrak{p} : q \leq N, \#X(\mathbb{F}_q) = i\}}{\#\{\mathfrak{p} : q \leq N\}} = c_i.$$

To define the constant c_i, let G be the Galois group of the splitting field of f over K. Then G acts transitively on the roots of f in an algebraic closure of K, and c_i is the probability that a random element of G fixes exactly i of the roots.

For example, if $G = S_d$ (the generic case), then $c_d = 1/d!$ and $c_0 \approx 1/e$.

This is not the most precise formulation of the Chebotarev density theorem. The optimal version is an equidistribution statement on the group G, which we give next.

The Galois group

Theorem

Let $f \in \mathfrak{o}_K[x]$ be a squarefree polynomial of degree $d > 0$ and put $X = \operatorname{Spec} \mathfrak{o}_K[x]/(f)$. For $i = 0, \dots, d$, for a certain explicit rational number c_i,

$$\lim_{N \to \infty} \frac{\#\{\mathfrak{p} : q \leq N, \#X(\mathbb{F}_q) = i\}}{\#\{\mathfrak{p} : q \leq N\}} = c_i.$$

To define the constant c_i, let G be the Galois group of the splitting field of f over K. Then G acts transitively on the roots of f in an algebraic closure of K, and c_i is the probability that a random element of G fixes exactly i of the roots.

For example, if $G = S_d$ (the generic case), then $c_d = 1/d!$ and $c_0 \approx 1/e$.

This is not the most precise formulation of the Chebotarev density theorem. The optimal version is an equidistribution statement on the group G, which we give next.

Equidistribution in the Galois group

View G as a compact Lie group using the discrete topology. Equip G with the Haar measure, i.e., the uniform measure on the elements of G. Equip the set $\mathrm{Conj}(G)$ of conjugacy classes of G with the image measure μ, so each class has measure proportional to its size.

Excluding finitely many primes of bad reduction, each $\mathfrak{p}$ defines a *Frobenius conjugacy class* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$. These are *equidistributed for* μ: for any (continuous) function $f : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\#\{\mathfrak{p} : q \leq N\}} \sum_{\mathfrak{p}:q\leq N} f(\mathrm{Frob}_{\mathfrak{p}}) = \int_f d\mu.$$

That is, the space average equals the time average.

This somewhat ponderous formulation has the advantage of making sense when G is a compact but not necessarily finite Lie group.

Equidistribution in the Galois group

View G as a compact Lie group using the discrete topology. Equip G with the Haar measure, i.e., the uniform measure on the elements of G. Equip the set $\mathrm{Conj}(G)$ of conjugacy classes of G with the image measure μ, so each class has measure proportional to its size.

Excluding finitely many primes of bad reduction, each $\mathfrak{p}$ defines a *Frobenius conjugacy class* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$. These are *equidistributed for* μ: for any (continuous) function $f : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N \to \infty} \frac{1}{\#\{\mathfrak{p} : q \leq N\}} \sum_{\mathfrak{p} : q \leq N} f(\mathrm{Frob}_{\mathfrak{p}}) = \int_f d\mu.$$

That is, the space average equals the time average.

This somewhat ponderous formulation has the advantage of making sense when G is a compact but not necessarily finite Lie group.

Equidistribution in the Galois group

View G as a compact Lie group using the discrete topology. Equip G with the Haar measure, i.e., the uniform measure on the elements of G. Equip the set $\mathrm{Conj}(G)$ of conjugacy classes of G with the image measure μ, so each class has measure proportional to its size.

Excluding finitely many primes of bad reduction, each $\mathfrak{p}$ defines a *Frobenius conjugacy class* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$. These are *equidistributed for* μ: for any (continuous) function $f : \mathrm{Conj}(G) \to \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\#\{\mathfrak{p} : q \leq N\}} \sum_{\mathfrak{p}:q\leq N} f(\mathrm{Frob}_{\mathfrak{p}}) = \int_f d\mu.$$

That is, the space average equals the time average.

This somewhat ponderous formulation has the advantage of making sense when G is a compact but not necessarily finite Lie group.

Chebotarev in higher motivic weight

One may view the Chebotarev density theorem as an equidistribution property for a certain 0-motive (Artin motive). A conjectural generalization to motives of higher weight has been described by Serre, in which the Galois group G must be replaced by a certain compact Lie group; see references below.

In this talk, we make the description explicit for 1-motives associated to abelian varieties. We will especially emphasize the cases of abelian varieties of dimension at most 3. Sadly, very little can be proved; our focus will be on making the conjectures as explicit as possible.

References:
J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proceedings of Symposia in Pure Math. **55**, Amer. Math. Soc., 1994, 377–400.
J.-P. Serre, *Lectures on* $N_X(p)$, A.K. Peters, 2012.

Chebotarev in higher motivic weight

One may view the Chebotarev density theorem as an equidistribution property for a certain 0-motive (Artin motive). A conjectural generalization to motives of higher weight has been described by Serre, in which the Galois group G must be replaced by a certain compact Lie group; see references below.

In this talk, we make the description explicit for 1-motives associated to abelian varieties. We will especially emphasize the cases of abelian varieties of dimension at most 3. Sadly, very little can be proved; our focus will be on making the conjectures as explicit as possible.

References:
J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proceedings of Symposia in Pure Math. **55**, Amer. Math. Soc., 1994, 377–400.
J.-P. Serre, *Lectures on $N_X(p)$*, A.K. Peters, 2012.

Contents

1. Preface: the Chebotarev density theorem
2. The Sato-Tate conjecture for elliptic curves
3. The Sato-Tate group of an abelian variety
4. Sato-Tate groups of abelian surfaces

The Hasse interval

Let E be an elliptic curve over K. Fix a model X for E over $\mathfrak{o}_K$.

Theorem (Hasse)

For $\mathfrak{p}$ at which X has good reduction, the trace of Frobenius

$$a_{\mathfrak{p}} := q + 1 - \#X(\mathbb{F}_q)$$

satisfies $|a_{\mathfrak{p}}| \leq 2\sqrt{q}$.

One can then ask about the distribution of the normalized trace $\overline{a}_{\mathfrak{p}} := \frac{a_{\mathfrak{p}}}{2\sqrt{q}}$. Equivalently, Hasse's theorem implies a polynomial factorization

$$(1 - a_{\mathfrak{p}} T + qT^2) = (1 - \alpha_{\mathfrak{p}}\sqrt{q}T)(1 - \beta_{\mathfrak{p}}\sqrt{q}T)$$

in which

$$\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in \mathbb{C}, \quad |\alpha_{\mathfrak{p}}| = |\beta_{\mathfrak{p}}| = 1, \quad \mathrm{Imag}(\alpha_{\mathfrak{p}}) \geq 0$$

and we may ask about the distribution of $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ on the unit circle.

The Hasse interval

Let E be an elliptic curve over K. Fix a model X for E over $\mathfrak{o}_K$.

Theorem (Hasse)

For $\mathfrak{p}$ at which X has good reduction, the trace of Frobenius

$$a_{\mathfrak{p}} := q + 1 - \#X(\mathbb{F}_q)$$

satisfies $|a_{\mathfrak{p}}| \leq 2\sqrt{q}$.

One can then ask about the distribution of the normalized trace $\overline{a}_{\mathfrak{p}} := \frac{a_{\mathfrak{p}}}{2\sqrt{q}}$. Equivalently, Hasse's theorem implies a polynomial factorization

$$(1 - a_{\mathfrak{p}} T + qT^2) = (1 - \alpha_{\mathfrak{p}} \sqrt{q}\, T)(1 - \beta_{\mathfrak{p}} \sqrt{q}\, T)$$

in which

$$\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in \mathbb{C}, \quad |\alpha_{\mathfrak{p}}| = |\beta_{\mathfrak{p}}| = 1, \quad \mathrm{Imag}(\alpha_{\mathfrak{p}}) \geq 0$$

and we may ask about the distribution of $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ on the unit circle.

The case of CM curves

Theorem (Hecke)

Suppose E has complex multiplication. Then the $\alpha_{\mathfrak{p}}$ are equidistributed for the following measures on the semicircle $|\alpha_{\mathfrak{p}}| = 1, \mathrm{Imag}(\alpha_{\mathfrak{p}}) \geq 0$.

(a) *If the CM is defined over K, take the Lebesgue measure.*

(b) *If not, take half the Lebesgue measure plus half the discrete measure at $\alpha_{\mathfrak{p}} = i$.*

More precisely, the pairs $(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ occur as the eigenvalues of certain conjugacy classes of a compact Lie group $G = G(E, K)$ which are equidistributed for the image of Haar measure.

(a) If the CM is defined over K, we have $G = \mathrm{SO}(2)$.

(b) If not, G is the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. It has two connected components, on one of which the trace is identically 0, corresponding to the 50% of prime ideals at which E is supersingular.

The case of CM curves

Theorem (Hecke)

Suppose E has complex multiplication. Then the $\alpha_{\mathfrak{p}}$ are equidistributed for the following measures on the semicircle $|\alpha_{\mathfrak{p}}| = 1, \mathrm{Imag}(\alpha_{\mathfrak{p}}) \geq 0$.

(a) *If the CM is defined over K, take the Lebesgue measure.*

(b) *If not, take half the Lebesgue measure plus half the discrete measure at $\alpha_{\mathfrak{p}} = i$.*

More precisely, the pairs $(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ occur as the eigenvalues of certain conjugacy classes of a compact Lie group $G = G(E, K)$ which are equidistributed for the image of Haar measure.

(a) If the CM is defined over K, we have $G = \mathrm{SO}(2)$.

(b) If not, G is the normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$. It has two connected components, on one of which the trace is identically 0, corresponding to the 50% of prime ideals at which E is supersingular.

The case of non-CM curves: the Sato-Tate conjecture

Conjecture (Sato-Tate)

Suppose E has no complex multiplication. Then the $(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ occur as the eigenvalues of certain conjugacy classes of $G = \mathrm{SU}(2)$ which are equidistributed for the image of Haar measure.

This conjecture is supported by copious numerical evidence...

Theorem (Taylor et al.)

The Sato-Tate conjecture is true when K is a totally real field.

To prove this, one first obtains analytic continuation for some symmetric power L-functions using modularity techniques. An argument of Serre, simulating the prime number theorem, then gives equidistribution.

The case of non-CM curves: the Sato-Tate conjecture

Conjecture (Sato-Tate)

Suppose E has no complex multiplication. Then the $(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ occur as the eigenvalues of certain conjugacy classes of $G = \mathrm{SU}(2)$ which are equidistributed for the image of Haar measure.

This conjecture is supported by copious numerical evidence...

Theorem (Taylor et al.)

The Sato-Tate conjecture is true when K is a totally real field.

To prove this, one first obtains analytic continuation for some symmetric power L-functions using modularity techniques. An argument of Serre, simulating the prime number theorem, then gives equidistribution.

Contents

1. Preface: the Chebotarev density theorem
2. The Sato-Tate conjecture for elliptic curves
3. The Sato-Tate group of an abelian variety
4. Sato-Tate groups of abelian surfaces

The Sato-Tate problem

Let A be an abelian variety over K of dimension $g > 0$. Fix a model X for A over $\mathfrak{o}_K$.

Theorem (Weil)

For $\mathfrak{p}$ at which X has good reduction, there exist $\alpha_{1,\mathfrak{p}}, \dots, \alpha_{2g,\mathfrak{p}} \in \mathbb{C}$ with

$$\begin{gathered} |\alpha_{i,\mathfrak{p}}| = 1 \qquad (i = 1, \dots, 2g) \\ \alpha_{i,\mathfrak{p}}\alpha_{g+i,\mathfrak{p}} = 1 \qquad (i = 1, \dots, g) \\ \#X(\mathbb{F}_{q^e}) = q^e + 1 - q^{e/2}(\alpha_{1,\mathfrak{p}}^e + \dots + \alpha_{2g,\mathfrak{p}}^e) \quad (e = 1, 2, \dots). \end{gathered}$$

Such data determine a unique conjugacy class in the unitary symplectic group $\mathrm{USp}(2g)$. The *Sato-Tate problem*, in its simplest form, is to find a measure for which these classes are equidistributed.

We will focus on identifying the measure. Proving equidistribution is in most cases intractable: it awaits advances in the Langlands program.

The Sato-Tate problem

Let A be an abelian variety over K of dimension $g > 0$. Fix a model X for A over $\mathfrak{o}_K$.

Theorem (Weil)

For $\mathfrak{p}$ at which X has good reduction, there exist $\alpha_{1,\mathfrak{p}}, \dots, \alpha_{2g,\mathfrak{p}} \in \mathbb{C}$ with

$$\begin{gathered}
|\alpha_{i,\mathfrak{p}}| = 1 \qquad (i = 1, \dots, 2g) \\
\alpha_{i,\mathfrak{p}} \alpha_{g+i,\mathfrak{p}} = 1 \qquad (i = 1, \dots, g) \\
\#X(\mathbb{F}_{q^e}) = q^e + 1 - q^{e/2}(\alpha_{1,\mathfrak{p}}^e + \cdots + \alpha_{2g,\mathfrak{p}}^e) \quad (e = 1, 2, \dots).
\end{gathered}$$

Such data determine a unique conjugacy class in the unitary symplectic group $\mathrm{USp}(2g)$. The *Sato-Tate problem*, in its simplest form, is to find a measure for which these classes are equidistributed.

We will focus on identifying the measure. Proving equidistribution is in most cases intractable: it awaits advances in the Langlands program.

The Sato-Tate group

Conjecture (Refined Sato-Tate conjecture)

There exist a compact Lie group $G = \mathrm{ST}(A, K) \subseteq \mathrm{USp}(2g)$ *and some conjugacy classes* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ *with eigenvalues* $\alpha_{1,\mathfrak{p}}, \dots, \alpha_{2g,\mathfrak{p}}$ *(which we will describe explicitly later), such that these classes are equidistributed for the image of Haar measure.*

This *Sato-Tate group* will be realized as a maximal compact subgroup of a certain reductive $\mathbb{Q}$-algebraic subgroup $\mathrm{AST}(A, K)$ of $\mathrm{Sp}(2g, \mathbb{C})$. This latter subgroup, the *algebraic Sato-Tate group*, can be identified unconditionally in cases where standard motivic conjectures (Hodge, Mumford-Tate) are known. In particular, this includes all cases with $g \leq 3$.

This conjecture predicts the distribution of any symmetric function of the $\alpha_{i,\mathfrak{p}}$ as the distribution of the corresponding function of eigenvalues of a random matrix of $\mathrm{ST}(A, K)$. This is again supported by evidence...

The Sato-Tate group

Conjecture (Refined Sato-Tate conjecture)

There exist a compact Lie group $G = \mathrm{ST}(A, K) \subseteq \mathrm{USp}(2g)$ *and some conjugacy classes* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ *with eigenvalues* $\alpha_{1,\mathfrak{p}}, \dots, \alpha_{2g,\mathfrak{p}}$ *(which we will describe explicitly later), such that these classes are equidistributed for the image of Haar measure.*

This *Sato-Tate group* will be realized as a maximal compact subgroup of a certain reductive $\mathbb{Q}$-algebraic subgroup $\mathrm{AST}(A, K)$ of $\mathrm{Sp}(2g, \mathbb{C})$. This latter subgroup, the *algebraic Sato-Tate group*, can be identified unconditionally in cases where standard motivic conjectures (Hodge, Mumford-Tate) are known. In particular, this includes all cases with $g \leq 3$.

This conjecture predicts the distribution of any symmetric function of the $\alpha_{i,\mathfrak{p}}$ as the distribution of the corresponding function of eigenvalues of a random matrix of $\mathrm{ST}(A, K)$. This is again supported by evidence...

The Sato-Tate group

Conjecture (Refined Sato-Tate conjecture)

There exist a compact Lie group $G = \mathrm{ST}(A, K) \subseteq \mathrm{USp}(2g)$ *and some conjugacy classes* $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Conj}(G)$ *with eigenvalues* $\alpha_{1,\mathfrak{p}}, \dots, \alpha_{2g,\mathfrak{p}}$ *(which we will describe explicitly later), such that these classes are equidistributed for the image of Haar measure.*

This *Sato-Tate group* will be realized as a maximal compact subgroup of a certain reductive $\mathbb{Q}$-algebraic subgroup $\mathrm{AST}(A, K)$ of $\mathrm{Sp}(2g, \mathbb{C})$. This latter subgroup, the *algebraic Sato-Tate group*, can be identified unconditionally in cases where standard motivic conjectures (Hodge, Mumford-Tate) are known. In particular, this includes all cases with $g \leq 3$.

This conjecture predicts the distribution of any symmetric function of the $\alpha_{i,\mathfrak{p}}$ as the distribution of the corresponding function of eigenvalues of a random matrix of $\mathrm{ST}(A, K)$. This is again supported by evidence...

Construction of the algebraic Sato-Tate group

Fix an embedding $K \hookrightarrow \mathbb{C}$. The homology space $H = H_1(A_{\mathbb{C}}, \mathbb{Q})$ carries a symplectic form (cup product) and hence an action of $\mathrm{GSp}(2g, \mathbb{Q})$. Meanwhile, $H \otimes_{\mathbb{Q}} \mathbb{R}$ may be identified with the tangent space of $A_{\mathbb{C}}$, and hence carries a complex structure. Take the minimal $\mathbb{Q}$-algebraic subgroup of $\mathrm{GSp}(2g, \mathbb{Q})$ containing $\mathbb{C}^\times$, then intersect with $\mathrm{Sp}(2g, \mathbb{Q})$ to get the *Hodge group* of A.

The Hodge group is connected and acts trivially on absolute Hodge cycles of A. To get the algebraic Sato-Tate group $\mathrm{AST}(A, K)$, add elements of $\mathrm{Sp}(2g, \mathbb{Q})$ which act on absolute Hodge cycles via some element of $\mathrm{Gal}(\overline{K}/K)$.

For $g \leq 3$, we may use endomorphisms instead of absolute Hodge cycles. The component group $\pi_0(\mathrm{AST}(A, K)) \cong \pi_0(\mathrm{ST}(A, K))$ is then identified with $\mathrm{Gal}(L/K)$ for L/K the minimal extension over which all endomorphisms of $A_{\overline{K}}$ are realized.

Construction of the algebraic Sato-Tate group

Fix an embedding $K \hookrightarrow \mathbb{C}$. The homology space $H = H_1(A_{\mathbb{C}}, \mathbb{Q})$ carries a symplectic form (cup product) and hence an action of $\mathrm{GSp}(2g, \mathbb{Q})$. Meanwhile, $H \otimes_{\mathbb{Q}} \mathbb{R}$ may be identified with the tangent space of $A_{\mathbb{C}}$, and hence carries a complex structure. Take the minimal $\mathbb{Q}$-algebraic subgroup of $\mathrm{GSp}(2g, \mathbb{Q})$ containing $\mathbb{C}^\times$, then intersect with $\mathrm{Sp}(2g, \mathbb{Q})$ to get the *Hodge group* of A.

The Hodge group is connected and acts trivially on absolute Hodge cycles of A. To get the algebraic Sato-Tate group $\mathrm{AST}(A, K)$, add elements of $\mathrm{Sp}(2g, \mathbb{Q})$ which act on absolute Hodge cycles via some element of $\mathrm{Gal}(\overline{K}/K)$.

For $g \leq 3$, we may use endomorphisms instead of absolute Hodge cycles. The component group $\pi_0(\mathrm{AST}(A, K)) \cong \pi_0(\mathrm{ST}(A, K))$ is then identified with $\mathrm{Gal}(L/K)$ for L/K the minimal extension over which all endomorphisms of $A_{\overline{K}}$ are realized.

Construction of the algebraic Sato-Tate group

Fix an embedding $K \hookrightarrow \mathbb{C}$. The homology space $H = H_1(A_{\mathbb{C}}, \mathbb{Q})$ carries a symplectic form (cup product) and hence an action of $\mathrm{GSp}(2g, \mathbb{Q})$. Meanwhile, $H \otimes_{\mathbb{Q}} \mathbb{R}$ may be identified with the tangent space of $A_{\mathbb{C}}$, and hence carries a complex structure. Take the minimal $\mathbb{Q}$-algebraic subgroup of $\mathrm{GSp}(2g, \mathbb{Q})$ containing $\mathbb{C}^{\times}$, then intersect with $\mathrm{Sp}(2g, \mathbb{Q})$ to get the *Hodge group* of A.

The Hodge group is connected and acts trivially on absolute Hodge cycles of A. To get the algebraic Sato-Tate group $\mathrm{AST}(A, K)$, add elements of $\mathrm{Sp}(2g, \mathbb{Q})$ which act on absolute Hodge cycles via some element of $\mathrm{Gal}(\overline{K}/K)$.

For $g \leq 3$, we may use endomorphisms instead of absolute Hodge cycles. The component group $\pi_0(\mathrm{AST}(A, K)) \cong \pi_0(\mathrm{ST}(A, K))$ is then identified with $\mathrm{Gal}(L/K)$ for L/K the minimal extension over which all endomorphisms of $A_{\overline{K}}$ are realized.

Construction of Frobenius conjugacy classes

Fix a prime ℓ and an embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.

Under standard conjectures (which hold if $g \leq 3$), the image of $\mathrm{Gal}(\overline{K}/K)$ on the ℓ-adic Tate module is an open subgroup of $\mathrm{AST}(A, K) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ (theorem of Bogomolov). Taking the image of $\mathrm{Frob}_{\mathfrak{p}}$ in $\mathrm{AST}(A, K) \otimes_{\mathbb{Q}} \mathbb{C}$, then dividing by $q^{1/2}$, gives a well-defined (up to conjugacy) element of $\mathrm{ST}(A, K)$.

Contents

1. Preface: the Chebotarev density theorem
2. The Sato-Tate conjecture for elliptic curves
3. The Sato-Tate group of an abelian variety
4. Sato-Tate groups of abelian surfaces

The Sato-Tate axioms

Proposition (Sato-Tate axioms)

Suppose $G = \mathrm{ST}(A, K)$ *for some* A*. We then have the following.*

(a) *The group* G *is a closed subgroup of* $\mathrm{USp}(2g)$*.*

(b) *There exists a homomorphism* $\theta : \mathrm{U}(1) \to G^0$ *such that* $\theta(u)$ *has eigenvalues* u, u^{-1} *each with multiplicity* g*.*

(c) *For each component* H *of* G *and each irreducible character* χ *of* $\mathrm{GL}(d, \mathbb{C})$*, the average of* $\chi(\gamma)$ *over* $\gamma \in H$ *is an integer.*

Theorem (FKRS)

For $g = 2$*, there are* 55 *conjugacy classes of subgroups of* $\mathrm{USp}(4)$ *satisfying the Sato-Tate axioms.*

Sato-Tate groups and endomorphism algebras

Theorem (FKRS)

The group $\mathrm{ST}(A, K)$ *determines the real endomorphism algebra* $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{R}$ *and its action of* $\mathrm{Gal}(\overline{K}/K)$*. For* $g = 2$*, the converse is also true.*

Ignoring the Galois action, the options for $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{R}$ for $g = 2$ are

$$\mathbb{R}, \mathbb{R} \times \mathbb{R}, \mathbb{R} \times \mathbb{C}, \mathbb{C} \times \mathbb{C}, \mathrm{M}^2(\mathbb{R}), \mathrm{M}^2(\mathbb{C})$$

corresponding to Sato-Tate groups with connected parts

$$\mathrm{USp}(4), \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{SU}(2) \times \mathrm{U}(1), \mathrm{U}(1) \times \mathrm{U}(1), \mathrm{SU}(2), \mathrm{U}(1).$$

This conflates certain cases that one might otherwise distinguish. For instance, $\mathbb{C} \times \mathbb{C}$ occurs both for the product of two nonisogenous CM elliptic curves and for an absolutely simple CM abelian surface.

Sato-Tate groups for $g = 2$: main result

Theorem (FKRS)

There exist exactly 52 *groups which occur as the Sato-Tate groups of abelian surfaces. Of these, exactly* 34 *groups occur for abelian surfaces over* $\mathbb{Q}$*.*

This result includes an explicit description of each group and an example of a genus 2 curve whose Jacobian provably realizes this Sato-Tate group. (It does not include equidistribution!)

Corollary

Assume $g = 2$*. Let* L/K *be the minimal extension such that* $\mathrm{End}(A_L) = \mathrm{End}(A_{\overline{K}})$*. Then* $[L : K] \in \{1, 2, 3, 4, 6, 8, 12, 24, 48\}$*.*

This improves the case $g = 2$ of a result of Silverberg, which implies that $[L : K]$ divides $23040 = 2^9 \cdot 3^2 \cdot 5$.

Sato-Tate groups for $g = 2$: main result

Theorem (FKRS)

There exist exactly 52 *groups which occur as the Sato-Tate groups of abelian surfaces. Of these, exactly* 34 *groups occur for abelian surfaces over* $\mathbb{Q}$*.*

This result includes an explicit description of each group and an example of a genus 2 curve whose Jacobian provably realizes this Sato-Tate group. (It does not include equidistribution!)

Corollary

Assume $g = 2$*. Let* L/K *be the minimal extension such that* $\mathrm{End}(A_L) = \mathrm{End}(A_{\overline{K}})$*. Then* $[L : K] \in \{1, 2, 3, 4, 6, 8, 12, 24, 48\}$*.*

This improves the case $g = 2$ of a result of Silverberg, which implies that $[L : K]$ divides $23040 = 2^9 \cdot 3^2 \cdot 5$.

Some examples for $g = 2$

Most of the Sato-Tate groups for $g = 2$ have connected part U(1). These groups all occur among Jacobians of twists of two curves with many automorphisms:

$$y^2 = x^5 - x, \qquad y^2 = x^6 + 1.$$

For example, one finds examples with component groups $D_6 \times C_2$ and $S_4 \times C_2$; since any subgroup of these can then occur, this implies that our previous corollary is sharp.

Theorem (Fité-Sutherland)

The Sato-Tate conjecture holds for the Jacobian of any twist of one of these two curves.

Some examples for $g = 2$

Most of the Sato-Tate groups for $g = 2$ have connected part U(1). These groups all occur among Jacobians of twists of two curves with many automorphisms:

$$y^2 = x^5 - x, \qquad y^2 = x^6 + 1.$$

For example, one finds examples with component groups $D_6 \times C_2$ and $S_4 \times C_2$; since any subgroup of these can then occur, this implies that our previous corollary is sharp.

Theorem (Fité-Sutherland)

The Sato-Tate conjecture holds for the Jacobian of any twist of one of these two curves.

What about $g = 3$?

For $g = 3$, there are 14 possibilities for the connected part of $\mathrm{ST}(A, K)$. It is not yet know how many Sato-Tate groups can occur, but it is definitely at least 200.

In order to realize Sato-Tate groups with large component groups, one needs abelian threefolds with large endomorphism algebras. Some obvious examples arise from curves with many automorphisms (i.e., no deformations preserving all automorphisms). These were listed by Wolfart:

$$y^2 = x^8 - x, \quad y^2 = x^7 - x, \quad y^2 = x^8 - 1,$$
$$y^2 = x^8 - 14x^4 + 1, \quad y^3 = x^3(x-1), \quad y^4 + x^3 = 1,$$
$$y^4 + x^4 = 1, \quad x^3y + y^3z + z^3x = 1.$$

However, curves are probably not enough! For instance, the Hessian group of order 216 appears to arise as a component group, but the automorphism group of a genus 3 curve can have at most 168 elements (Hurwitz bound).

What about $g = 3$?

For $g = 3$, there are 14 possibilities for the connected part of $\mathrm{ST}(A, K)$. It is not yet know how many Sato-Tate groups can occur, but it is definitely at least 200.

In order to realize Sato-Tate groups with large component groups, one needs abelian threefolds with large endomorphism algebras. Some obvious examples arise from curves with many automorphisms (i.e., no deformations preserving all automorphisms). These were listed by Wolfart:

$$y^2 = x^8 - x, \quad y^2 = x^7 - x, \quad y^2 = x^8 - 1,$$
$$y^2 = x^8 - 14x^4 + 1, \quad y^3 = x^3(x-1), \quad y^4 + x^3 = 1,$$
$$y^4 + x^4 = 1, \quad x^3y + y^3z + z^3x = 1.$$

However, curves are probably not enough! For instance, the Hessian group of order 216 appears to arise as a component group, but the automorphism group of a genus 3 curve can have at most 168 elements (Hurwitz bound).

What about $g = 3$?

For $g = 3$, there are 14 possibilities for the connected part of $\mathrm{ST}(A, K)$. It is not yet know how many Sato-Tate groups can occur, but it is definitely at least 200.

In order to realize Sato-Tate groups with large component groups, one needs abelian threefolds with large endomorphism algebras. Some obvious examples arise from curves with many automorphisms (i.e., no deformations preserving all automorphisms). These were listed by Wolfart:

$$y^2 = x^8 - x, \quad y^2 = x^7 - x, \quad y^2 = x^8 - 1,$$
$$y^2 = x^8 - 14x^4 + 1, \quad y^3 = x^3(x-1), \quad y^4 + x^3 = 1,$$
$$y^4 + x^4 = 1, \quad x^3y + y^3z + z^3x = 1.$$

However, curves are probably not enough! For instance, the Hessian group of order 216 appears to arise as a component group, but the automorphism group of a genus 3 curve can have at most 168 elements (Hurwitz bound).