Towards a precise Sato-Tate conjecture in genus 2

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.mit.edu/~kedlaya/papers/talks.shtml

Explicit Methods in Number Theory
Oberwolfach, July 19, 2011

Joint work *in progress* with Francesc Fité, Victor Rotger, Andrew V. Sutherland and with Grzegorz Banaszak.

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

Advertisement

Come to the Algorithmic Number Theory Symposium (ANTS-X), July 9-13, 2012, at the University of California, San Diego!

We expect to have some funding for graduate students and postdocs. Watch for news at the web site:

`http://math.ucsd.edu/~kedlaya/ants10`

Contents

Contents

Notations

Throughout, let A be an abelian variety of dimension g over a number field k. Write the L-function of A (or rather the part coming from primes of good reduction) as an Euler product

$$L(A/k, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(A/k, q^{-s})^{-1} \qquad (q = \mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}))$$

Here $L_{\mathfrak{p}}$ is an integer polynomial of degree $2g$. If we renormalize by setting

$$\overline{L}_{\mathfrak{p}}(A/k, T) = L_{\mathfrak{p}}(A/k, q^{-1/2}T),$$

then $\overline{L}_{\mathfrak{p}}(A/k, T)$ has its roots in conjugate pairs on the unit circle. In particular, it occurs as the characteristic polynomial of a unique conjugacy class in the unitary symplectic group $\mathrm{USp}(2g)$.

The Sato-Tate conjecture: imprecise to precise

Conjecture (Imprecise Sato-Tate)

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ *of the Haar measure on some closed subgroup H of* $\mathrm{USp}(2g)$.

One way to make this precise is to give a recipe for H; more on that soon.

For $g = 2$, we also do the following.

- We classify subgroups consistent with this construction. (There are 55 of them up to conjugacy.)
- We correlate these groups with the Galois action on endomorphism algebras. (This leaves 52 possibilities, of which 34 can occur over $\mathbb{Q}$.)
- We obtain strong numerical evidence for the resulting predictions.

The Sato-Tate conjecture: imprecise to precise

Conjecture (Imprecise Sato-Tate)

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ *of the Haar measure on some closed subgroup H of* $\mathrm{USp}(2g)$.

One way to make this precise is to give a recipe for H; more on that soon.

For $g = 2$, we also do the following.

- We classify subgroups consistent with this construction. (There are 55 of them up to conjugacy.)
- We correlate these groups with the Galois action on endomorphism algebras. (This leaves 52 possibilities, of which 34 can occur over $\mathbb{Q}$.)
- We obtain strong numerical evidence for the resulting predictions.

The Sato-Tate conjecture: imprecise to precise

Conjecture (Imprecise Sato-Tate)

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ *of the Haar measure on some closed subgroup H of* $\mathrm{USp}(2g)$.

One way to make this precise is to give a recipe for H; more on that soon.

For $g = 2$, we also do the following.

- We classify subgroups consistent with this construction. (There are 55 of them up to conjugacy.)
- We correlate these groups with the Galois action on endomorphism algebras. (This leaves 52 possibilities, of which 34 can occur over $\mathbb{Q}$.)
- We obtain strong numerical evidence for the resulting predictions.

The Sato-Tate conjecture: imprecise to precise

Conjecture (Imprecise Sato-Tate)

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on some closed subgroup H of $\mathrm{USp}(2g)$.

One way to make this precise is to give a recipe for H; more on that soon.

For $g = 2$, we also do the following.

- We classify subgroups consistent with this construction. (There are 55 of them up to conjugacy.)
- We correlate these groups with the Galois action on endomorphism algebras. (This leaves 52 possibilities, of which 34 can occur over $\mathbb{Q}$.)
- We obtain strong numerical evidence for the resulting predictions.

Example: the case of dimension 1

Conjecture

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on some closed subgroup H of $\mathrm{USp}(2g)$.

Suppose $g = 1$, so $A = E$ is an elliptic curve.

- If E has complex multiplication defined over k, then the conjecture holds with $H = \mathrm{SO}(2)$ (classical).
- If E has complex multiplication not defined over k, then the conjecture holds with $H = N(\mathrm{SO}(2))$ (not connected!).
- If E does not have complex multiplication, then one expects $H = \mathrm{USp}(2) = \mathrm{SU}(2)$. Known for k totally real (Barnet-Lamb, Clozel, Gee, Geraghty, Harris, Taylor).

Example: the case of dimension 1

Conjecture

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on some closed subgroup H of $\mathrm{USp}(2g)$.

Suppose $g = 1$, so $A = E$ is an elliptic curve.

- If E has complex multiplication defined over k, then the conjecture holds with $H = \mathrm{SO}(2)$ (classical).
- If E has complex multiplication not defined over k, then the conjecture holds with $H = N(\mathrm{SO}(2))$ (not connected!).
- If E does not have complex multiplication, then one expects $H = \mathrm{USp}(2) = \mathrm{SU}(2)$. Known for k totally real (Barnet-Lamb, Clozel, Gee, Geraghty, Harris, Taylor).

Example: the case of dimension 1

Conjecture

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on some closed subgroup H of $\mathrm{USp}(2g)$.

Suppose $g = 1$, so $A = E$ is an elliptic curve.

- If E has complex multiplication defined over k, then the conjecture holds with $H = \mathrm{SO}(2)$ (classical).
- If E has complex multiplication not defined over k, then the conjecture holds with $H = N(\mathrm{SO}(2))$ (not connected!).
- If E does not have complex multiplication, then one expects $H = \mathrm{USp}(2) = \mathrm{SU}(2)$. Known for k totally real (Barnet-Lamb, Clozel, Gee, Geraghty, Harris, Taylor).

Example: the case of dimension 1

Conjecture

For fixed A/k, as $\mathfrak{p}$ varies over prime ideals of good reduction, the $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on some closed subgroup H of $\mathrm{USp}(2g)$.

Suppose $g = 1$, so $A = E$ is an elliptic curve.

- If E has complex multiplication defined over k, then the conjecture holds with $H = \mathrm{SO}(2)$ (classical).
- If E has complex multiplication not defined over k, then the conjecture holds with $H = N(\mathrm{SO}(2))$ (not connected!).
- If E does not have complex multiplication, then one expects $H = \mathrm{USp}(2) = \mathrm{SU}(2)$. Known for k totally real (Barnet-Lamb, Clozel, Gee, Geraghty, Harris, Taylor).

Contents

The Mumford-Tate group

Let G_k be the absolute Galois group of k. For ℓ a prime, let $\rho_{A/K,\ell} : G_k \to \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ be the ℓ-adic Galois representation of A.

Let G_ℓ be the image of $\rho_{A/k,\ell}$. Let G_ℓ^{Zar} denote the Zariski closure of G_ℓ in $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$; note that G_ℓ is open in $G_\ell^{\mathrm{Zar}}(\mathbb{Q}_\ell)$ (Bogomolov).

Conjecture (Mumford-Tate)

The identity component $G_\ell^{\mathrm{Zar},0}$ of G_ℓ^{Zar} equals the **Mumford-Tate group**, *the minimal algebraic group over $\mathbb{Q}$ whose $\mathbb{R}$-points contain the action of $\mathbb{C}^\times$ on $H_1(A_{\mathbb{C}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R}$ coming from the complex structure on the latter.*

In particular, $G_\ell^{\mathrm{Zar},0}$ should descend to an algebraic group over $\mathbb{Q}$ which does not depend on ℓ.

An ℓ-adic Sato-Tate group (after Serre)

Let $G_{\ell,1}$ be the kernel of $G_\ell \to \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell^\times$, where the last map comes from the Weil pairing. Let $G_{\ell,1}^{\mathrm{Zar}}$ denote the Zariski closure of $G_{\ell,1}$ in $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. It is generally not connected!

Conjecture (Algebraic Sato-Tate)

The group $G_{\ell,1}^{\mathrm{Zar}}$ descends to an algebraic group G_1^{Zar} over $\mathbb{Q}$ which does not depend on ℓ.

We call G_1^{Zar} the *algebraic Sate-Tate group* of A/k, denoted $\mathrm{AST}(A/k)$. The *Sato-Tate group* $\mathrm{ST}(A/k)$ is a maximal compact subgroup of $\mathrm{AST}(A/K) \otimes_{\mathbb{Q}} \mathbb{C}$.

Conjecture (Refined Sato-Tate)

The $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on $\mathrm{ST}(A/k)$. (A stronger statement gives an equidistribution on $\mathrm{Cl}(\mathrm{ST}(A/k))$.)

An ℓ-adic Sato-Tate group (after Serre)

Let $G_{\ell,1}$ be the kernel of $G_\ell \to \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell^\times$, where the last map comes from the Weil pairing. Let $G_{\ell,1}^{\mathrm{Zar}}$ denote the Zariski closure of $G_{\ell,1}$ in $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. It is generally not connected!

Conjecture (Algebraic Sato-Tate)

The group $G_{\ell,1}^{\mathrm{Zar}}$ descends to an algebraic group G_1^{Zar} over $\mathbb{Q}$ which does not depend on ℓ.

We call G_1^{Zar} the *algebraic Sate-Tate group* of A/k, denoted $\mathrm{AST}(A/k)$. The *Sato-Tate group* $\mathrm{ST}(A/k)$ is a maximal compact subgroup of $\mathrm{AST}(A/K) \otimes_{\mathbb{Q}} \mathbb{C}$.

Conjecture (Refined Sato-Tate)

The $\overline{L}_{\mathfrak{p}}(A/k, T)$ are equidistributed for the image on $\mathrm{Cl}(\mathrm{USp}(2g))$ of the Haar measure on $\mathrm{ST}(A/k)$. (A stronger statement gives an equidistribution on $\mathrm{Cl}(\mathrm{ST}(A/k))$.)

Sato-Tate and endomorphism algebras

Theorem-in-progress (with Banaszak)

For $g \leq 3$, the algebraic Sato-Tate conjecture holds for A/k.

This is obtained by proving an open image theorem relating $\mathrm{AST}(A/k)$ to an upper bound defined using $\mathrm{End}_{\mathbb{Q}}(A_{\overline{k}})$. The argument applies to a large class of cases in which each simple factor of $A_{\overline{k}}$ has "enough" endomorphisms, by following the treatment of the Mumford-Tate conjecture in these cases by Banaszak-Gajda-Krasoń.

As a corollary of the proof, one identifies $\mathrm{AST}(A/k)/\mathrm{AST}(A/k)^0$ with $\mathrm{Gal}(L/k)$ for L the minimal extension of k for which $\mathrm{End}(A_L) = \mathrm{End}(A_{\overline{k}})$.

Contents

Properties of Sato-Tate groups

Under standard conjectures, the group $G = \mathrm{ST}(A/k)$ has these properties.

(ST1) The real Lie group G is the intersection of $\mathrm{USp}(2g)$ with a reductive $\mathbb{Q}$-algebraic subgroup of Sp_{2g}.

(ST2) There exists a homomorphism $\theta : \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g, and $\theta(-1) = -1 \in \mathrm{USp}(2g)$. The image of such a homomorphism θ is called a *Hodge circle*.

(ST3) The group G^0 is generated by the Hodge circles.

(ST4) Each component of G contains an element whose characteristic polynomial $P(T)$ is such that $P(T/\sqrt{m})$ has rational coefficients for some positive integer m.

For given g, this limits $\mathrm{ST}(A/k)$ to *finitely many* groups up to conjugacy.

Properties of Sato-Tate groups

Under standard conjectures, the group $G = \mathrm{ST}(A/k)$ has these properties.

(ST1) The real Lie group G is the intersection of $\mathrm{USp}(2g)$ with a reductive $\mathbb{Q}$-algebraic subgroup of Sp_{2g}.

(ST2) There exists a homomorphism $\theta : \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g, and $\theta(-1) = -1 \in \mathrm{USp}(2g)$. The image of such a homomorphism θ is called a *Hodge circle*.

(ST3) The group G^0 is generated by the Hodge circles.

(ST4) Each component of G contains an element whose characteristic polynomial $P(T)$ is such that $P(T/\sqrt{m})$ has rational coefficients for some positive integer m.

For given g, this limits $\mathrm{ST}(A/k)$ to *finitely many* groups up to conjugacy.

Properties of Sato-Tate groups

Under standard conjectures, the group $G = \mathrm{ST}(A/k)$ has these properties.

(ST1) The real Lie group G is the intersection of $\mathrm{USp}(2g)$ with a reductive $\mathbb{Q}$-algebraic subgroup of Sp_{2g}.

(ST2) There exists a homomorphism $\theta : \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g, and $\theta(-1) = -1 \in \mathrm{USp}(2g)$. The image of such a homomorphism θ is called a *Hodge circle*.

(ST3) The group G^0 is generated by the Hodge circles.

(ST4) Each component of G contains an element whose characteristic polynomial $P(T)$ is such that $P(T/\sqrt{m})$ has rational coefficients for some positive integer m.

For given g, this limits $\mathrm{ST}(A/k)$ to *finitely many* groups up to conjugacy.

Properties of Sato-Tate groups

Under standard conjectures, the group $G = \mathrm{ST}(A/k)$ has these properties.

(ST1) The real Lie group G is the intersection of $\mathrm{USp}(2g)$ with a reductive $\mathbb{Q}$-algebraic subgroup of Sp_{2g}.

(ST2) There exists a homomorphism $\theta : \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g, and $\theta(-1) = -1 \in \mathrm{USp}(2g)$. The image of such a homomorphism θ is called a *Hodge circle*.

(ST3) The group G^0 is generated by the Hodge circles.

(ST4) Each component of G contains an element whose characteristic polynomial $P(T)$ is such that $P(T/\sqrt{m})$ has rational coefficients for some positive integer m.

For given g, this limits $\mathrm{ST}(A/k)$ to *finitely many* groups up to conjugacy.

Properties of Sato-Tate groups

Under standard conjectures, the group $G = \mathrm{ST}(A/k)$ has these properties.

(ST1) The real Lie group G is the intersection of $\mathrm{USp}(2g)$ with a reductive $\mathbb{Q}$-algebraic subgroup of Sp_{2g}.

(ST2) There exists a homomorphism $\theta : \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g, and $\theta(-1) = -1 \in \mathrm{USp}(2g)$. The image of such a homomorphism θ is called a *Hodge circle*.

(ST3) The group G^0 is generated by the Hodge circles.

(ST4) Each component of G contains an element whose characteristic polynomial $P(T)$ is such that $P(T/\sqrt{m})$ has rational coefficients for some positive integer m.

For given g, this limits $\mathrm{ST}(A/k)$ to *finitely many* groups up to conjugacy.

Classification in genus 2

Theorem (with Fité, Rotger, Sutherland)

For $g = 2$, there are exactly 55 *conjugacy classes of subgroups G of* $\mathrm{USp}(4)$ *satisfying (ST1)-(ST4). In this list,*

$$G^0 \in \{\mathrm{SO}(2) \text{ (32 cases)}, \mathrm{SU}(2) \text{ (10 cases)}, \mathrm{SO}(2) \times \mathrm{SO}(2) \text{ (8 cases)}, \mathrm{SO}(2) \times \mathrm{SU}(2) \text{ (2 cases)}, \mathrm{SU}(2) \times \mathrm{SU}(2) \text{ (2 cases)}, \mathrm{USp}(4) \text{ (1 case)}\}.$$

(Hint: $\mathrm{USp}(4)/\{\pm 1\} \cong \mathrm{SO}(5)$.) The cases $G^0 = \mathrm{SO}(2)$ come from finite subgroups of $\mathrm{SU}(2)/\{\pm 1\} \cong \mathrm{SO}(3)$. The icosahedral group fails (ST4), but the tetrahedral and octahedral groups survive!

Problem

Carry out the same exercise for $g = 3$.

Matching to Galois type

For $g = 2$, one can determine $\mathrm{ST}(A/k)$ in terms of $\mathrm{End}_{\mathbb{Q}}(A_{\overline{k}})$, using both the algebra structure and the G_k-action (though the former plays a surprisingly small role). The right package of data (definition omitted) is what we call the *Galois type*.

Theorem-in-progress (with Fité, Rotger, Sutherland)

There are exactly 52 *Galois types. Of these, exactly* 34 *can be realized with* $k = \mathbb{Q}$.

Detailed information about the distributions over $\mathbb{Q}$ can be found here:

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

Contents

Computing $\overline{L}_{\mathfrak{p}}(A/k, T)$

To test the refined Sato-Tate conjecture numerically, one chooses A/k and then computes $L_{\mathfrak{p}}(A/k, T)$ for many prime ideals $\mathfrak{p}$. For example, for $k = \mathbb{Q}$, for A the Jacobian of a hyperelliptic curve, we can compute $L_p(A/k, T)$ for all $p \leq 2^{30}$. (This is far more data than is really needed!)

The key technique is Sutherland's highly optimized version of the baby steps-giant steps algorithm; see our ANTS 8 paper. Methods of p-adic cohomology, as optimized by David Harvey, do not beat this until $p \geq 2^{40}$. Schoof-type methods, as optimized by Gaudry-Schost, kick in even later except maybe in some special cases, e.g., real multiplication (Gaudry-Kohel-Smith).

Give me a moment...

To deal with this mass of data, we find it easiest to use *moment statistics*.

Theorem

For any group $G \subseteq \mathrm{USp}(2g)$ satisfying (ST1)-(ST4), the expected value of any symmetric function of the eigenvalues is an integer.

For G given explicitly, it is easy to compute these expected values for powers of the first or second coefficient of the characteristic polynomial. We then use these to test equidistribution. See again

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

for animations illustrating many cases.

Contents

What can be proved in dimension 2?

Current technology on modularity of Galois representations seems incapable of proving Sato-Tate in even a single case with $g = 2$ and $\mathrm{ST}(A/k) = \mathrm{USp}(4)$. (It seems crucial to have distinct Hodge-Tate weights, i.e., to have a *regular* motive.)

However, it should be possible to handle *every* case with $g = 2$ and $\mathrm{ST}(A/k) \neq \mathrm{USp}(4)$. The most delicate cases are when $\mathrm{ST}(A/k)$ contains $\mathrm{SU}(2) \times \mathrm{SU}(2)$; these should be tractable using Rankin-Selberg convolution, as observed by Michael Harris. (This does not generalize to $\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$.)

Problem

Prove the refined Sato-Tate conjecture for all A/k with k totally real, $g = 2$, and $\mathrm{ST}(A/k) \neq \mathrm{USp}(4)$.

Finding Mumford's fourfolds

Mumford described a family of abelian fourfolds for which the endomorphism algebra is trivial but the Mumford-Tate group is not. This discrepancy should be reflected in the Sato-Tate distribution.

Problem

Identify the Sato-Tate distribution corresponding to Mumford's fourfolds, and compute moments. Then find A with $g = 4$ for which the Sato-Tate distribution appears to have matching moments.

It is not clear over which number fields one should find such examples, or what form they may take. (E.g., it seems unlikely that they occur as Jacobians.)