The Sato-Tate Conjecture
Lecture 12

Elisa Lorenzo García

9th May 2016

Contents

1 The Sato-Tate Conjecture

We will start motivating the study of the Sato-Tate Conjecture with a simple example.

1.1 Counting points

Let us consider the (complex multiplication) elliptic curve given by the equation

$$E : y^2 = x^3 + x/\mathbb{Q}.$$

It has good reduction at every prime. In the table below, we show the number of points of this curve over the finite field $\mathbb{F}_p$ for the first values of the prime p.

p	3	5	7	11	13	17	19	23	29
$\#E(\mathbb{F}_p) = 1 + p - a_1(p)$	4	4	8	12	20	16	20	24	20

Here, $a_1(p)$ demotes the trace of the Frobenius endomorphism. In other words, if we denote the ℓ–Tate module by $V_\ell(E) := T_\ell(E) \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^2$ and we consider the natural Galois representation attached to it

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_\ell),$$

the image of a Frobenius element in $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfies the equation

$$L_p(E/\mathbb{Q}, T) := T^2 - a_1(p)T + p = 0.$$

p	3	5	7	11	13	17	19	23	29
$\#E(\mathbb{F}_p) = 1 + p - a_1(p)$	4	4	8	12	20	16	20	24	20
$a_1(p)$	0	2	0	0	-6	2	0	0	10

Weil's Conjecture (now, a Theorem by Deligne [7]) implies that $a_1(p)$ is an integer number in the interval $[-2\sqrt{p}, 2\sqrt{p}]$. So, we can work with the normalized coefficient $\overline{a}_1(p) = a_1(p)/\sqrt{p} \in [-2, 2]$. We can also define the number $\theta_p = \arccos(\frac{\overline{a}_1(p)}{2})$ $(2\cos(\theta_p) = \overline{a}_1(p))$.

So, we can consider the functions $\overline{a}_1$ and θ as random variables from the set of primes of good reduction of the elliptic curve E to the intervals $[-2, 2]$ and $[0, \pi]$ respectively.

$$\overline{a}_1 : \{\text{primes of good reduction}\} \longrightarrow [-2, 2],$$

$$\theta : \{\text{primes of good reduction}\} \longrightarrow [0, \pi].$$

p	3	5	7	11	13	17	19	23	29
$\#E(\mathbb{F}_p) = 1 + p - a_1(p)$	4	4	8	12	20	16	20	24	20
$a_1(p)$	0	2	0	0	-6	2	0	0	10
$\overline{a}_1(p)$	0	0,89...	0	0	$-1,66...$	0,48...	0	0	1,86...

What's the distribution of $\overline{a}_1$?

1.2 The statement of the Conjecture

We are now ready to state the Sato-Tate Conjecture:

Conjecture 1.1 (Sato-Tate)**.** *Let E be an elliptic curve defined over a number field k without CM. The random variable $\overline{a}_1$ has the semicircular distribution. Equivalently, the angles θ are equidistributed with respect to the measure $\frac{2}{\pi}\sin^2\theta\,\mathrm{d}\theta$ on $[0, \pi]$. Which is again equivalent to say, that the polynomials $L_{\mathfrak{p}}(E/k, T/\sqrt{\mathrm{N}\mathfrak{p}})$ are equidistributed with respect to the characteristic polynomials of the elements of the algebraic group* USp_2 [1] *with the Haar measure μ*[2]*.*

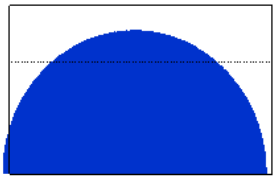

Figure 1 – The distribution function of $\overline{a}_1$, $f(t) = \frac{1}{2\pi}\sqrt{4 - t^2}$.

Remark 1.2. *We can reinterpret the angles θ as a parametrization of the symplectic characteristic polynomials $T^2 - 2\cos(\theta)T + 1$ with complex conjugated roots $e^{i\theta}$, $e^{-i\theta}$.*

[1] We denote by GSp_{2g} the group of symplectic matrices, that is, $\gamma \in \mathrm{GL}_{2g}$ such that $\gamma^* J \gamma = \lambda J$ for some non-zero λ and some skew-symmetric matrix J. By Sp_{2g}, we mean the subgroup of the previous group with $\lambda = 1$, and by USp_{2g} the subgroup with $\det(\gamma) = 1$. We denote by $\mathrm{U}(n)$ the group of $n \times n$ unitary matrices $(M \cdot M^* = \mathrm{I})$, and by $\mathrm{SU}(n)$, the subgroup of matrices with determinant equal to 1 in $\mathrm{U}(n)$. There is a natural embedding of $\mathrm{U}(n)$ into $\mathrm{SU}(2n)$. Notice the $\mathrm{USp}_2 = \mathrm{SU}(2)$

[2] The Haar measure μ is the only measure with "good" properties in a compact Lie group up to rescaling.

[3] The figures have been obtained from A.V. Sutherland website math.mit.edu/~drew/, where so many other interesting distributions can be found

The Sato-Tate Conjecture was independently conjectured by Sato, after numerically experiments, and Tate, from theoretical evidences, in the 60's. One of the main evidences was the equivalent result for complex multiplication curves stated by Hecke in 1920, [16].

Theorem 1.3 (Hecke)**.** *Let E be an elliptic curve defined over a number field k with CM. Then the random variables $\overline{a}_1$ defined above are equidistributed with respect to the traces of the matrices in the groups* $\mathrm{U}(1)$ *or* $\mathrm{N}(\mathrm{U}(1))$ *(normalizer of* $\mathrm{U}(1)$ *in* $\mathrm{SU}(2)$*) depending on whenever the CM is also defined or not over k.*

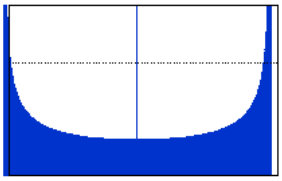

Figure 2 – The distribution function of $\overline{a}_1$, $f(t) = \frac{1}{2\pi}\frac{1}{\sqrt{4-t^2}} + \frac{1}{2}\delta_0(t)$.

In the first case, when the CM is not defined over the base field k, the distribution is not a continuous distribution. the density function has a continuous part plus a discrete one. The discrete contribution disappears when the CM is defined over k. This is explained by the fact that in the first case half of the primes happen to be supersingular. While in the second case the density of the supersingular primes becomes equal to zero[4].

The Sato-Tate conjecture is only proved (2006) for totally real number fields after some works of Clozel, Harris, Shepherd-Barron and Taylor, [2], [6], [17].

2 The Generalized Sato-Tate Conjecture

For this section we suggest to read the main references [8] and [24].

Let A/k be an abelian variety defined over a number field k of dimension g. Given a prime ℓ of good reduction, we have the Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

the image by this representation of a Frobenius $\mathrm{Frob}_\mathfrak{p} \in \mathrm{G}_k$ satisfies

$$L_\mathfrak{p}(A/k, T) = \sum_{i=0}^{2g} (-1)^i a_i(\mathfrak{p}) T^i = 0,$$

where again, Weil's Conjectures imply that

$$a_i \in \left[-(\mathrm{N}\,\mathfrak{p})^{i/2} \binom{2g}{i}, (\mathrm{N}\,\mathfrak{p})^{i/2} \binom{2g}{i} \right] \cap \mathbb{Z},$$

and that the polynomial $L_\mathfrak{p}(A/k, T/\sqrt{\mathrm{N}\,\mathfrak{p}}) = \sum_{i=0}^{2g} (-1)^i \overline{a}_i(\mathfrak{p}) T^i$ is symmetric and symplectic. Which means that the numbers

$$\overline{a}_{2g-i}(\mathfrak{p}) = \overline{a}_i(\mathfrak{p}) = a_i q^{i/2} \in \left[-\binom{2g}{i}, \binom{2g}{i} \right]$$

lie in an interval that does not depend on the prime $\mathfrak{p}$.

This time, we define the angles $\{\theta_1, ..., \theta_g\} \in [0, \pi]$ as the angles that produce the eigenvalues $\sqrt{\mathrm{N}\,\mathfrak{p}} e^{i\theta_j}$ of the equation $L_\mathfrak{p}(A/k, T) = 0$.

[4] Prove this as an exercise

What's about the distribution of $\overline{a}_i$'s

and, how to describe it?

We will answer first the second question. We will use a group, a group whose elements are matrices, and we will conjecture that the distribution of the $\overline{a}_i$'s will be the same that the distribution of the coefficients of the characteristic polynomials of the matrices in such group, that we will call the Sato-Tate group, $\mathrm{ST}_k(A)$. It will be a compact Lie group and then, there will be a unique Haar measure up to rescaling.

For instance, for the genus 1 case, we got three different options

$$\mathrm{ST}_k(E) = \begin{cases} \mathrm{SU}(2) & \text{non CM case} \\ \mathrm{U}(1) & \text{CM defined over } k \\ \mathrm{N}(\mathrm{U}(1)) & \text{CM not defined over } k \end{cases}$$

More explicitly, we have:

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C}, \text{ s.t. } a\overline{a} + b\overline{b} = 1 \right\}$$

$$\mathrm{U}(1) = \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} : \theta \in [0, 2\pi] \right\}$$

$$\mathrm{N}(\mathrm{U}(1)) = \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}, \begin{pmatrix} 0 & e^{i\theta} \\ -e^{-i\theta} & 0 \end{pmatrix} : \theta \in [0, 2\pi] \right\}$$

2.1 The statement of the Conjecture

We can now state the Generalized Sato-Tate (GST) Conjecture.

Conjecture 2.1 (Generalized Sato-Tate)**.** *Let A/k be an abelian variety defined over a number field k. Then, the local factors $L_{\mathfrak{p}}(A/k, T/(\mathrm{N}\mathfrak{p})^{1/2})$ are equidistributed with respect to the distribution of the characteristic polynomials of the matrices in $\mathrm{ST}_k(A)$ with respect to the Haar measure μ.*

The only case proved is due to Johansson in [18], where he proves that the conjectures is true for complex multiplication abelian varieties.

There exists an extra generalization to this conjecture due to Jean-Pierre Serre, [24]. This generalization is for *motives*, but we can think in a simpler one for varieties, where we have to switch the Tate module $V_\ell(A)$ by the cohomology set $\mathrm{H}^{\dim(X)}_{et}(X, \mathbb{Q}_\ell)$.

Example 2.2. *A zero case of this generalization is the well-known Chebotarev's Density Theorem. Our object is a Galois number field extension L/k, the primes of bad reduction the ramified ones and the Sato-Tate group the Galois group $\mathrm{Gal}(L/k)$. Let us fix a conjugacy class $c \in \mathrm{Gal}(L/k)$, the set of primes such that $\mathrm{frob}_{\mathfrak{p}} = c$ has density $\frac{\#c}{[L:k]}$.*

2.2 The Sato-Tate group

In this section, we will try to give a more precise definition of the Sato-Tate group. Let us start with an abelian variety A/k defined over a number field k with dimension g. Let us fix ℓ a prime of good reduction and let us consider the Galois representation attached to it.

$$\rho_\ell : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{Aut}(\mathrm{V}_\ell(A)) = \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

let us denote by $G_{k,\ell}$ the kernel in $\mathrm{Gal}(\overline{k}/k)$ of the cyclotomic character[5], and by G_ℓ the Zariski closure of the image of $G_{k,\ell}$ by the representation ρ_ℓ, which we view as a $\mathbb{Q}_\ell$-algebraic subgroup of Sp_{2g} (Weil pairing allows

[5]The cyclotomic character $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell)$ is the natural one given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the l^nth-roots of unity.

us to consider only symmetric matrices). Choose an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and denote by $G_{\ell,\iota} \subseteq \mathrm{Sp}_{2g}(\mathbb{C})$ the group of complex points of $G_\ell \otimes_\iota \mathbb{C}$.

Definition 2.3 (Sato-Tate group)**.** *The Sato-Tate group of the abelian variety A/k is a maximal compact subgroup of $G_{\ell,\iota}$. It is a compact Lie group, and we denote it by $\mathrm{ST}_k(A)$.*

Remark 2.4. *The Sato-Tate group is well-defined: there is up to conjugation a unique compact subgroup and the definition does not depend on the choice of the prime ℓ and the embedding ι. On the other hand, it depends on the field of definition of the abelian variety, so it is sensitive to base field extension.*

In [24], Serre states some axioms that a general Sato-Tate group may satisfy. These axioms are useful in order to list all the possible Sato-Tate groups of certain varieties of fixed dimension.

Conjecture 2.5 (Serre)**.** *The Sato-Tate group $\mathrm{ST}_k(A)$ of an abelian variety of dimension g satisfies the following properties:*

i) It is a closed subgroup of $\mathrm{USp}_{2g}(\mathbb{C})$.

ii) (Hodge condition) There exists a subgroup H, called a Hodge circle, which is the image of a homomorphism $\theta : \mathrm{U}(1) \longrightarrow \mathrm{ST}_k^0(A)$ with some extra properties.

iii) (Rationality condition) For each component C of $\mathrm{ST}_k(A)$ and for each character χ of GL_{2g}, the expected value

$$\int_{g \in C} \chi(g)\mu(g)$$

is an integer.

This conjecture is in fact a theorem for $g \leq 3$, [1], [10].

Before starting to show some particular examples, we will review a useful result to characterize the distributions we are interested in due to Kedlaya and Sutherland.

Proposition 2.6 (Proposition 1 and 2, section 4 in [19])**.** *Under the generalized Sato-Tate conjecture, the moments of the random variables $\overline{a}_i$ exist and determine the distribution. Moreover, the expected values $M_n(\overline{a}_i) = \mathrm{E}[\overline{a}_i^n]$ are integer numbers.*

Example 2.7. *The moment sequence for the three genus 1 case are*

$$\begin{aligned} \mathrm{SU}(2) &: 1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, ... \\ \mathrm{U}(1) &: 1, 0, 2, 0, 6, 0, 20, 0, 70, 0, 252, 0, ... \\ \mathrm{N}(\mathrm{U}(1)) &: 1, 0, 1, 0, 3, 0, 10, 0, 35, 0, 126, 0, ... \end{aligned}$$

Exercise 2.8. *Prove that the moment sequences in 2.7 correspond to the Sato-Tate groups claimed.*

We will also mention here the main result to compute Sato-Tate groups, [1]. all the Sato-Tate groups known not corresponding to elliptic curves have been computed by using it.

Definition 2.9 (Lefschetz twisted group)**.** *Given an abelian variety A/k with endomorphism algebra $D = \mathrm{End}^0(A)$ defined over a extension L/k, we define the Lefschetz group of A/k as*

$$\mathrm{L}_k(A) = \bigcup_{\tau \in \mathrm{Gal}(L/k)} \mathrm{L}_k^\tau(A),$$

where for each $\tau \in \mathrm{Gal}(L/k)$ we get the component

$$\mathrm{L}_k^\tau(A) = \{\gamma \in \mathrm{Sp}_{2g} : \gamma\beta\gamma^{-1} =^\tau \beta \text{ for all } \beta \in D\}.$$

Theorem 2.10 (Banaszak, Kedlaya)**.** *For A/k an abelian variety of dimension $g \leq 3$ or with CM, the Sato-Tate group $\mathrm{ST}_k(A)$ is a maximal compact subgroup of $\mathrm{L}_k(A)$.*

Remark 2.11. *Banaszak and Kedlaya prove that Theorem 2.10 also holds for more general varieties, but for our purposes this cases are enough.*

Exercise 2.12. *Compute explicitly the Sato-Tate group $\mathrm{ST}_{\mathbb{Q}}(E)$, for $E : y^2 = x^3 - x$, using Theorem 2.10.*

3 The genus 2 case

The main references for this section are [19] and [10], [14]. Fité, Kedalaya, Rotger and Sutherland prove, using Serre axioms that there are 55 Sato-Tate possibilities for the Sato-Tate group of an abelian surface. They prove that in fact, only 52 of them appear as Sato-Tate groups, and even more, all of them are reached by jacobians of genus 2 curves. Among these 52 groups, only 34 of them can be realized with abelian varieties defined over $\mathbb{Q}$. They find candidate curves that attain these Sato-Tate groups and provide numerically evidences of the matches. See again Sutherland website for animate diagrams: math.mit.edu/~drew/. After Johansson's results [18], the Sato-Tate conjecture is proven for the genus 2 curves with CM. For example, for the curves $y^2 = x^6 + 1$ and $y^2 = x^5 - x$. Fité and Sutherland compute the Sato-Tate groups for them and their twists, [14], obtaining 18 out of the 52 (34 over $\mathbb{Q}$) possibilities for these groups. In order to compute these groups, they use the results of Banaszak and kedlaya concerning the Lefschez group, [1].

4 The genus 3 case

The main references for this section are [13], [20] and [15]. The computation of a list with the candidates a Sato-Tate group is still work in progress by Fité, Kedalaya and Sutherland. For elliptic curves, there are 3 possibilities. For genus 2 curves, we have already seen that there are 52, so the number expected for genus 3 curves is really big. Tt is expected, again, that considering twists of curves with so many automorphism (and with CM, so the conjecture is proved by Johansson [18]), we will be able to realize so many of these groups. Fié and Sutherland compute these groups for some twists of the two hyperelliptic genus 3 curves $y^2 = x^8 + 1$ and $y^2 = x^7 - x$, [15], and both of them and Lorenzo in [20, Chapter 4] and [13] compute the Sato-Tate groups and distributions for all the twists of the non-hyperelliptic genus 3 curves $x^4 + y^4 + z^4 = 0$ and $x^3y + y^3z + z^3x = 0$, obtaining 59 and 22 (respectively) different distributions. Numerically confirmation for these distribution is waiting for an efficient implementation of an algorithm to compute number of points over finite fields of genus 3 non-hyperelliptic curves due to Sutherland and Harvey. The other examples studied were all of them hyperelliptic curves where such an algorithm already exists.

5 Other examples

The only proved cases of the Sato-Tate conjecture for curves of genus greater than 1 are the complex multiplication cases due to the work of Johansson [18]. The only explicit known examples are quotients of Fermat curves [12] and Fermat curves themselves [20, Chapter 5], [23] of arbitrary big genus g.

References

[1] G. Banaszak, K.S. Kedlaya, *An algebraic Sato-Tate group and Sato-Tate conjec- ture*, to appear in the Indiana University Mathematics Journal, 2 014.

[2] T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, *A family of Calabi-Yau varieties and potential automorphy. II*, Publ. Res. Inst. Math. Sci 47 (1): 29-98, 2011.

[3] A. Bucur, K.S. Kedlaya, *An application of the effective Sato-Tate conjecture*, to appear in the proceedings of the conference "Frobenius distributions" celebrated in Luminy in 2014, Contemporary Mathematics, 2015. .

[4] G. Cardona, *Models Racionals de Corbes de Genere 2*, thesis, 2001.

[5] C. David, *Curves and Zeta functions over finite fields*, Arizona Winter school 2014: Arithmetic statistics.

[6] L. Clozel, M. Harris, R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. 108: 1-181, 2008.

[7] P. Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l'IHES 43, 273-307, 1974.

[8] F. Fité, *Equidistribution, L-functions, and Sato-Tate groups*, Contemporary Mathematics 649, 63-88, 2015.

[9] F. Fité, X. Guitart, *Fields of definition of elliptic k-curves and the realizability of all genus* 2 *Sato-Tate groups over a number field*

[10] F. Fité, K.S. Kedlaya, V. Rotger, A.V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compositio Mathematica 148, n. 5, 1390-1442, 2012.

[11] F. Fité, K.S. Kedlaya, A.V. Sutherland, *Sato-Tate groups of some weight 3 motives*, to appear in the proceedings of the conference "Frobenius distributions" celebrated in Luminy in 2014, Contemporary Mathematics, 2015.

[12] F. Fité, J. González, J.-C. Lario, *Frobenius distribution for quotients of Fermat curves of prime exponent*, to appear in the Canadian Journal of Mathematics.

[13] F. Fité, E. Lorenzo, A.V. Sutherland, *Sato-Tate distributions of twists of the Fermat and Klein quartics*, preprint.

[14] F. Fité, A.V. Sutherland, *Sato-Tate distributions of twists of* $y^2 = x^5 - x$ *and* $y^2 = x^6 + 1$, Algebra & Number Theory 8 n. 3, 543-585, 2014.

[15] F. Fité, A.V. Sutherland, *Sato-Tate groups of* $y^2 = x^8 + c$ *and* $y^2 = x^7 - cx$, to appear in the proceedings of the conference "Frobenius distributions" celebrated in Luminy in 2014, Contemporary Mathematics, 2015.

[16] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Ve rteilung der Primzahlen*, Zweite Mitteilung, Math. Zeit.6, 11-51, 1920.

[17] M. Harris, N. Shepherd-Barron, R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Annals of Mathematics 171 (2), 779-813, 2010.

[18] C. Johansson, *On the Sato-Tate conjecture for non-generic abelian surfaces*, to appear in Transactions of the A.M.S.

[19] K.S. Kedlaya, A.V. Sutherland, *Hyperelliptic curves, L -polynomials, and random matrices* , Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT 2007), Contemporary Math. 487 , Amer. Math. Soc., 119-162, 2009.

[20] E. Lorenzo, *Arithmetic properties of non-hyperelliptici genus* 3 *curves*, thesis, 2014.

[21] E. Lorenzo, *Twists of non-hyperelliptic curves*, to appear in Revista Matemática Iberoamericana.

[22] E. Lorenzo, *Twists of non-hyperelliptic genus* 3 *curves*, preprint.

[23] E. Lorenzo, *Sato-Tate conjecture for Fermat hypersurfaces*, preprint.

[24] J.-P. Serre, *Lectures on NX(p)*, A.K. Peters, 2012.

[25] J.H. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.