# SATO-TATE DISTRIBUTIONS
## ARIZONA WINTER SCHOOL 2016

ANDREW V. SUTHERLAND
ASSISTED BY FRANCESC FITÉ

### COURSE OUTLINE

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. For each prime $p$ of good reduction for $E$ (all but finitely many), let $E_p := E \bmod p$ denote the reduced curve and let

$$a_p := p + 1 - \#E_p(\mathbb{F}_p)$$

be the *trace of Frobenius*. By a theorem of Hasse, each normalized trace $x_p := a_p/\sqrt{p}$ is a real number in the interval $[-2, 2]$. The $x_p$ vary with $p$ in an apparently unpredictable way, and in the absence of any other information, one might suppose that they should be uniformly distributed over $[-2, 2]$. A few experiments quickly dispels this notion (here is a typical example), however, the distribution of the $x_p$ does appear to be converging to *something*. Remarkably, with just a few exceptions, it does not seem to matter which elliptic curve we use (here is an extreme example), the picture always looks the same asymptotically. This was observed some fifty years ago by Mikio Sato and John Tate, who independently conjectured that the semicircular distribution visible in two of the three linked examples above is the limiting distribution of the $x_p$ for every elliptic curve $E/\mathbb{Q}$ without complex multiplication (this means $\mathrm{End}(E_{\overline{\mathbb{Q}}}) = \mathbb{Z}$, which is typically the case). Thanks to recent work by Richard Taylor and others [5, 13, 34], the Sato-Tate conjecture is now a celebrated theorem.

The Frobenius traces $a_p$ also appear as coefficients in the $L$-series of the elliptic curve. One can ask similar questions about other $L$-functions, such as those attached to modular forms (with rational coefficients), algebraic curves, abelian varieties, Galois representations, or more generally, any *motivic L-function*. Almost all of these more general questions remain open, but a rich theory and a precise set of conjectures has arisen around them that suggest deep connections between the analytic and arithmetic aspects of these $L$-functions (this may be viewed as part of the Langlands program).

The goal of this course is to introduce *Sato-Tate distributions*, both from an analytic perspective (as distributions of normalized Euler factors of $L$-functions), and an arithmetic perspective (as distributions of normalized Frobenius polynomials), and to describe the generalized *Sato-Tate conjecture*, which postulates that in each case these distributions are governed by the Haar measure of a certain compact Lie group, the *Sate-Tate group* (of the $L$-function or motive).

**Lecture 1. Introduction to Sato-Tate distributions.** We introduce the topic of Sato-Tate distributions by first considering the situation in dimension zero, in which the $L$-functions of interest are Artin $L$-functions, Sato-Tate groups arise as images of Artin representations, and equidistribution is implied by the Chebotarev density theorem. We then present the Sato-Tate Conjecture/Theorem for elliptic curves over $\mathbb{Q}$.

**Lecture 2. Equidistribution, $L$-functions, and moment sequences.** We formally define the notion of equidistribution with respect to a measure and relate it to $L$-functions arising from representations of compact groups as Euler products over primes of a given number field. We then prove the Sato–Tate conjecture for CM elliptic curves and present Tate's formulation of the Sato–Tate conjecture for non-CM elliptic curves $E$ as a statement about the analytic properties of a family of associated $L$-functions [27, 33].

**Lecture 3. Sato-Tate groups.** Following Serre [30, 31], we define the *Sato–Tate group* of an abelian variety over a number field and state the generalized Sato–Tate conjecture. We then relate the identity component of the Sato–Tate group to the Mumford–Tate and Hodge groups associated to an abelian variety and show that the group of components can be realized as a Galois group. We also discuss the *algebraic Sato–Tate group* of Banaszak and Kedlaya [2, 3].

**Lecture 4. Sato–Tate axioms.** We present the *Sato–Tate axioms* for abelian varieties (and for self-dual motives with rational coefficients), following [9, §2] and [31, Ch. 8], and consider the problem of classifying the groups that satisfy the Sato–Tate axioms for a given weight and choice of Hodge numbers. We then introduce *Galois endomorphism types* and explain their relationship with Sato-Tate groups, which has produced a complete classification in dimension $g \le 2$ and partial results in dimension 3. Finally, we consider the problem of computing the Haar measure for a given Sato-Tate group, via the Weyl integration formulas [37], and explain how these may be used to compute moment sequences and moment generating functions.

## Project Descriptions

**Project 1. Sato-Tate groups of trinomial hyperelliptic curves.** For each integer $g \ge 2$ we may consider the following one-parameter families of hyperelliptic curves of genus $g$:

$$C_1(a)\colon y^2 = x^{2g+2} - a, \qquad C_2(a)\colon y^2 = x^{2g+1} - ax, \qquad C_3(a)\colon y^2 = x^{2g+1} - a,$$

with $a \in \mathbb{Q}^\times$. As explained in [12, §2], the Hasse–Witt matrices of these curves have a particularly simple form that makes it possible to use an optimized version of the average polynomial-time algorithm in [17] to compute statistic of normalized Frobenius traces very quickly for moderate values of $g$ (say $2 \le g \le 10$). In many cases one can do even better by applying explicit trace formulas, as in [12, §3.1] and [36], for example. For $g = 3$ the families $C_1(a)$ and $C_2(a)$ are analyzed in [12].

The goal of this project is to similarly analyze the trace distributions for curves in these families for various values of $g$ as follows:

- **(a)** Compute trace formulas for each family, following [12, §3].
- **(b)** Determine the possible shapes of the corresponding Hasse-Witt matrices as in [12, §4] and use this to determine the density of zero traces for generic values of $a$.
- **(c)** Determine trace moment sequences for generic values of $a$.
- **(d)** Refine your answers to (b) and (c) for special values of $a$.
- **(e)** Using your knowledge of the trace distributions, try to determine (or at least guess) the identity component of the Sato-Tate group (as in [12, §5], for example).

Note that in steps (b)–(e), you can empirically check/guide your work by computing moment statistics of example curves (software to do so will be provided [14, 15, 16, 17, 23, 32]).

**Project 2. Classifying Sato-Tate groups of abelian threefolds with finite centralizer.** A key step in the classification of Sato-Tate groups of abelian surfaces was determining, up to conjugacy, the 55 subgroups of USp(4) that satisfy the Sato-Tate axioms [9, §3] (it turns out that only 52 of these arise as Sato-Tate groups of an abelian surface [9, §4]). The corresponding classification for USp(6), which includes the Sato-Tate groups of all abelian threefolds, remains open, although some progress has been made; for example, the connected Sato-Tate groups are known (a complete list can be found here).

The main obstacle to completing the classification of candidate Sato-Tate groups in USp(6) is that some of the connected Sato-Tate groups have very large centralizers, and this makes it difficult to exhaustively determine all candidates with this identity component. The goal of this project is to address the easier cases, those for which the centralizer of $G^0$ is finite. In parallel, we would also like to find or construct abelian threefolds (ideally as Jacobians of genus 3 curves) whose Sato-Tate groups appear to match these candidates, by comparing moment statistics to moment sequences (as the case of abelian surfaces demonstrates, there is no reason to expect that we will be able to do so in every case).

The goal of this project is to classify the Sato-Tate groups USp(6) with finite centralizer by proceeding as follows:

- **(a)** Determine which connected Sato-Tate groups $G^0 \subseteq \mathrm{USp}(6)$ have finite centralizer $Z$.
- **(b)** For each pair $(G^0, Z)$, determine a complete list (up to conjugacy) of the subgroups of USp(6) that satisfy the Sato-Tate axioms and have identity component $G^0$.
- **(c)** Compute moment sequences for each of the candidate Sato-Tate groups.
- **(d)** For each candidate Sato-Tate group, try to find a genus 3 curve whose moment statistics appear to match the moment sequences computed in (c).
- **(e)** (optional) Determine Galois endomorphism types corresponding to your candidate Sato-Tate groups and attempt to prove that the Jacobians of the curves identified in (d) have the Sato-Tate group whose moments they appear to match.

**Project 3. Twisting Sato-Tate groups of genus 3 hyperelliptic curves.** Of the 34 possible Sato-Tate groups of an abelian surface over $\mathbb{Q}$, more than than half are realized by Jacobians of twists[1] of the hyperelliptic curves $y^2 = x^6+1$ and $y^2 = x^5-x$; the Sato-Tate conjecture has been proved in all such cases [11]. These curves represent two isolated points in the moduli space of genus 2 curves distinguished by their exceptionally large automorphism groups; both have Jacobians that are $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with complex multiplication (CM), which makes proving the Sato-Tate conjecture much easier.

The classification of the Sato-Tate groups of these twists, and the proof that they satisfy the Sato-Tate conjecture was achieved through an analysis of the *twisting Sato-Tate group*, a closed subgroup of $\mathrm{USp}(2g)$ associated to a genus $g$ curve $C/\mathbb{Q}$ that contains (with finite index) the Sato-Tate group of the Jacobian of every twist of $C$; see [11, Def. 2.4].

In this project we wish to consider the twisting Sato-Tate groups of the hyperelliptic curves

$$C_1 : y^2 = x^8 + 1, \qquad C_2 : y^2 = x^7 - x, \qquad C_3 : y^2 = x^8 - 14x^4 + 1,$$

of genus 3, all of which have extremal automorphism groups. As in genus 2, the Jacobians of these curves are all $\overline{\mathbb{Q}}$-isogenous to products of elliptic curves, but each of these products is of a distinctly different type:

[1] Recall that two objects defined over a field $k$ are said to be *twists* if their base changes to $\bar{k}$ are isomorphic.

- $\mathrm{Jac}(C_1)$ is $\overline{\mathbb{Q}}$-isogenous to $E_1^2 \times E_2$, where $E_1$ and $E_2$ are non-isogenous CM elliptic curves;
- $\mathrm{Jac}(C_2)$ is $\overline{\mathbb{Q}}$-isogenous to the cube of an elliptic curve with CM;
- $\mathrm{Jac}(C_3)$ is $\overline{\mathbb{Q}}$-isogenous to the cube of an elliptic curve without CM.

The Sato-Tate groups of these curves have been determined (see [12] for the first two), but little is known about their twisting Sato-Tate groups other than its identity component, which necessarily coincides with that of the corresponding Sato-Tate group. The goal of this project is to analyze the twisting Sato-Tate groups of $C_1, C_2, C_3$ as follows:

**(a)** Determine the twisting Sato-Tate group of each curve $C_i$ along with a list $S_i$ of the subgroups that can arise as the Sato-Tate group of a twist of $C_i$.
**(b)** Determine moment sequences for each candidate Sato-Tate group in $S_i$.
**(c)** Find or construct twists of $C_i$ whose Jacobians realize the Sato-Tate groups in $S_i$.
**(d)** (optional) Prove the Sato-Tate conjecture for Jacobians of twists of $C_i$.

This is a substantial project. The solutions may be quite different for each curve $C_i$, due to the different identity components of their Sato-Tate groups; depending on the number of participants we may want to divide the work, or simply pick a particular curve to focus on.

**Project 4. Lang-Trotter conjectures for non-generic abelian surfaces.** Let $E/\mathbb{Q}$ be an elliptic curve and let $t$ be an integer. Suppose that $\mathrm{End}(E_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}$ or $t \neq 0$. For each prime $p$ of good reduction for $E$, let $a_p$ be the trace of Frobenius. The *Lang-Trotter conjecture* [24] states that

$$\pi_E(x;t) := \#\{p \le x \mid E \text{ has good reduction at } p \text{ and } a_p = t\} \sim c(E,t)\frac{\sqrt{x}}{\log x},$$

where $c(E,t) \in \mathbb{R}$ is an explicit constant defined in terms of the image of the *Galois representation* (a continuous homomorphism)

$$\rho_E \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

which is defined as the inverse limit of representations $\rho_{E,m} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ arising from the action of the absolute Galois group of $\mathbb{Q}$ on the $m$-torsion subgroup of $E$.

Unlike the Sato-Tate conjecture for elliptic curves over $\mathbb{Q}$, the Lang-Trotter conjecture remains open. In a recent preprint [8] Cojocaru et al. propose a generalization of the Lang-Trotter conjecture for principally polarized abelian varieties over $\mathbb{Q}$ that are *generic*. An abelian variety $A$ of dimension $g$ is said to be *generic* if its Sato-Tate group $\mathrm{ST}(A)$ is isomorphic to $\mathrm{USp}(2g)$; this implies $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}$.[2] Otherwise we say that $A$ is *non-generic* (or *exceptional*).

To understand the role that the Sato-Tate group plays in these conjectures, recall that the constant $c(E,t)$ in the Lang-Trotter conjecture depends on the image of the Galois representation $\rho_E$. For an abelian variety of dimension $g$ we similarly have a Galois representation

$$\rho_A \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}),$$

where $\mathrm{GSp}_{2g}$ denotes the group of *symplectic similitudes* (the subgroup of $\mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$ that preserves a symplectic form associated to the Weil pairing, up to a scalar multiple) A key ingredient to the conjecture formulated in [8] is that the image of $\rho_A$ is an open subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ and therefore has finite index; this is known to hold for generic $A$ when $g$ is 2, 6, or odd by results of Serre [28, 29]. However, when $A$ is not generic the image of $\rho_A$ will not have finite

[2] The converse holds for $g \le 3$ but not in general; as shown by Mumford, for $g = 4$ there are abelian varieties $A$ for which $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}$ but $\mathrm{ST}(A) \not\simeq \mathrm{USp}(2g)$.

index in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. Indeed, one can directly relate the $\mathbb{Q}_\ell$-dimension of an associated $\ell$-adic representation $\rho_{A,\ell}$ to the real dimension of the identity component of the Sato-Tate group $\mathrm{ST}(A)^0$; in every non-generic case this dimension will be strictly smaller than it is generically. The approach in [8] will thus need to be modified.

The only non-generic case for $g = 1$ is a CM elliptic curve, which is already addressed by the Lang-Trotter conjecture (except when $t = 0$, but then $\pi_E(x;0) \sim x/(2\log x)$). The next case to consider is when $A/\mathbb{Q}$ is an abelian surface. As shown in [9], there are 33 non-generic Sato-Tate groups to consider, with 5 distinct identity components.

The goal of this project is to investigate analogs of the Lang-Trotter conjecture for non-generic abelian surfaces as follows:

**(a)** Propose a Lang-Trotter type conjecture for abelian surfaces $A/\mathbb{Q}$ with non-generic Sato-Tate group (see [9] for a list), including a specification of the leading constant $c(A,t)$ (you may find [1, §3] and [7, §4] helpful). You may assume that $A/\mathbb{Q}$ is principally polarized, and may wish to restrict your attention to a subset of the 33 possible Sato-Tate groups (for example, those with a particular identity component).

**(b)** Check for numerical agreement between the conjectures formulated in (a) and some actual examples (software will be provided to assist with this task). Explicit equations for genus 2 curves over $\mathbb{Q}$ whose Jacobians realize each of the 33 non-generic Sato-Tate groups can be found in [9, Table 11].

## References


[1] J. Achter and J. Holden, *Notes on an analogue of the Fontaine-Mazur conjecture*, Journal de Théorie des Nombres de Bordeaux **15** (2003), 627–637.

[2] G. Banaszak and K.S. Kedlaya, *An algebraic Sato-Tate group and Sato-Tate conjecture*, Indiana University Mathematics Journal **64** (2015), 245–274.

[3] G. Banaszak and K.S. Kedlaya, *Motivic Serre group, algebraic Sato-Tate group and Sato-Tate conjecture*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 11–44.

[4] T. Barnet-Lamb, D. Geraghty, and T. Gee, *The Sato-Tate conjecture for Hilbert modular forms*, Journal of the AMS **24** (2011), 411–469.

[5] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publications of the Research Institute for Mathematical Sciences **47** (2011), 29–98.

[6] A. Bucur and K.S. Kedlaya, *An application of the effective Sato-Tate conjecture*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 45–56.

[7] W. Castryck, A. Folsom, H. Hubrechts, and A.V. Sutherland, *The probability that the number of points on the Jacobian of a genus 2 curve is prime*, Proceedings of the London Mathematical Society **104** (2012), 1235–1270.

[8] A.C. Cojocaru, R. Davis, A. Silverberg, and K.E. Stange, *Arithmetic properties of the Frobenius traces defined by a rational abelian variety*, with two appendices by J-P. Serre, arXiv:1504.00902, 2015.

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

[10] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato-Tate groups of some weight 3 motives*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 57–102.

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

[12] F. Fité and A.V. Sutherland, *Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 103–126.

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

[14] D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Annals of Mathematics **179** (2014), 783–803.
[15] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proceedings of the London Mathematical Society **111** (2015), 1379–1401.
[16] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, in *Algorithmic Number Theory 11th International Symposium (ANTS XI)*, LMS Journal of Computation and Mathematics **17** (2014), 257–273.
[17] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 127–148
[18] C. Johansson, *On the Sato-Tate conjecture for non-generic abelian surfaces*, with an appendix by Francesc Fité, Transactions of the AMS, to appear.
[19] N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Colloquium Publications **45**, AMS, 1999.
[20] K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society **16** (2001), 323–338.
[21] K.S. Kedlaya, *Computing zeta functions via p-adic cohomology*, in *Algorithmic Number Theory 6th International Symposium (ANTS VI)*, Lecture Notes in Computer Science **3076**, Springer 2004, 1–17.
[22] K.S. Kedlaya and A.V. Sutherland, *Computing L-series of hyperelliptic curves*, in *Algorithmic Number Theory 8th International Symposium (ANTS VIII)*, Lecture Notes in Computer Science **5011**, Springer, 2008, 312–326.
[23] K.S. Kedlaya and A.V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, in *Arithmetic Geometry, Cryptography, and Coding Theory (AGCCT-11)*, Contemporary Mathematics **487**, American Mathematical Society, 2000, 119–162.
[24] S. Lang and H. Trotter, *Frobenius distributions in $\mathrm{GL}_2$-extensions*, Lecture Notes in Mathematics **504** (1976), Springer.
[25] V.K. Murty, *Explicit formulae and the Lang-Trotter conjecture*, Rocky Mountain Journal of Mathematics **15** (1985), 535–551.
[26] J. Rouse and J. Thorner, *The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions*, preprint, arXiv:1305.5283.
[27] J.-P. Serre, *Abelian $\ell$-adic representations and elliptic curves*, Research Notes in Mathematics **7**, A.K. Peters, 1998.
[28] J.-P. Serre, *Résumé des cours de 1985-1986, Annuaire du Collège de France, 1986, 95–99*; in *Oeuvres – Collected Papers, Volume IV*, Springer, 2003, 33–37.
[29] J.-P. Serre, *Lettre à Marie-France Vignéras du 10/2/1986*, in *Oeuvres – Collected Papers, Volume IV*, Springer, 2003, 38–55.
[30] J.-P. Serre, *Propriétés conjecturales des groups de Galois motiviques et des représentations $\ell$-adiques*, in *Motives*, AMS Proceedings of Symposia in Pure Mathematics **55** (1994), 377–400.
[31] J.-P. Serre, *Lectures on $N_X(p)$*, Research Notes in Mathematics **11**, CRC Press, 2012.
[32] A.V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Mathematics of Computation **80** (2011), 477–500.
[33] J. Tate, *Algebraic cycles and poles of zeta functions*, in *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, Harper & Row, New York, 1965.
[34] R. Taylor, *Automorphy for some $\ell$-adic lifts of automorphic mod $\ell$ Galois representations II*, Publ. Math. IHES **108** (2008) 183–239.
[35] J. Thorner, *The error term in the Sato-Tate conjecture*, Archiv der Mathematik **103** (2014), 147–156.
[36] P. van Wamelen, *On the CM character of the curves $y^2 = x^q - 1$*, Journal of Number Theory **64** (1997), 59–83.
[37] H. Weyl, *The classical groups: their invariants and representations*, Princeton University Press, 1966.