Let \( E : y^2 = x^3 + Ax + B \) be an elliptic curve over \( \mathbb{Q} \) with \( A, B \in \mathbb{Z} \). For each prime \( p \) of good reduction for \( E \) (all but finitely many), let \( E_p := E \mod p \) 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 \( \text{End}(E_{\mathbb{Q}}) = \mathbb{Z} \), which is true generically). Thanks to recent work by Richard Taylor and others \([5, 14]\), 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. Virtually 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 the subject (which 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 Sato-Tate group (of the \( L \)-function or motive).

**Lecture 1. Introduction to Sato-Tate distributions.** This introductory lecture provides an overview of Sato-Tate distributions with lots of explicit examples, including a preliminary discussion of equidistribution, Sato-Tate groups and the generalized Sato-Tate conjecture. We will then briefly summarize what is currently known about them \([4, 5, 6, 9, 11, 14, 20, 38]\).

**Lecture 2. Equidistribution, \( L \)-functions, and moment sequences.** We recall the notion of equidistribution and its connection to \( L \)-functions (following \([31, \text{Ch. I Appendix}]\)), and review the Haar measures on some of the classical groups and the Weyl integration formulas \([40]\).
We then discuss moment sequences, and highlight their connection to random matrix theory, combinatorics, and representation theory [13, 21, 25].

Lecture 3. Sato-Tate groups. Following Serre [34, 35], we define the Sato-Tate group of a motive, focusing on abelian varieties (motives of weight 1), and state the generalized Sato-Tate conjecture. We also discuss the algebraic Sato-Tate group of Banaszak-Kedlaya [2, 3], and its connection to Mumford-Tate groups and Hodge-groups. We then present the Sato-Tate axioms for self-dual motives with rational coefficients ([9, §2], [35, Ch. 8]), and consider the classification problem: for a fixed weight and choice of Hodge numbers, determine up to conjugacy the finite list of groups satisfying the Sato-Tate axioms, as in [9, §3] and [10, §2].

Lecture 4. Computing Sato-Tate distributions. We survey methods for explicitly computing Sato-Tate distributions associated to abelian varieties, and more generally, arithmetic schemes. These include generic group algorithms [24, 36, 37], p-adic cohomology [15, 22, 23], CRT-based methods [29, 30, 28], and, crucially, the average polynomial-time approach introduced by Harvey [16, 17, 18, 19], which has recently made it feasible to compute Sato-Tate distributions to a level of precision far beyond what was previously practical.

Project Descriptions

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

\[ C_1(a): y^2 = x^{2g+2} - a, \quad C_2(a): y^2 = x^{2g+1} - ax, \quad C_3(a): y^2 = x^{2g+1} - a, \]

with $a \in \mathbb{Q}^\times$. As explained in [12, §2], the Hasse-Witt matrices of these curves have a particularly simple form. This makes it possible to use a optimized version of the average polynomial-time algorithm in [19] to compute statistic of normalized Frobenius traces very quickly, even for moderately large values of $g$ (say $2 \leq g \leq 10$), and in many cases one can do even better by applying explicit trace formulas, as in [12, §3.1] and [39], 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 [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).

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] (as it turns out, only 52 of these are Sato-Tate groups of an abelian surface [9, §4]). The corresponding classification for USp(6), which contains the Sato-Tate groups of all abelian threefolds, remains
open, although some progress has been made; for example, the connected Sato-Tate groups are all 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 an abelian threefold (ideally as Jacobians of genus 3 curves) whose Sato-Tate groups appears to match each candidate, 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 in USp(6) with finite centralizer by proceeding as follows:

(a) Determine which connected Sato-Tate groups $G^0 \subseteq \text{USp}(6)$ 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 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 $\mathbb{Q}$-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 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

\[ C_1: y^2 = x^8 + 1, \quad C_2: y^2 = x^7 - x, \quad C_3: y^2 = x^8 - 14x^4 + 1, \]

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:

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

---

1Recall that two objects defined over a field $k$ are said to be twists if their base changes to $\bar{k}$ are isomorphic.
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 the curves $C_1, C_2, C_3$ 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 $\text{End}(E_{\mathbb{F}_p}) \cong \mathbb{Z}$ 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* [26] states that

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

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

$$\rho_E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}),$$

which is defined as the inverse limit of representations $\rho_{E,m} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$ 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 $\text{ST}(A)$ is isomorphic to $\text{USp}(2g)$; this implies $\text{End}(A_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}$. 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

$$\rho_A : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GSp}_{2g}(\mathbb{Z}),$$

where $\text{GSp}_{2g}$ denotes the group of symplectic similitudes (the subgroup of $\text{GL}_{2g}(\mathbb{Z})$ that preserves a symplectic form associated to the Weil pairing, up to scalars). A key ingredient to the conjecture formulated in [8] is that the image of $\rho_A$ is an open subgroups $\text{GSp}_{2g}(\mathbb{Z})$; in particular, it has finite index; this is known to hold for generic $A$ when $g$ is 2, 6, or odd (by results of Serre [32, 33]). However, when $A$ is not generic the image of $\rho_A$ will definitely not have finite index in $\text{GSp}_{2g}(\mathbb{Z})$. Indeed, one can directly relate the $\mathbb{Q}_l$-dimension of an associated $\ell$-adic representation $\rho_{A,\ell}$ to the real dimension of the identity component of the Sato-Tate group.

\[\text{The converse holds for } g \leq 3 \text{ but not in general; as shown by Mumford, for } g = 4 \text{ there are abelian varieties } A \text{ for which } \text{End}(A_{\overline{\mathbb{Q}}}) \cong \mathbb{Z} \text{ but } \text{ST}(A) \neq \text{USp}(2g).\]
the Lang-Trotter conjecture (except when $ST(A)^0$; 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 $A/Q$ 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 $A/Q$ 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 $A/Q$ 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

[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 on Curves, Contemporary Mathematics, AMS, to appear.