Journal of Algebra 597 (2022) 241–265

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Sato-Tate distributions of $y^2 = x^p - 1$ and $y^2 = x^{2p} - 1$

Melissa Emory [a,*], Heidi Goodson [b]

[a] *Department of Mathematics, University of Toronto; 40 St. George Street, Toronto, Ontario, M5S 2E4, Canada*
[b] *Department of Mathematics, Brooklyn College, City University of New York; 2900 Bedford Avenue, Brooklyn, NY 11210, USA*

ARTICLE INFO

Article history:
Received 14 November 2020
Available online 11 January 2022
Communicated by Kirsten Eisentraeger

MSC:
11M50
11G10
11G20
14G10

Keywords:
Sato-Tate groups
Sato-Tate distributions
Hyperelliptic curves

ABSTRACT

We determine the Sato-Tate groups and prove the generalized Sato-Tate conjecture for the Jacobians of curves of the form $y^2 = x^p - 1$ and $y^2 = x^{2p} - 1$, where p is an odd prime. Our results rely on the fact the Jacobians of these curves are nondegenerate, a fact that we prove in the paper. Furthermore, we compute moment statistics associated to the Sato-Tate groups. These moment statistics can be used to verify the equidistribution statement of the generalized Sato-Tate conjecture by comparing them to moment statistics obtained for the traces in the normalized L-polynomials of the curves.

1. Introduction

The original Sato-Tate conjecture is a statistical conjecture regarding the distribution of the normalized traces of Frobenius on an elliptic curve without complex multiplication

* Corresponding author.
E-mail addresses: memory@math.toronto.edu (M. Emory), heidi.goodson@brooklyn.cuny.edu (H. Goodson).

https://doi.org/10.1016/j.jalgebra.2022.01.002
0021-8693/

(CM), and the conjecture was recently generalized to higher genus curves by Serre [31]. Recent results on this topic of determining Sato-Tate distributions in genus 2 and 3 curves have been achieved in [3,12–16,23,26]. In 2016, Fité-González-Lario [11] obtained Sato-Tate equidistribution results for a family of curves of arbitrarily high genus. The main purposes of this paper are to compute the Sato-Tate groups and to prove the generalized Sato-Tate conjecture for the following two families of hyperelliptic curves of arbitrarily high genus

$$C_p : y^2 = x^p - 1 \text{ and } C_{2p} : y^2 = x^{2p} - 1,$$

where p is an odd prime. The generalized Sato-Tate conjecture is known for CM abelian varieties due to the work of Johansson in [22]; in our proof for C_p we follow Serre's strategy from [30]. We provide numerical evidence to support our results by computing moment statistics associated to the curves.

We start by recalling the original Sato-Tate conjecture for elliptic curves. Let F be a number field, E/F be an elliptic curve without complex multiplication, and v be a finite prime of F such that E has good reduction at v. By a theorem of Hasse, the number of $\mathbb{F}_{q_v}$ points of E is $q_v + 1 - a_v$, where $\mathbb{F}_{q_v}$ denotes the residue field of v and a_v is an integer (called the trace of Frobenius at v) satisfying $|a_v| \leq 2{q_v}^{1/2}$. The Sato-Tate conjecture predicts that, as v varies through the primes of good reduction for E, the normalized Frobenius traces $a_v/{q_v}^{1/2}$ are equidistributed in the interval $[-2, 2]$ with respect to the image of the Haar measure on the special unitary group SU(2). This conjecture has been proven for non-CM elliptic curves defined over totally real fields (see [6,7,17,36]). The distributions of the normalized Frobenius traces are also known for CM elliptic curves over all fields: they are distributed with respect to the image under the trace map of the Haar measure on either the unitary group U(1) or the normalizer of U(1) in SU(2), depending on whether or not the field of definition contains the field of complex multiplication (see, for example, [1] or [5]).

The generalized Sato-Tate conjecture for an abelian variety predicts the existence of a compact Lie group that determines the limiting distribution of normalized local Euler factors. We now state the conjecture more precisely for abelian varieties that are the Jacobians of curves defined over $\mathbb{Q}$, following the exposition of [11].

Let C be a smooth, projective, genus g curve defined over $\mathbb{Q}$ and let K be the minimal extension over which all endomorphisms of $\mathrm{Jac}(C)$ are defined. The Sato-Tate group of the Jacobian of C, $\mathrm{ST}(\mathrm{Jac}(C)) \subseteq \mathrm{USp}(2g)$, is a compact Lie group satisfying the following property. For each prime p at which C has good reduction, there exists a conjugacy class x_p of $\mathrm{ST}(\mathrm{Jac}(C))$ whose characteristic polynomial equals the normalized L-polynomial

$$\overline{L}_p(C, T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \cdots + a_2 T^2 + a_1 T + 1. \tag{1}$$

Let F be a number field and let X_F be the set of conjugacy classes of $\mathrm{ST}(\mathrm{Jac}(C)_F)$. Let $\{p_i\}_{i \geq 1}$ be an ordering by norm of the set of primes of good reduction for C over F

and define a map that sends p_i to x_{p_i} in X_F. We can now state the generalized Sato-Tate conjecture.

Conjecture 1.1 *(Generalized Sato-Tate conjecture). The sequence* $\{x_{p_i}\}_{i\geq 1}$ *is equidistributed on* X_F *with respect to the image on* X_F *of the Haar measure of* $\mathrm{ST}(\mathrm{Jac}(C)_F)$.

Our goals in this paper are to determine the Sato-Tate groups of the Jacobians of the curves C_p and C_{2p} (see Theorem 4.2 and Theorem 4.4) and to prove the equidistribution predicted by the generalized Sato-Tate conjecture for these two families of curves (see Theorem 5.5 and Theorem 5.6).

Theorem 1.2. *Let* p *be an odd prime. The generalized Sato-Tate conjecture holds for the Jacobians of the curves* $C_p : y^2 = x^p - 1$ *and* $C_{2p} : y^2 = x^{2p} - 1$.

The Sato-Tate conjecture was proven for CM abelian varieties in [22], and the Jacobians of both curves in Theorem 1.2 are CM abelian varieties. However, to provide an explicit description of the limiting distribution of the normalized L-polynomial, we need the explicit embedding of the Sato-Tate group of the Jacobian of the curve inside $\mathrm{USp}(2g)$, where g is the genus of the curve. Our approach is similar to that of, for example, [11] and [26].

This paper is organized as follows. In Section 2, we establish the nondegeneracy of the Jacobians of C_p and C_{2p}. In Section 3, we prove that the twisted Lefschetz group of the Jacobian, defined by Banaszak and Kedlaya in [5], is equal to the algebraic Sato-Tate group; this essentially follows from the work of [4] since the Jacobians of our curves are nondegenerate. The equality of the twisted Lefschetz group and the algebraic Sato-Tate group allows one to interpret the Sato-Tate group as a maximal compact subgroup of the group of $\mathbb{C}$-points of the base change of the algebraic Sato-Tate group to $\mathbb{C}$.

In Section 4, we apply the work of Section 3 to determine the Sato-Tate groups of the Jacobians of the curves C_p and C_{2p}. We first determine the identity components of the Sato-Tate groups (see Proposition 4.1 and Proposition 4.3). Note that these propositions confirm Conjectures 6.8 and 6.9 of [9]. The computation of the twisted Lefschetz groups then gives the generators of the component groups (see Theorems 4.2 and 4.4). We give explicit examples of some of these generators in Table 3 in Appendix A.

In Section 5, we establish Conjecture 1.1 for C_p and C_{2p}. For the curve C_p, we prove the generalized Sato-Tate conjecture by following Serre's strategy in [30], i.e. showing that a certain L-function attached to the irreducible nontrivial representations of the Sato-Tate group of the Jacobian of the curve does not vanish. We then use a theorem of Hecke that the L-function attached to a nontrivial unitarized Hecke character does not vanish for $\mathrm{Re}(s) \geq 1$. This proof technique requires a cyclic Galois group $\mathrm{Gal}(K/\mathbb{Q})$, where K is the minimal extension over which all endomorphisms of the Jacobian are defined. The Galois group associated to the curve C_{2p} is not cyclic, so we use the work of [22] to prove the generalized Sato-Tate conjecture in this case.

In Section 6, we compute moment statistics associated to the Sato-Tate groups of the Jacobians of C_p and C_{2p}. These moment statistics can be used to verify the equidistribution statement of the generalized Sato-Tate conjecture by comparing them to moment statistics obtained for the traces a_i in the normalized L-polynomial $\overline{L}_p(C,T)$ in Equation (1). Note that the numerical moment statistics are an approximation since one can only ever compute them up to some prime. It is of interest to those dealing with equidistribution statements to compare how close these two computations are. We compare the moments in Table 2 in Section 6.

Notation and conventions. We begin by fixing notation used in later sections. Let C be a smooth projective curve defined over $\mathbb{Q}$. We write $\mathrm{End}(\mathrm{Jac}(C)_k)$ for the ring of endomorphisms defined over the field k of the Jacobian of C. Let $K := K_C$ denote the minimal extension $L/\mathbb{Q}$ over which all the endomorphisms of the abelian variety $\mathrm{Jac}(C)$ are defined, i.e. the minimal extension for which $\mathrm{End}(\mathrm{Jac}(C)_L) \simeq \mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}})$; the field K is called the endomorphism field of $\mathrm{Jac}(C)$.

We denote the Sato-Tate group of the Jacobian of C by $\mathrm{ST}(\mathrm{Jac}(C)) := \mathrm{ST}(\mathrm{Jac}(C)_{\mathbb{Q}})$ with identity component denoted $\mathrm{ST}^0(\mathrm{Jac}(C)) := \mathrm{ST}^0(\mathrm{Jac}(C)_{\mathbb{Q}})$ and component group $\mathrm{ST}(\mathrm{Jac}(C))/\mathrm{ST}^0(\mathrm{Jac}(C))$. The curve $y^2 = x^m - 1$ is denoted by C_m, and when we specialize to C_p or to C_{2p} we assume throughout the paper that p is an odd prime. We will write ζ_m for a primitive m^{th} root of unity. For any rational number x whose denominator is coprime to an integer r, $\langle x \rangle_r$ denotes the unique representative of x modulo r between 0 and $r-1$.

Define the two matrices

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The symplectic form considered throughout the paper is given by $\mathrm{diag}(J, \ldots, J)$. Lastly, for any positive integer n, we define the following subgroups of the unitary symplectic group $\mathrm{USp}(2n)$.

$$\mathrm{U}(1)_n := \left\langle \mathrm{diag}(\underbrace{u, \overline{u}, \ldots, u, \overline{u}}_{n-\text{times}}) : u \in \mathbb{C}^\times, |u| = 1 \right\rangle$$

and

$$\mathrm{U}(1)^n := \left\langle \mathrm{diag}(u_1, \overline{u_1}, \ldots, u_n, \overline{u_n}) : u_i \in \mathbb{C}^\times, |u_i| = 1 \right\rangle.$$

Acknowledgments. This material is based upon work supported by the National Security Agency under Grant No. H98230-19-1-0119, The Lyda Hill Foundation, The McGovern Foundation, and Microsoft Research, while the authors were in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the summer of 2019.

The first named author was supported by NSF grant DMS-2002085 and an AMS-Simons Travel Award. The second author also received support for this project provided by a PSC-CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York.

We would like to thank Francesc Fité for enlightening discussions while working on this project and Drew Sutherland for creating the histogram in Fig. 1 for us (see also [34]). We also thank Christelle Vincent, Holley Friedlander, and Fatma Cicek for their help with the Sage code to compute the matrices γ and the characteristic polynomials during Sage Days 103. Lastly, we thank the reviewer for their thorough and helpful comments.

2. Nondegenerate abelian varieties

Our main results hold for curves whose Jacobians are nondegenerate. In this section we define the term nondegenerate and give some known results that will be relevant to our later work.

Let A be a nonsingular projective variety over $\mathbb{C}$. We denote (as in [33]) the (complexified) Hodge ring of A by

$$\mathscr{B}^*(A) := \sum_{d=0}^{\dim(A)} \mathscr{B}^d(A),$$

where $\mathscr{B}^d(A) = (H^{2d}(A,\mathbb{Q}) \cap H^{d,d}(A)) \otimes \mathbb{C}$ is the $\mathbb{C}$-span of Hodge cycles of codimension d on A. Furthermore, we define the ring

$$\mathscr{D}^*(A) := \sum_{d=0}^{\dim(A)} \mathscr{D}^d(A)$$

where $\mathscr{D}^d(A)$ is the $\mathbb{C}$-span of classes of intersection of d divisors. This is the subring of $\mathscr{B}^*(A)$ generated by the divisor classes, i.e. generated by $\mathscr{B}^1(A)$. In general, it is known that we have containment $\mathscr{D}^*(A) \subseteq \mathscr{B}^*(A)$ [33].

Definition 2.1. [2] An abelian variety A is said to be **nondegenerate** if $\mathscr{D}^*(A) = \mathscr{B}^*(A)$. If $\mathscr{D}^*(A) \neq \mathscr{B}^*(A)$, then A is said to be **degenerate**.

Definition 2.2. [2,20] An abelian variety A is said to be **stably nondegenerate** if, for any integer $k \geq 1$, $\mathscr{D}^*(A^k) = \mathscr{B}^*(A^k)$.

Hazama proves in Theorem 1.2 of [20] that A is stably nondegenerate if and only if the dimension of its Hodge group is maximal. Note that in [11], the authors use the word *nondegenerate* to describe abelian varieties with this property.

Nondegeneracy is related to the CM-type of an abelian variety. Let $A/\mathbb{Q}$ be a dimension d abelian variety. Suppose that there is a number field K with $[K:\mathbb{Q}] = 2d$ and an injective ring homomorphism $\iota : K \to \mathrm{End}(A) \otimes \mathbb{Q}$. The map ι induces a representation Φ of K on the space of holomorphic 1-forms on A and we say that (A, ι) is of **CM-type** (F, Φ) (see, for example, [2,24,28,32]). When A is an absolutely simple abelian variety with complex multiplication, stable nondegeneracy is equivalent to the CM-type being nondegenerate, i.e. the CM-type has maximal rank (see, for example, [2,24]).

Let $\mathscr{C}^d(A)$ be the subspace of $\mathscr{B}^d(A)$ generated by the classes of algebraic cycles on A of codimension d. Then

$$\mathscr{D}^d(A) \subseteq \mathscr{C}^d(A) \subseteq \mathscr{B}^d(A)$$

and the Hodge Conjecture for A asserts that $\mathscr{C}^d(A) = \mathscr{B}^d(A)$ for all d [2,33]. It is clear from Definition 2.1 that if A is nondegenerate then the Hodge Conjecture holds. However, there are many cases where the Hodge Conjecture holds for degenerate abelian varieties. For example, Shioda verified the Hodge Conjecture for $\mathrm{Jac}(C_m)$ for all $m \leq 21$, though $\mathrm{Jac}(C_9)$, $\mathrm{Jac}(C_{15})$, and $\mathrm{Jac}(C_{21})$ are degenerate (see [33, Section 6]).

The following results are crucial to our work with the curves C_p and C_{2p}.

Proposition 2.3. *[33, Corollary 5.3] If $p \geq 3$ is a prime number, then the Hodge ring $\mathscr{B}^*(\mathrm{Jac}(C_p))$ is generated by $\mathscr{B}^1(\mathrm{Jac}(C_p))$. The same result holds for arbitrary powers of $\mathrm{Jac}(C_p)$.*

By definition, this tells us that $\mathrm{Jac}(C_p)$ is stably nondegenerate. The nondegenerate CM-type for the curve C_p is $\{\mathbb{Q}(\zeta_p), \{\sigma_1, \sigma_2, \ldots, \sigma_{(p-1)/2}\}\}$, where each $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is defined by ${}^{\sigma_t}(\zeta_p) = \zeta_p^t$ (see, for example, [32, Section 15.4]). The CM-type for the curve C_p is primitive (see, for example, [24] for a definition) which implies that $\mathrm{Jac}(C_p)$ is absolutely irreducible.

Proposition 2.4. *[9, Lemma 4.1] Let $g = 2k$ be an even integer, and $C_{2g+2} : y^2 = x^{2g+2} + c$, where $c \in \mathbb{Q}^\times$. Then we have the following isogeny over $\overline{\mathbb{Q}}$*

$$\mathrm{Jac}(C_{2g+2}) \sim \mathrm{Jac}(C_{g+1})^2,$$

where $C_{g+1} : y^2 = x^{g+1} + c$.

Combining these two results yields the following.

Corollary 2.5. *For any prime $p \geq 3$, $\mathrm{Jac}(C_p)$ and $\mathrm{Jac}(C_{2p})$ are nondegenerate.*

Proof. Note that if p is an odd prime, then we can write $p = 2k+1$, for some integer k. Hence, $2p = 2(2k+1) = 2(2k)+2$ and Proposition 2.4 tells us that for $C_{2p} : y^2 = x^{2p} - 1$,

$$\mathrm{Jac}(C_{2p}) \sim \mathrm{Jac}(C_p)^2.$$

Thus, $\mathrm{Jac}(C_{2p})$ is a power of $\mathrm{Jac}(C_p)$, and we apply Proposition 2.3 to get the desired result. □

An alternative proof that $\mathrm{Jac}(C_p)$ is nondegenerate is Theorem 2 in [24]. Note that curve C_{2p} has CM field $\mathbb{Q}(\zeta_{4p})$. See the proof of Theorem 4.4 for the generators of the reduced automorphism group of C_{2p}.

3. The algebraic Sato-Tate group

We start by defining notation as in [11] and [35, Section 3]. For more detailed background information, see [35, Section 3.2].

Let A/k be an abelian variety of dimension g defined over the number field k. Let ℓ be a prime and we define the Tate module $T_\ell := \varprojlim_n A[\ell^n]$ to be a free $\mathbb{Z}_\ell$-module of rank $2g$, and the rational Tate module $V_\ell := T_\ell \otimes_{\mathbb{Z}} \mathbb{Q}$ to be a $\mathbb{Q}_\ell$-vector space of dimension $2g$. The Galois action on the Tate module is given by an ℓ-adic representation

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(V_\ell) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Let G_ℓ denote the image of this map, and let G_ℓ^{Zar} be the Zariski closure of G_ℓ in $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. We then define $G_\ell^{1,Zar} := G_\ell^{Zar} \cap \mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$.

Definition 3.1. The Sato-Tate group of A, denoted by $\mathrm{ST}(A)$, is a maximal compact Lie subgroup of $G_\ell^{1,Zar} \otimes_{\mathbb{Q}_\ell} \mathbb{C}$ contained in $\mathrm{USp}(2g)$

The algebraic Sato-Tate Conjecture for $\mathrm{Jac}(C)$ predicts the existence of an algebraic Sato-Tate group $\mathrm{AST}(\mathrm{Jac}(C))$ of $\mathrm{Sp}_{2g}/\mathbb{Q}$ such that

$$G_\ell^{1,Zar} = \mathrm{AST}(\mathrm{Jac}(C)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$$

for every prime ℓ (see, for example, [12, Conjecture 2.13] and [5, Conjecture 2.1]).

For each $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, define the set

$$\mathrm{L}(\mathrm{Jac}(C))(\tau) := \{\gamma \in \mathrm{Sp}_{2g} \,|\, \gamma\alpha\gamma^{-1} = \tau(\alpha) \text{ for all } \alpha \in \mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}\}$$

where α is viewed as an endomorphism of $H_1((\mathrm{Jac}(C)_{\mathbb{C}}, \mathbb{Q})$.

Definition 3.2. [5] The twisted Lefschetz group $\mathrm{TL}(\mathrm{Jac}(C))$ is defined to be

$$\mathrm{TL}(\mathrm{Jac}(C)) := \bigcup_{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \mathrm{L}(\mathrm{Jac}\, C)(\tau).$$

When τ is the identity automorphism, $\mathrm{L}(\mathrm{Jac}(C))(\tau)$ forms a group, called the Lefschetz group, which we denote simply by $\mathrm{L}(\mathrm{Jac}(C))$.

Proposition 3.3. *Let p be an odd prime and C_p be the curve $y^2 = x^p - 1$. Then the algebraic Sato-Tate Conjecture holds for $\mathrm{Jac}(C_p)$ with $\mathrm{AST}(\mathrm{Jac}(C_p)) = \mathrm{TL}(\mathrm{Jac}(C_p))$.*

Proof. This follows from [5, Theorem 6.6] since $\mathrm{Jac}(C_p)$ is a nondegenerate CM abelian variety. Still, we include a proof that is similar to the proof of [11, Lemma 3.5] for the sake of completion. By [12, Theorem 2.16(a)], we need to verify two criteria: the Hodge group $\mathrm{Hg}(\mathrm{Jac}(C_p))$ equals the Lefschetz group $\mathrm{L}(\mathrm{Jac}(C_p))$, and that the Mumford-Tate Conjecture holds for $\mathrm{Jac}(C_p)$. The Mumford-Tate Conjecture is known to be true for CM abelian varieties (see, for example, [11,28,39]), so we only need to verify the first of the criteria.

By Deligne [8, I, Proposition 6.2] and [5, Definition 4.4], we have

$$G_\ell^{1,Zar,0}(\mathrm{Jac}(C_p)) \subseteq \mathrm{Hg}(\mathrm{Jac}(C_p)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subseteq \mathrm{L}(\mathrm{Jac}(C_p)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \tag{2}$$

for every prime ℓ. We will show that $G_\ell^{1,Zar,0}(\mathrm{Jac}(C_p)) = \mathrm{L}(\mathrm{Jac}(C_p)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ to obtain the desired result. Note that it is sufficient to show this for any prime ℓ.

Since p is prime, $\mathrm{Jac}(C_p)$ is simple (see, for example, [32, Section 15.4]). Furthermore, Proposition 2.3 tells us that $\mathrm{Jac}(C_p)$ has nondegenerate CM-type. We apply the results of Section 2 of [4] to get, for every prime ℓ of good reduction for which $\mathrm{Jac}(C_p)$ splits completely in $\mathbb{Q}(\zeta_p)$,

$$G_\ell^{1,Zar,0}(\mathrm{Jac}(C_p)) = \{\mathrm{diag}(x_1, y_1, \ldots, x_g, y_g) \in \mathbb{Q}_\ell^\times \mid x_1 y_1 = \cdots = x_g y_g = 1\}, \tag{3}$$

where $g = (p-1)/2$ is the genus of C_p.

We now compute the Lefschetz group $\mathrm{L}(\mathrm{Jac}(C)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. In order for a matrix $\gamma \in \mathrm{Sp}_{2g}$ to commute with any matrix $\alpha \in \mathrm{End}(H_1(\mathrm{Jac}(C_p)_{\mathbb{C}}, \mathbb{C}))$, it must be diagonal. Hence,

$$\mathrm{L}(\mathrm{Jac}(C_p)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \{\mathrm{diag}(x_1, y_1, \ldots, x_g, y_g) \in \mathbb{Q}_\ell^\times \mid x_1 y_1 = \cdots = x_g y_g = 1\},$$

which yields the desired result. □

Corollary 3.4. *If p is an odd prime then the algebraic Sato-Tate Conjecture holds for $\mathrm{Jac}(C_{2p})$ with $\mathrm{AST}(\mathrm{Jac}(C_{2p})) = \mathrm{TL}(\mathrm{Jac}(C_{2p}))$.*

Proof. Recall from Proposition 2.4 that

$$\mathrm{Jac}(C_{2p}) \sim (\mathrm{Jac}(C_p))^2.$$

Corollary 2.5 tells us that both $\mathrm{Jac}(C_{2p})$ and $\mathrm{Jac}(C_p)$ are nondegenerate. Furthermore, they are both abelian varieties with CM. Hence, as in the proof of Lemma 3.5 of [11], proving the inclusions in Equation (2) were actually equalities gives us

$$G_\ell^{1,Zar,0}(\mathrm{Jac}(C_{2p})) = \mathrm{Hg}(\mathrm{Jac}(C_{2p})) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{L}(\mathrm{Jac}(C_{2p})) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell. \quad \square$$

Note that we cannot apply Theorem A of [4] to determine $G_\ell^{1,Zar,0}(\mathrm{Jac}(C_{2p}))$ since $\mathrm{Jac}(C_{2p})$ is not simple. We will determine the identity component of the Sato-Tate group of $\mathrm{Jac}(C_{2p})$ using another method in Section 4.2.

Corollary 3.5. *The group of components of* $G_\ell^{1,Zar}(\mathrm{Jac}(C_p))$ *and* $\mathrm{AST}(\mathrm{Jac}(C_p))$ *are isomorphic to* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. *Also, the group of components of* $G_\ell^{1,Zar}(\mathrm{Jac}(C_{2p}))$ *and* $\mathrm{AST}(\mathrm{Jac}(C_{2p}))$ *are isomorphic to* $\mathrm{Gal}(\mathbb{Q}(\zeta_{4p})/\mathbb{Q})$.

Proof. This follows from Proposition 3.3 (see [12, Prop 2.17]). $\square$

Remark. Although [12, Prop 2.17] is stated for $g \leq 3$, Proposition 3.3 is for curves of arbitrarily high genus, and since the Mumford-Tate conjecture holds for $\mathrm{Jac}(C_p)$ the requirement that $g \leq 3$ in [12, Prop 2.17] can be removed for the proof of Corollary 3.5.

It is known that when the algebraic Sato-Tate conjecture holds, we may interpret the Sato-Tate group $\mathrm{ST}(\mathrm{Jac}(C))$ as a maximal compact subgroup of $\mathrm{AST}(\mathrm{Jac}(C)) \otimes_{\mathbb{Q}} \mathbb{C}$ (see, for example, [12, Section 2.2]).

4. Sato-Tate groups

In this section we compute the Sato-Tate groups of the Jacobians of the curves $C_p : y^2 = x^p - 1$ and $C_{2p} : y^2 = x^{2p} - 1$. For both families of curves, we obtain the component group of the Sato-Tate group by computing the twisted Lefschetz groups (recall the results of Proposition 3.3 and Corollary 3.4).

4.1. The Sato-Tate group of $y^2 = x^p - 1$

We first determine the identity component of the Sato-Tate group.

Proposition 4.1. *If* p *is an odd prime then*

$$\mathrm{ST}^0(\mathrm{Jac}(C_p)) \simeq \mathrm{U}(1)^g$$

where $g = (p-1)/2$ *is the genus of* C_p.

Proof. Let ℓ be a prime, and take an embedding of $\mathbb{Q}_\ell$ into the complex numbers. By definition, $\mathrm{ST}^0(\mathrm{Jac}(C))$ is a maximal compact subgroup of $\mathrm{AST}^0(\mathrm{Jac}(C)) \otimes_{\mathbb{Q}} \mathbb{C}$. From Proposition 3.3 and Equation (3), it follows that we can take the maximal compact subgroup $\mathrm{U}(1)^g$. $\square$

Remark. Proposition 4.1 could also be derived from [11] where they consider the curve $\mathcal{C}_k : v^\ell = u(u+1)^{\ell-k-1}$. If we let $k = p-2$ and $\ell = p$, then the curve $\mathcal{C}_{p-2}$ is isomorphic to C_p over the field $\mathbb{Q}(4^{1/p}, i)$. This immediately gives the identity component of the Sato-Tate group of the Jacobian of C_p since the connected component only depends on the variety over $\overline{\mathbb{Q}}$.

The main result of the following theorem is determining the component group of the Sato-Tate group of $\mathrm{Jac}(C_p)$. Explicit examples of the generator of the component group are given in Table 3 in Appendix A.

Theorem 4.2. *Let $S = \{1, \dots, g\}$ and let a be a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. Up to conjugation in $\mathrm{USp}(2g)$,*

$$\mathrm{ST}(\mathrm{Jac}(C_p)) = \langle \mathrm{U}(1)^g, \gamma \rangle ,$$

where γ is a $2g \times 2g$ matrix whose block entries are given by

$$\gamma_{i,j} = \begin{cases} I & \text{if } j = \langle ai \rangle_p \text{ and } \langle ai \rangle_p \in S, \\ J & \text{if } j = p - \langle ai \rangle_p \text{ and } \langle ai \rangle_p \notin S, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Furthermore, there is an isomorphism

$$\mathrm{ST}(\mathrm{Jac}(C_p)) \simeq \mathrm{U}(1)^g \rtimes (\mathbb{Z}/p\mathbb{Z})^\times .$$

Proof. We compute the twisted Lefschetz group of $\mathrm{Jac}(C_p)$. Applying Proposition 3.3 then yields the desired result.

We can identify the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ via the isomorphism that maps $t \in G$ to the Galois element σ_t, where ${}^{\sigma_t}(\zeta_p) := \zeta_p^t$.

A basis for the space of regular 1-forms of a genus g hyperelliptic curve is given by $\{\omega_j = x^j dx/y \ : \ j = 0, \cdots, g-1\}$ (see, for example, [37, Section 3]). We consider the automorphism $\alpha : C_p \to C_p$ defined by $\alpha(x, y) = (\zeta_p x, y)$, and compute the pullbacks of the differentials to be

$$\alpha^*(\omega_j) = \zeta_p^{j+1} \omega_j .$$

We now write the endomorphism $\alpha \in \mathrm{End}(\mathrm{Jac}(C_K))$ in terms of a symplectic basis of $H_1(\mathrm{Jac}(C_p)_{\mathbb{C}}, \mathbb{C})$ (with respect to the matrix $\mathrm{diag}(J)$) and get the diagonal matrix $\alpha = \mathrm{diag}(X_1, X_2, \dots, X_g)$, where each X_i is a block matrix defined by

$$X_i := \mathrm{diag}\left(\zeta_p^i, \overline{\zeta_p^i}\right) .$$

Let σ_a be a generator for the cyclic Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Since the action of the Galois element σ_a is given by ${}^{\sigma_a}(\zeta_p) = \zeta_p^a$, we have

$$ {}^{\sigma_a}X_i = \mathrm{diag}\left(\zeta_p^{ai}, \overline{\zeta_p^{ai}}\right).$$

Hence, letting $S = \{1, \ldots, g\}$, we can write

$$ {}^{\sigma_a}X_i = \begin{cases} X_{\langle ai\rangle_p} & \text{if } \langle ai\rangle_p \in S, \\ \overline{X_{p-\langle ai\rangle_p}} & \text{if } \langle ai\rangle_p \notin S, \end{cases}$$

where

$$ \overline{X_m} := \mathrm{diag}\left(\overline{\zeta_p}^m, {\zeta_p}^m\right).$$

Note that $JX_m(-J) = \overline{X_m}$. This characterization allows to express each ${}^{\sigma_a}X_i$ in the form X_j or $\overline{X_j}$, for some $1 \le j \le g$.

We will now verify that $\gamma\alpha\gamma^{-1} = {}^{\sigma_a}\alpha$, where γ is as defined in Equation (4). Note that there is only one nonzero block entry in each row and each column in the block matrix γ. Furthermore, one easily checks that the entries of the inverse of γ are given by

$$ {\gamma^{-1}}_{j,i} = \begin{cases} I & \text{if } j = \langle ai\rangle_p \text{ and } \langle ai\rangle_p \in S, \\ -J & \text{if } j = p - \langle ai\rangle_p \text{ and } \langle ai\rangle_p \notin S, \\ 0 & \text{otherwise.} \end{cases}$$

Some basic linear algebra shows that the only nonzero blocks in the product $\gamma\alpha\gamma^{-1}$ will be the diagonal entries. We will now determine what those diagonal entries will be. Suppose that the only nonzero block in column j of γ is in row i. Based on the definitions of γ and γ^{-1}, this nonzero entry will yield the following product in the ith diagonal entry of $\gamma\alpha\gamma^{-1}$

$$ \gamma_{i,j}{X_j{\gamma^{-1}}}_{j,i} = \begin{cases} X_j & \text{if } j = \langle ai\rangle_p \text{ and } \langle ai\rangle_p \in S, \\ \overline{X_j} & \text{if } j = p - \langle ai\rangle_p \text{ and } \langle ai\rangle_p \notin S. \end{cases}$$

Hence, $\gamma\alpha\gamma^{-1} = {}^{\sigma_a}\alpha$, which confirms that γ is an element of the twisted Lefschetz group.

We now show that $\gamma^{p-1} \in \mathrm{ST}^0(\mathrm{Jac}(C_p))$, but $\gamma^d \notin \mathrm{ST}^0(\mathrm{Jac}(C_p))$ for any proper divisor d of $p-1$, which will prove that $\mathrm{ST}(\mathrm{Jac}(C_p)) = \langle \mathrm{U}(1)^g, \gamma\rangle \simeq \mathrm{U}(1)^g \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$.

Since σ_a generates the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we have $|\sigma_a| = 2g$ and, for $1 \le d \le 2g$,

$$ (\sigma_a)^d(\zeta_p) = \begin{cases} \zeta_p & \text{if } d = 2g, \\ \overline{\zeta_p} & \text{if } d = g, \end{cases}$$

and $(\sigma_a)^d(\zeta_p) \neq \zeta_p$ nor $\overline{\zeta}_p$ otherwise. Hence, the action of σ_a on the block matrix X_i satisfies

$$(\sigma_a)^d(X_i) = \begin{cases} X_i & \text{if } d = 2g, \\ \overline{X_i} & \text{if } d = g, \\ X_j \text{ or } \overline{X_j} & \text{otherwise,} \end{cases}$$

for some $j \in \{1, \ldots, g\}$ not equal to i.

We have seen that $\gamma\alpha\gamma^{-1} = {}^{\sigma_a}\alpha$, and so conjugating α by γ permutes (and sometimes conjugates) the diagonal block entries of α. Since $\gamma\alpha\gamma^{-1}$ is again a diagonal block matrix, conjugating this by γ will again just permute (and sometimes conjugate) the diagonal block entries. Hence, $\gamma^d\alpha\gamma^{-d}$ is a diagonal block matrix for any d. In fact, we can write $\gamma^d\alpha\gamma^{-d} = {}^{(\sigma_a)^d}\alpha$.

Thus, γ^d has a nonzero, off-diagonal block entry if and only if there is some i for which ${}^{(\sigma_a)^d}X_i = X_j$ or $\overline{X_j}$ with $j \neq i, p-i$. This is possible if and only if $d \neq 2g$ or g.

If $d = g$, then ${}^{(\sigma_a)^d}X_i = \overline{X_i}$ for all i. Hence, all of the diagonal block entries of γ^g must be J or $-J$ since $JX_i(-J) = -JX_iJ = \overline{X_i}$. Thus, $\gamma^g \notin \mathrm{ST}^0(\mathrm{Jac}(C_p))$. However, $J^2 = (-J)^2 = -I$, so $\gamma^{2g} = -\mathrm{Id}$, which is an element of $\mathrm{ST}^0(\mathrm{Jac}(C_p))$. Thus, $\mathrm{ST}(\mathrm{Jac}(C_p)) \simeq \mathrm{U}(1)^g \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$. □

4.2. The Sato-Tate group of $y^2 = x^{2p} - 1$

We use the results of Section 2 and Proposition 4.1 to determine the identity component of the Sato-Tate group of C_{2p}.

Proposition 4.3. *If p is an odd prime and $C_{2p} : y^2 = x^{2p} - 1$, then*

$$\mathrm{ST}^0(\mathrm{Jac}(C_{2p})) \simeq (\mathrm{U}(1)_2)^{g/2}$$

where $g = p - 1$ is the genus of C_{2p}.

Proof. Recall from Proposition 2.4 that

$$\mathrm{Jac}(C_{2p}) \sim (\mathrm{Jac}(C_p))^2.$$

The curve C_p has genus $g' = (p-1)/2 = g/2$, and Proposition 4.1 gives the identity component for the Sato-Tate group of its Jacobian. It follows that the identity component of $\mathrm{ST}^0(\mathrm{Jac}(C_{2p}))$ is $\mathrm{ST}^0(\mathrm{Jac}(C_p))$ embedded into $\mathrm{USp}(2g)$, yielding $\mathrm{ST}^0(\mathrm{Jac}(C_{2p})) \simeq (\mathrm{U}(1)^{g/2})_2 \simeq (\mathrm{U}(1)_2)^{g/2}$. □

The main result of the following theorem is determining the component group of the Sato-Tate group of $\mathrm{Jac}(C_{2p})$. This is an interesting addition to the literature as the Sato-Tate groups of these curves do not have cyclic component groups.

Theorem 4.4. *Let p be an odd prime, $g = p-1$, $S = \{1, \dots, g\}$, and a be a generator of the cyclic group $(\mathbb{Z}/2p\mathbb{Z})^*$. Up to conjugation in $\mathrm{USp}(2g)$, the Sato-Tate group of $C_{2p} : y^2 = x^{2p} - 1$ is*

$$\mathrm{ST}(\mathrm{Jac}(C_{2p})) = \left\langle (\mathrm{U}(1)_2)^{g/2}, \gamma, \gamma' \right\rangle,$$

where the 2×2 block entries of γ are given by

$$\gamma_{i,j} = \begin{cases} I & \text{if } j = \langle ai \rangle_{2p} \text{ and } \langle ai \rangle_{2p} \in S, \\ J & \text{if } i < \lfloor \frac{p}{2} \rfloor,\ j = p - \langle ai \rangle_{2p}, \text{ and } \langle ai \rangle_{2p} \notin S, \\ -J & \text{if } i > \lfloor \frac{p}{2} \rfloor,\ j = p - \langle ai \rangle_{2p}, \text{ and } \langle ai \rangle_{2p} \notin S, \\ 0 & \text{otherwise,} \end{cases}$$

for $1 \le i, j \le g$, and $\gamma' = \mathrm{diag}(I, -I, \dots, I, -I)$. Furthermore, there is an isomorphism

$$\mathrm{ST}(\mathrm{Jac}(C_{2p})) \simeq (\mathrm{U}(1)_2)^{g/2} \rtimes \mathrm{Gal}(\mathbb{Q}(\zeta_{4p})/\mathbb{Q}).$$

See Table 3 in Appendix A for explicit examples of the matrix γ.

Proof. The reduced automorphism group of C_{2p} is isomorphic to the dihedral group D_{2p} (see, for example, [27]). We consider the following generators of the automorphism group of C_{2p}. Let

$$\alpha(x, y) = (\zeta_{2p} x, y) \quad \text{and} \quad \beta(x, y) = (x^{-1}, iyx^{-p}),$$

where ζ_{2p} is a primitive $2p^{th}$ root of unity. Thus, $\mathrm{End}(\mathrm{Jac}(C_{2p})_K) \simeq \mathrm{End}(\mathrm{Jac}(C_{2p})_{\overline{\mathbb{Q}}})$, where $K = \mathbb{Q}(\zeta_{2p}, i) = \mathbb{Q}(\zeta_{4p})$.

We compute pullbacks of the differentials $\omega_j = x^j dx/y$, where $0 \le j < g = p-1$, in order to determine the generators of the endomorphism ring $\mathrm{End}(\mathrm{Jac}(C_{2p})_K)$. As in the proof of Theorem 4.2, the pullback α^* leads to the endomorphism $\alpha = \mathrm{diag}(X_1, X_2, \dots, X_g)$. Computing the pullback β^* on the differential ω_j yields

$$\beta^* \omega_j = \frac{x^{-j} d(x^{-1})}{iyx^{-p}} = i\omega_{p-2-j}.$$

Thus, the endomorphism $\beta \in \mathrm{End}(\mathrm{Jac}(C_{2p})_K)$ is the antidiagonal matrix $\beta = \mathrm{antidiag}(\underbrace{Z, Z, \dots, Z}_{g})$, where $Z = \mathrm{diag}\,(i, -i)$.

We choose two elements σ_a, σ_b that generate the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/4p\mathbb{Z})^\times$ and satisfy

$$\sigma_a : \begin{cases} \zeta_{2p} \mapsto \zeta_{2p}^a \\ i \mapsto i \end{cases} \qquad \sigma_b : \begin{cases} \zeta_{2p} \mapsto \zeta_{2p} \\ i \mapsto -i, \end{cases}$$

where a is a generator of $(\mathbb{Z}/4p\mathbb{Z})^\times$.

Let γ and γ' be defined as in the statement of the theorem. One can verify that

$$^{\sigma_a}\alpha = \gamma\alpha\gamma^{-1}, \quad ^{\sigma_a}\beta = \gamma\beta\gamma^{-1}, \quad ^{\sigma_b}\alpha = \gamma'\alpha\gamma'^{-1}, \text{ and } ^{\sigma_b}\beta = \gamma'\beta\gamma'^{-1}$$

using a similar strategy to the one used in the proof Theorem 4.2, so we omit the proof here. In this case, the matrix γ contains both J and $-J$ as entries so that it conjugates β properly.

Lastly, one can show as in the proof of Theorem 4.2 that the component group of $\mathrm{ST}(\mathrm{Jac}(C_{2p}))$ is $\langle\gamma, \gamma'\rangle$. □

Corollary 4.5. *Up to conjugation in* $\mathrm{USp}(2g, \mathbb{C})$*, the Sato-Tate group of* C_{2p} *over* $\mathbb{Q}(i)$ *is*

$$\mathrm{ST}(\mathrm{Jac}(C_{2p})_{\mathbb{Q}(i)}) = \left\langle (\mathrm{U}(1)_2)^{g/2}, \gamma \right\rangle.$$

Proof. This follows from the fact that the minimal extension $L/\mathbb{Q}(i)$ over which all the endomorphisms of $\mathrm{Jac}(C)_{\mathbb{Q}(i)}$ are defined is $L = \mathbb{Q}(\zeta_{4p}) = \mathbb{Q}(\zeta_{2p,i})$. □

5. Equidistribution results

In this section we prove Theorem 1.2, which states that the generalized Sato-Tate conjecture holds for the Jacobians of C_p and C_{2p}. We first specify to the curve C_p. We begin by discussing the L-functions associated to the curve and then state the generalized Sato-Tate conjecture. We then prove the generalized Sato-Tate conjecture following the strategy of Serre [30]. Finally, we prove the generalized Sato-Tate conjecture for the Jacobian of C_{2p} using a result of [22].

5.1. Hecke characters and L-functions

We follow the exposition in [11, Section 2.2], specifying to the curve C_p. For a more thorough review of Hecke characters, we refer the reader to [25] and [38]. Let $\mathfrak{p}$ be a prime ideal to p in $\mathbb{Q}(\zeta_p)$ and let x be an element in the ring of integers of $\mathbb{Q}(\zeta_p)$. Then there is precisely one p^{th} root of unity $\chi_\mathfrak{p}(x)$ satisfying the condition

$$\chi_\mathfrak{p}(x) \equiv x^{(N(\mathfrak{p})-1)/p} \mod \mathfrak{p}.$$

We extend this to all of $\mathbb{Q}(\zeta_p)$ by setting $\chi_\mathfrak{p}(x) = 0$ whenever $x \equiv 0 \pmod{\mathfrak{p}}$, and, thus, $\chi_\mathfrak{p}$ is a multiplicative character of order p on $\mathbb{F}_\mathfrak{p} := \mathcal{O}_{\mathbb{Q}(\zeta_p)}/\mathfrak{p}$.

We now define the Jacobi sums that appear in the L-functions of our curves. For all $h = (h_1, h_2) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and for any ideal $\mathfrak{p}$ in $\mathbb{Q}(\zeta_p)$ not dividing p, we define

$$J_h(\mathfrak{p}) := -\sum_{x \in \mathbb{F}_\mathfrak{p}} \chi_\mathfrak{p}(x)^{h_1} \chi_\mathfrak{p}(1-x)^{h_2}$$

(see [25, Section 1.4]) and $J_h(\mathfrak{p})$ can be viewed as a function on $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in terms of the characters on $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (see [38]). For each h we extend the definition of $J_h(\mathfrak{p})$ to all ideals prime to p in $\mathbb{Q}(\zeta_p)$ by multiplicativity.

Lemma 5.1. *Let h be of the form $((p-2)a, a)$ for $a \in G = (\mathbb{Z}/p\mathbb{Z})^\times$ then*

$$L((C_p)_{\mathbb{Q}(\zeta_p)}, s) = L(J_h, s)^{p-1} \quad \text{and} \quad L(C_p, s) = L(J_h, s).$$

Proof. This follows from the remark after Proposition 4.1. One can also see this by computing the set M_{p-2} as defined in [11, (2.2)]:

$$M_{p-2} = \{j \in G : \langle j \rangle_p < \langle (p-1)j \rangle_p\} = \{j \in G : \langle j \rangle_p < \langle -j \rangle_p\} = \{1, 2, \ldots, (p-1)/2\}$$

which gives the CM type for the curve C_p. Using the Hecke characters J_h for these h, [11, Lemma 2.10] gives the desired result. □

5.2. Generalized Sato-Tate conjecture

We specify the generalized Sato-Tate conjecture to the Jacobian of the curve C_p. Before we state the conjecture, we need to set up some notation.

Let $E/\mathbb{Q}$ be a subextension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Denote the set of conjugacy classes of $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$ by X_E. Let P be an infinite subset of primes of a number field, and $\{\mathfrak{p}_i\}_{i\geq 1}$ be an ordering by norm of P. Define a map $A_E : P \to X_E$ by sending $\mathfrak{p}$ to $x_\mathfrak{p}$. For any representation $\rho : \mathrm{ST}(\mathrm{Jac}(C_p)_E) \to GL_n(\mathbb{C})$ of $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$, write

$$L_{A_E}(\rho, s) = \prod_{\mathfrak{p} \in P} \det(1 - \rho(x_\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

We specify a theorem of Serre to the curve C_p (see also [11, Theorem 3.12]).

Theorem 5.2. *[30, page I-23] Suppose that for every irreducible nontrivial representation ρ of $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$ the Euler product $L_A(\rho, s)$ converges for $Re(s) > 1$ and extends to a holomorphic and nonvanishing function for $Re(s) \geq 1$. Then the sequence $\{x_{\mathfrak{p}_i}\}_{i\geq 1}$ is equidistributed over X_E with respect to the projection on X_E of the Haar measure of $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$.*

For a prime q of E, let x_q be the conjugacy class of $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$ using the isomorphism $\mathrm{ST}(\mathrm{Jac}(C_p)_E) \simeq \mathrm{ST}(\mathrm{Jac}(C_p)_{\mathbb{Q}(\zeta_p)}) \rtimes \mathrm{Gal}(\mathbb{Q}(\zeta_p)/E)$. Specifically, set

$$x_q := \left(\mathrm{diag}\left(\frac{J_{r_1}(\mathfrak{p})}{N(\mathfrak{p})^{1/2}}, \frac{J_{r_1}(\overline{\mathfrak{p}})}{N(\mathfrak{p})^{1/2}}, \ldots, \frac{J_{r_{(p-1)/2}}(\mathfrak{p})}{N(\mathfrak{p})^{1/2}}, \frac{J_{r_{(p-1)/2}}(\overline{\mathfrak{p}})}{N(\mathfrak{p})^{1/2}} \right), \mathrm{Frob}_q \right) \in X_\mathbb{Q},$$

where each $r_i = ((p-2)i, i)$. The set $\{r_1, r_2, \ldots, r_{(p-1)/2}\}$ is a complete set of representatives of M, and $\mathfrak{p}$ is a prime of $\mathbb{Q}(\zeta_p)$ lying over q.

Now specify P to be the set of primes of good reduction for $(C_p)_E$ and let $\{p_i\}_{i\geq 1}$ be an ordering by norm of P. We can now state the generalized Sato-Tate conjecture for $\mathrm{Jac}(C_p)$ (see, for example, [30, page I-23]).

Conjecture 5.3 *(Generalized Sato-Tate). The sequence $x_E := \{x_{p_i}\}_{i\geq 1}$ is equidistributed on X_E with respect to the image on X_E of the Haar measure of* $\mathrm{ST}(\mathrm{Jac}(C_p)_E)$.

The following theorem specifies this conjecture to $E = \mathbb{Q}(\zeta_p)$.

Theorem 5.4. *The generalized Sato-Tate conjecture holds for* $\mathrm{Jac}(C_p)$ *over* $\mathbb{Q}(\zeta_p)$.

Proof. See [10, Theorem 3.6]. □

To prove Conjecture 5.3 for $\mathrm{Jac}(C_p)$ over $\mathbb{Q}$, we will prove the convergence condition of Theorem 5.2. We first describe the irreducible representations of $\mathrm{ST}(\mathrm{Jac}(C_p))$ as in [29]. Let $\mathcal{G} = \mathrm{ST}(\mathrm{Jac}(C_p))$ so that $\mathcal{G}^0 = \mathrm{ST}^0(\mathrm{Jac}(C_p))$. We associate to any tuple $\underline{b} = (b_1, b_2, \ldots, b_{(p-1)/2}) \in \mathbb{Z}^{(p-1)/2}$ the irreducible representation $\phi_{\underline{b}} : \mathrm{U}(1)^{(p-1)/2} \to \mathbb{C}^\times$ defined by

$$\phi_{\underline{b}}(u_1, \ldots, u_{(p-1)/2}) = \prod_{i=1}^{(p-1)/2} u_i^{b_i},$$

where $U = \mathrm{diag}(u_1, \overline{u}_1, \ldots, u_{(p-1)/2}, \overline{u}_{(p-1)/2}) \in \mathrm{U}(1)^{(p-1)/2}$.

Let $H_{\underline{b}} \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the subgroup such that

$$\phi_{\underline{b}}(u_1, \ldots, u_{(p-1)/2}) = \phi_{\underline{b}}({}^h(u_1, \ldots, u_{(p-1)/2})) \tag{5}$$

for every $h \in H_{\underline{b}}$. Let $\mathcal{H} := \mathcal{G}^0 \rtimes H_{\underline{b}}$. Then we can extend $\phi_{\underline{b}}$ to $\mathcal{H}$ via the map

$$\phi_{\underline{b}} : \mathcal{H} \to \mathbb{C}^\times, \quad \phi_{\underline{b}}(u_1, \ldots, u_{(p-1)/2}, h) = \prod_{i=1}^{(p-1)/2} u_i^{b_i}.$$

By work of Serre [29], every irreducible representation of $\mathcal{G}$ is of the form $\Theta := \mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}}(\chi \otimes \phi_{\underline{b}})$, where χ is a character of $H_{\underline{b}}$ viewed as a character of $\mathcal{H}$ using composition with the projection $\mathcal{H} \to H_{\underline{b}}$.

Theorem 5.5. *The generalized Sato-Tate conjecture holds for* $\mathrm{Jac}(C_p)$ *over* $\mathbb{Q}$.

Proof. We wish to apply Theorem 5.2, so we need to show

$$L_{A_{\mathbb{Q}}}(\Theta, s) = \prod_{p_i} \det(1 - \Theta(x_{p_i}) p_i^{-s})^{-1}$$

is holomorphic and non-vanishing on $Re(s) \geq 1$.

Let n be the cardinality of $H_{\underline{b}}$. We first consider the case where χ is the trivial character. The theory of L-functions gives

$$\begin{aligned} L_{A_{\mathbb{Q}}}(\phi_{\underline{b}}, s) &= L_{A_{\mathbb{Q}}}(\mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}} \mathrm{Ind}_{\mathcal{G}^0}^{\mathcal{H}} \phi_{\underline{b}}, s) \\ &= L_{A_{\mathbb{Q}}}(n \mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}} \phi_{\underline{b}}, s) \\ &= L_{A_{\mathbb{Q}}}(\Theta, s)^n. \end{aligned}$$

Note that the second equality holds by Equation (5). By [10, Section 3.5], we then have $L_{A_{\mathbb{Q}}}(\phi_{\underline{b}}, s) = L(\Psi, s)$ up to a finite number of Euler factors, where Ψ is a Grössencharacter and $L(\Psi, s)$ is holomorphic and nonvanishing on $\mathrm{Re}(s) \geq 1$.

We now consider the case where χ is non-trivial. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic there exists a character $\widetilde{\chi}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\widetilde{\chi}$ restricted to $H_{\underline{b}}$ equals χ. Thus,

$$\Theta = \mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}}(\chi \otimes \phi_{\underline{b}}) = \widetilde{\chi} \otimes \mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}} \phi_{\underline{b}}.$$

Furthermore, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ being cyclic also gives us that

$$n\Theta = \widetilde{\chi} \otimes \mathrm{Ind}_{\mathcal{G}^0}^{\mathcal{G}} \phi_{\underline{b}} = \mathrm{Ind}_{\mathcal{G}^0}^{\mathcal{G}} \phi_{\underline{b}}.$$

Hence, we again have that $L_{A_{\mathbb{Q}}}(\Theta, s)^n = L(\Psi, n)$ up to a finite number of Euler factors, where Ψ is a Grössencharacter and $L(\Psi, s)$ is holomorphic and nonvanishing on $\mathrm{Re}(s) \geq 1$. □

Remark. The result also follows from [22, Prop. 16].

Theorem 5.6. *Let $E/\mathbb{Q}$ be any subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}$. Then the generalized Sato-Tate conjecture holds for $\mathrm{Jac}(C_{2p})$ over E.*

Proof. By Proposition 2.4, $\mathrm{Jac}(C_{2p}) \sim \mathrm{Jac}(C_p)^2$. The result then follows from [22, Prop. 16]. □

6. Moment statistics

In this Section we compute moment statistics associated to the Sato-Tate groups. These moment statistics can be used to verify the equidistribution statement of the generalized Sato-Tate conjecture by comparing them to moment statistics obtained for the traces a_i in the normalized L-polynomial $\overline{L}_p(C, T)$ in Equation (1).

6.1. Preliminaries

The following background information has been adapted from [26, Section 4] and [35, Section 4]. We start by recalling some basic properties of moment statistics. We define

the nth moment (centered at 0) of a probability density function to be the expected value of the nth power of the values, i.e. $M_n[X] = E[X^n]$.

Recall that for independent variables X and Y we have $E[X+Y] = E[X]+E[Y]$ and $E[XY] = E[X]E[Y]$ (see, for example, [26]). Thus, we have the following

$$M_n[XY] = M_n[X]M_n[Y], \tag{6}$$
$$M_a[X]M_b[X] = M_{a+b}[X], \tag{7}$$

and

$$M_n[X_1 + \cdots + X_m] = \sum_{a_1+\cdots+a_m=n} \binom{n}{a_1, \ldots, a_m} M_{a_1}[X_1] \cdots M_{a_m}[X_m]. \tag{8}$$

Furthermore, for any constant b, we have $M_n[b] = b^n$.

We will now work to define the Haar measure on the groups that we obtain for the identity component $\mathrm{ST}^0(\mathrm{Jac}(C))$. From Propositions 4.1 and 4.3 we see that the possible groups are

$$\mathrm{U}(1)^g \text{ and } (\mathrm{U}(1)_2)^{g/2}.$$

For each of these groups, we are interested in the pushforward of the Haar measure onto the set of conjugacy classes $\mathrm{conj}(\mathrm{U}(1)^g)$ or $\mathrm{conj}((\mathrm{U}(1)_2)^{g/2})$.

We start with the unitary group $\mathrm{U}(1)$ and consider the trace map tr on $U \in \mathrm{U}(1)$ defined by $z := \mathrm{tr}(U) = u + \overline{u} = 2\cos(\theta)$, where $u = e^{i\theta}$. This trace map takes values in $[-2, 2]$. From here we see that $dz = 2\sin(\theta)d\theta$ and

$$\mu_{\mathrm{U}(1)} = \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}} = \frac{1}{\pi}d\theta$$

gives a uniform measure of $\mathrm{U}(1)$ on $\theta \in [-\pi, \pi]$ (see [35, Section 2]). We can deduce the following pushforward measures

$$\mu_{\mathrm{U}(1)^n} = \prod_{i=1}^{n} \frac{1}{\pi}\frac{dz_i}{\sqrt{4-z_i^2}} = \prod_{i=1}^{n} \frac{1}{\pi}d\theta_i \quad \text{and} \quad \mu_{(\mathrm{U}(1)_2)^n} = \prod_{i=1}^{n} \frac{1}{\pi}\frac{dz_i}{\sqrt{4-z_i^2}} = \prod_{i=1}^{n} \frac{1}{\pi}d\theta_i.$$

Note that though the measure $\mu_{(\mathrm{U}(1)_2)^n}$ is expressed the same as the measure $\mu_{\mathrm{U}(1)^n}$, we will get a different distribution since in the former case each eigenangle θ_i occurs with multiplicity 2 (see, for example, [35, Section 4.3]).

We can now define the moment sequence $M[\mu]$, where μ is a positive measure on some interval $I = [-d, d]$. The n^{th} moment $M_n[\mu]$ is, by definition, the expected value of ϕ_n with respect to μ, where ϕ_n is the function $z \mapsto z^n$. It is therefore given by

$$M_n[\mu] = \int_I z^n \mu(z).$$

For U(1) we have $M_n[\mu_{\mathrm{U}(1)}] = \binom{n}{n/2}$, where $\binom{n}{n/2} = 0$ if n is odd. Hence,

$$M[\mu_{\mathrm{U}(1)}] = (1, 0, 2, 0, 6, 0, 20, 0, \ldots).$$

From here, we can compute $M_n[\mu_{\mathrm{U}(1)_2}] = 2^n\binom{n}{n/2}$, and take binomial convolutions to obtain

$$M_n[\mu_{\mathrm{U}(1)\times\mathrm{U}(1)}] = \sum_{r=0}^{n} \binom{n}{r} M_n[\mu_{\mathrm{U}(1)}] M_{n-r}[\mu_{\mathrm{U}(1)}].$$

We can combine these strategies with Equations (6), (7), and (8) to compute moments for $\mu_{\mathrm{U}(1)^g}$ and $\mu_{(\mathrm{U}(1)_2)^{g/2}}$.

For each $i \in \{1, 2, \ldots, g\}$, denote by μ_i the projection of the Haar measure onto the interval $\left[-\binom{2g}{i}, \binom{2g}{i}\right]$. We can compute $M_n[\mu_i]$ by averaging over the components of the Sato-Tate group. For example, in the case where the curve has CM by $\mathbb{Q}(\zeta_d)$, we will denote the restriction of μ_i to the component $\mathrm{ST}^0(\mathrm{Jac}(C)) \cdot \gamma^k$ by ${}^k\mu_i$ and

$$\mu_i = \frac{1}{d}\sum_{k=0}^{d} {}^k\mu_i \quad \text{and} \quad M_n[\mu_i] = \frac{1}{d}\sum_{k=0}^{d} M_n[{}^k\mu_i].$$

6.2. Characteristic polynomials

In this subsection, we give results for the characteristic polynomials in each component of the Sato-Tate groups of C_p and C_{2p}.

6.2.1. Characteristic polynomials for C_p

We start with a random matrix U in the identity component $\mathrm{ST}^0(\mathrm{Jac}(C_p))$. We will denote the characteristic polynomial of $U\gamma^i$ by $P_{\gamma^i}(T)$. Since $\gamma^{p-1} \in \mathrm{ST}^0(C_p)$, we only compute $P_{\gamma^i}(T)$ for $i = 0, \ldots, p-2$.

Example 6.1. We compute the characteristic polynomials of the curve $C_{11}\colon y^2 = x^{11} - 1$. This yields $P_{\gamma^1}(T) = P_{\gamma^3}(T) = P_{\gamma^7}(T) = P_{\gamma^9}(T) = T^{10} + 1$ and

$$\begin{aligned}
P_{\gamma^0}(T) &= \prod_{i=1}^{5}(T - u_i)(T - \overline{u_i}),\\
P_{\gamma^2}(T) = P_{\gamma^6}(T) &= (T^5 + u_1\overline{u_2}u_3u_4u_5)(T^5 + \overline{u_1}u_2\overline{u_3u_4u_5}),\\
P_{\gamma^4}(T) = P_{\gamma^8}(T) &= (T^5 - u_1\overline{u_2}u_3u_4u_5)(T^5 - \overline{u_1}u_2\overline{u_3u_4u_5}),\\
P_{\gamma^5}(T) &= (T^2 + 1)^5.
\end{aligned}$$

We have two general results for the characteristic polynomials associated to the Sato-Tate group of C_p, which we combine into the following proposition.

Proposition 6.2. *Let C_p be the genus g curve $y^2 = x^p - 1$, where $p = 2g + 1$ is prime. Then*

$$P_{\gamma^0}(T) = \prod_{i=1}^{g}(T - u_i)(T - \overline{u_i}) \quad \text{and} \quad P_{\gamma^g}(T) = (T^2 + 1)^g.$$

Proof. The first equality is a consequence of Proposition 4.1 which tells us that $\mathrm{ST}^0(\mathrm{Jac}(C_p)) = \mathrm{U}(1)^g$.

For a justification of the second equality, we recall from our work in the proof of Theorem 4.2. There we proved that γ^g is a diagonal block matrix with $\pm J$ on its diagonal entries. Multiplying U by γ^g yields a diagonal block matrix, whose diagonal blocks are of the form

$$\begin{pmatrix} 0 & u_i \\ -\overline{u_i} & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -u_i \\ \overline{u_i} & 0 \end{pmatrix},$$

depending on whether we multiplied by J or $-J$. In either case, the factor of the characteristic polynomial associated to this block is of the form

$$T^2 + u_1\overline{u_1} = T^2 + 1.$$

Thus, since there are g diagonal blocks, the characteristic polynomial is

$$P_{\gamma^g}(T) = (T^2 + 1)^g. \quad \square$$

6.2.2. Characteristic polynomials for C_{2p}

We again start with a random matrix U in the identity component of the Sato-Tate group. Recall that the Sato-Tate group of C_{2p} has two generators for the component group: γ and γ'. We will denote the characteristic polynomial of $U\gamma^i(\gamma')^j$ by $P_{i,j}(T)$. Since $\gamma^{p-1}, (\gamma')^2 \in \mathrm{ST}^0(C_{2p})$, we only compute $P_{i,j}(T)$ for $i = 0, \ldots, p-2$ and $j = 0, 1$.

Example 6.3. We compute the characteristic polynomials of the curve $C_{10}\colon y^2 = x^{10} - 1$. This yields $P_{1,0}(T) = P_{3,0}(T) = P_{1,1}(T) = P_{3,1}(T) = (T^4 + 1)^2$ and

$$\begin{aligned}
P_{0,0}(T) &= \prod_{i=1}^{2}(T - u_i)^2(T - \overline{u_i})^2, \\
P_{2,0}(T) &= (T^2 + 1)^4, \\
P_{0,1}(T) &= T^8 - 2(u_1\overline{u}_2 + \overline{u}_1u_2)T^6 + (4 + (u_1\overline{u}_2)^2 + (\overline{u}_1u_2)^2)T^4 \\
&\quad - 2(u_1\overline{u}_2 + \overline{u}_1u_2)T^2 + 1, \\
P_{2,1}(T) &= T^8 + 2(u_1\overline{u}_2 + \overline{u}_1u_2)T^6 + (4 + (u_1\overline{u}_2)^2 + (\overline{u}_1u_2)^2)T^4 \\
&\quad + 2(u_1\overline{u}_2 + \overline{u}_1u_2)T^2 + 1.
\end{aligned}$$

We have two general results for the characteristic polynomials associated to the Sato-Tate group of C_{2p}, which we combine into the following proposition.

Proposition 6.4. *Let C_{2p} be the genus g curve $y^2 = x^{2p} - 1$, where p is prime. Then*

$$P_{0,0}(T) = \prod_{i=1}^{g/2} (T - u_i)^2 (T - \overline{u_i})^2 \quad \text{and} \quad P_{g/2,0}(T) = (T^2 + 1)^g.$$

Proof. The first equality is a consequence of Proposition 4.3 which tells us that $\mathrm{ST}^0(\mathrm{Jac}(C_p)) = (\mathrm{U}(1)_2)^{g/2}$. For a justification of the second equality, see the proof of Proposition 6.2. □

We also have the following conjecture.

Conjecture 6.5. *Let C_{2p} be the genus g curve $y^2 = x^{2p} - 1$, where p is prime. Then $P_{d,j}(T) = (T^g + 1)^2$, for any d relatively prime to $2g$ and $j = 0$ or 1.*

6.3. General results for the moments

Based on the results of Section 6.2.1, we have the following general result for the moment statistics associated to the Sato-Tate group of C_p.

Proposition 6.6. *For the curve C_p we have*

$$M_n[{}^g\mu_i] = \begin{cases} \binom{g}{i/2}^n & \text{if } i \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Recall from Proposition 6.2 that $P_{\gamma^g}(T) = (T^2 + 1)^g$. Expanding this yields

$$P_{\gamma^g}(T) = \sum_{i=0}^{g} \binom{g}{j} T^{2j}.$$

Thus, $a_i = \binom{g}{i/2}$ when i is even and it equals 0 when i is odd. It is then clear that $\mu_i(\phi_n)$ in this case is $\binom{g}{i/2}^n$ when i is even and 0 when i is odd □

We also have the following conjecture for characteristic polynomials and moments.

Conjecture 6.7. *Let C_p be the genus g curve $y^2 = x^p - 1$, where $p = 2g + 1$ is prime. Then $P_{\gamma^d}(T) = T^{2g} + 1$, for any d relatively prime to $2g$ and $M_n[{}^k\mu_i] = 0$.*

Table 1
Moment Statistics for $y^2 = x^{11} - 1$.

$M[\mu_1]$	$(1, 0, 1, 0, 27, 0, 1090, \ldots)$
$M[\mu_2]$	$(1, 1, 9, 133, 2873, 75453, 2200605, \ldots)$
$M[\mu_3]$	$(1, 0, 24, 0, 1381080, 0, 161935061760, \ldots)$
$M[\mu_4]$	$(1, 2, 64, 4688, 498236, 61887736, 8430343600, \ldots)$
$M[\mu_5]$	$(1, 0, 72, 0, 934332, 0, 22782049800, \ldots)$

Table 2
Table of μ_1- and a_1-moments for $y^2 = x^m - 1$ over $\mathbb{Q}$.

m		M_2	M_4	M_6	M_8
10	μ_1	2	72	3200	156800
	a_1	1.989	71.484	3172.685	155240.208
11	μ_1	1	27	1090	55195
	a_1	0.991	26.425	1049.681	52204.146
13	μ_1	1	33	1660	106785
	a_1	0.999	33.108	1677.458	108839.689
14	μ_1	2	120	9920	954240
	a_1	1.982	118.214	9694.808	923186.514
17	μ_1	1	45	3160	290605
	a_1	0.991	44.178	3068.003	279757.762
19	μ_1	1	51	4090	432915
	a_1	0.995	50.601	4040.554	425599.259
22	μ_1	2	216	34880	7064960
	a_1	1.996	213.572	34047.140	6805376.261

6.4. Explicit examples of moment statistics

We first determine moment statistics for the genus 5 curve $C_{11} : \ y^2 = x^{11} - 1$. Using characteristic polynomials $P_{\gamma^k}(T)$ that were computed for each component in Example 6.1 and the properties in Equations (6), (7), and (8), we can compute the nth moments for each μ_i, $1 \leq i \leq 5$. These moments, given in Table 1, are easily computed using Sage [21]. See Table 2 in Section 6.5 for a comparison of $M[\mu_1]$ to the numerical moments $M[a_1]$ of the normalized L-polynomial of the curve.

Using the same strategy as above, we determine that the μ_1-moment statistics for the Sato-Tate group of $C_{10}\colon y^2 = x^{10} - 1$ are

$$M[\mu_1] = (1, 0, 2, 0, 72, 0, 3200, 0, 156800, 0, 8128512 \ldots).$$

In Fig. 1 we give a histogram of a_1-values of $y^2 = x^{10} - 1$, as well as moment statistics (up to the 10th moment). Observe that the numerical moments $M[a_1]$, which are computed using primes up to 2^{28}, are quite close to what we obtained for $M[\mu_1]$. See [34] for an animated histogram of the a_1-distribution. The algorithm used to make the histogram is described in [18] and [19].

See Table 2 in Section 6.5 for moment statistics for other curves.

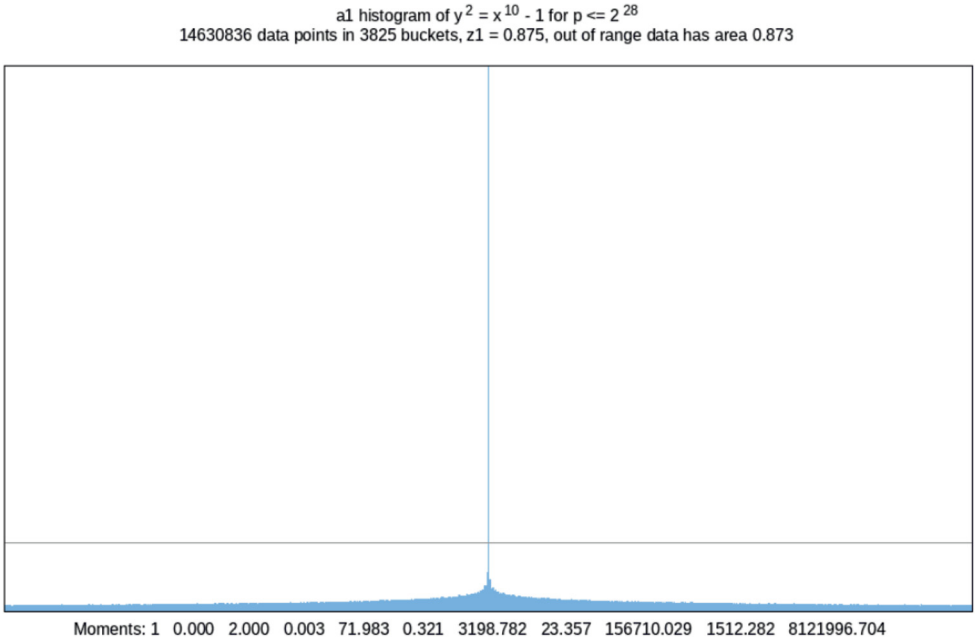

Fig. 1. Histogram of a_1 values of $y^2 = x^{10} - 1$ for primes less than 2^{28}. See [34].

6.5. Tables of μ_1- and a_1-moment statistics

We first consider curves of the form $C_p: \ y^2 = x^p - 1$. Note that $M[^k\mu_1] = 0$ for all $0 < k < p - 1$. One can easily determine from Proposition 6.2 that the coefficient of T in $P_{\gamma^0}(T)$ is $\sum_{i=1}^{g} s_i$, where $s_i = -(u_i + \overline{u_i})$. Hence,

$$M_n[^0\mu_1] = \sum_{\alpha_1,\ldots,\alpha_g=0}^{n} \binom{n}{\alpha_1, \alpha_2, \ldots, \alpha_g} M_{\alpha_1}[s_1] M_{\alpha_2}[s_2] \cdots M_{\alpha_g}[s_g]. \tag{9}$$

Similarly, for curves of the form $C_{2p}: \ y^2 = x^{2p} - 1$,

$$M_n[^{k,j}\mu_1] = 2^n \sum_{\alpha_1,\ldots,\alpha_{g/2}=0}^{n} \binom{n}{\alpha_1, \alpha_2, \ldots, \alpha_{g/2}} M_{\alpha_1}[s_1] M_{\alpha_2}[s_2] \cdots M_{\alpha_{g/2}}[s_{g/2}] \tag{10}$$

whenever $k = j = 0$ and $M_n[^{k,j}\mu_1] = 0$ otherwise.

We used Sage [21] to evaluate Equations (9) and (10), and then average over the components, to get the μ_1-moments shown in Table 2. Note that $M_n[\mu_1] = 0$ for all odd n, so we omit those values from the table. For comparison, we computed the numerical a_1-moments for primes up to 2^{23}.

Appendix A. Examples of the γ matrix

In Table 3 we give examples of the matrix γ from Theorems 4.2 and 4.4. These were computed in Sage [21] using Sage's chosen generators for $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/2p\mathbb{Z})^\times$.

Table 3
Examples of γ matrices for $y^2 = x^m - 1$.

m	γ	m	γ
10	$\begin{pmatrix} 0 & 0 & J & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & -J & 0 & 0 \end{pmatrix}$	13	$\begin{pmatrix} 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I \\ 0 & 0 & 0 & 0 & J & 0 \\ 0 & 0 & J & 0 & 0 & 0 \\ J & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
11	$\begin{pmatrix} 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & J \\ 0 & 0 & J & 0 & 0 \\ J & 0 & 0 & 0 & 0 \end{pmatrix}$	14	$\begin{pmatrix} 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I \\ 0 & 0 & 0 & 0 & J & 0 \\ 0 & -J & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 \end{pmatrix}$

References

[1] P.B. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B.V.L. Hung, J. Newton, P. Scholze, R. Taylor, J.A. Thorne, Potential Automorphy over CM Fields, 2018.
[2] N. Aoki, Hodge cycles on CM abelian varieties of Fermat type, Comment. Math. Univ. St. Pauli 51 (1) (2002) 99–130.
[3] S. Arora, V. Cantoral-Farfán, A. Landesman, D. Lombardo, J.S. Morrow, The twisting Sato-Tate group of the curve $y^2 = x^8 - 14x^4 + 1$, Math. Z. 290 (3–4) (2018) 991–1022.
[4] G. Banaszak, W. Gajda, P. Krasoń, On Galois representations for abelian varieties with complex and real multiplications, J. Number Theory 100 (1) (2003) 117–132.
[5] G. Banaszak, K.S. Kedlaya, An algebraic Sato-Tate group and Sato-Tate conjecture, Indiana Univ. Math. J. 64 (1) (2015) 245–274.
[6] 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) (2011) 29–98.
[7] 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 (2008) 1–181, With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.
[8] P. Deligne, J.S. Milne, A. Ogus, K.-y. Shih, Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982.
[9] M. Emory, H. Goodson, A. Peyrot, Towards the Sato-Tate groups of trinomial hyperelliptic curves, Int. J. Number Theory 17 (2021) 2175–2206.
[10] F. Fité, Equidistribution, L-functions, and Sato-Tate groups, in: Trends in Number Theory, in: Contemp. Math., vol. 649, Amer. Math. Soc., Providence, RI, 2015, pp. 63–88.
[11] F. Fité, J. González, J.-C. Lario, Frobenius distribution for quotients of Fermat curves of prime exponent, Can. J. Math. 68 (2) (2016) 361–394.
[12] F. Fité, K.S. Kedlaya, V. Rotger, A.V. Sutherland, Sato-Tate distributions and Galois endomorphism modules in genus 2, Compos. Math. 148 (5) (2012) 1390–1442.
[13] F. Fité, K.S. Kedlaya, A.V. Sutherland, Sato-Tate groups of abelian threefolds: a preview of the classification, ArXiv e-prints, arXiv:1911.02071, Nov. 2019.
[14] F. Fité, E. Lorenzo García, A.V. Sutherland, Sato-Tate distributions of twists of the Fermat and the Klein quartics, Res. Math. Sci. 5 (4) (2018) 41.
[15] 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 (3) (2014) 543–585.
[16] F. Fité, 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, in: Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 103–126.
[17] M. Harris, N. Shepherd-Barron, R. Taylor, A family of Calabi-Yau varieties and potential automorphy, Ann. Math. (2) 171 (2) (2010) 779–813.

[18] D. Harvey, A.V. Sutherland, Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, LMS J. Comput. Math. 17 (suppl. A) (2014) 257–273.
[19] D. Harvey, A.V. Sutherland, Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II, in: Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures, in: Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147.
[20] F. Hazama, Algebraic cycles on nonsimple abelian varieties, Duke Math. J. 58 (1) (1989) 31–37.
[21] S. Inc., CoCalc collaborative computation online, https://cocalc.com/, 2020.
[22] C. Johansson, On the Sato-Tate conjecture for non-generic abelian surfaces, Trans. Am. Math. Soc. 369 (9) (2017) 6303–6325, With an appendix by Francesc Fité.
[23] K.S. Kedlaya, A.V. Sutherland, Hyperelliptic curves, L-polynomials, and random matrices, in: Arithmetic, Geometry, Cryptography and Coding Theory, in: Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 119–162.
[24] T. Kubota, On the field extension by complex multiplication, Trans. Am. Math. Soc. 118 (1965) 113–122.
[25] S. Lang, Cyclotomic Fields I and II, second edition, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin.
[26] J.-C. Lario, A. Somoza, The Sato-Tate conjecture for a Picard curve with complex multiplication (with an appendix by Francesc Fité), in: Number Theory Related to Modular Curves—Momose Memorial Volume, in: Contemp. Math., vol. 701, Amer. Math. Soc., Providence, RI, 2018, pp. 151–165.
[27] N. Müller, R. Pink, Hyperelliptic curves with many automorphisms, arXiv e-prints, arXiv:1711.06599, Nov 2017.
[28] H. Pohlmann, Algebraic cycles on abelian varieties of complex multiplication type, Ann. Math. (2) 88 (1968) 161–180.
[29] J.-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York-Heidelberg, 1977, Translated from the second French edition by Leonard L. Scott.
[30] J.-P. Serre, Abelian l-Adic Representations and Elliptic Curves, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.
[31] J.-P. Serre, Lectures on $N_X(p)$, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012.
[32] G. Shimura, Y. Taniyama, Complex Multiplication of Abelian Varieties and Its Applications to Number Theory, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.
[33] T. Shioda, Algebraic cycles on abelian varieties of Fermat type, Math. Ann. 258 (1) (1981/1982) 65–80.
[34] A.V. Sutherland, Sato-Tate distribution of $y^2 = x^{10} - 1$, http://math.mit.edu/~drew/x10m1_a1f.gif, 2019. (Accessed 9 October 2019).
[35] A.V. Sutherland, Sato-Tate distributions, in: Analytic Methods in Arithmetic Geometry, in: Contemp. Math., vol. 740, Amer. Math. Soc., Providence, RI, 2019, pp. 197–248.
[36] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. II, Publ. Math. Inst. Hautes Études Sci. 108 (2008) 183–239.
[37] P. van Wamelen, Equations for the Jacobian of a hyperelliptic curve, Trans. Am. Math. Soc. 350 (8) (1998) 3083–3106.
[38] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Am. Math. Soc. 73 (1952) 487–495.
[39] C.-F. Yu, A note on the Mumford-Tate conjecture for CM abelian varieties, Taiwan. J. Math. 19 (4) (2015) 1073–1084.