

JOURNAL

de Théorie des Nombres

de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Heidi GOODSON

Sato–Tate Distributions of Catalan Curves

Tome 35, n° 1 (2023), p. 87-113.

<https://doi.org/10.5802/jtnb.1238>

© Les auteurs, 2023.



Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

Sato–Tate Distributions of Catalan Curves

par HEIDI GOODSON

RÉSUMÉ. Étant donnés deux nombres premiers impairs distincts p et q , nous définissons la courbe de Catalan $C_{p,q}$ donnée par l'équation affine $y^q = x^p - 1$. Dans cet article, nous construisons les groupes de Sato–Tate des variétés jacobiniennes de ces courbes, afin d'étudier les distributions asymptotiques des coefficients de leurs polynômes de Weil normalisés. Ces jacobiniennes de Catalan sont non-dégénérées et simples et le groupe de Galois de leur corps d'endomorphismes sur $\mathbb{Q}$ n'est pas cyclique, ce qui en font des variétés intéressantes dans le contexte des groupes de Sato–Tate. Dans cet article, nous calculons les moments statistiques et numériques des distributions asymptotiques. Enfin, nous déterminons les types des modules galoisiens donnés par l'algèbre réelle des endomorphismes de ces jacobiniennes, en utilisant des techniques connues ainsi que certaines nouvelles techniques.

ABSTRACT. For distinct odd primes p and q , we define the Catalan curve $C_{p,q}$ by the affine equation $y^q = x^p - 1$. In this article we construct the Sato–Tate groups of the Jacobians in order to study the limiting distributions of coefficients of their normalized L -polynomials. Catalan Jacobians are non-degenerate and simple with noncyclic Galois groups (of the endomorphism fields over $\mathbb{Q}$), thus making them interesting varieties to study in the context of Sato–Tate groups. We compute both statistical and numerical moments for the limiting distributions. Lastly, we determine the Galois endomorphism types of the Jacobians using both old and new techniques.

1. Introduction

Let p and q be distinct odd primes. The nonsingular genus $(p-1)(q-1)/2$ curve $C_{p,q}$ defined by the affine equation

$$y^q = x^p - 1$$

is called the *Catalan curve*, likely named after the famous Catalan conjecture¹ regarding consecutive integers that are perfect powers. The primary

Manuscrit reçu le 21 octobre 2021, révisé le 4 octobre 2022, accepté le 21 octobre 2022.

2010 *Mathematics Subject Classification*. 11M50, 11G10, 11G20, 14G10.

Mots-clefs. Sato–Tate groups, Sato–Tate distributions, Jacobian varieties, endomorphism algebras.

Goodson was partially supported by National Science Foundation grant (DMS-2201085) and by a PSC-CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York.

¹The Catalan conjecture was proved by Mihăilescu [25] more than 150 years after Catalan published his conjecture.

goals of this article are to study the limiting distributions of coefficients of normalized L -polynomials of the Jacobians of Catalan curves and to study their real endomorphism algebras. These types of distributions are called *Sato–Tate distributions*, named for Mikio Sato and John Tate who independently made conjectures for those associated to elliptic curves in the 1960s. Their conjectures are known to be true for elliptic curves without complex multiplication defined over totally real fields and for all elliptic curves with complex multiplication.

Recent work has expanded this field to the study of distributions for abelian varieties of dimension at least 2. The generalized Sato–Tate conjecture predicts that the distributions converge to the distributions of traces in a compact Lie group referred to as the Sato–Tate group. The Sato–Tate group is related to the Mumford–Tate group, Hodge group, motivic Galois group, and l -adic monodromy group, thus placing this area of research at the intersection of many important fields in number theory, group theory, and algebraic geometry.

Before describing the work in higher genus, we first recall the original Sato–Tate conjecture for elliptic curves. Let F be a number field, E/F be an elliptic curve without complex multiplication (CM), and v be a finite prime of F such that E has good reduction at v . By a theorem of Hasse, the number of F_{q_v} points of E is $q_v + 1 - a_v$, where F_{q_v} denotes the residue field of v and a_v is an integer (called the trace of Frobenius) satisfying $|a_v| \leq 2q_v^{1/2}$. 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 distributed in the interval $[-2, 2]$ with respect to the image of the Haar measure on the special unitary group $SU(2)$. This conjecture was proved in 2008 for non-CM elliptic curves defined over totally real fields (see [6, 8, 18, 33]).

The distributions of the normalized Frobenius traces were known much earlier for CM elliptic curves over all fields: they are distributed with respect to the image 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 the exposition in [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 (see, for example, [32]). In our work, the abelian varieties will be the Jacobians of curves, and so we now state the conjecture specifically for Jacobian varieties.

Let C be a smooth, projective, genus g curve defined over a number field F . The Sato–Tate group of the Jacobian of C , $ST(\text{Jac}(C)) \subseteq \text{USp}(2g)$, is a compact Lie group satisfying the following property: for each prime $\mathfrak{p}$ at

which C has good reduction, there exists a conjugacy class of $\mathrm{ST}(\mathrm{Jac}(C))$ whose characteristic polynomial equals the normalized L -polynomial at $\mathfrak{p}$

$$(1.1) \quad \bar{L}_{\mathfrak{p}}(C, T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \cdots + a_2 T^2 + a_1 T + 1.$$

Conjecture 1.1 (Generalized Sato–Tate Conjecture). *Let $(x_{\mathfrak{p}})$ be the sequence of conjugacy classes of normalized images of Frobenius elements in $\mathrm{ST}(\mathrm{Jac}(C))$ at primes $\mathfrak{p}$ of good reduction for $\mathrm{Jac}(C)$, ordered by norm. Then the sequence $(x_{\mathfrak{p}})$ is equidistributed with respect to the pushforward of the Haar measure of $\mathrm{ST}(\mathrm{Jac}(C))$ to its space of conjugacy classes.*

The generalized Sato–Tate conjecture was proved for CM abelian varieties in [23]. Beyond proving the generalized Sato–Tate conjecture, we would also like a precise description of the limiting distributions of coefficients of the normalized L -polynomials. For a nondegenerate abelian variety A , the component group of the Sato–Tate group is isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$, where K is the endomorphism field of A . However, knowing this is not enough to give the limiting distributions. For this, we need an explicit description of the identity component and of the generators of the component group of the Sato–Tate group.

Determining these Sato–Tate groups is the source of ongoing interest and work. The current literature contains many articles for abelian varieties of fixed, small genus. For example, [12] and [14, 13] determine all possible Sato–Tate groups in dimension 2 and 3, respectively, by determining which subgroups of the unitary symplectic group satisfy certain axioms (see Section 2.4). Other articles determine Sato–Tate groups for certain families of genus 2 and 3 curves (see [17, 24]) or for twists of curves (see [3, 15, 16]).

As noted in [13], it is not expected, in dimension greater than 3, that every group satisfying the Sato–Tate axioms (see Section 2.4) can be realized using Jacobians of curves. There are currently two articles that study the Sato–Tate groups of families of Jacobian varieties of arbitrarily high genus (see [10, 11]). In this article we provide a new example of an infinite family of Sato–Tate groups that can be realized by higher dimensional Jacobian varieties. Unlike the earlier articles, the component groups of these Sato–Tate groups are products of cyclic groups. Furthermore, we go a step further by computing the Galois endomorphism types of the Jacobians.

Organization of the paper. In Section 2 we provide an overview of this area of research, as well as some results that will be applied when computing the Sato–Tate groups of Jacobians of Catalan curves (Catalan Jacobians). In Section 3 we give a complete description of the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$ on the endomorphisms of the Jacobian – this description is needed in order to determine the twisted Lefschetz groups of Catalan Jacobians. The main result of Section 4 is the explicit description of the Sato–Tate groups of Catalan Jacobians. In Section 5, we compute

moment statistics associated to the Sato–Tate groups of Catalan Jacobians. Lastly, in Section 6, we study the Galois endomorphism types of Catalan Jacobians through data obtained from moment statistics and by working with Rosati forms.

Notation and conventions. We begin by fixing notation used in later sections. Let A be an abelian variety defined over a number field F . The ring of endomorphisms of A/F is denoted by $\text{End}(A_F)$, or simply $\text{End}(A)$ if the field of definition is clear from the context.

The curve $y^q = x^p - 1$ is denoted by $C_{p,q}$, and we assume throughout the paper that p and q are distinct odd primes. 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 $r - 1$.

Let I denote the 2×2 identity matrix and define the matrices

$$(1.2) \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$(1.3) \quad Z = Z_{pq} = \text{diag}(\zeta_{pq}, \overline{\zeta_{pq}})$$

The symplectic form considered throughout the paper is given by

$$(1.4) \quad H = \text{diag}(\underbrace{J, \dots, J}_g).$$

Lastly, embed $\text{U}(1)$ in $\text{SU}(2)$ via $u \mapsto \begin{pmatrix} u & \\ & \bar{u} \end{pmatrix}$ and, for any positive integer n , define the following subgroup of the unitary symplectic group $\text{USp}(2n)$

$$\text{U}(1)^n := \langle \text{diag}(u_1, \bar{u}_1, \dots, u_n, \bar{u}_n) : u_i \in \mathbb{C}^\times, |u_i| = 1 \rangle.$$

2. Background

2.1. An ℓ -adic construction of the Sato–Tate group. We begin by defining both the algebraic Sato–Tate group and the Sato–Tate group. We follow the exposition of [10] and [32, Section 3.2]. See also [30, Chapter 8].

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

$$(2.1) \quad \rho_{A,\ell} : \text{Gal}(\bar{F}/F) \rightarrow \text{Aut}(V_\ell) \cong \text{GL}_{2g}(\mathbb{Q}_\ell).$$

The ℓ -adic monodromy group of A , denoted $G_{A,\ell}$, is the Zariski closure of the image of this map in $\text{GL}_{2g}(\mathbb{Q}_\ell)$, and we define $G_{A,\ell}^1 := G_{A,\ell} \cap \text{Sp}_{2g}(\mathbb{Q}_\ell)$.

Banaszak and Kedlaya proposed in [5, Conjecture 2.1] the following conjecture that was partly intended to be a refinement of the Mumford–Tate conjecture.

Conjecture 2.1 (Algebraic Sato–Tate Conjecture). *There is an algebraic subgroup $\text{AST}(A)$ of Sp_{2g} over $\mathbb{Q}$, called the algebraic Sato–Tate group of A , such that $\text{AST}^0(A)$ is reductive and, for each prime ℓ , $G_{A,\ell}^1 = \text{AST}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$.*

When this conjecture holds we can define the *Sato–Tate group* of A , denoted $\text{ST}(A)$, to be a maximal compact Lie subgroup of $G_{A,\ell}^1 \otimes_{\mathbb{Q}_{\ell}} \mathbb{C} = \text{AST}(A) \otimes_{\mathbb{Q}} \mathbb{C}$ contained in $\text{USp}(2g)$. It is conjectured that $\text{ST}(A)$ is, up to conjugacy in $\text{USp}(2g)$, independent of the choice of the prime ℓ and of the embedding of $\mathbb{Q}_{\ell}$ in $\mathbb{C}$ and so we will refer to $\text{ST}(A)$ as *the* Sato–Tate group of A (see, for example, [32]). While the Sato–Tate group is a compact Lie group, it may not be connected [17]. We denote the connected component of the identity (also called the identity component) of $\text{ST}(A)$ by $\text{ST}^0(A)$.

2.2. Nondegeneracy. Let A be a nonsingular projective variety over $\mathbb{C}$. We denote the (complexified) Hodge ring of A by

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

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

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

where $\mathcal{D}^d(A)$ is the $\mathbb{C}$ -span of classes of intersection of d -divisors. This is the subring of $\mathcal{B}^*(A)$ generated by the divisor classes, i.e. generated by $\mathcal{B}^1(A)$. In general, it is known that we have containment $\mathcal{D}^*(A) \subseteq \mathcal{B}^*(A)$, and we say that an abelian variety A is *nondegenerate* if we have equality, i.e. $\mathcal{D}^*(A) = \mathcal{B}^*(A)$ (see [1]). Furthermore, an abelian variety A is said to be *stably nondegenerate* if, for any integer $k \geq 1$, $\mathcal{D}^*(A^k) = \mathcal{B}^*(A^k)$ [1, 21]. If $\mathcal{B}^*(A)$ is not generated by the divisor classes $\mathcal{B}^1(A)$, i.e. $\mathcal{D}^*(A) \neq \mathcal{B}^*(A)$, then A is said to be *degenerate*. The additional Hodge cycles that are not generated by divisor classes are referred to as *exceptional cycles* or *exceptional classes* (see, for example, [26]).

While nondegeneracy extends to powers of stably nondegenerate abelian varieties, it does not necessarily apply to products of nonisogenous varieties. For example, Shioda demonstrates in [31] that the Jacobian of the genus 4 curve $y^2 = x^9 - 1$ is degenerate, though it is the product of two simple, nondegenerate varieties. Aoki proves in [2] that generalized Catalan curves

$C_{p^\mu, q^\nu} : y^{q^\nu} = x^{p^\mu} - 1$, where $(\mu, \nu) \neq (1, 1)$, also exhibit this phenomenon: each of the factors of the Jacobian are nondegenerate but $\text{Jac}(C_{p^\mu, q^\nu})$ is itself degenerate. Hazama explains in [21] that this can occur when one of the simple factors is of type-IV in the Albert's classification.

Hazama proves in Theorem 1.2 of [21] that A is stably nondegenerate if and only if the dimension of its Hodge group is maximal². When A is an abelian variety with CM and is absolutely simple, this is equivalent to saying that the CM type is nondegenerate (see, for example, [1, 11]). The following result is proved in [22].

Proposition 2.2. *The Jacobian variety $\text{Jac}(C_{p,q})$ of the Catalan curve is absolutely simple and nondegenerate.*

Hazama proves the nondegeneracy by proving that the CM-type is nondegenerate. This is done by verifying the non-vanishing of certain character sums attached to the Jacobian.

Nondegeneracy is related to the Hodge conjecture. Let $\mathcal{C}^d(A)$ be the subspace of $\mathcal{B}^d(A)$ generated by the classes of algebraic cycles on A of codimension d . Then

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

and the *Hodge conjecture* for A asserts that $\mathcal{C}^d(A) = \mathcal{B}^d(A)$ for all d [1, 31]. It is clear from the definition that if A is nondegenerate then the Hodge conjecture holds, and if the Hodge conjecture does not hold then A must be degenerate. However, there are many cases where the Hodge conjecture holds for degenerate abelian varieties (see, for example, [27, 31]).

2.3. The Twisted Lefschetz group. Banaszak and Kedlaya introduced in [5] the *twisted Lefschetz group*, denoted $\text{TL}(A)$, which is a closed algebraic subgroup of Sp_{2g} defined by

$$(2.2) \quad \text{TL}(A) := \bigcup_{\tau \in \text{Gal}(\bar{F}/F)} \text{L}(A)(\tau),$$

where $\text{L}(A)(\tau) := \{\gamma \in \text{Sp}_{2g} \mid \gamma \alpha \gamma^{-1} = \tau(\alpha) \text{ for all } \alpha \in \text{End}(A_{\bar{F}})_{\mathbb{Q}}\}$. When τ is the identity automorphism, $\text{L}(A)(\tau)$ forms a group, called the Lefschetz group, which is denoted in the literature as simply $\text{L}(A)$.

Banaszak and Kedlaya prove in [5, Theorem 6.1] that if the Mumford–Tate conjecture is explained by endomorphisms and the twisted Lefschetz group of $A/\bar{F}$ is connected, then the algebraic Sato–Tate conjecture holds and $\text{AST}(A) = \text{TL}(A)$. In this case, we say that the algebraic Sato–Tate conjecture is also explained by endomorphisms. It follows from [5, Theorem 6.1] and work of Serre in [30, Section 8.3.4] that when the algebraic

²In [11], the authors use the word *nondegenerate* to describe abelian varieties with this property.

Sato–Tate conjecture is explained by endomorphisms the component group $\mathrm{ST}(A)/\mathrm{ST}^0(A)$ is isomorphic to the Galois group $\mathrm{Gal}(K/F)$, where K is the *endomorphism field* of A , i.e. the minimal extension over which all the endomorphisms of the abelian variety A are defined (see, for example, [32, Theorem 3.12] and [12, Proposition 2.17]). We can use the twisted Lefschetz group to write down explicit generators of the component group of the Sato–Tate group.

The Jacobian varieties we study in this paper satisfy these conditions, and so we have the following result.

Proposition 2.3. *The algebraic Sato–Tate Conjecture holds for the Catalan curve $\mathrm{Jac}(C_{p,q})$ with $\mathrm{AST}(\mathrm{Jac}(C_{p,q})) = \mathrm{TL}(\mathrm{Jac}(C_{p,q}))$.*

Proof. In Proposition 2.2 we saw that $\mathrm{Jac}(C_{p,q})$ is a nondegenerate CM abelian variety. The result then follows from Theorems 6.1 and 6.6 in [5]. $\square$

2.4. The Sato–Tate axioms. We conclude the background section by recalling some necessary conditions for a subgroup of $\mathrm{USp}(2g)$ to occur as a Sato–Tate group. These axioms will not be used in our work, but they have been used to classify all possible Sato–Tate groups for a given dimension $g \leq 3$ (see, for example, [12, 14, 13]). We state the axioms as they are laid out in [13]. For a group G with identity component G^0 , the Sato–Tate group axioms in dimension g are as follows.

- (ST1) The group G is a closed subgroup of $\mathrm{USp}(2g)$.
- (ST2) (Hodge condition) There exists a homomorphism $\theta: \mathrm{U}(1) \rightarrow G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} each with multiplicity g . The image of such a θ is called a *Hodge circle*, and the set of all Hodge circles generates a dense subgroup of G^0 .
- (ST3) (Rationality condition) For each component H of G and irreducible character χ of $\mathrm{GL}(\mathbb{C}^{2g})$, the expected value (under the Haar measure) of $\chi(\gamma)$ over $\gamma \in H$ is an integer.
- (ST4) (Lefschetz condition) The subgroup of $\mathrm{USp}(2g)$ fixing $\mathrm{End}(\mathbb{C}^{2g})^{G^0}$ is equal to G^0 .

Proposition 3.2 of [12] proves that, for any abelian variety satisfying both the Mumford–Tate conjecture and the algebraic Sato–Tate conjecture, the Sato–Tate group $G = \mathrm{ST}(A)$ satisfies the first three axioms. The last axiom is satisfied if, in addition, the Hodge group of A equals the Lefschetz group of A (see [13, Proposition 3.3]). Catalan Jacobians satisfy these properties, and so their Sato–Tate groups satisfy the four axioms.

3. Endomorphisms of Catalan Jacobians

Let $p \neq q$ be odd primes. The Jacobian of $C_{p,q}$ has complex multiplication by the field $K = \mathbb{Q}(\zeta_{pq})$, and so the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a product of cyclic groups $\mathbb{Z}/p\mathbb{Z}^\times \times \mathbb{Z}/q\mathbb{Z}^\times$. The main goals

of this section are to give an explicit model of a generator for the group of endomorphisms of $\text{Jac}(C_{p,q})$ and to describe how the Galois group acts on the endomorphism. We begin by defining some necessary notation that will be used when defining both the endomorphism and the Sato–Tate group of $\text{Jac}(C_{p,q})$.

3.1. Galois elements and some notation. Let c be a generator for $\mathbb{Z}/p\mathbb{Z}^\times$ and d be a generator for $\mathbb{Z}/q\mathbb{Z}^\times$. These elements yield the following generators of $\text{Gal}(K/\mathbb{Q})$:

$$\sigma_p: \begin{cases} \zeta_p \mapsto \zeta_p^c \\ \zeta_q \mapsto \zeta_q \end{cases} \quad \sigma_q: \begin{cases} \zeta_p \mapsto \zeta_p \\ \zeta_q \mapsto \zeta_q^d \end{cases}.$$

In this paper, we will be working with powers of ζ_{pq} of the form $\zeta_{pq}^{q(a+1)-pb}$. We compute the actions of the Galois elements on these powers of ζ_{pq} to be

$$(3.1) \quad \sigma_p \left(\zeta_{pq}^{q(a+1)-pb} \right) = \zeta_{pq}^{qc(a+1)-pb} \quad \text{and} \quad \sigma_q \left(\zeta_{pq}^{q(a+1)-pb} \right) = \zeta_{pq}^{q(a+1)-pbd}.$$

We now define some additional notation. Let $k_0 = 0$ and for any b satisfying $1 \leq b \leq q-1$, define

$$(3.2) \quad k_b = \left\lfloor \frac{pb - q - 1}{q} \right\rfloor.$$

The k_b -values are increasing with respect to b : $k_{b_1} \leq k_{b_2}$ whenever $b_1 \leq b_2$. When $p < q$, the value k_b may be negative for some values of b , and we let κ_t be the sum

$$(3.3) \quad \kappa_t = \sum_{\substack{b=0 \\ k_b \geq 0}}^t (k_b + 1),$$

where we restrict to adding only the nonnegative values k_b .

3.2. Defining the endomorphism. Let $\alpha: C_{p,q} \rightarrow C_{p,q}$ be the curve automorphism defined by $\alpha(x, y) = (\zeta_p x, \zeta_q y) = (\zeta_{pq}^q x, \zeta_{pq}^p y)$. This automorphism has order pq , and so it is a generator of the automorphism group of $C_{p,q}$. It is then clear that the endomorphism ring of $\text{Jac}(C_{p,q})$ satisfies the following.

Proposition 3.1. *Let $K = \mathbb{Q}(\zeta_{pq})$. Then*

$$\text{End}(\text{Jac}(C_{p,q})_K) \simeq \mathbb{Z}[\zeta_{pq}].$$

For any intermediate field $L \subseteq K$, the endomorphism ring $\text{End}(\text{Jac}(C_{p,q})_L)$ is isomorphic to

$$\mathcal{O}_L = \mathcal{O}_K^{\text{Gal}(K/L)} \subseteq \mathcal{O}_K \simeq \text{End}(\text{Jac}(C_{p,q})_K).$$

Proof. The second half of the statement follows from the fact that the isomorphism in the first half of the statement is Galois-equivariant. $\square$

Let a and b be integers satisfying

$$(3.4) \quad 1 \leq b \leq q-1$$

$$(3.5) \quad 0 \leq a < p \quad \text{and} \quad a \leq k_b.$$

The genus of $C_{p,q}$ is $g = (p-1)(q-1)/2$ and we take as a basis for the space of regular 1-forms $\Omega^1(C_{p,q})$ the set

$$(3.6) \quad B = \left\{ \omega_{a,b} = \frac{x^a dx}{y^b} \left| \begin{array}{l} b \text{ satisfies Equation (3.4)} \\ a \text{ satisfies Equation (3.5)} \end{array} \right. \right\}.$$

We compute pullbacks of the differentials with respect to α in order to determine the associated endomorphism α of $\text{Jac}(C_{p,q})$:

$$\alpha^*(\omega_{a,b}) = \zeta_{pq}^{q(a+1)-pb} \omega_{a,b}.$$

We can now define the induced endomorphism α of $H_1(\text{Jac}(C_{p,q})_{\mathbb{C}}, \mathbb{Q})$.

Definition 3.2. By taking the symplectic basis of $H_1(\text{Jac}(C_{p,q})_{\mathbb{C}}, \mathbb{C})$ (with respect to the matrix $H = \text{diag}(J, \dots, J)$) corresponding to B in Equation (3.6), α is the diagonal matrix whose i^{th} diagonal 2×2 block is

$$\alpha[i] = Z^{q(a_i+1)-pb_i},$$

where $a_i = i - \kappa_{b_i-1} - 1$ and b_i is the largest integer satisfying Equation (3.4) such that $a_i > 0$.

Example 3.3. Consider the genus 6 curve $C_{7,3}: y^3 = x^7 - 1$. Using the strategy described above, we write the basis of $\Omega^1(C_{p,q})$ as

$$\{\omega_{0,1}, \omega_{1,1}, \omega_{0,2}, \omega_{1,2}, \omega_{2,2}, \omega_{3,2}\}$$

and the endomorphism α as

$$\alpha = \text{diag}(Z^{q-p}, Z^{2q-p}, Z^{q-2p}, Z^{2q-2p}, Z^{3q-2p}, Z^{4q-2p}).$$

3.3. The actions of the Galois elements on α . The main results of this subsection are Propositions 3.5 and 3.6, where we describe the action of the Galois elements on the endomorphism α . The following lemma will be referenced in the proofs of these propositions.

Lemma 3.4. *Let β be a positive integer satisfying Inequality (3.4), and define two quantities $y_1 = (p(q-\beta)-q+1)/q$ and $y_2 = (p(q-\beta)-q-1)/q$. Then any integer λ satisfying $\lambda < y_1$ also satisfies $\lambda \leq \lfloor y_2 \rfloor$.*

Proof. The quantities y_1 and y_2 differ by $2/q$: $y_2 = y_1 - 2/q$. Let λ be any integer less than y_1 . We split the proof of the lemma into two cases: $y_1 \in \mathbb{Z}$ and $y_1 \notin \mathbb{Z}$.

First suppose that $y_1 \in \mathbb{Z}$ so that $\lambda \leq y_1 - 1$. Since $0 < 2/q < 1$, the inequalities $y_1 - 1 < y_1 - 2/q < y_1$ hold. Hence, $y_1 - 1 = \lfloor y_1 - 2/q \rfloor = \lfloor y_2 \rfloor$, and so $\lambda \leq \lfloor y_2 \rfloor$.

Suppose instead that $y_1 \notin \mathbb{Z}$. We claim that $y_1 - 1/q$ is also not an integer. Observe that

$$y_1 - \frac{1}{q} = \frac{p(q - \beta) - q}{q} = p - 1 - \frac{p\beta}{q}.$$

Since both p and β are relatively prime to q , the fractional term $\frac{p\beta}{q}$ and, hence, $y_1 - 1/q$ are not integers. This implies that $y_1 > \lfloor y_1 - 1/q \rfloor = \lfloor y_1 - 2/q \rfloor = \lfloor y_2 \rfloor$. Combining this with the requirement that λ is an integer less than y_1 yields the desired result of $\lambda \leq \lfloor y_2 \rfloor$. $\square$

We will now give a complete description of the action of σ_q on the endomorphism α . We will do this by studying the action on an arbitrary diagonal block entry of the matrix. Using the action described in Equation (3.1), we see that

$$\sigma_q \alpha[i] = Z^{q(a_i+1)-p d b_i}.$$

A particularly nice property of this action is that $\sigma_q \alpha[i]$ is either equal to or is the conjugate of some block diagonal entry of the matrix α (we denote the conjugate of $\alpha[j]$ by $\overline{\alpha[j]}$).

Proposition 3.5. *Let d be a generator of the cyclic group $\mathbb{Z}/q\mathbb{Z}^\times$ and let $t_i = \langle db_i \rangle_q$. Define the quantities $\iota_1 = \kappa_{t_i-1} + a_i + 1$ and $\iota_2 = \kappa_{t'_i-1} + p - (a_i + 1)$, where $t'_i = q - t_i$. Then $\sigma_q \alpha$ is the diagonal matrix whose i^{th} diagonal 2×2 block is*

$$\sigma_q \alpha[i] = \begin{cases} \alpha[\iota_1] & \text{if } 0 \leq a_i \leq k_{t_i}, \\ \overline{\alpha[\iota_2]} & \text{if } a_i > k_{t_i}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First suppose that a_i satisfies $0 \leq a_i \leq k_{t_i}$. Then t_i and a_i together satisfy the bounds of Equations (3.4) and (3.5). Hence, $\sigma_q \alpha[i] = Z^{q(a_i+1)-p t_i} = \alpha[\iota]$, for some ι . Comparing this to the definition of κ and doing a bit of arithmetic shows that $\iota = \iota_1$.

Suppose instead that a_i satisfies

$$a_i \geq k_{t_i} + 1 > \frac{p t_i - q - 1}{q}.$$

Note that this includes the case where $k_{t_i} < 0$. Then t_i and a_i do not satisfy the bounds of Equations (3.4) and (3.5). Let $a'_i = p - a_i - 2$ and $t'_i = q - t_i$. Then

$$Z^{q(a_i+1)-p t_i} = \overline{Z^{q(a'_i+1)-p t'_i}}.$$

The bounds on t_i imply that t'_i satisfies $1 \leq t'_i \leq q-1$ and the bounds on a_i imply

$$\begin{aligned} a'_i &< p - \frac{pt_i - q - 1}{q} - 2 \\ &= \frac{p(q - t_i) - q + 1}{q} \\ &= \frac{pt'_i - q + 1}{q}. \end{aligned}$$

By Lemma 3.4, we can conclude that $a'_i \leq \lfloor (pt'_i - q - 1)/q \rfloor = k_{t'_i}$. Thus, a'_i and t'_i together satisfy the bounds of Inequalities (3.4) and (3.5). Hence, $Z^{q(a'_i+1)-pt'_i}$ appears as a block entry of α and

$$\sigma_q \alpha[i] = \overline{Z^{q(a'_i+1)-pt'_i}} = \overline{\alpha[\iota]}$$

for some ι . Comparing this to the definition of κ and working out a bit of arithmetic shows that $\iota = \iota_2$. $\square$

We can use a similar strategy to describe of the action of σ_p on the endomorphism α . Using the action described in Equation (3.1), we see that

$$\sigma_p \alpha[i] = Z^{qc(a_i+1)-pb_i}.$$

This leads to the following proposition.

Proposition 3.6. *Let c be a generator of the cyclic group $\mathbb{Z}/p\mathbb{Z}^\times$ and let $s_i = \langle c(a_i + 1) \rangle_p - 1$. Let $\iota_1 = \kappa_{b_i-1} + s_i + 1$ and $\iota_2 = \kappa_{b'_i-1} + p - (s_i + 1)$, where $b'_i = q - b_i$. Then $\sigma_q \alpha$ is the diagonal matrix whose i^{th} diagonal 2×2 block is*

$$\sigma_p \alpha[i] = \begin{cases} \alpha[\iota_1] & \text{if } 0 \leq s_i \leq k_{b_i}, \\ \overline{\alpha[\iota_2]} & \text{if } s_i > k_{b_i}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The bounds for s_i are $0 \leq s_i < p-1$, and $k_{b_i} \geq 0$ since it is associated to a pair a_i, b_i that appear in an entry of the endomorphism α . We follow the method of proof for Proposition 3.5 and split into two cases.

First suppose that s_i satisfies $0 \leq s_i \leq k_{b_i}$. Then b_i and s_i together satisfy the bounds of Equations (3.4) and (3.5). Hence, $\sigma_p \alpha[i] = Z^{q(s_i+1)-pb_i} = \alpha[\iota]$, for $\iota = \iota_1$.

Suppose instead that s_i satisfies

$$s_i \geq k_{b_i} + 1 > \frac{pb_i - q - 1}{q}.$$

Let $s'_i = p - s_i - 2$ and $b'_i = q - b_i$. Then $Z^{q(s_i+1)-pb_i} = \overline{Z^{q(s'_i+1)-pb'_i}}$. The bounds on s_i imply that

$$\begin{aligned} s'_i &< p - \frac{pb_i - q - 1}{q} - 2 \\ &= \frac{p(q - b_i) - q + 1}{q} \\ &= \frac{pb'_i - q + 1}{q}. \end{aligned}$$

By Lemma 3.4, this proves that $s'_i \leq \lfloor (pb'_i - q - 1)/q \rfloor = k_{b'_i}$. Thus, b'_i and s'_i together satisfy the bounds of Equations (3.4) and (3.5). Hence, $Z^{q(s'_i+1)-pb'_i}$ appears as a block entry of α and

$$\sigma_q \alpha[i] = \overline{Z^{q(s'_i+1)-pb'_i}}$$

which is the conjugate of the block $\alpha[\iota]$, for $\iota = \kappa_{b'_i-1} + s'_i + 1 = \kappa_{b'_i-1} + p - s_i - 1 = \iota_2$. $\square$

Example 3.7. We return to the curve $C_{7,3}$ from Example 3.3. The action of σ_q (using $d = 2$) on α yields the diagonal matrix

$$\sigma_q \alpha = \text{diag}(Z^{q-2p}, Z^{2q-2p}, Z^{q-p}, Z^{2q-p}, \overline{Z^{4q-2p}}, \overline{Z^{3q-2p}}).$$

The action of σ_p (using $c = 3$) on α yields

$$\sigma_p \alpha = \text{diag}(\overline{Z^{4q-2p}}, \overline{Z^{q-2p}}, Z^{3q-2p}, \overline{Z^{q-p}}, Z^{2q-2p}, \overline{Z^{2q-p}}).$$

4. The Sato–Tate Group of $\text{Jac}(C_{p,q})$

The main goal of this section is to compute the Sato–Tate groups of Catalan Jacobians. Since the algebraic Sato–Tate conjecture for Catalan Jacobians is explained by endomorphisms, the component group of the Sato–Tate group is isomorphic to the Galois group $\text{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$. This immediately tells us that the component group is a product of cyclic groups of orders $p - 1$ and $q - 1$. Still, we give explicit generators for the component group in Theorem 4.7 in order to obtain the limiting distribution of normalized local Euler factors.

We begin with a definition and a lemma that we need in order to define the component group.

4.1. Preliminaries.

Definition 4.1. A *signed permutation matrix* is a square matrix that has exactly one entry of 1 or -1 in each row and each column and 0s everywhere else. We will define a *block signed permutation matrix* to be an even dimension signed permutation matrix that is partitioned into 2×2 blocks that are either I , J , or the zero matrix.

For any matrix partitioned X into 2×2 blocks, we will let $X[i, j]$ be the block in the i^{th} row partition and j^{th} column partition.

The general strategy for writing down a matrix in the component group of the Sato–Tate group that is associated to a Galois element $\sigma \in \text{Gal}(K/\mathbb{Q})$ is described in the following lemma.

Lemma 4.2. *Let A be a diagonal matrix partitioned into 2×2 blocks and let B be a block signed permutation matrix. Then BAB^{-1} is a diagonal matrix. Furthermore, if $B[i, j] = I$ then $BAB^{-1}[i, i] = A[j, j]$ and if $B[i, j] = J$ then $BAB^{-1}[i, i] = -JA[j, j]J$.*

Proof. The proof requires little more than elementary linear algebra. The first statement, that BAB^{-1} is a diagonal matrix, comes from the fact that A is diagonal and B is a block signed permutation matrix.

Now note that the block entry $B^{-1}[j, i]$ is the inverse of the block $B[i, j]$. The i^{th} diagonal block entry of BAB^{-1} is the product

$$BAB^{-1}[i, i] = B[i, j] \cdot A[j, j] \cdot B^{-1}[j, i].$$

Thus, if $B[i, j] = I$ then the i^{th} entry of BAB^{-1} is $A[j, j]$. If, instead, $B[i, j] = J$ then $BAB^{-1}[i, i] = JA[j, j]J^{-1} = -JA[j, j]J$. $\square$

Remark 4.3. This lemma can be applied to more varieties than those we study in this paper. For example, this lemma could be used for the varieties studied in [10, 11, 24] and [17] (for certain values of c).

4.2. The identity component and the component group. We begin this subsection with a result about the identity component of the Sato–Tate group.

Proposition 4.4. *The identity component of the Sato-Group of $\text{Jac}(C_{p,q})$ is*

$$\text{ST}^0(\text{Jac}(C_{p,q})) \simeq \text{U}(1)^g,$$

where $g = (p-1)(q-1)/2$ is the genus of $C_{p,q}$.

Proof. Recall the definition of the algebraic Sato–Tate group in Conjecture 2.1. If we consider the same construction but restrict the domain of the ℓ -adic representation $\rho_{A,\ell}$ to $\text{Gal}(\mathbb{Q}/K)$, where K is the CM field of $\text{Jac}(C_{p,q})$, we obtain the identity component of $\text{AST}(\text{Jac}(C_{p,q}))$. The identity component of the Sato–Tate group of $\text{Jac}(C_{p,q})$ is a maximal compact subgroup of this.

This restricted map is exactly the map that appears in Theorem A of [4], and so we can apply that result to our situation. The theorem states that the image of the restricted map is contained in the group of diagonal matrices of the form

$$\{\text{diag}(x_1, y_1, \dots, x_g, y_g) \mid x_i, y_i \in \mathbb{Q}_\ell^\times, x_1 y_1 = \dots = x_g y_g = 1\}.$$

The Jacobian of $C_{p,q}$ is absolutely simple and nondegenerate (see Proposition 2.2), and so, as in [10, 11], we can go one step further and conclude that the containment is actually an equality. It follows that we can choose $\mathrm{ST}^0(\mathrm{Jac}(C_{p,q}))$ to be the maximal compact subgroup $\mathrm{U}(1)^g$. $\square$

We now define two matrices. We will then prove that they form a generating set for the component group of the Sato–Tate group. For the following definitions, let g be the genus of $C_{p,q}$.

Definition 4.5. Let d be a generator of the cyclic group $\mathbb{Z}/q\mathbb{Z}^\times$. For any integer i satisfying $1 \leq i \leq g$, let $t_i = \langle db_i \rangle_q$ and $r_i = i - \kappa_{b_i-1} - 1$, where b_i is the largest positive integer such that r_i is nonnegative. Define γ_q to be the $2g \times 2g$ block signed permutation matrix whose ij^{th} block is

$$\gamma_q[i, j] = \begin{cases} I & \text{if } j = \kappa_{t_i-1} + r_i + 1 \text{ and } 0 \leq r_i \leq k_{t_i}, \\ J & \text{if } j = \kappa_{t'_i-1} + p - (r_i + 1), \text{ and } r_i > k_{t_i}, \\ 0 & \text{otherwise,} \end{cases}$$

where $t'_i = q - t_i$.

Definition 4.6. Let c be a generator of the cyclic group $\mathbb{Z}/p\mathbb{Z}^\times$, r_i and b_i be as defined in Definition 4.5, and $s_i = \langle cr_i \rangle_p - 1$. Define γ_p to be the $2g \times 2g$ block signed permutation matrix whose ij^{th} block is

$$\gamma_p[i, j] = \begin{cases} I & \text{if } j = \kappa_{b_i-1} + s_i + 1 \text{ and } 0 \leq s_i \leq k_{b_i}, \\ J & \text{if } j = \kappa_{b'_i-1} + p - (s_i + 1) \text{ and } s_i > k_{b_i}, \\ 0 & \text{otherwise,} \end{cases}$$

where $b'_i = q - b_i$.

Theorem 4.7. *Let $q \neq p$ be odd primes and γ_q, γ_p be as defined in Definitions 4.5 and 4.6. The Sato–Tate group of the Jacobian of the genus g curve $C_{p,q}$ is*

$$\mathrm{ST}(\mathrm{Jac}(C_{p,q})) \simeq \langle \mathrm{Uu}(1)^g, \gamma_q, \gamma_p \rangle.$$

Proof. We proved in Proposition 4.4 that the identity component of the Sato–Tate group is $\mathrm{U}(1)^g$. We will now prove the claim regarding the component group.

It follows from Proposition 2.3 that we can use the twisted Lefschetz group of $\mathrm{Jac}(C_{p,q})$ to write down explicit generators of the component group. Choose generators c and d of $\mathbb{Z}/p\mathbb{Z}^\times$ and $\mathbb{Z}/q\mathbb{Z}^\times$, respectively. Propositions 3.5 and 3.6 show that the actions of the Galois elements simply rearrange and sometimes conjugate the diagonal entries of the endomorphism α . Since $-JJZ = \bar{Z}$, where Z is defined in Equation (1.3), we can apply Lemma 4.2 to determine the component group generators.

From here, we simply compare Definition 4.5 to Proposition 3.5 and Definition 4.6 to Proposition 3.6. For the former, $r_i = a_i$ and so the definition

of γ_q yields the correct rearranging and conjugating as determined by the action of σ_q . For the latter, we used the same notation and so it is clear that the definition of γ_p yields the rearranging and conjugating determined by the action of σ_p . Thus, γ_q and γ_p , when taken with the identity component, are generators of $\text{TL}(\text{Jac}(C_{p,q}))$. $\square$

The description of γ_q simplifies rather nicely in the case where $q = 3$, and so we present the following corollary.

Corollary 4.8. *Let $q = 3$, $p > 3$ be prime, and $m = \lfloor \frac{p-4}{3} \rfloor + 1$. Then the component group generator γ_q is*

$$\gamma_q = \left(\begin{array}{c|c|c} & I_{2m} & \\ \hline I_{2m} & & \\ \hline & & J_{g-2m} \end{array} \right),$$

where I_{2m} is the $2m \times 2m$ identity matrix and $J_{g-2m} = \text{antidiag}(\underbrace{J, J, \dots, J}_{g-2m})$.

Proof. If $q = 3$, then the genus is $g = p - 1$ and the values of b satisfying Equation (3.4) are $b_1 = 1$ and $b_2 = 2$. We choose $d = 2$ as the generator of $\mathbb{Z}/q\mathbb{Z}^\times$, which leads to $t_1 = 2$ and $t_2 = 1$. Furthermore, $k_1 = m - 1$, $\kappa_1 = m$, and $k_2 = \lfloor (2p - 4)/3 \rfloor$.

The values of i associated to b_1 are $1 \leq i \leq m$ (so that $r_i \geq 0$). For these values of i , $0 \leq r_i \leq$ is always satisfied. Hence, $\gamma_q[i, j] = I$ when

$$j = \kappa_1 + r_i + 1 = m + i.$$

This verifies that the I_{2m} in the top rows of γ_q in the statement of the corollary are correct.

The values of i associated to b_2 are then $m + 1 \leq i \leq g = p - 1$. The associated values are r_i are split into to intervals: $0 \leq r_i \leq m - 1$ and $r_i \geq m$. In the first interval we have $m + 1 \leq i \leq 2m$, which leads to $\gamma_q[i, j] = I$ when $j = i - m$. This verifies that the I_{2m} in the middle rows of γ_q in the statement of the corollary are correct.

In the second interval, $r_i \geq m$ and we need to determine which values of j will lead to $\gamma_q[i, j] = J$. Let $i = 2m + h$, where $1 \leq h \leq g - 2m$, so that $r_i = m + h - 1$. Then the value of j we need is

$$j = m + p - (m + h) = p - h = g - (h - 1).$$

Thus, the J blocks will start in row $i = 2m + 1$, column $j = g$, and will then cascade down and to the left. This verifies that the J_{g-2m} in the bottom rows of γ_q in the statement of the corollary are correct. $\square$

Remark 4.9. See the Appendix for examples of the component group generators.

5. Moment Statistics

In this section, we describe the distributions of the coefficients of the characteristic polynomial of random conjugacy classes in the Sato–Tate groups in Theorem 4.7. 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. The numerical moment statistics are an approximation since one can only ever compute them up to some prime. In Table 5.5, we give both numerical and Sato–Tate moments for some Catalan Jacobians.

5.1. Preliminaries. The background information in this section has been adapted from [10, Section 6].

We start by recalling some basic properties of moment statistics. We define the n^{th} moment (centered at 0) of a probability density function to be the expected value of the n th 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, [24]). This yields the following identity

$$M_n[X_1 + \cdots + X_m] = \sum_{\beta_1 + \cdots + \beta_m = n} \binom{n}{\beta_1, \dots, \beta_m} M_{\beta_1}[X_1] \cdots M_{\beta_m}[X_m].$$

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

We start with the unitary group $U(1)$ and consider the trace map on $U \in U(1)$ defined by $z := \text{tr}(U) = u + \bar{u}$. This trace map takes values in $[-2, 2]$. From here we see that

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

gives a uniform measure of $U(1)$ (see [32, Section 2]). We can deduce the following pushforward measure

$$\mu_{U(1)^n} = \prod_{i=1}^n \frac{1}{\pi} \frac{dz_i}{\sqrt{4 - z_i^2}}.$$

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, $\mu(\phi_n)$, where ϕ_n is the function $z \mapsto z^n$. This yields $M_n[\mu_{U(1)}] = \binom{n}{n/2}$, where $\binom{n}{n/2} = 0$ if n is odd. Hence, $M[\mu_{U(1)}] = (1, 0, 2, 0, 6, 0, 20, 0, \dots)$. From here, we take binomial convolutions to obtain

$$(5.1) \quad M_n[\mu_{U(1)^g}] = \sum_{\beta_1 + \cdots + \beta_g = n} \binom{n}{\beta_1, \dots, \beta_g} M_{\beta_1}[\mu_{U(1)}] \cdots M_{\beta_g}[\mu_{U(1)}].$$

In what follows, for each $i \in \{1, 2, \dots, g\}$, 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.

5.2. Characteristic polynomials. In this subsection, we give results for the characteristic polynomials in each component of the Sato–Tate group. Let U be a random matrix in the identity component of $\text{ST}(\text{Jac}(C_{p,q}))$ and let $A_{m,n} = \gamma_p^m \gamma_q^n$ be a matrix in the component group of the Sato–Tate group. The characteristic polynomial of $U \cdot A_{m,n}$ is a degree $2g$ palindromic polynomial of the form

$$P_{m,n}(T) = T^{2g} + b_1 T^{2g-1} + b_2 T^{2g-2} + \dots + b_2 T^2 + b_1 T + 1.$$

We now present two propositions regarding the coefficients of the characteristic polynomials.

Proposition 5.1. *Only matrices in the identity component $\text{ST}^0(\text{Jac}(C_{p,q}))$ have a characteristic polynomial with nonzero b_1 -coefficient.*

Proof. The b_1 -coefficient of the characteristic polynomial of $P_{m,n}$ is the trace of the matrix product $U \cdot A_{m,n}$. We will show that this trace is nonzero if and only if $m \equiv 0 \pmod{p-1}$ and $n \equiv 0 \pmod{q-1}$.

To do this it is sufficient to show that $A_{m,n}$ has no nonzero diagonal entries. If $A_{m,n}$ has a nonzero diagonal entry then, for some j , the j^{th} diagonal block entry of $A_{m,n}$ is I and α satisfies

$$(5.2) \quad (\sigma_p)^m \circ (\sigma_q)^n \alpha[j] = \alpha[j].$$

To determine if and when this is possible, we consider the action of the corresponding Galois element $(\sigma_p)^m \circ (\sigma_q)^n$. Let $\alpha[j] = Z^{q(a+1)-pb}$. Equation (5.2) holds if and only if the following is true:

$$\zeta_{pq}^{q(a+1)-pb} = (\sigma_p)^m \circ (\sigma_q)^n \left(\zeta_{pq}^{q(a+1)-pb} \right) = \zeta_{pq}^{qc^m(a+1)-pd^nb}.$$

This equality implies that

$$\zeta_p^{(a+1)} \bar{\zeta}_q^b = \zeta_p^{c^m(a+1)} \bar{\zeta}_q^{d^nb}.$$

Since p and q are relatively prime, we can conclude from here that

$$\zeta_p^{(a+1)} = \zeta_p^{c^m(a+1)} = (\sigma_p)^m \zeta_p^{(a+1)} \quad \text{and} \quad \bar{\zeta}_q^b = \bar{\zeta}_q^{d^nb} = (\sigma_q)^n \bar{\zeta}_q^b.$$

Since σ_p and σ_q are generators of $\text{Gal}(K/\mathbb{Q})$ and have orders $p-1$ and $q-1$, respectively, the above equalities hold if and only if $m \equiv 0 \pmod{p-1}$ and $n \equiv 0 \pmod{q-1}$. $\square$

One benefit of this result is that, in order to compute the μ_1 -moment statistics of the Sato–Tate group, we need only compute moments for a random matrix U in the identity component of $\text{ST}(\text{Jac}(C_{p,q}))$. To average

over the components we simply divide this value by the size of the Galois group.

Proposition 5.2. *Let $m = (p-1)/2$ and $n = (q-1)/2$. Then the characteristic polynomial of $U \cdot A_{m,n}$ in the Sato–Tate group is*

$$P_{m,n}(T) = (T^2 + 1)^g$$

for any U in the identity component.

Proof. We will show that the matrix $A_{m,n}$ for these values of m and n has J or $-J$ as each of its g diagonal blocks. Since the characteristic polynomial of $\pm J$ is $T^2 + 1$, this will yield the desired result.

The actions and orders of the Galois elements σ_p and σ_q tell us that $\sigma_p^m(\zeta_p) = \bar{\zeta}_p$ and $\sigma_q^n(\zeta_q) = \bar{\zeta}_q$. Thus,

$$\begin{aligned} \sigma_p^m \circ \sigma_q^n(\zeta_{pq}^{q(a+1)-pb}) &= \sigma_p^m \circ \sigma_q^n(\zeta_p^{(a+1)} \bar{\zeta}_q^b) \\ &= \bar{\zeta}_p^{(a+1)} \zeta_q^b \\ &= \overline{\zeta_{pq}^{q(a+1)-pb}}. \end{aligned}$$

Thus, every diagonal entry of α satisfies

$$\sigma_p^m \circ \sigma_q^n \alpha[j] = \overline{\alpha[j]},$$

which means that the block diagonal entries of the corresponding matrix are all either J or $-J$. $\square$

Example 5.3. We determine moment statistics for the genus 4 curve $C_{5,3} : y^3 = x^5 - 1$ over each subfield of the CM field $K = \mathbb{Q}(\zeta_{15})$. Using characteristic polynomials, we can compute the n th moments for each μ_i , $1 \leq i \leq 4$. There is a table corresponding to each of the four subfields: $\mathbb{Q}$ (Table 5.1), $\mathbb{Q}(\zeta_3)$ (Table 5.2), $\mathbb{Q}(\zeta_5)$ (Table 5.3), and $\mathbb{Q}(\zeta_{15})$ (Table 5.4). These moments were computed using Sage [28].

TABLE 5.1. Moment Statistics for $y^3 = x^5 - 1$ over $\mathbb{Q}$.

$M[\mu_1]$	(1, 0, 1, 0, 21, 0, 640, 0, 23765, ...)
$M[\mu_2]$	(1, 1, 8, 76, 1168, 20956, 414284, 8643328, 187416464, ...)
$M[\mu_3]$	(1, 0, 13, 0, 11745, 0, 17177080, 0, 31036079585, ...)
$M[\mu_4]$	(1, 2, 27, 476, 18391, 689812, 34599990, 1677458008, 91894386279, ...)

TABLE 5.2. Moment Statistics for $y^3 = x^5 - 1$ over $\mathbb{Q}(\zeta_3)$.

$M[\mu_1]$	(1, 0, 2, 0, 42, 0, 1280, 0, 47530, ...)
$M[\mu_2]$	(1, 1, 11, 136, 2263, 41656, 827444, 17282560, 374815319, ...)
$M[\mu_3]$	(1, 0, 26, 0, 23490, 0, 34354160, 0, 62072159170, ...)
$M[\mu_4]$	(1, 2, 42, 890, 36418, 1377502, 69187410, 3354841408, 183788328258, ...)

TABLE 5.3. Moment Statistics for $y^3 = x^5 - 1$ over $\mathbb{Q}(\zeta_5)$.

$M[\mu_1]$	(1, 0, 4, 0, 84, 0, 2560, 0, 95060, ...)
$M[\mu_2]$	(1, 2, 22, 272, 4526, 83312, 1654888, 34565120, 749630638, ...)
$M[\mu_3]$	(1, 0, 52, 0, 46980, 0, 68708320, 0, 124144318340, ...)
$M[\mu_4]$	(1, 4, 82, 1780, 72830, 2755004, 138374800, 6709682816, 367576656446, ...)

TABLE 5.4. Moment Statistics for $y^3 = x^5 - 1$ over $\mathbb{Q}(\zeta_{15})$.

$M[\mu_1]$	(1, 0, 8, 0, 168, 0, 5120, 0, 190120, ...)
$M[\mu_2]$	(1, 4, 40, 544, 9016, 166624, 3309376, 69130240, 1499256376, ...)
$M[\mu_3]$	(1, 0, 104, 0, 93960, 0, 137416640, 0, 248288636680, ...)
$M[\mu_4]$	(1, 6, 156, 3528, 145512, 5509296, 276746016, 13419347136, 735153215448, ...)

5.3. Tables of μ_1 - and α_1 -moment statistics. Table 5.5 gives both $M[\mu_1]$ and the numerical moments of the normalized L -polynomial of some Catalan Jacobians (over $\mathbb{Q}$). The numerical moments were computed for primes up to 2^N , where N is given in the last column of the table, using an algorithm described in [19] and [20]. As the genus grows, the computations require more processing power, and so a smaller bound N was used. This leads to less accurate estimates for the numerical moments in higher genus, which make it more difficult to compare them to the theoretical moments obtained from the Sato–Tate groups.

In Proposition 5.1 we proved that only matrices in the identity component have characteristic polynomials with nonzero b_1 -coefficient. Let $M_n^{[0]\mu_1}$ denote the n^{th} moment of the identity component. As noted in the proof of Proposition 5.1, the b_1 -coefficient of the characteristic polynomial is the trace of a random matrix $U \in \text{U}(1)^g$. Thus, $M_n^{[0]\mu_1} = M_n[\mu_{\text{U}(1)^g}]$ and we can use the formula in Equation (5.1). To compute $M_n[\mu_1]$, we average over the components by dividing $M_n[\mu_{\text{U}(1)^g}]$ by the size of the Galois group.

TABLE 5.5. Table of some μ_1 - and a_1 -moments $\text{Jac}(C_{p,q})$ over $\mathbb{Q}$.

(p, q)	g		M_2	M_4	M_6	M_8	N
(5,3)	4	μ_1	1	21	640	23765	23
		a_1	0.994	20.726	625.606	22961.668	
(7,3)	6	μ_1	1	33	1660	106785	23
		a_1	0.998	32.718	1628.656	103534.931	
(11,3)	10	μ_1	1	57	5140	615545	19
		a_1	0.972	55.306	4836.457	532489.325	
(13,3)	12	μ_1	1	69	7600	1121925	19
		a_1	0.998	68.164	7570.201	1178539.197	
(7,5)	12	μ_1	1	69	7600	1121925	19
		a_1	0.998	68.164	7570.201	1178539.197	
(17,3)	16	μ_1	1	93	13960	2840285	18
		a_1	0.954	91.335	15348.411	3864179.550	

Note that $M_2[\mu_1]$ equals 1 for each example in Table 5.5. We prove that this is true for every Catalan Jacobian in Proposition 5.5.

Remark 5.4. In many cases, the μ_1 -moments of Catalan Jacobians match those of the Fermat quotients considered in [11]. This occurs when the genera are the same and the identity components are the same (some of the identity components in [11] are of the form $(\text{U}(1)_{g/3})^3$), where

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

These Jacobian varieties have a similar property to ours: only the identity components of the Sato–Tate groups contribute to the b_1 -coefficients of the characteristic polynomials. However we expect to see a difference in the moments of the higher traces.

For example, consider the two genus 6 curves $y^3 = x^7 - 1$ (Catalan curve) and $v^{13} = u(u+1)^{10}$ (a curve from [11]) over $\mathbb{Q}$. Both of their associated Sato–Tate groups have identity component $\text{U}(1)^6$, but their component groups are different. We can see this difference in the μ_2 -moments:

$$\begin{aligned} y^3 = x^7 - 1: \quad M[\mu_2] &= (1, 1, 12, 206, 5796, \dots), \\ v^{13} = u(u+1)^{10}: \quad M[\mu_2] &= (1, 1, 11, 206, 5781, \dots). \end{aligned}$$

5.4. General results for moment statistics.

Proposition 5.5. *Over $\mathbb{Q}$, the second moment $M_2[\mu_1]$ equals 1 for every Catalan Jacobian. Over $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_q)$, and $\mathbb{Q}(\zeta_{pq})$, the moment $M_2[\mu_1]$ is $p-1$, $q-1$, and $(p-1)(q-1)$, respectively.*

Proof. In Proposition 5.1 we proved that only the identity component contributes to the b_1 -coefficient of the characteristic polynomial. We will demonstrate that the value obtained for the second moment $M_2[\mu_1]$ is $(p-1)(q-1)$, so that when averaging over all components we obtain the desired results.

This amounts to computing the sum in Equation (5.1) when $n = 2$. In this situation, we are summing over β_i values that add to 2. There are two types of summands to consider: ones where there are only two nonzero values $\beta_i = \beta_j = 1$ for some $i \neq j$ and ones where there is only one nonzero value $\beta_i = 2$ for some i .

The first type does not contribute to the sum because $M_1[\mu_{U(1)}] = 0$ and, hence the entire term equals 0. On the other hand, each term of the second type will simplify to

$$\binom{2}{2, 0, \dots, 0} M_2[\mu_{U(1)}] M_0[\mu_{U(1)}] \cdots M_0[\mu_{U(1)}] = 2$$

since $M_0[\mu_{U(1)}] = 1$ and $M_2[\mu_{U(1)}] = 2$. There are exactly g terms of this form since this is essentially counting the number of g -tuples with a single nonzero entry. Hence, $M_n[\mu_1] = 2g = (p-1)(q-1)$.

We now consider the size of the component group for each of the subfields of $\mathbb{Q}(\zeta_{pq})$. Over $\mathbb{Q}$, the component group has size $(p-1)(q-1)$. Over $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_q)$, $\mathbb{Q}(\zeta_{pq})$, the sizes are $q-1$, $p-1$, and 1, respectively. Averaging $M_n[\mu_1]$ over these values yields the desired results. $\square$

6. Galois Endomorphism Types and Related Results

In this section, we study the Galois endomorphism types of Catalan Jacobians. There is a nice correspondence between the Sato–Tate group and the real endomorphism algebra for abelian varieties of dimension $g \leq 3$ (see [12, Theorem 1.4]). This may not always extend to higher dimension, but it does for Catalan Jacobians and other nondegenerate abelian varieties. We approach this problem in two ways: through data obtained from moment statistics and by working with Rosati forms. The latter is the more traditional method of determining real endomorphism algebras, whereas the former is a new technique that uses recent results of Costa, Fité, and Sutherland [9].

We begin this section with some notation and terminology. Let A/F be an abelian variety defined over a number field F , and let K be the endomorphism field of A . We will denote the real endomorphism algebra of A by $\text{End}(A_F)_{\mathbb{R}} := \text{End}(A_F) \otimes_{\mathbb{Z}} \mathbb{R}$. Let $\mathbb{H}$ denote the quaternions and let $M_n(R)$ denote the $n \times n$ matrix ring over a ring R . Wedderburn’s structure

theorem tells us that the $\mathbb{R}$ -algebra $\text{End}(A_F)_{\mathbb{R}}$ satisfies

$$(6.1) \quad \text{End}(A_F)_{\mathbb{R}} \simeq \prod_i M_{t_i}(\mathbb{R}) \times \prod_i M_{n_i}(\mathbb{H}) \times \prod_i M_{p_i}(\mathbb{C}),$$

for some nonnegative integers t_i, n_i, p_i .

Let $\mathcal{C}$ be the category of pairs (G, E) , where G is a finite group and E is an $\mathbb{R}$ -algebra equipped with an $\mathbb{R}$ -linear action of G . The *Galois endomorphism type* of A/F is the isomorphism class in $\mathcal{C}$ of the pair $[\text{Gal}(K/F), \text{End}(A_F)_{\mathbb{R}}]$ [12, Definition 1.3]. If $L \subseteq K$ is an intermediate field corresponding to a subgroup $N \subseteq \text{Gal}(K/F)$, then $\text{End}(A_L)_{\mathbb{R}} \simeq (\text{End}(A_K)_{\mathbb{R}})^N$ (see, for example, [17, Section 6]). In this section, we will prove the following result for the Galois endomorphism types of Catalan Jacobians.

Theorem 6.1. *Let $K = \mathbb{Q}(\zeta_{pq})$ and let L be any intermediate field $\mathbb{Q} \subseteq L \subseteq K$. Then*

$$\text{End}(\text{Jac}(C_{p,q})_L)_{\mathbb{R}} = \begin{cases} \mathbb{R}^{[L:\mathbb{Q}]} & \text{if } L \subseteq \mathbb{R}, \\ \mathbb{C}^{[L:\mathbb{Q}]/2} & \text{otherwise.} \end{cases}$$

Additionally, we will prove the following result regarding the Néron–Severi group $\text{NS}(\text{Jac}(C_{p,q})_L)$ of the Catalan Jacobian.

Theorem 6.2. *For any intermediate field $\mathbb{Q} \subseteq L \subseteq K$, the rational Néron–Severi group of the Catalan Jacobian is $\text{NS}(\text{Jac}(C_{p,q})_L)_{\mathbb{Q}} \simeq \mathbb{Q}^r$, where*

$$r = \begin{cases} [L:\mathbb{Q}] & \text{if } L \subseteq \mathbb{R}, \\ \frac{1}{2}[L:\mathbb{Q}] & \text{otherwise.} \end{cases}$$

We will prove these results using data obtained from moment statistics and using Rosati forms.

6.1. Data obtained from moment statistics. We start with some notation. The Sato–Tate group of $\text{Jac}(C_{p,q})$ is equipped with a faithful, self-dual representation $\rho: \text{ST}(\text{Jac}(C_{p,q})) \rightarrow \text{GL}(V)$, where V is a $2g$ -dimensional $\mathbb{C}$ -vector space. We can use this representation to view $\text{ST}(\text{Jac}(C_{p,q}))$ as a compact real Lie subgroup of $\text{USp}(2g)$. From here, we define the following virtual characters of the Sato–Tate group of $\text{Jac}(C_{p,q})$:

$$a_1 = \text{Tr}(V), \quad a_2 = \text{Tr}(\wedge^2 V), \quad s_2 = a_1^2 - a_2,$$

where $\wedge^k V$ denotes the k^{th} -exterior power of V . We will be interested in certain moments of these characters: $M_2[a_1]$, $M_1[a_2]$, and $M_1[s_2]$. These moments satisfy the following equations

$$(6.2) \quad M_2[a_1] = M_2[\mu_1], \quad M_1[a_2] = M_1[\mu_2], \quad M_1[s_2] = M_2[a_1] - 2M_1[a_2],$$

where μ_1 and μ_2 are the measures defined in Section 5.1.

The moment $M_1[s_2]$ can be interpreted as a Frobenius–Schur indicator of the standard representation of $\text{ST}(A)$ (see the exposition in Remark 5

of [9] for more details). For an irreducible representation, this value can only be $-1, 0$, or 1 (see [29, Proposition 39]).

We can use the results of [9] to obtain further identities for these moments. Proposition 1 of [9] states that, for any abelian variety A defined over a field k ,

$$M_2[a_1] = \mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A_k)).$$

Proposition 6.3. *The real endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C_{p,q})_{\mathbb{Q}})_{\mathbb{R}}$ for any Catalan Jacobian is $\mathbb{R}$.*

Proof. We proved in Proposition 5.5 that $M_2[\mu_1] = 1$. This implies that $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(\mathrm{Jac}(C_{p,q})_{\mathbb{Q}})) = 1$, and the only possibility for $\mathrm{End}(\mathrm{Jac}(C_{p,q})_{\mathbb{Q}})_{\mathbb{R}}$ is $\mathbb{R}$. $\square$

Corollary 6.4. *The rank of the Néron–Severi group of $\mathrm{Jac}(C_{p,q})_{\mathbb{Q}}$ is 1.*

Proof. This follows from Proposition 6.3 and the fact that the Néron–Severi group of a principally polarized abelian variety A embeds into $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Alternatively, we can use Lemma 3 of [9] to prove the result. Applying this lemma to our situation yields the following equation:

$$1 - 2 \cdot \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(\mathrm{Jac}(C_{p,q})_{\mathbb{Q}})) = -1.$$

Hence, $\mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(\mathrm{Jac}(C_{p,q})_{\mathbb{Q}})) = 1$. $\square$

Proposition 2 of [9] gives an additional identity for the rank of $\mathrm{NS}(A_F)$:

$$M_1[a_2] = \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A_F)).$$

Thus, we obtain the following corollary.

Corollary 6.5. *For the Catalan Jacobian $\mathrm{Jac}(C_{p,q})_{\mathbb{Q}}$, we have*

$$M_1[a_2] = 1.$$

Corollary 6.6. *Over $\mathbb{Q}$, the moment $M_1[s_2]$ equals -1 for every Catalan Jacobian. Over $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_q)$, and $\mathbb{Q}(\zeta_{pq})$, the moment is $M_1[s_2] = 0$.*

Proof. Over $\mathbb{Q}$, we have already proved that $M_2[a_1] = 1$ and $M_1[a_2] = 1$ in Proposition 5.5 and Corollary 6.5. Thus, $M_1[s_2] = 1 - 2 = -1$ as desired. $\square$

In some cases, we can use the results of [9] to uniquely determine the real endomorphism algebras and ranks of Néron–Severi groups. For example, this seems to be possible in dimension 2 and 3 (see the tables of moment statistics in [12, 13]). However, this is not the case for higher genus Catalan Jacobians. In order to further classify real endomorphism algebras, we will use Rosati forms.

6.2. Further information from Rosati forms. Every polarization on an abelian variety induces an anti-involution, called the Rosati involution (see [7, Chapter 5]). Theorem 5.5.6 of [7], combined with the fact that Catalan Jacobians are Type IV in the Albert’s classification of abelian varieties, tells us that the Rosati involution on $\text{End}(\text{Jac}(C_{p,q})_K)_\mathbb{Q}$ corresponds to complex conjugation on $\mathbb{Z}[\zeta_{pq}]$. We now complete the proofs of Theorems 6.1 and 6.2.

Proof of Theorem 6.2. For any intermediate field $\mathbb{Q} \subset L \subseteq K$, the symmetric elements of $\text{End}(\text{Jac}(C_{p,q})_L)_\mathbb{Q}$ (i.e., those fixed by the Rosati involution) correspond to the elements of L fixed by complex conjugation. Proposition 5.2.1 of [7] gives an isomorphism between the set of symmetric elements and the rational Néron–Severi group of an abelian variety. Applying this to our situation yields the desired result. $\square$

Proof of Theorem 6.1. Either the intermediate field L is totally real or it is not. When the field L is totally real, the Rosati involution is trivial on $\text{End}(\text{Jac}(C_{p,q})_L) \simeq \mathcal{O}_L$ since it acts as complex conjugation. Hence, $\text{End}(\text{Jac}(C_{p,q})_L)_\mathbb{R}$ equals $\mathbb{R}^{[L:\mathbb{Q}]}$.

Otherwise, by Theorem 5.5.6 of [7], the rational endomorphism algebra of $\text{Jac}(C_{p,q})_L$ admits a positive anti-involution of the second kind (the Rosati involution). The center of $\text{End}(\text{Jac}(C_{p,q})_L)_\mathbb{Q}$ is a totally complex quadratic extension of a totally real field. In fact, in our setting, the center equals $\text{End}(\text{Jac}(C_{p,q})_L)_\mathbb{Q}$. Thus, by Proposition 5.5.7 of [7], the real endomorphism algebra $\text{End}(\text{Jac}(C_{p,q})_L)_\mathbb{R}$ equals $\mathbb{C}^{[L:\mathbb{Q}]/2}$. $\square$

Corollary 6.7. *The real endomorphism algebra $\text{End}(\text{Jac}(C_{p,q})_K)_\mathbb{R}$ is $\mathbb{C}^g$.*

Remark 6.8. This result follows from Theorem 6.1, but it can also be proved by through computations with Rosati forms. Since $\text{Jac}(C_{p,q})/K$ is nondegenerate, its complex endomorphism algebra is the subspace of $M_{2g}(\mathbb{C})$ fixed by the action of the identity component of the Sato–Tate group, and the real endomorphism algebra $\text{End}(\text{Jac}(C_{p,q})_K)_\mathbb{R}$ is the subspace of half the dimension for which the Rosati form is positive definite (see [12, Definition 2.18]).

Corollary 6.9. *For any intermediate field $L \subseteq K$, the Frobenius–Schur indicator is*

$$M_1[s_2] = \begin{cases} -[L : \mathbb{Q}] & \text{if } L \text{ is totally real,} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Recall from Equation (6.2) that $M_1[s_2] = M_2[a_1] - 2M_1[a_2]$. Propositions 1 and 2 of [9] show that $M_2[a_1] = \text{rk}_\mathbb{Z}(\text{End}(\text{Jac}(C_{p,q})_L))$ and $M_1[a_2] = \text{rk}_\mathbb{Z}(\text{NS}(\text{Jac}(C_{p,q})_L))$. The results of Theorem 6.1 tell us that the rank of the endomorphism ring is $[L : \mathbb{Q}]$ for any intermediate field L . Combining

this with the value of the rank of the Néron–Severi group from Theorem 6.2 yields the result. $\square$

Acknowledgements. Thank you to the anonymous reviewer for their helpful comments on an earlier draft of this article. Many thanks to Edgar Costa, Francesc Fité, and Drew Sutherland while working on Section 6.1, and to Mckenzie West for patiently answering my Sage and GitHub questions while I was working on Table 5.5. I would like to thank Drew Sutherland for sharing access to a server at MIT while I was computing the numerical moments given in Table 5.5. Merci à Christelle Vincent pour son aide avec le résumé.

I am grateful for the support and encouragement of Matt Montesano, Alanna Hoyer-Letizel, and the Rethinking Number Theory Workshop co-organizers, project leaders, and participants. They provided a sense of community during a difficult time, and it would not have been possible to write this article during a pandemic without them.

Appendix A. Examples of the component group generators

In Table A.1 we give examples of the matrices γ_q and γ_p from Definitions 4.5 and 4.6. These were computed in Sage [28] using Sage’s chosen generators for $(\mathbb{Z}/q\mathbb{Z})^\times$ and $(\mathbb{Z}/p\mathbb{Z})^\times$.

TABLE A.1. Examples of γ_p and γ_q matrices for $y^q = x^p - 1$.

(p, q)	γ_p	γ_q
$(5, 3)$	$\begin{pmatrix} 0 & 0 & 0 & J \\ 0 & 0 & I & 0 \\ J & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & J \\ 0 & 0 & J & 0 \end{pmatrix}$
$(7, 3)$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & J \\ 0 & 0 & J & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 \\ J & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 \\ 0 & J & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & J \\ 0 & 0 & 0 & 0 & J & 0 \end{pmatrix}$

References

- [1] N. AOKI, “Hodge cycles on CM abelian varieties of Fermat type”, *Comment. Math. Univ. St. Pauli* **51** (2002), no. 1, p. 99-130.
- [2] ———, “The Hodge conjecture for the Jacobian varieties of generalized Catalan curves”, *Tokyo J. Math.* **27** (2004), no. 2, p. 313-335.
- [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** (2018), no. 3-4, p. 991-1022.

- [4] G. BANASZAK, W. GAJDA & P. KRASOŃ, “On Galois representations for abelian varieties with complex and real multiplications”, *J. Number Theory* **100** (2003), no. 1, p. 117-132.
- [5] G. BANASZAK & K. S. KEDLAYA, “An algebraic Sato–Tate group and Sato–Tate conjecture”, *Indiana Univ. Math. J.* **64** (2015), no. 1, p. 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** (2011), no. 1, p. 29-98.
- [7] C. BIRKENHAKE & H. LANGE, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften, vol. 302, Springer, 1992, viii+435 pages.
- [8] L. CLOZEL, M. HARRIS & R. TAYLOR, “Automorphy for some l -adic lifts of automorphic mod l Galois representations”, *Publ. Math., Inst. Hautes Étud. Sci.* (2008), no. 108, p. 1-181, with Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.
- [9] E. COSTA, F. FITÉ & A. V. SUTHERLAND, “Arithmetic invariants from Sato–Tate moments”, *C. R. Math. Acad. Sci. Paris* **357** (2019), no. 11-12, p. 823-826.
- [10] M. EMORY & H. GOODSON, “Sato–Tate distributions of $y^2 = x^p - 1$ and $y^2 = x^{2p} - 1$ ”, *J. Algebra* **597** (2022), p. 241-265.
- [11] F. FITÉ, J. GONZÁLEZ & J.-C. LARIO, “Frobenius distribution for quotients of Fermat curves of prime exponent”, *Can. J. Math.* **68** (2016), no. 2, p. 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** (2012), no. 5, p. 1390-1442.
- [13] F. FITÉ, K. S. KEDLAYA & A. V. SUTHERLAND, “Sato–Tate groups of abelian threefolds”, <https://arxiv.org/abs/2106.13759>, 2021.
- [14] ———, “Sato–Tate groups of abelian threefolds: a preview of the classification”, in *Arithmetic, geometry, cryptography and coding theory*, Contemporary Mathematics, vol. 770, American Mathematical Society, 2021, p. 103-129.
- [15] F. FITÉ, E. LORENZO GARCÍA & A. V. SUTHERLAND, “Sato–Tate distributions of twists of the Fermat and the Klein quartics”, *Res. Math. Sci.* **5** (2018), no. 4, article no. 41 (40 pages).
- [16] 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** (2014), no. 3, p. 543-585.
- [17] ———, “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, vol. 663, American Mathematical Society, 2016, p. 103-126.
- [18] M. HARRIS, N. SHEPHERD-BARRON & R. TAYLOR, “A family of Calabi–Yau varieties and potential automorphy”, *Ann. Math.* **171** (2010), no. 2, p. 779-813.
- [19] D. HARVEY & A. V. SUTHERLAND, “Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time”, *LMS J. Comput. Math.* **17** (2014), p. 257-273.
- [20] ———, “Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II”, in *Frobenius distributions: Lang–Trotter and Sato–Tate conjectures*, Contemporary Mathematics, vol. 663, American Mathematical Society, 2016, p. 127-147.
- [21] F. HAZAMA, “Algebraic cycles on nonsimple abelian varieties”, *Duke Math. J.* **58** (1989), no. 1, p. 31-37.
- [22] ———, “Hodge cycles on the Jacobian variety of the Catalan curve”, *Compos. Math.* **107** (1997), no. 3, p. 339-353.
- [23] C. JOHANSSON, “On the Sato–Tate conjecture for non-generic abelian surfaces”, *Trans. Am. Math. Soc.* **369** (2017), no. 9, p. 6303-6325, with an appendix by Francesc Fité.
- [24] 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*, Contemporary Mathematics, vol. 701, American Mathematical Society, 2018, p. 151-165.
- [25] P. MIHĂILESCU, “Primary cyclotomic units and a proof of Catalan’s conjecture”, *J. Reine Angew. Math.* **572** (2004), p. 167-195.
- [26] V. K. MURTY, “Exceptional Hodge classes on certain abelian varieties”, *Math. Ann.* **268** (1984), no. 2, p. 197-206.
- [27] H. POHLMANN, “Algebraic cycles on abelian varieties of complex multiplication type”, *Ann. Math.* **88** (1968), p. 161-180.

- [28] I. SAGEMATH, *CoCalc Collaborative Computation Online*, 2020, <https://cocalc.com/>.
- [29] J.-P. SERRE, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer, 1977, translated from the second French edition by Leonard L. Scott, 170 pages.
- [30] ———, *Lectures on $N_X(p)$* , CRC Research Notes in Mathematics, vol. 11, CRC Press, 2012, x+163 pages.
- [31] T. SHIODA, “Algebraic cycles on abelian varieties of Fermat type”, *Math. Ann.* **258** (1981), no. 1, p. 65–80.
- [32] A. V. SUTHERLAND, “Sato–Tate distributions”, in *Analytic methods in arithmetic geometry*, Contemporary Mathematics, vol. 740, American Mathematical Society, 2019, p. 197–248.
- [33] R. TAYLOR, “Automorphy for some l -adic lifts of automorphic mod l Galois representations. II”, *Publ. Math., Inst. Hautes Étud. Sci.* (2008), no. 108, p. 183–239.

Heidi GOODSON

Department of Mathematics

Brooklyn College, City University of New York

2900 Bedford Avenue, Brooklyn, NY 11210 USA

E-mail: heidi.goodson@brooklyn.cuny.edu

URL: <https://sites.google.com/site/heidigoodson/>