THE TWISTING SATO-TATE GROUP OF THE CURVE $y^2 = x^8 - 14x^4 + 1$

SONNY ARORA, VICTORIA CANTORAL-FARFÁN, AARON LANDESMAN, DAVIDE LOMBARDO, AND JACKSON S. MORROW

ABSTRACT. We determine the twisting Sato-Tate group of the genus 3 hyperelliptic curve $y^2 = x^8 - 14x^4 + 1$ and show that all possible subgroups of the twisting Sato-Tate group arise as the Sato-Tate group of an explicit twist of $y^2 = x^8 - 14x^4 + 1$. Furthermore, we prove the generalized Sato-Tate conjecture for the Jacobians of all $\mathbb{Q}$-twists of the curve $y^2 = x^8 - 14x^4 + 1$.

1. INTRODUCTION

In this paper, we prove the generalized Sato-Tate conjecture for all $\mathbb{Q}$-twists of the genus 3 hyperelliptic curve $y^2 = x^8 - 14x^4 + 1$, which corresponds to an isolated point in the moduli space of genus 3 hyperelliptic curves due to its large geometric automorphism group. In doing so, we exhibit a $\mathbb{Q}$-twist of this curve with its full automorphism group defined over $\mathbb{Q}$, and to the authors' knowledge, this is the first example of a curve over $\mathbb{Q}$ with Sato-Tate distribution, the distribution of the normalized traces of Frobenius, given by the measure

$$\frac{1}{6\pi} \int_a^b \sqrt{4 - \left(\frac{t}{3}\right)^2} \, dt$$

for all intervals $[a, b] \subset [-6, 6]$.

We begin in subsection 1.1 and subsection 1.3 with some background on the generalized Sato-Tate conjecture. We then describe the special properties of the genus 3 curve $y^2 = x^8 - 14x^4 + 1$ in subsection 1.4, and conclude the introduction by elaborating on our main results in subsection 1.6.

1.1. **The generalized Sato-Tate conjecture.** Let A be an abelian variety of dimension g defined over $\mathbb{Q}$. The generalized **Sato-Tate conjecture** predicts that the Haar measure of a certain compact group G, with $G \subset \mathrm{USp}(2g)$, governs the distribution of the normalized Euler factors $\overline{L}_p(A, T)$, as p varies over the primes of good reduction of A. The normalized Euler factor at a prime p is the polynomial $\overline{L}_p(A, T) = L_p(A, T/p^{1/2})$, where $L_p(A, T)$ is the L-polynomial of A at p. Define α_i so that $L_p(A, T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$. Recall that the L-polynomial has the defining property that for each positive integer n,

$$\#A(\mathbb{F}_{p^n}) = \prod_{i=1}^{2g}(1 - \alpha_i^n).$$

We now explain what we mean when we say G "governs" the distribution of the L-polynomials. Serre [Ser12] has defined, using ℓ-adic monodromy groups, a compact real

Lie subgroup of $USp(2g)$ called the **Sato-Tate group** of A, denoted $ST(A)$, satisfying the following condition: for each p at which A has good reduction, there exists a conjugacy class of $ST(A)$ whose characteristic polynomial equals $\overline{L}_p(A, T) := \sum_{i=0}^{2g} a_i(A)(p)T^i$. For a brief summary of this construction, see [FKRS12, Section 2.1]. For $i = 0, 1, \ldots, 2g$, let I_i denote the interval $\left[-\binom{2g}{i}, \binom{2g}{i}\right]$, and consider the map

$$\Phi_i \colon ST(A) \subset USp(2g) \longrightarrow I_i \subset \mathbb{R}$$

that sends an element of $ST(A)$ to the ith coefficient of its characteristic polynomial. Let $\mu(ST(A))$ denote the Haar measure of $ST(A)$ and let $\Phi_{i*}(\mu(ST(A)))$ denote the pushforward of the Haar measure on I_i. We now state the generalized Sato-Tate conjecture.[1]

Conjecture 1.2 (Generalized Sato-Tate). *For each $i = 0, 1, \ldots, 2g$, the $a_i(A)(p)$'s are equidistributed, with respect to increasing size, on I_i with respect to $\Phi_{i*}(\mu(ST(A)))$.*

1.3. **Progress on proving the generalized Sato-Tate conjecture.** The classical Sato-Tate conjecture is concerned with the case that A is an elliptic curve over $\mathbb{Q}$ without CM. Here, $g = 1$ and $ST(A) \cong USp(2) \cong SU(2)$. This form of the conjecture was recently proved in culmination of a project several years in the making; see [Ser12, Example 8.1.5.2] for a complete list of references. For elliptic curves E with CM over a general number field K, there are two cases. If E has CM defined over K, then $ST(E) \cong U(1)$ where $U(1) \hookrightarrow SU(2)$ via $u \mapsto \left(\begin{smallmatrix} u & 0 \\ 0 & \overline{u} \end{smallmatrix}\right)$. If E has CM not defined over K, then $ST(E)$ is isomorphic to the normalizer of $U(1)$ in $SU(2)$.

The recent work of Fité, Kedlaya, Rotger, and Sutherland has presented an explicit version of the generalized Sato-Tate conjecture for abelian surfaces over number fields K. The classification in [FKRS12, Table 8] gives a description in the form of explicit equations of curves whose Jacobians realized each of the 52 Sato-Tate groups that can and do arise for abelian surfaces. The authors of [FKRS12] also show that only 34 of these arise for Jacobians of genus 2 curves defined over $\mathbb{Q}$. In [FS14], the authors prove that 18 of these 34 subgroups can be realized as the Sato-Tate group of a $\mathbb{Q}$-twist of either the curve $y^2 = x^5 - x$ or $y^2 = x^6 + 1$ and that the generalized Sato-Tate conjecture holds for the Jacobians of $\mathbb{Q}$-twists of the aforementioned curves.

For higher dimensional abelian varieties, there have been a few sporadic results which we briefly recall. Fité and Sutherland [FS16] provide effective algorithms to compute the traces of Frobenius at primes of good reduction for the curves $y^2 = x^8 + c$ and $y^2 = x^7 - cx$ and determine the Sato-Tate groups that arise generically and for specific $c \in \mathbb{Q}^*$. In her thesis [Lor14], Lorenzo, in joint work with Fité and Sutherland, computed the Sato-Tate groups and Sato-Tate distributions for $\mathbb{Q}$-twists of the Fermat and Klein quartics and proved Conjecture 1.2 for the Jacobians of these curves. Another result worth mentioning is [FKS16], where the authors establish a group-theoretic classification of Sato-Tate groups of self-dual motives of weight 3 with rational coefficients and prescribed Hodge numbers.

In this article, we continue the investigation of Sato-Tate in genus 3 by computing the Sato-Tate groups of the Jacobians of $\mathbb{Q}$-twists of the genus 3 curve $y^2 = x^8 - 14x^4 + 1$ and proving the generalized Sato-Tate conjecture for such twists.

---

[1]The generalized Sato-Tate conjecture naturally extends to abelian varieties defined over number fields K, however we shall only be concerned with the case of $K = \mathbb{Q}$.

Notation. Throughout, let $\overline{\mathbb{Q}}$ denote a fixed algebraic closure of $\mathbb{Q}$, and let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the absolute Galois group of $\mathbb{Q}$. For any algebraic variety X defined over $\mathbb{Q}$ and any extension $L/\mathbb{Q}$, we use X_L to denote the algebraic variety obtained over L by the base change of $\mathbb{Q} \hookrightarrow L$. For abelian varieties A and B defined over $\mathbb{Q}$, we write $A \sim_L B$ (resp. $A \sim B$) to indicate that there is an isogeny between A and B defined over L (resp. $\mathbb{Q}$).

1.4. **An isolated point in the moduli space of genus 3 hyperelliptic curves.** Let C_0 denote the hyperelliptic curve $y^2 = x^8 - 14x^4 + 1$ defined over $\mathbb{Q}$. In this paper, we first compute the twisting Sato-Tate group $\mathrm{ST}_{\mathrm{Tw}}(C_0)$, which is a compact Lie group with the property that the Sato-Tate group of the Jacobian of any twist of C_0 is isomorphic to a subgroup of $\mathrm{ST}_{\mathrm{Tw}}(C_0)$.

In [GSS12, Table 1], the authors determine the automorphism groups of genus 3 hyperelliptic curves. The curve C_0 is particularly fascinating, because the geometric automorphism group of C_0 is isomorphic to $S_4 \times \mathbb{Z}/2\mathbb{Z}$, and, up to $\overline{\mathbb{Q}}$-isomorphism, C_0 is the unique genus 3 hyperelliptic curve with $\#\mathrm{Aut}((C_0)_{\overline{\mathbb{Q}}}) = 48$. Further, there are no genus 3 hyperelliptic curves with automorphism group of size more than 48 and $\mathrm{Jac}\, C_0 \sim_{\overline{\mathbb{Q}}} E^3$ where E is the non-CM elliptic curve $y^2 = x^4 - 14x^2 + 1$. Magma computes that $\mathrm{Aut}(C_0) \cong (\mathbb{Z}/2\mathbb{Z})^3$ and that all of the automorphisms of C_0 are defined over $\mathbb{Q}(\zeta_8)$.

For computational reasons, we shall primarily work with the $\mathbb{Q}(\zeta_8)$-twist C of C_0 defined by $y^2 = x^8 + 14x^4 + 1$. We compute that $\mathrm{Aut}(C) \cong D_8$ and that all of the automorphisms of C are defined over $\mathbb{Q}(i)$. In section 4, we shall determine a twist C' of C with its full geometric automorphism group defined over $\mathbb{Q}$. For convenience, we record the defining equations for these three twists:

$$C_0: y^2 = x^8 - 14x^4 + 1 \quad C: y^2 = x^8 + 14x^4 + 1 \quad C': \begin{cases} x^2 + y^2 + z^2 = 0 \\ -2t^2 = x^4 + y^4 + z^4, \end{cases} \quad (1.4.1)$$

where the latter curve C' lives in the weighted projective space $\mathbb{P}_{\mathbb{Q}}(1,1,1,2)$ with variables x, y, z of weight 1 and t of weight 2.

Remark 1.5. The family of $\mathbb{Q}$-twists of C is interesting, not only due to the extremal, geometric automorphism group, but also because they are twists of the modular curve $X_0(48)$; this can be checked with the Magma intrinsic

`SimplifiedModel(SmallModularCurve(48));`

By [BN15], $X_0(48)$ is one of two hyperelliptic modular curves whose hyperelliptic involution does not correspond to the Atkin-Lehner involution, and via *loc. cit.* Theorem 6, the points on $X_0(48)$ give rise to an infinite isogeny class with maximal size, namely 16, of elliptic curves over quadratic fields.

1.6. **Main results.** In this paper, we show that all possible subgroups of the twisting Sato-Tate group of C_0 (see Definition 2.5) arise as the Sato-Tate groups of twists of C_0. We also give explicit equations for a representative curve with every such subgroup; see Table 1. Using this classification, we prove the generalized Sato-Tate conjecture for all $\mathbb{Q}$-twists of C_0.

Theorem A. *Let $\widetilde{C}$ be a $\mathbb{Q}$-twist of C_0.*

(1) *There are exactly 9 distinct possibilities for the Sato-Tate group* $\mathrm{ST}(\mathrm{Jac}\,\widetilde{C})$, *and an explicit twist $\widetilde{C}$ realizing each Sato-Tate group is given in Table 1.*

(2) *For $i = 0, \ldots, 6$, the $a_i(\widetilde{C})(p)$ are equidistributed on $I_i = \left[-\binom{6}{i}, \binom{6}{i} \right]$ with respect to a measure $\mu(a_i(\widetilde{C}))$ that is uniquely determined by the Sato-Tate group $\mathrm{ST}(\mathrm{Jac}(\widetilde{C}))$.*

(3) *Conjecture 1.2 holds for $\widetilde{C}$.*

We prove Theorem A(1) in section 4.4 after we compute the twisting Sato-Tate group of C in Lemma 3.3. In Propositions 5.6 and 5.13, we compute pushforwards of measures determined by the distinct Sato-Tate groups and establish Theorem A(2). Finally, in Theorem 5.14, we complete the proof of Theorem A(3).

Remark 1.7. In this paper, we give an example of a curve, namely C' from (1.4.1), over $\mathbb{Q}$, whose Sato-Tate distribution is given by the measure

$$\frac{1}{6\pi} \int_a^b \sqrt{4 - \left(\frac{t}{3}\right)^2}\, dt,$$

where $[a, b] \subset [-6, 6]$. Although examples of a curve over $\mathbb{Q}$ with such a distribution were likely known to the experts, to the authors' knowledge, all previous in print examples of curves with such a distribution were defined over an extension of $\mathbb{Q}$, such as $\mathbb{Q}(\sqrt{-3})$. This twist has the interesting property that it is hyperelliptic after base change to $\overline{\mathbb{Q}}$, but it does not have a degree 2 map to $\mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$.

1.8. **Organization.** The outline of this paper is as follows: In section 2, we recall the definition of the algebraic Sato-Tate group [BK15] and the twisting algebraic Sato-Tate group [FS14]. In section 3, we compute the twisting algebraic Sato-Tate group of the curve $y^2 = x^8 - 14x^4 + 1$. In section 4, we construct an explicit twist of C_0 with all automorphisms defined over $\mathbb{Q}$, and use this twist to compute explicit models for all other twists along with the corresponding Sato-Tate groups. Then, in section 5, we prove the generalized Sato-Tate conjecture for all twists of C_0. In section 6 we compute the moment sequences of all twists of C_0. In the appendix, section A, we include an application of our classification of twists of C_0, showing that the only Sato-Tate group of a 3-dimensional abelian variety whose first moment sequence agrees with that of C' is $\mathrm{SU}(2)_3$. Finally, in section B, we give a table summarizing key properties of the twists of C and three tables displaying the first few theoretical and experimental values of the three moment sequences associated to the twists of C.

---

[2]This can be found at `http://math.mit.edu/~drew/aws/g3AWSProjectSatoTateDistributions.html`.

2. BACKGROUND

After specifying our conventions for the matrix groups $U(6)$, $Sp(6)$ and $USp(6)$, we recall the definition of the twisting algebraic Sato-Tate group and the twisting Sato-Tate group.

Definition 2.1. Set

$$J := \begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & & \\ & & 0 & 1 & & \\ & & -1 & 0 & & \\ & & & & 0 & 1 \\ & & & & -1 & 0 \end{pmatrix}$$

and for K a field, define

$$Sp(6)/K := \{M \in GL(6)/K : M^t J M = J\}.$$

We often omit K when K is clear from context. When $K = \mathbb{R}$ is the field of real numbers, we also define

$$U(6)/\mathbb{R} := \{M \in GL(6)/\mathbb{C} : M^H M = id\},$$

where M^H is the Hermitian conjugate of M. We then define

$$USp(6)/\mathbb{R} := U(6)/\mathbb{R} \cap Sp(6)/\mathbb{R}.$$

Let A be an abelian variety of dimension ≤ 3 defined over $\mathbb{Q}$. Fix an embedding $\iota \colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and a symplectic basis for the singular homology group $H_1(A_\mathbb{C}^{top}, \mathbb{Q})$ where the superscript refers to the underlying topological space. We can use this basis to equip this space with an action of $GSp(2g)/\mathbb{Q}$. For each $\tau \in G_\mathbb{Q}$, define the **twisting Lefschetz group** by

$$L(A, \tau) := \left\{ \gamma \in Sp(2g) : \gamma^{-1} \alpha \gamma = {}^\tau \alpha \text{ for all } \alpha \in End(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} \right\}. \tag{2.1.1}$$

Definition 2.2. We define the **algebraic Sato-Tate group** of A, notated $AST(A)$, as the union

$$AST(A) = \bigcup_{\tau \in G_\mathbb{Q}} L(A, \tau).$$

We also define the **Sato-Tate group** of A, notated $ST(A)$, as a maximal compact subgroup of $AST(A) \otimes_\mathbb{Q} \mathbb{C}$; see [BK15, Theorem 6.1, Theorem 6.10].

Remark 2.3. The Sato-Tate group is not invariant under arbitrary twisting, however, it is invariant under quadratic twisting which acts through the hyperelliptic involution; see [FS14, Remark 2.1].

In this paper, we shall only be concerned with the case where $A = Jac\,C$ where C is a genus 3 hyperelliptic curve over $\mathbb{Q}$, and hence we shall notate $AST(C) := AST(Jac\,C)$ and $ST(C) := ST(Jac\,C)$. Using the identification of H_1 of the Jacobian with the tangent space to the Jacobian, we may view $Aut(C)$ as a subgroup of $GL(H_1(Jac\,C_\mathbb{C}^{top}), \mathbb{Q})$. This identification allows us to define the twisting algebraic Sato-Tate group.

Definition 2.4. The **twisting algebraic Sato-Tate group** of C is the algebraic subgroup of $\mathrm{Sp}(2g)/\mathbb{Q}$ defined by

$$\mathrm{AST}_{\mathrm{Tw}}(C) := \mathrm{AST}(\mathrm{Jac}\, C) \cdot \mathrm{Aut}(C_{\overline{\mathbb{Q}}}).$$

Let $\widetilde{C}$ be a twist of C, meaning that $\widetilde{C}$ is defined over $\mathbb{Q}$ and there exists a finite extension $L/\mathbb{Q}$ with $\widetilde{C}_L \cong C_L$. Let $\phi \colon \widetilde{C}_L \to C_L$ be a fixed isomorphism. By considering the induced isomorphism $H_1(\mathrm{Jac}\, \widetilde{C}_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}) \to H_1(\mathrm{Jac}\, C_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q})$, which we denote as $\widetilde{\phi}$, we see that

$$L(\mathrm{Jac}\, \widetilde{C}, \tau) = \widetilde{\phi}^{-1} L(\mathrm{Jac}\, C, \tau)(^{\tau}\widetilde{\phi}). \tag{2.4.1}$$

If we identity $\gamma' \in L(\mathrm{Jac}\, \widetilde{C}, \tau)$ with $\widetilde{\phi}^{-1}\gamma(^{\tau}\widetilde{\phi})$ with $\gamma \in L(\mathrm{Jac}\, C, \tau)$, then [FS14, Lemma 2.3] asserts that the map

$$\Lambda_{\widetilde{\phi}} \colon \mathrm{AST}(\mathrm{Jac}\, \widetilde{C}) \longrightarrow \mathrm{AST}_{\mathrm{Tw}}(C)$$
$$\gamma' \longmapsto \gamma(^{\tau}\widetilde{\phi})\widetilde{\phi}^{-1}$$

is a well-defined monomorphism of groups. This lemma allows us to define the twisting Sato-Tate group of C.

Definition 2.5. The **twisting Sato-Tate group** $\mathrm{ST}_{\mathrm{Tw}}(C)$ of C is a maximal compact subgroup of $\mathrm{AST}_{\mathrm{Tw}}(C) \otimes \mathbb{C}$.

Remark 2.6. From [FS14, Lemma 2.3], we have that for any twist $\widetilde{C}$ of C, the Sato-Tate group $\mathrm{ST}(C)$ is isomorphic to a subgroup of $\mathrm{ST}_{\mathrm{Tw}}(C)$. Further, the component groups of $\mathrm{ST}_{\mathrm{Tw}}(C)$ and $\mathrm{AST}_{\mathrm{Tw}}(C) \otimes \mathbb{C}$ are isomorphic, and the identity components of $\mathrm{ST}_{\mathrm{Tw}}(C)$ and $\mathrm{ST}(C)$ are equal.

We conclude this section with a proposition which informs us as to which subgroups can arise as Sato-Tate groups of twists of a particular curve. First, we recall the following simple but fundamental lemma, describing the action of twisting on the twisting Lefschetz group of a curve.

Lemma 2.7 ([FKRS12, Definition 2.20]). *Let* $C/\mathbb{Q}$ *be a curve and let* ξ *be a continuous 1-cocycle* $\xi \colon G_{\mathbb{Q}} \to \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$. *Let* C^{ξ} *be the twist of C by* ξ. *For all* $\tau \in G_{\mathbb{Q}}$ *the following equality holds:*

$$L_{C^{\xi}}(\tau) = L_C(\tau)\xi(\tau)^{-1}.$$

Proposition 2.8. *Let* $C/\mathbb{Q}$ *be a curve such that* $\mathrm{Aut}(C) = \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ *and let* $G \in \mathrm{Aut}(C)$ *be a subgroup such that the inverse Galois problem for G has a solution. Then there exists a twist* C^G *of C, defined over* $\mathbb{Q}$, *such that* $\mathrm{ST}(C^G)/\mathrm{ST}(C^G)^0 = G$.

Remark 2.9. Notice that $\mathrm{ST}(C^G)/\mathrm{ST}(C^G)^0 = G$ is an actual equality and not just an abstract isomorphism. By [FS14, Lemma 2.3], we have a canonical monomorphism

$$\mathrm{ST}(C^G) \hookrightarrow \mathrm{AST}(C^G) \hookrightarrow \mathrm{AST}_{\mathrm{Tw}}(C)$$

which induces an injection $\mathrm{ST}(C^G)/\mathrm{ST}(C^G)^0 \hookrightarrow \mathrm{ST}_{\mathrm{Tw}}(C^G)/\mathrm{ST}_{\mathrm{Tw}}(C^G)^0$. The equality above is to be interpreted as relative to this embedding.

Proof. Recall that twists of C are in bijection with cohomology classes in $H^1(G_{\mathbb{Q}}, \mathrm{Aut}(C))$. Given that the Galois action on $\mathrm{Aut}(C)$ is trivial, a cocycle representing such a cohomology class amounts to a continuous homomorphism $\xi \colon G_{\mathbb{Q}} \to \mathrm{Aut}(C)$. Fix a Galois extension L of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ and choose as ξ the canonical projection $G_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q})$ followed by an (arbitrary) isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \cong G$. We shall show that one can take C^G to be C^ξ, the twist of C corresponding to ξ.

By our construction of C, we know that for all $\tau \in G_{\mathbb{Q}}$ we have
$$L_C(\tau) = L_C(\mathrm{id}) = L_C(\mathrm{id})^0,$$
and hence
$$\mathrm{AST}(C^\xi) = \bigcup_{\tau \in G} L_{C^\xi}(\tau) = \bigcup_{\tau \in G} L_C(\mathrm{id})\xi(\tau)^{-1}.$$
Therefore, $\mathrm{AST}(C^\xi)$, seen as a subgroup of $\mathrm{AST}_{\mathrm{Tw}}(C) = \mathrm{AST}_{\mathrm{Tw}}(C)$, is precisely the union of those connected components that intersect the image of ξ. By construction of ξ, this implies that the group of components of $\mathrm{AST}(C^\xi)$ is G. Since $\mathrm{ST}(C^\xi)$ is a maximal compact subgroup of $\mathrm{AST}(C^\xi) \otimes_{\mathbb{Q}} \mathbb{C}$, we have that
$$\mathrm{ST}(C^\xi)/\mathrm{ST}(C^\xi)^0 = \mathrm{AST}(C^\xi)/\mathrm{AST}(C^\xi)^0 = G.$$
$\square$

3. THE TWISTING ALGEBRAIC SATO-TATE GROUP

The main result of this section is Proposition 3.4, in which we determine the twisting Sato-Tate group for the curve C. In order to compute the twisting Sato-Tate group, we first compute the algebraic Sato-Tate group in Lemma 3.3. To do this, we now compute the decomposition of the Jacobian of C in Lemma 3.1.

Lemma 3.1. *The Jacobian of C decomposes as* $\mathrm{Jac}\, C \sim (E_1)^2 \times E_2$ *where*
$$E_1 \colon y^2 = x^3 - x^2 - 4x + 4,$$
$$E_2 \colon y^2 = x^3 + x^2 - 4x - 4$$
are non-CM elliptic curves; moreover $\mathrm{End}(\mathrm{Jac}\, C) \otimes_{\mathbb{Z}} \mathbb{Q} = M_2(\mathbb{Q}) \times \mathbb{Q}$.

Proof. By computing curve quotients using Magma's intrinsic

`CurveQuotient(AutomorphismGroup(C,[a]));`

where $a \in \mathrm{Aut}(C)$, we see that $\mathrm{Jac}\, C_{\mathbb{Q}} \sim E_1 \times E_2 \times E_3$ where E_1, E_2 are defined above and E_3 is some elliptic curve. Since $\mathrm{End}(\mathrm{Jac}\, C)$ is non-commutative and $\mathrm{Aut}(C)$ embeds into $\mathrm{End}(\mathrm{Jac}\, C)$, we have that E_3 is isogenous to either E_1 or E_2, and by considering local zeta functions, we conclude that $E_3 \sim E_1$. The statement that $\mathrm{End}(\mathrm{Jac}\, C) \otimes_{\mathbb{Z}} \mathbb{Q} = M_2(\mathbb{Q}) \times \mathbb{Q}$ follows from the curves being non-CM. $\square$

Remark 3.2. Recall that as mentioned in subsection 1.4, all automorphisms of C are defined over $\mathbb{Q}(i)$. Analogously to [FS14, Lemma 4.2], one can show that the minimal number field over which all the automorphisms of $C_{\overline{\mathbb{Q}}}$ are defined coincides with the minimal number field over which all the endomorphism of $(\mathrm{Jac}\, C)_{\overline{\mathbb{Q}}}$ are defined; since $\mathrm{Jac}\, C$ decomposes up to isogeny as the product of three non-CM elliptic curves, we do not need to invoke any auxiliary results.

7

Lemma 3.3. *We have that*

$$
\mathrm{AST}(C) = \left\{ \left(\begin{array}{c|c|c} M & & \\ \hline & M & \\ \hline & & \pm M \end{array} \right) : M \in \mathrm{SU}(2) \right\}.
$$

Proof. Since all of the automorphisms of C are defined over $\mathbb{Q}(i)$, Remark 3.2 asserts that all of the endomorphisms of $\mathrm{Jac}\,C$ are defined over $\mathbb{Q}(i)$. Moreover, the action of $G_{\mathbb{Q}}$ on $\mathrm{End}((\mathrm{Jac}\,C)_{\overline{\mathbb{Q}}})$ must factor through $\mathbb{Q}(i)$. To explicitly compute the twisting Lefschetz group, we need to consider how $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle \delta \rangle$, where δ denotes complex conjugation, acts on $\mathrm{End}((\mathrm{Jac}\,C)_{\overline{\mathbb{Q}}})$.

Since the action of Galois will fix the diagonal matrices, one can check (using implicitly our description of $\mathrm{End}(\mathrm{Jac}\,C)$ from Lemma 3.1) that Galois acts via

$$
\left(\begin{array}{cc|c} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \hline a_{31} & a_{32} & a_{33} \end{array} \right) \mapsto \left(\begin{array}{cc|c} a_{11} & a_{12} & -a_{13} \\ a_{21} & a_{22} & -a_{23} \\ \hline -a_{31} & -a_{32} & a_{33} \end{array} \right).
$$

To complete the proof, it suffices to check

$$
L(\mathrm{Jac}(C), \mathrm{id}) = \left\{ \left(\begin{array}{c|c|c} M & 0 & 0 \\ \hline 0 & M & 0 \\ \hline 0 & 0 & M \end{array} \right) : M \in \mathrm{SL}(2) \right\},
$$

$$
L(\mathrm{Jac}\,C, \delta) = \left\{ \left(\begin{array}{c|c|c} M & 0 & 0 \\ \hline 0 & M & 0 \\ \hline 0 & 0 & -M \end{array} \right) : M \in \mathrm{SL}(2) \right\}.
$$

We can check these directly from the definition. To compute $L(\mathrm{Jac}\,C, \mathrm{id})$, taking

$$
\alpha = \left(\begin{array}{c|c|c} \mathrm{id} & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & 0 \end{array} \right), \gamma = \left(\begin{array}{c|c|c} a_{11} & a_{12} & a_{13} \\ \hline a_{21} & a_{22} & a_{23} \\ \hline a_{31} & a_{32} & a_{33} \end{array} \right)
$$

the condition that $\gamma\alpha = \alpha\gamma$ implies $a_{12} = a_{13} = a_{21} = a_{31} = 0$. Similarly, taking α to be other block matrices with eight of the blocks equal to 0, and the ninth equal to the identity, we obtain $a_{ij} = 0$ if $i \neq j$ and $a_{11} = a_{22} = a_{33}$, as claimed. The computation for $L(\mathrm{Jac}\,C, \delta)$ is analogous, this time using that $\alpha\gamma = {}^{\delta}\alpha\gamma$ as α ranges over the matrices with a single nonzero block which is equal to the identity. $\square$

Before we compute the twisting Sato-Tate group of C, we introduce the following notation. Let

$$
\mathrm{SL}(2)_3 := \left\langle \left(\begin{array}{c|c|c} M & & \\ \hline & M & \\ \hline & & M \end{array} \right) : M \in \mathrm{SL}(2) \right\rangle
$$

denote the diagonal embedding of $\mathrm{SL}(2)$ inside $\mathrm{Sp}(6)$; the image of $\mathrm{SU}(2)$ under this embedding will likewise be denoted by $\mathrm{SU}(2)_3$.

Proposition 3.4. *The twisting algebraic Sato-Tate group of C is*

$$\mathrm{AST}_{\mathrm{Tw}}(C) = \left\langle \mathrm{SL}(2)_3, \left(\begin{array}{c|c|c} 0 & 0 & \mathrm{id} \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & \mathrm{id} & 0 \end{array} \right), \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline -\mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle \subset \mathrm{Sp}(6),$$

and hence the twisting Sato-Tate group of C is

$$\mathrm{ST}_{\mathrm{Tw}}(C) = \left\langle \mathrm{SU}(2)_3, \left(\begin{array}{c|c|c} 0 & 0 & \mathrm{id} \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & \mathrm{id} & 0 \end{array} \right), \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline -\mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle \subset \mathrm{USp}(6).$$

Proof. By Definition 2.4, it suffices to realize the generators of $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ as a subgroup of $\mathrm{Sp}(6)$, which we accomplish by computing the action of $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ on $\mathrm{Jac}\,C$. First, we identify the tangent space to $\mathrm{Jac}\,C$ at the identity with the space of regular differentials, which has basis given by the following differentials:

$$\omega_1 := \frac{2x}{y}dx, \qquad \omega_2 := \frac{(1-x^2)}{y}dx, \qquad \omega_3 := \frac{(1+x^2)}{y}dx. \qquad (3.4.1)$$

Using `Magma`, we compute that $\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) = \mathrm{Aut}(C_{\mathbb{Q}(i)}) = \langle \iota, \alpha_1, \alpha_2 \rangle$, where ι is the hyperelliptic involution and

$$\alpha_1 \colon (x,y) \longmapsto \left(\frac{-i(x-1)}{(x+1)}, \frac{-4y}{(x+1)^4} \right),$$

$$\alpha_2 \colon (x,y) \longmapsto \left(\frac{-i(x+i)}{(x-i)}, \frac{4y}{(x-i)^4} \right).$$

By pulling back ω_i along $\iota, \alpha_1, \alpha_2$, we realize $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ as the subgroup of $\mathrm{Sp}(6)$ generated by

$$\left\langle \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & -\mathrm{id} & 0 \\ \hline 0 & 0 & -\mathrm{id} \end{array} \right), \left(\begin{array}{c|c|c} 0 & 0 & -\mathrm{id} \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & \mathrm{id} & 0 \end{array} \right), \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline -\mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle.$$

This implies the first statement in the proposition, because $-\mathrm{id}$ is already an element of $\mathrm{SL}(2)_3$ The second statement follows immediately from the first upon noticing that $\mathrm{SU}(2)$ is a maximal compact subgroup of $\mathrm{SL}(2)$ and it contains $-\mathrm{id}$. $\qquad \square$

Remark 3.5. For the rest of the paper, we shall consistently use the differentials $\omega_1, \omega_2, \omega_3$ as defined in (3.4.1) as a basis for the tangent space to $\mathrm{Jac}\,C$ at the identity. This choice of coordinates allows us to identify $\mathrm{ST}_{\mathrm{Tw}}(C)$ with the concrete subgroup of $\mathrm{USp}(6)$ given in the statement of Proposition 3.4. The explicit description of $\mathrm{ST}_{\mathrm{Tw}}(C)$ also enables to compute its group of components, which is easily seen to be isomorphic to the subgroup of $\mathrm{GL}_3(\mathbb{Z})$ generated by

$$\sigma := \left(\begin{array}{c|c|c} 0 & 0 & 1 \\ \hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \end{array} \right) \qquad \tau := \left(\begin{array}{c|c|c} 0 & 1 & 0 \\ \hline -1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array} \right).$$

Moreover, we see that $\mathrm{ST}_{\mathrm{Tw}}(C)/\mathrm{ST}_{\mathrm{Tw}}(C)^0$ is isomorphic to S_4 by sending $\sigma \mapsto (143)$ and $\tau \mapsto (1234)$. We will find it useful to have one further description of the group of components of $\mathrm{ST}(C)$. Notice that σ and τ generate precisely the (octahedral) subgroup O of

9

$GL_3(\mathbb{Z})$ consisting of signed permutation matrices with positive determinant. Furthermore, the group of all 3×3 signed permutation matrices is $O \times \mathbb{Z}/2\mathbb{Z}$ (where the factor $\mathbb{Z}/2\mathbb{Z}$ is generated by $-\operatorname{id}$), hence it is isomorphic to $S_4 \times \mathbb{Z}/2\mathbb{Z} \cong \operatorname{Aut}(C_{\overline{\mathbb{Q}}})$. We shall use these identifications to write $\operatorname{ST}_{\operatorname{Tw}}(C)/\operatorname{ST}_{\operatorname{Tw}}(C)^0$ as an index-2 subgroup of $\operatorname{Aut}(C_{\overline{\mathbb{Q}}})$, which in turn we can consider as a subgroup of $GL_3(\mathbb{Z})$.

4. The right twist

Given C we now find the twist C' with full geometric automorphism group defined over $\mathbb{Q}$ and whose Jacobian has connected Sato-Tate group. As described in Remark 4.2, it is not difficult to show C' is a twist of C with the desired properties, but we prefer to illustrate how one would look for C' in the proof of Proposition 4.1.

Proposition 4.1. *The curve C' in weighted projective space $\mathbb{P}_{\mathbb{Q}}(1,1,1,2)$ defined by*

$$\begin{cases} x^2 + y^2 + z^2 = 0 \\ -2t^2 = x^4 + y^4 + z^4 \end{cases}$$

where the variables x, y, z have weight 1 and t has weight 2 is a twist of C with $\operatorname{Aut}(C') \cong \operatorname{Aut}(C_{\overline{\mathbb{Q}}})$ and for which $\operatorname{ST}(C)$ is connected.

Remark 4.2. It is easy to check using `Magma`'s intrinsic `AutomorphismGroup` that the automorphism group of the twist C' is $S_4 \times \mathbb{Z}/2\mathbb{Z}$, but we write out this proof to illustrate how to find the twist with a prescribed connected component of its Sato-Tate group. In the proof, we show that C' corresponds to the cohomology class in $H^1(G_{\mathbb{Q}}, \operatorname{Aut}(C_{\overline{\mathbb{Q}}}))$ of the unique cocycle that factors through $\operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ and sends the nontrivial element of this group to the automorphism

$$(x, y) \mapsto \left(-\frac{1}{x}, -\frac{y}{x^4} \right)$$

of C.

Proof. Recall from Lemmas 3.3 and 2.7 that for all $\sigma \in G_{\mathbb{Q}}$, we have $L_C(\sigma) = L_C(\operatorname{id}) \cdot \pi(\sigma)$, where

$$\pi \colon G_{\mathbb{Q}} \longrightarrow \operatorname{GSp}(6)/\mathbb{Q}$$

$$\sigma \longmapsto \begin{cases} \begin{pmatrix} \operatorname{id} & & \\ & \operatorname{id} & \\ & & \operatorname{id} \end{pmatrix} & \text{if } \sigma \text{ acts trivially on } \mathbb{Q}(i), \\ \begin{pmatrix} & \operatorname{id} & \\ \operatorname{id} & & \\ & & -\operatorname{id} \end{pmatrix} & \text{otherwise.} \end{cases}$$

Let $\xi \colon G_{\mathbb{Q}} \to \operatorname{Aut}(C_{\overline{\mathbb{Q}}})$ be a cocycle. We have

$$\operatorname{AST}(\operatorname{Jac} C^{\xi}) = \bigcup_{\sigma \in G_{\mathbb{Q}}} L_{C^{\xi}}(\sigma) = \bigcup_{\sigma \in G_{\mathbb{Q}}} L_C(\sigma)\xi(\sigma)^{-1} = \bigcup_{\sigma \in G_{\mathbb{Q}}} L_C(\operatorname{id})\pi(\sigma)\xi(\sigma)^{-1}. \tag{4.2.1}$$

So, in order for $\operatorname{ST}(\operatorname{Jac} C^{\xi})$ to be connected, it is necessary and sufficient that $\pi(\sigma)\xi(\sigma)^{-1}$ be an element of $L_C(\operatorname{id})$ for all $\sigma \in G_{\mathbb{Q}}$.

10

Now notice that

$$\left(\begin{array}{c|c|c} \text{id} & & \\ \hline & \text{id} & \\ \hline & & -\text{id} \end{array}\right) \in \text{Aut}(\text{Jac } C)$$

is induced by the automorphism $(x, y) \mapsto \left(-\frac{1}{x}, -\frac{y}{x^4}\right)$ of C, so π itself can be interpreted as a cocycle with values in $\text{Aut}(C_{\overline{Q}})$. Indeed, it is the unique continuous homomorphism $G_Q \to \text{Aut}(C_{\overline{Q}})$ that factors through $\text{Gal}\,(Q(i)/Q)$ and sends the nontrivial element of this latter group to the automorphism $\psi\colon (x, y) \mapsto \left(-\frac{1}{x}, -\frac{y}{x^4}\right)$. To check that this is indeed a cocycle, we simply notice that ψ is defined over Q, so a cocycle with values in $\{\text{id}, \psi\}$ is a (continuous) homomorphism with values in this group.

If we now take $\xi = \pi$, formula (4.2.1) shows that

$$\text{AST}(\text{Jac } C^\xi) = \bigcup_{\sigma \in G_Q} L_C(\text{id})\pi(\sigma)\pi(\sigma)^{-1} = L_C(\text{id}),$$

so that $\text{AST}(\text{Jac } C^\xi)$ is connected. By Definition 2.2, $\text{ST}(C^\xi)$ and $\text{AST}(C^\xi)$ have the same group of connected components, and hence the Sato-Tate group of C^ξ is connected.

We now want to compute explicit equations for C^ξ. In order to do this, recall that the function field of C^ξ can be identified with the set of fixed points for a certain action of G_Q on $\overline{Q}(C)$. More precisely, an element $\sigma \in G_Q$ acts on $\overline{Q}(C) = \overline{Q}(x, y)$ by the rule

$$\begin{cases} \sigma \cdot x = -\frac{1}{x} \\ \sigma \cdot y = -y/x^4 \\ \sigma \cdot \alpha = \sigma(\alpha) \quad \forall \alpha \in \overline{Q}. \end{cases}$$

Observe that the three functions

$$a := x - \frac{1}{x}, \qquad\qquad b := i\left(x + \frac{1}{x}\right), \qquad\qquad c := i\frac{y}{x^2}$$

are invariant under this Galois action, and we claim that they generate the function field of $Q(C^\xi)$. To show this, it suffices to prove that (after extending the scalars to $\overline{Q}$) they generate $\overline{Q}(C) = \overline{Q}(x, y)$. This holds because we have

$$x = \frac{ia + b}{2}, \qquad\qquad y = \frac{cx^2}{i} = \frac{c}{i}\left(\frac{ia + b}{2}\right)^2.$$

Furthermore, the functions a, b, c satisfy $a^2 + b^2 = -4$ and $c^2 + a^4 + 4a^2 + 16$. By considering these equations in weighted projective space $\mathbb{P}_Q(1, 1, 1, 2)$, our twist is defined by the equations

$$\begin{cases} a^2 + b^2 + c^2 = 0 \\ d^2 - a^2b^2 + c^4 = 0, \end{cases}$$

where the variables a, b, and c have weight 1 and d has weight 2. Since

$$a^2b^2 = \frac{1}{2}(a^2 + b^2)^2 - \frac{1}{2}(a^4 + b^4) = \frac{1}{2}(c^4 - a^4 - b^4)$$

11

we have

$$d^2 = a^2b^2 - c^4 = \frac{1}{2}(c^4 - a^4 - b^4) - c^4 = -\frac{1}{2}(a^4 + b^4 + c^4).$$

So, we can realize the model for our curve C' as

$$\begin{cases} a^2 + b^2 + c^2 = 0 \\ -2d^2 = a^4 + b^4 + c^4. \end{cases}$$

Replacing (a, b, c, d) by (x, y, z, t) yields the result. $\qquad\square$

Remark 4.3. This model helps clarify the action of the automorphism group $S_4 \times \mathbb{Z}/2\mathbb{Z}$. The hyperelliptic involution sends t to $-t$, while S_4 acts on (x, y, z) through the well-known isomorphism

$$S_4 \cong \{\pm 1\}^3 \rtimes S_3 / \langle (-1, -1, -1, \mathrm{id}) \rangle;$$

that is, an element in S_4 induces a permutation of (x, y, z), followed by a change of sign of some of these three coordinates. Notice that in weighted projective space $[x : y : z : t]$ and $[-x : -y : -z : t]$ are the same point, because t has weight 2 while the others have weight one.

4.4. **Groups arising as component groups of** $ST(C^\xi)$ **for some twist** C^ξ.
In this subsection, we obtain a complete list of twists of C' whose Sato-Tate groups realize all possible subgroups of $ST_{Tw}(C')$. Recall that Shafarevich [Sha58] proved that every finite solvable group is realizable as a Galois group of a number field. Since S_4 is solvable, Proposition 2.8 asserts that there are at most 11 Sato-Tate groups arising from the 11 conjugacy classes of S_4, which we recall in Table 1. In the next lemma, we prove that only 9 of these conjugacy classes correspond to distinct Sato-Tate groups, which yields a proof of Theorem A(1).

Lemma 4.5. *Conjugacy classes 2 and 3 from Table 1 correspond to isomorphic Sato-Tate groups. More concretely, consider the subgroups of* $\mathrm{USp}(6)$ *given by*

$$G_2 := \left\langle \mathrm{SU}(2)_3, \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle \quad and \quad G_3 := \left\langle \mathrm{SU}(2)_3, \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & \mathrm{id} & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle;$$

there exists an element $g \in \mathrm{USp}(6)$ *such that* $gG_2g^{-1} = G_3$. *Likewise, conjugacy classes 5 and 6 from Table 1 also correspond to isomorphic Sato-Tate groups, that is, the groups*

$$G_5 := \left\langle \mathrm{SU}(2)_3, \left(\begin{array}{c|c|c} \pm\mathrm{id} & 0 & 0 \\ \hline 0 & \pm\mathrm{id} & 0 \\ \hline 0 & 0 & \pm\mathrm{id} \end{array} \right) \right\rangle, G_6 := \left\langle \mathrm{SU}(2)_3, \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right), \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & -\mathrm{id} & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) \right\rangle$$

are conjugate in $\mathrm{USp}(6)$. *All other conjugacy classes give pairwise non-isomorphic Sato-Tate groups.*

Proof. First, notice that the last statement is immediate, since Sato-Tate groups that have non-isomorphic component groups correspond to different conjugacy classes. Let

$$g := \begin{pmatrix} 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 & 0 \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 & 0 & 0 \\ 0 & -1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 & 0 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

One checks that the equalities $gg^{\mathsf{T}} = \mathrm{id}$ and $g^{\mathsf{T}}Jg = J$ hold for J in Definition 2.1, so that $g \in \mathrm{USp}(6)$. Furthermore, we have

$$g \left(\begin{array}{c|c|c} 0 & \mathrm{id} & 0 \\ \hline \mathrm{id} & 0 & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) g^{-1} = \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & \mathrm{id} & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right)$$

and

$$g \, \mathrm{diag}_3 \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) g^{-1} = \mathrm{diag}_3 \left(\begin{smallmatrix} d & -c \\ -b & a \end{smallmatrix} \right),$$

where by $\mathrm{diag}_3(M)$ denotes the 6×6 matrix that is block-diagonal with 3 identical 2×2 blocks given by M. This shows that conjugation by g stabilizes $\mathrm{SU}(2)_3$ and sends G_2 to G_3 as claimed. Finally, one checks that

$$g \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & -\mathrm{id} & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right) g^{-1} = \left(\begin{array}{c|c|c} -\mathrm{id} & 0 & 0 \\ \hline 0 & -\mathrm{id} & 0 \\ \hline 0 & 0 & \mathrm{id} \end{array} \right),$$

which (combined with the first part of the lemma) easily implies the claim about G_5 and G_6. $\qquad\square$

As in Proposition 4.1, we can compute twists of C' whose Sato-Tate group has group of components isomorphic to a specific subgroup of S_4. We now provide another detailed example to illustrate this technique.

4.6. A $\mathbb{Z}/4\mathbb{Z}$-twist. We show how to compute a twist of C' whose Sato-Tate group has group of components isomorphic to $\mathbb{Z}/4\mathbb{Z}$. According to section 4.4, a twist C^ξ will have this property precisely if the image of $\xi \colon G_{\mathbb{Q}} \to \mathrm{Aut}(C')$ is a cyclic group of order 4, which means that the kernel of ξ defines a degree-4 cyclic extension of $\mathbb{Q}$. Among all such extensions, the one with smallest discriminant is the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive 5th root of unity. Since we are free to choose ξ, we take $\ker \xi$ to be $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta)\right)$. To completely describe ξ, we now need to choose an injective homomorphism of $\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ into $\mathrm{Aut}(C')$. As a generator of $\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$, we take the unique automorphism σ of $\mathbb{Q}(\zeta)/\mathbb{Q}$ that sends ζ to ζ^2, and we define our ξ by requiring that $\varphi := \xi(\sigma) \in \mathrm{Aut}(C')$ acts on the function field $\mathbb{Q}(C')$ as follows:

$$\varphi(t/z^2) = t/z^2, \quad \varphi(x/z) = -y/z, \quad \varphi(y/z) = x/z.$$

In order to compute equations for the twist C^ξ, simply recall (see for example [Sil09, Chapter X.2]) that the function field $\mathbb{Q}(C^\xi)$ is the fixed field of $\mathbb{Q}(\zeta)(C')$ under the twisted

13

Galois action given by

$$\sigma(\zeta) = \zeta^2 \qquad\qquad \sigma(x/z) = \varphi(x/z) = -y/z$$
$$\sigma(y/z) = \varphi(y/z) = x/z \qquad \sigma(t/z^2) = \varphi(t/z^2) = t/z^2.$$

We now determine the field of invariants for this action. Clearly t/z^2 is fixed under Galois. For all $j \in \mathbb{Z}$ we have another invariant function given by

$$\sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} g \cdot (\zeta^j x/z).$$

Taking $j = 1$ and $j = 2$, we find that the functions u and v given by

$$\begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} \zeta - \zeta^4 & \zeta^3 - \zeta^2 \\ \zeta^2(1-\zeta) & \zeta\,(1-\zeta^3) \end{pmatrix} \begin{pmatrix} x/z \\ y/z \end{pmatrix} \tag{4.6.1}$$

are Galois invariants. Since the matrix appearing in this formula is invertible over $\mathbb{Q}(\zeta)$, the function fields $\mathbb{Q}(\zeta)(u, v, t/z^2)$ and $\mathbb{Q}(\zeta)(x/z, y/z, t/z^2)$ coincide. Hence the curve (defined over $\mathbb{Q}$) whose function field is $\mathbb{Q}(u, v, t/z^2)$ becomes isomorphic to C' over $\mathbb{Q}(\zeta)$; in other words, we have already found generators for the full field of invariants. Now we just need to find the equations satisfied by u, v and t/z^2. Defining M to be the 2×2 matrix appearing in (4.6.1), we can write

$$\begin{pmatrix} x/z \\ y/z \end{pmatrix} = M^{-1} \begin{pmatrix} u \\ v \end{pmatrix} = \frac{1}{1 - \zeta^2 - 2\zeta^3 + 2\zeta^4} \begin{pmatrix} (\zeta^2 + \zeta + 1)\,u + \zeta v \\ \zeta u - (\zeta^2 + \zeta + 1)\,v \end{pmatrix},$$

and we know that $x/z, y/z$ and t/z^2 satisfy the two equations

$$\begin{cases} (x/z)^2 + (y/z)^2 + 1 = 0 \\ -2(t/z^2)^2 = (x/z)^4 + (y/z)^4 + 1. \end{cases}$$

Replacing $x/z, y/z$ by their expressions in terms of u, v and expanding, the previous system becomes

$$\begin{cases} u^2 + v^2 - 5 = 0 \\ (t/z^2)^2 = \dfrac{1}{125}\left(3u^4 + 4u^3v + 12u^2v^2 - 4uv^3 + 3v^4\right) + 1. \end{cases}$$

In particular, the first equation defines a conic section with a $\mathbb{Q}$-rational point, so this curve admits a hyperelliptic model over $\mathbb{Q}$; Magma's intrinsic `IsHyperelliptic` returns the hyperelliptic model

$$y^2 = -5x^8 - 5x^7 - 35x^6 + 35x^5 - 35x^3 - 35x^2 + 5x - 5. \tag{4.6.2}$$

Finally, since quadratic twists do not change the Sato-Tate group of a curve (cf. Remark 2.3), and since $\sqrt{5}$ belongs to $\mathbb{Q}(\zeta)$, we can further take the quadratic twist by 5 of (4.6.2) without changing either the splitting field of the twist or the group of components of the corresponding Sato-Tate group. Thus, we arrive at the following model for the $\mathbb{Z}/4\mathbb{Z}$-twist:

$$y^2 = -x^8 - x^7 - 7x^6 + 7x^5 - 7x^3 - 7x^2 + x - 1.$$

5. PROVING SATO-TATE FOR ALL THE TWISTS

The goal of this section is to prove the generalized Sato-Tate conjecture for all twists of C, which will complete the proof of our main theorem Theorem A, by proving Theorem A(3). We accomplish this at the end of the section in Theorem 5.14. To prove this, our method is to observe the equality of the distribution of the $a_i(A)(p)$ and the pushforward of the Haar measure μ by Φ_i through direct computation. The computation of the distribution of $a_i(A)(p)$ as A ranges over twists of C is done in Proposition 5.11, while the computation of the pushforward of Haar measure is given in Proposition 5.13.

Before proceeding, we briefly recall the definitions of equidistribution and moment sequences. Let X be a compact topological space equipped with a Radon measure μ. Denote by $C(X)$ the normed space of continuous, complex valued functions f on X with norm given by $\|f\| := \sup_{x \in X} |f(x)|$. We say that a sequence $\{x_i\}_{i \in \mathbb{N}}$ is **equidistributed** with respect to μ if for all $f \in C(X)$ we have

$$\mu(f) = \lim_{m \to \infty} \frac{1}{m} \sum_{i=1}^{m} f(x_i).$$

We restrict our attention to the case where X is an interval. In this case, the nth **moment**, if it exists, is defined as

$$M_n(\{x_i\}) = \lim_{m \to \infty} \frac{1}{m} \sum_{i \leq m} x_i^n.$$

Notice, that if the sequence $\{x_i\}$ is equidistributed with respect to the measure μ, we have that the nth moment exists and is equal to $\mu(\psi_n)$ where $\psi_n(x) = x^n$. In fact a partial converse statement holds. If the nth moment of a sequence $\{x_i\}$ exists for every $n \geq 0$, then there exists a unique measure μ such that $\{x_i\}$ is equidistributed with respect to μ (see Remark 2.5 of [Sut16] for details).

We notate the moments associated to the measure μ by $\mathbb{E}_\mu[x^n]$. For later use, we denote by $n_*\mu$ the pushforward of μ by the multiplication-by-n map; in particular, if μ is supported on the interval $[-a, a]$, then $n_*\mu$ is supported on $[-na, na]$. Further define ϕ to be the Sato-Tate distribution of a non-CM elliptic curve (which is given by $\phi(f) = \frac{1}{2\pi} \int_{-2}^{2} f(x)\sqrt{4 - x^2}dx$ for $f \in C([-2, 2])$) and define δ_0 to be the point mass at 0, which we will use in the tables in Appendix B.

Remark 5.1. A straightforward direct computation gives

$$\mathbb{E}_\phi[x^n] = \Gamma\left(\frac{n+1}{2}\right) \Gamma\left(\frac{n+4}{2}\right)^{-1} (2\sqrt{\pi})^{-1} \cdot (2^n + (-2)^n),$$

and by definition we have $\mathbb{E}_{3_*\phi}[x^n] = 3^n \mathbb{E}_\phi[x^n]$.

5.2. **Finding the distribution of traces of Frobenius.** Before computing the distribution of $a_i(A)(p)$ for all i in subsection 5.7, we first work out the instructive special case when $i = 1$ in the main result of this subsection, Proposition 5.6. That is, we are looking for the distribution of the trace of Frobenius.

15

Let C^{ξ} be a twist of C' corresponding to a twisting cocycle $\xi\colon G_{\mathbb{Q}} \to \mathrm{Aut}(C')$. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^4 - 14x^2 + 1$. We know that $\mathrm{Jac}\,C^{\xi}$ is $\overline{\mathbb{Q}}$-isogenous to E^3. Moreover, for every prime p we know by [MT10, Proposition 11] that the action of the Frobenius at p on $\mathrm{Jac}\,C^{\xi}$ is given by $F_p \circ \xi(\mathrm{Frob}_p)$, where F_p is the automorphism of $\mathrm{Jac}\,C$ induced by the Frobenius at p (notice that the Frobenius at p acts on $(\mathrm{Jac}\,C)_{\overline{\mathbb{F}_p}} \cong (\mathrm{Jac}\,C^{\xi})_{\overline{\mathbb{F}_p}}$. Considering the matrix representation of the automorphisms of the form $\xi(\mathrm{Frob}_p)$, we can understand the trace of Frobenius acting on C^{ξ} in terms of the trace of Frobenius for E.

Lemma 5.3. *Let $\ell \neq p$ be some prime. For each $g \in \mathrm{Aut}(C')$, there is a function $f_g\colon \mathbb{R} \to \mathbb{R}$ such that*

$$\frac{1}{\sqrt{p}}\,\mathrm{tr}\left(\mathrm{Frob}_p \mid H^1_{\text{ét}}((\mathrm{Jac}\,C^{\xi})_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)\right) = f_g\left(\frac{1}{\sqrt{p}}\,\mathrm{tr}\left(\mathrm{Frob}_p \mid H^1_{\text{ét}}(E_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)\right)\right)$$

whenever $\xi(\mathrm{Frob}_p) = g$. Moreover, f_g depends only on the conjugacy class of g in $\mathrm{Aut}(C')$; more precisely, we have

$$f_g(x) = \begin{cases} 3x & \text{if } g = \mathrm{id}, \\ \pm x & \text{if } g \text{ has order 2 or 4}, \\ 0 & \text{if } g \text{ has order 3}. \end{cases}$$

Proof. Notice that the matrix representation of F_p has the form $A \otimes \mathrm{id}_3$, where A is the 2×2 matrix representation of Frob_p acting on $H^1_{\text{ét}}(E_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$. Also notice that $\xi(\mathrm{Frob}_p) \in \mathrm{GL}_6(\mathbb{Z})$ is of the form $\mathrm{id}_2 \otimes \Pi$, with Π a signed permutation matrix: indeed, the action of Frobenius on $\mathrm{Jac}(C^{\xi})$ permutes the three 1-dimensional factors in the decomposition $\mathrm{Jac}(C^{\xi})_{\overline{\mathbb{Q}}} \sim E^3$ and acts on each of them via an automorphism, which (since E does not have CM) can only be $\pm\mathrm{id}$. Since the action of the Frobenius at p on $H^1_{\text{ét}}((\mathrm{Jac}\,C^{\xi})_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$ is given by $F_p \circ \xi(\mathrm{Frob}_p)$, we obtain

$$\frac{1}{\sqrt{p}}\,\mathrm{tr}\left(\mathrm{Frob}_p \mid H^1_{\text{ét}}((\mathrm{Jac}\,C^{\xi})_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)\right) = \frac{1}{\sqrt{p}}\,\mathrm{tr}\left((A \otimes \mathrm{id}_3)(\mathrm{id}_2 \otimes \Pi)\right)$$

$$= \frac{1}{\sqrt{p}}\,\mathrm{tr}(A)\,\mathrm{tr}(\Pi)$$

$$= \frac{1}{\sqrt{p}}\,\mathrm{tr}\left(\mathrm{Frob}_p \mid H^1_{\text{ét}}(E_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)\right) \cdot \mathrm{tr}\,\Pi,$$

which proves the lemma (notice that a permutation matrix of order 2 or 4 has trace ±1, while a permutation matrix of order 3 has trace 0). For more details related, see also [MT10, Proposition 12]. $\square$

5.3.1. *Further Notation.* For simplicity, denote by b_p the normalized trace of the Frobenius at p acting on E and by a_p^{ξ} the normalized trace of Frob_p acting on $\mathrm{Jac}\,C^{\xi}$. We shall also write

$$f(g, p) := f_g(b_p) = f_g\left(\frac{1}{\sqrt{p}}\,\mathrm{tr}\left(\mathrm{Frob}_p \mid H^1_{\text{ét}}(E_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)\right)\right).$$

These quantities make sense for all but finitely many primes; let S be the set of bad primes at which either E or C^{ξ} has bad reduction.

16

We now compute the limiting distribution for the normalized traces of Frobenius a_p^ξ for the twist C^ξ (hence for all the twists, since we haven't made any assumptions about ξ). Let K_ξ be the fixed field of the kernel of ξ, that is the minimal extension of $\mathbb{Q}$ splitting the twist. By passing to the quotient, ξ induces an isomorphism $\mathrm{Gal}(K_\xi/\mathbb{Q}) \cong \xi(G_\mathbb{Q}) \subseteq \mathrm{Aut}(C')$.

Lemma 5.4. *Keeping the notation above, let $H := \xi(G_\mathbb{Q})$, and let $\mathcal{D}$ be the set of conjugacy classes of H. Then, for any $k \in \mathbb{N}$,*

$$\sum_{p \leq x, p \notin S} (a_p^\xi)^k = \sum_{D \in \mathcal{D}} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} f(D, p)^k.$$

Proof. We trivially have (for any $k \in \mathbb{N}$)

$$\sum_{p \leq x, p \notin S} (a_p^\xi)^k = \sum_{p \leq x, p \notin S} f(\xi(\mathrm{Frob}_p), p)^k = \sum_{h \in H} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) = h}} f(h, p)^k.$$

Now observe that f_h depends on h only through its conjugacy class in $\mathrm{Aut}(C')$, so a fortiori, it can only depend on h through its conjugacy class in $\xi(G_\mathbb{Q})$. Indeed, as $\xi(G_\mathbb{Q})$ is a subgroup of $\mathrm{Aut}(C')$, conjugacy in $\xi(G_\mathbb{Q})$ is a finer invariant than conjugacy in $\mathrm{Aut}(C')$. If D is a conjugacy class in H, then, it makes sense to set $f(D, p) := f(h, p)$ where h is any element of D.

It follows that if we let $\mathcal{D}$ be the set of conjugacy classes of H we have

$$\sum_{p \leq x, p \notin S} (a_p^\xi)^k = \sum_{D \in \mathcal{D}} \sum_{h \in D} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) = h}} f(h, p)^k$$

$$= \sum_{D \in \mathcal{D}} \sum_{h \in D} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) = h}} f(D, p)^k$$

$$= \sum_{D \in \mathcal{D}} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} f(D, p)^k.$$

$\square$

Lemma 5.5. *Retain the notation of subsubsection 5.3.1 and Lemma 5.4. Let $\pi(x)$ denote the number of primes bounded by x. We have*

$$\frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_p^\xi)^k = \sum_{D \in \mathcal{D}} \frac{|D|}{|H|} \left(\int_{SU(2)} f_D(\mathrm{tr}(g))^k dg \right) + o(1).$$

Proof. By the refined Sato-Tate conjecture for E, which asserts the equidistribution of b_p when we restrict to primes p having a given Artin symbol in the extension $K_\xi/\mathbb{Q}$ (cf. [MM10, Theorem 1]), we know that

$$\sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} f(D, p)^k = \left(\int_{SU(2)} f_D(\mathrm{tr}(g))^k dg \right) \left(\sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} 1 \right) + o_D \left(\sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} 1 \right) \quad (5.5.1)$$

as $x \to \infty$. We now apply Chebotarev's theorem, in the form

$$\frac{1}{\pi(x)} \left(\sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} 1 \right) = \frac{|D|}{|H|} + o_D(1) \text{ as } x \to \infty.$$

Dividing equation (5.5.1) by $\pi(x)$, we find

$$\frac{1}{\pi(x)} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} f(D, p)^k = \frac{|D|}{|H|} \left(\int_{SU(2)} f_D(\mathrm{tr}(g))^k dg \right) + o_D(1).$$

By summing over $D \in \mathcal{D}$ and using Lemma 5.4, we deduce

$$\frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_p^\xi)^k = \frac{1}{\pi(x)} \sum_{D \in \mathcal{D}} \sum_{\substack{p \leq x, p \notin S \\ \xi(\mathrm{Frob}_p) \in D}} f(D, p)^k$$

$$= \sum_{D \in \mathcal{D}} \frac{|D|}{|H|} \left(\int_{SU(2)} f_D(\mathrm{tr}(g))^k dg \right) + o(1).$$

$\square$

Proposition 5.6. *With notation as in subsubsection 5.3.1, let C^ξ be the twist of C' corresponding to a homomorphism $\xi \colon G_\mathbb{Q} \to \mathrm{Aut}(C')$; let H be the image of ξ; let b be the number of elements in H having order 2 or 4; and let $M_k := \int_{SU(2)} \mathrm{tr}(g)^k dg$. For every $k > 0$, we have*

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_p^\xi)^k = \frac{3^k + b}{|H|} M_k, \tag{5.6.1}$$

while for $k = 0$ we trivially have $\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_p^\xi)^0 = 1$.

Proof. Consider the elements of H as permutations in S_4. By Lemma 5.3,

$$f_D(x) = \begin{cases} 3x & \text{if } D = \{\mathrm{id}\}, \\ \pm x & \text{if the elements of } D \text{ have order 2 or 4}, \\ 0 & \text{if the elements of } D \text{ have order 3}. \end{cases}$$

Using this and Lemma 5.5, we have

$$\frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_p^\xi)^k = \sum_{D \in \mathcal{D}} \frac{|D|}{|H|} \left(\int_{SU(2)} f_D(\mathrm{tr}(g))^k dg \right) + o(1)$$

$$= \frac{|\{h \in H : \mathrm{ord}(h) = 2 \text{ or } 4\}|}{|H|} M_k + \frac{1}{|H|} \cdot 3^k M_k + o(1).$$

$\square$

18

5.7. **Distributions of all** a_i. We now generalize Proposition 5.6 to all coefficients of the characteristic polynomial of the normalized Frobenius automorphism. This is accomplished in the main result of this subsection, Proposition 5.11.

Lemma 5.8. *Let F_p^ξ be the automorphism of $H^1_{\text{ét}}((\text{Jac } C^\xi)_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$ given by the action of the Frobenius at p, and let $H_p^\xi(t)$ be the characteristic polynomial of F_p^ξ and $h_p^\xi(t) := \frac{1}{p^3} H_p^\xi(\sqrt{p}\, t)$. The polynomial $h_p^\xi(t)$, which we call the **normalized characteristic polynomial of the Frobenius at** p, can be computed purely in terms of b_p and of $\xi(\text{Frob}_p)$.*

Proof. The 6×6 matrix $\text{diag}_3(A)$ representing the automorphism F_p is block-diagonal, each of the three identical 2×2 blocks A being given by the action of Frobenius on the 2-dimensional vector space $H^1_{\text{ét}}(E_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$. As in the proof of Lemma 5.3, one sees that the matrix M representing the action of F_p^ξ is the tensor product of A with a certain 3×3 signed permutation matrix Π which only depends on $\xi(\text{Frob}_p)$. Let α_1, α_2 be the roots of the characteristic polynomial of A and π_1, π_2, π_3 be the roots of the characteristic polynomial of Π. The characteristic polynomial $H_p^\xi(t)$ of $M = A \otimes \Pi$ is then given by

$$H_p^\xi(t) = \prod_{j=1}^{3} \prod_{i=1}^{2} (t - \alpha_i \pi_j) = \prod_{j=1}^{3} (t^2 - (\alpha_1 + \alpha_2)\pi_j t + \alpha_1 \alpha_2 \pi_j^2).$$

Thus, we have that

$$h_p^\xi(t) = \frac{1}{p^3} \prod_{j=1}^{3} (pt^2 - \sqrt{p}(\alpha_1 + \alpha_2)\pi_j t + p\pi_j^2)$$

$$= \prod_{j=1}^{3} \left(t^2 - \frac{\alpha_1 + \alpha_2}{\sqrt{p}} \pi_j t + \pi_j^2\right) \tag{5.8.1}$$

$$= \prod_{j=1}^{3} (t^2 - b_p \pi_j t + \pi_j^2).$$

Since the π_j are determined by Π, which in turn is determined by $\xi(\text{Frob}_p)$, this proves the lemma. $\qquad\square$

As an immediate consequence of the explicit expression for $h_p^\xi(t)$ given by equation (5.8.1), we also have the following result, which generalizes Lemma 5.3:

Corollary 5.9. *There exist polynomials $f_{g,i}(x)$ for $i = 0, \ldots, 6$ and $g \in \text{Aut}(C')$ such that the following holds: for every cocycle $\xi \colon G_{\mathbb{Q}} \to \text{Aut}(C')$ and every prime p, the normalized characteristic polynomial of the Frobenius at p acting on $H^1_{\text{ét}}((\text{Jac } C^\xi)_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$ is given by*

$$h_p^\xi(t) = \sum_{i=0}^{6} f_{\xi(\text{Frob}_p),i}(b_p)t^i.$$

Moreover, the polynomials $f_{g,i}(x)$ only depend on g through its conjugacy class in $\text{Aut}(C') \cong S_4 \times \mathbb{Z}/2\mathbb{Z} \subset \text{GL}_3(\mathbb{Z})$, and are given explicitly as follows:

- $f_{g,0}(x) = f_{g,6}(x) = 1$;

19

- $f_{g,1}(x) = f_{g,5}(x) = -\operatorname{tr}(g)x;$
- $f_{g,2}(x) = f_{g,4}(x) = \operatorname{tr}(g^2) + \dfrac{x^2}{2}\left(\operatorname{tr}(g)^2 - \operatorname{tr}(g^2)\right);$
- $f_{g,3}(x) = -\frac{1}{3}\left(\operatorname{tr}(g)^3 - \operatorname{tr}(g^3) - 6\det(g)\right)x - x^3\det(g).$

Here in order to compute the trace and determinant of g we consider it as a 3×3 signed permutation matrix.

Remark 5.10. More generally, formula (5.8.1) shows the following: if $g \in GL_3(\mathbb{Z})$ is a signed permutation matrix and A is an arbitrary element of $SU(2)$, then $f_{g,i}(\operatorname{tr} A)$ is the ith coefficient of the characteristic polynomial of $A \otimes g$.

Since the functions $f_{g,i}$ are clearly continuous, the same argument that leads to Proposition 5.6 shows

Proposition 5.11. *Retaining the notation from Proposition 5.6, let*

$$h_p^\xi(t) = a_{6,p}^\xi t^6 + a_{5,p}^\xi t^5 + \cdots + a_{1,p}^\xi t + a_{0,p}^\xi$$

denote the normalized characteristic polynomial of the Frobenius at p acting on $\operatorname{Jac} C^\xi$. For each conjugacy class D in H, define $f_{D,i}(x) := f_{h,i}(x)$, where h is any element of D of positive determinant. The functions $f_{D,i}(x)$ are well-defined, and for each $i = 0,\ldots,6$ and every $k \geq 0$ we have

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x, p \notin S} (a_{i,p}^\xi)^k = \sum_{D \in \mathcal{D}} \frac{|D|}{|H|} \int_{SU(2)} f_{D,i}(\operatorname{tr}(x))^k dx.$$

5.12. **Completing the Proof.** For each of the Sato-Tate groups corresponding to twists of our curve C', we find in Proposition 5.13 the pushforward of the Haar measure along each coefficient of the normalized characteristic polynomial. We conclude our proof of the main Theorem A in Theorem 5.14.

Proposition 5.13. *Let G be a subgroup of $ST_{\mathrm{Tw}}(C)$ such that $G^0 = ST_{\mathrm{Tw}}(C)^0$; let H be the group of components of G, seen as a subgroup of $S_4 \subset \{x \in GL_3(\mathbb{Z}) : \det x = 1\}$; let $\Phi_i \colon G \to \mathbb{R}$ for $i = 0,\ldots,6$ be the map sending $g \in G$ to the ith coefficient of the characteristic polynomial of g; let μ be the Haar measure on G. By pushing forward μ along Φ_i, we obtain probability measures μ_i on $\mathbb{R}$, and we have*

$$\mathbb{E}_{\mu_i}[x^k] = \sum_{D \in \mathcal{D}} \frac{|D|}{|H|} \int_{SU(2)} f_{D,i}(\operatorname{tr}(x))^k dx$$

where $k \geq 0$ and the functions $f_{D,i}$ were defined in Corollary 5.9.

Proof. For every connected component M of $ST(C^\xi)$, there is a signed permutation matrix $\Pi_M \in GL_3(\mathbb{Z})$ such that

$$A \in SU(2) \mapsto A \otimes \Pi_M \in M$$

20

is a bianalytic bijection between $SU(2)$ and M. Furthermore, one sees that the characteristic polynomial of $A \otimes \Pi_M$ is determined by A and by Π_M. Thus one obtains

$$
\begin{aligned}
\int_{ST(C^\xi)} \Phi_i(x)^n \, d\mu_{ST(C^\xi)}(x) &= \sum_M \int_M \Phi_i(x)^n \, d\mu_{ST(C^\xi)}(x) \\
&= \sum_M \frac{1}{|G|} \int_{SU(2)} \Phi_i(A \otimes \Pi_M)^n \, d\mu_{SU(2)}(A) \\
&= \sum_M \frac{1}{|G|} \int_{SU(2)} f_{M,i}(tr(A))^n \, d\mu_{SU(2)}(A),
\end{aligned}
$$

where we have set $f_{M,i}(x) := f_{\Pi_M,i}(x)$ and $f_{g,i}(x)$ is defined in the statement of Corollary 5.9 (notice that we can consider Π_M as an element of $S_4 \times \mathbb{Z}/2\mathbb{Z} \subset GL_3(\mathbb{Z})$, see Remark 3.5). $\qquad \square$

Theorem 5.14. *Let C^ξ be any twist of C'. The generalized Sato-Tate conjecture is true for C^ξ.*

Proof. Let $a_{i,p}^\xi$ be the ith coefficient of the normalized characteristic polynomial of the Frobenius at p acting on $\operatorname{Jac} C^\xi$, μ be the Haar measure of $ST(C^\xi)$, and $\Phi_i \colon ST(C^\xi) \to \mathbb{R}$ be the map giving the ith coefficient of the characteristic polynomial of an endomorphism. Propositions 5.11 and 5.13 imply that for $i = 0, \ldots, 6$ the moments of the sequence $(a_{i,p}^\xi)_p$ are the same as the moments of the measure $\Phi_{i*}(\mu)$. This implies that for fixed ξ and i the sequence $(a_{i,p}^\xi)_p$ is equidistributed with respect to $\Phi_{i*}(\mu)$. $\qquad \square$

6. COMPUTING MOMENT SEQUENCES OF TWISTS

Below in Proposition 6.1, we compute the Sato-Tate distribution of the each twist by summing the contribution corresponding to the cycle types over each component in the Sato-Tate group of that twist; the complete list of distributions is given in Table 1. We also obtain explicit formulas for the moment sequences for the coefficients $a_i(A)(p)$ for $i = 1, 2, 3$ of each twist.

Proposition 6.1. *Let C^ξ be a twist of C' and let G be the component group of $ST(C^\xi)$; let b (resp. c) be the number of elements in G of order 2 (resp. 4), μ be the Haar measure of $ST(C^\xi)$. Let $\Phi_i \colon ST(C^\xi) \to \mathbb{R}$ be the map giving the ith coefficient of the characteristic polynomial of an endomorphism; let μ_i be the pushforward of μ along Φ_i. For $n > 0$, the moment sequences of μ_1, μ_2, and μ_3 are given by:*

$$
\mathbb{E}_{\mu_1}[x^n] = \frac{(3^n + b + c)}{|G|} \cdot \mathbb{E}_\phi[x^n],
$$

$$
\mathbb{E}_{\mu_2}[x^n] = \frac{1}{|G|} \mathbb{E}_\phi[(3 + 3x^2)^n] + \frac{b}{|G|} \mathbb{E}_\phi[(3 - x^2)^n] + \frac{c}{|G|} \mathbb{E}_\phi[(-1 + x^2)^n],
$$

$$
\mathbb{E}_{\mu_3}[x^n] = \frac{1}{|G|} \mathbb{E}_\phi[(6x + x^3)^n] + \frac{b+c}{|G|} \mathbb{E}_\phi[(x^3 - 2x)^n] + \frac{|G| - b - c - 1}{|G|} \mathbb{E}_\phi[(3x - x^3)^n]
$$

for $n = 0$ we trivially have $\mathbb{E}_{\mu_i}[x^0] = 1$ for $i = 1, 2, 3$.

Proof. Our purpose is to compute, for every $n \geq 0$, the integrals

$$\int_{ST(C^\xi)} \Phi_1(x)^n \, d\mu_{ST(C^\xi)}(x), \quad \int_{ST(C^\xi)} \Phi_2(x)^n \, d\mu_{ST(C^\xi)}(x), \quad \int_{ST(C^\xi)} \Phi_3(x)^n \, d\mu_{ST(C^\xi)}(x),$$

which as above we write as $\sum_M \int_M \Phi_i(x)^n \, dx$. Notice first that the functions $\Phi_i \colon ST(C^\xi) \to \mathbb{R}$ are invariant under conjugation in $GL_6(\mathbb{R})$, so that in particular they are also invariant under conjugation in $ST_{Tw}(C)$ since $ST(C^\xi) \subseteq ST_{Tw}(C) \subset GL_6(\mathbb{R})$.

Secondly, observe that the Haar measure of $ST(C^\xi)$ is invariant under conjugation as well, which implies that different connected components of $ST(C^\xi)$ that are conjugated in $ST_{Tw}(C)$ give the same contribution to the integral $\int_{ST(C^\xi)} \Phi_i(x)^n \, d\mu_{ST(C^\xi)}(x)$. Since the connected components of $ST(C^\xi)$ are a subset of the connected components of $ST_{Tw}(C)$, it suffices to compute

$$\int_M \Phi_i(x)^n \, d\mu_{ST_{Tw}(C)}(x)$$

for every connected component M of $ST_{Tw}(C)$. If M is a connected component of $ST(C^\xi)$, then

$$\int_M \Phi_i(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{|ST_{Tw}(C)/ST_{Tw}(C)^0|}{|G|} \int_M \Phi_i(x)^n \, d\mu_{ST_{Tw}(C)}(x)$$

because the total mass of M for the Haar measure of $ST(C^\xi)$ (resp. $ST_{Tw}(C)$) is $1/|G|$ (resp. $1/|ST_{Tw}(C)/ST_{Tw}(C)^0|$), so we will need to account for this rescaling in what follows.

Now notice that if $\sigma_1, \sigma_2 \in S_4$ are permutations that index two connected components M_1, M_2 of $ST_{Tw}(C)$, then M_1, M_2 are conjugate in $ST_{Tw}(C)$ if and only if σ_1, σ_2 are conjugate in S_4, which occurs if and only if σ_1, σ_2 have the same cycle type. Thus, it suffices to understand the contribution of the five families of connected components, corresponding to the five cycle-types in S_4.

(1) Identity permutation, $M = ST(C^\xi)^0$: In this case, we have $\Pi_M = \mathrm{id}_3$, the 3×3 identity matrix. In order to employ the formulas from Corollary 5.9, we first compute that $\det(\Pi_M) = 1$ and $\mathrm{tr}(\Pi_M) = \mathrm{tr}(\Pi_M^2) = \mathrm{tr}(\Pi_M^3) = 3$. We obtain $f_{\Pi_M,1}(x) = 3x$, $f_{\Pi_M,2}(x) = 3 + 3x^2$, and $f_{\Pi_M,3}(x) = -x^3 - 6x$, that is, the equalities

$$\Phi_1(A \otimes \Pi_M) = f_{\Pi_M,1}(\mathrm{tr}(A)) = -3\,\mathrm{tr}(A),$$
$$\Phi_2(A \otimes \Pi_M) = f_{\Pi_M,2}(\mathrm{tr}(A)) = 3 + 3\,\mathrm{tr}(A)^2,$$
$$\Phi_3(A \otimes \Pi_M) = f_{\Pi_M,3}(\mathrm{tr}(A)) = -\mathrm{tr}(A)^3 - 6\,\mathrm{tr}(A),$$

hold for all $A \in SU(2)$. Now observe that $ST_{Tw}(C)$ has 24 connected components and that $ST_{Tw}(C)^0$ is isomorphic to $SU(2)$, and hence the restriction of $\mu_{ST_{Tw}(C)}$ to

22

$ST_{Tw}(C)^0$ is $\frac{1}{24}$-th of the standard Haar measure on $SU(2)$. It follows that

$$|G| \int_{ST(C^\xi)^0} \Phi_1(x)^n \, d\mu_{ST(C^\xi)}(x) = 24 \int_{ST_{Tw}(C)^0} \Phi_1(A \otimes id)^n \, d\mu_{ST_{Tw}(C)}(A)$$

$$= \int_{SU(2)} \Phi_1(A \otimes id)^n \, d\mu_{SU(2)}(A)$$

$$= \int_{SU(2)} (-3\operatorname{tr}(A))^n \, d\mu_{SU(2)}(A)$$

$$= \mathbb{E}_\phi \left[(-3x)^n \right] = \mathbb{E}_\phi \left[(3x)^n \right],$$

$$|G| \int_{ST(C^\xi)^0} \Phi_2(x)^n \, d\mu_{ST(C^\xi)}(x) = \int_{SU(2)} \Phi_2(A \otimes id)^n \, d\mu_{SU(2)}(A)$$

$$= \int_{SU(2)} (3 + 3\operatorname{tr}(A)^2)^n \, d\mu_{SU(2)}(A)$$

$$= \mathbb{E}_\phi \left[3^n (1 + x^2)^n \right],$$

and likewise

$$|G| \int_{ST(C^\xi)^0} \Phi_3(x)^n \, dx = \int_{SU(2)} \Phi_3(A \otimes id)^n \, d\mu_{SU(2)}(A)$$

$$= \int_{SU(2)} (-\operatorname{tr}(A)^3 - 6\operatorname{tr}(A))^n \, d\mu_{SU(2)}(A)$$

$$= \mathbb{E}_\phi \left[(-1)^n (x^3 + 6x)^n \right].$$

(2) <u>Order-three permutation</u>, $M = \left(\begin{smallmatrix} & & id \\ id & & \\ & id & \end{smallmatrix} \right) ST(C^\xi)^0$: In this case we can take $\Pi_M = \left(\begin{smallmatrix} & & 1 \\ 1 & & \\ & 1 & \end{smallmatrix} \right)$. We have $\operatorname{tr}(\Pi_M) = \operatorname{tr}(\Pi_M^2) = 0$, $\operatorname{tr}(\Pi_M^3) = 3$ and $\det(\Pi_M) = 1$, whence $f_{\Pi_M,1}(x) = 0$, $f_{\Pi_M,2}(x) = 0$ and $f_{\Pi_M,3}(x) = 3x - x^3$. Proceeding as in the previous case, we obtain

$$\int_M \Phi_1(x)^n \, d\mu_{ST(C^\xi)}(x) = 0,$$

$$\int_M \Phi_2(x)^n \, d\mu_{ST(C^\xi)}(x) = 0,$$

$$\int_M \Phi_3(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[(3x - x^3)^n].$$

(3) <u>Transposition</u>, $M = \left(\begin{smallmatrix} & id & \\ id & & \\ & & id \end{smallmatrix} \right) ST(C^\xi)^0$: We have $\Pi_M = \left(\begin{smallmatrix} & 1 & \\ 1 & & \\ & & 1 \end{smallmatrix} \right)$, $\operatorname{tr}(\Pi_M) = \operatorname{tr}(\Pi_M^3) = 1$, $\operatorname{tr}(\Pi_M^2) = 3$, and $\det(\Pi_M) = -1$. It follows that $f_{\Pi_M,1}(x) = -x$, $f_{\Pi_M,2}(x) = 3 - x^2$

and $f_{\Pi_M,3}(x) = x^3 - 2x$, whence

$$\int_M \Phi_1(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[x^n],$$

$$\int_M \Phi_2(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[(3-x^2)^n],$$

$$\int_M \Phi_3(x)^n d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[(x^3-2x)^n].$$

(4) <u>Double transposition</u>, $M = \begin{pmatrix} \mathrm{id} & \\ & \mathrm{id} & \\ & & -\mathrm{id} \end{pmatrix} ST(C^\xi)^0$: We have $\Pi_M = \begin{pmatrix} 1 & \\ & 1 & \\ & & -1 \end{pmatrix}$, and since $\begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}$ and Π_M are similar in $GL_3(\mathbb{R})$, we have the same values for each of the integrals as in (3).

(5) <u>Four-cycle</u>, $M = \begin{pmatrix} & -\mathrm{id} & \\ \mathrm{id} & & \\ & & \mathrm{id} \end{pmatrix} ST(C^\xi)^0$: By setting $\Pi_M = \begin{pmatrix} & -1 & \\ 1 & & \\ & & 1 \end{pmatrix}$, we can compute that $\mathrm{tr}(\Pi_M) = \mathrm{tr}(\Pi_M^3) = 1$, $\mathrm{tr}(\Pi_M^2) = -1$, $\det(\Pi_M) = 1$, and whence $f_{\Pi_M,1}(x) = -x$, $f_{\Pi_M,2}(x) = x^2 - 1$ and $f_{\Pi_M,3}(x) = 2x - x^3$. Notice that

$$\int_{SU(2)} (2\,\mathrm{tr}(A) - \mathrm{tr}(A)^3)^n \, d\mu_{SU(2)}(A) = \int_{SU(2)} (-2\,\mathrm{tr}(A) + \mathrm{tr}(A)^3)^n \, d\mu_{SU(2)}(A)$$

since both integrals vanish if n is odd, and they are clearly equal if n is even. Thus we obtain

$$\int_M \Phi_1(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[x^n],$$

$$\int_M \Phi_2(x)^n \, d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[(x^2-1)^n],$$

$$\int_M \Phi_3(x)^n d\mu_{ST(C^\xi)}(x) = \frac{1}{|G|} \mathbb{E}_\phi[(x^3-2x)^n].$$

Finally, we need to sum over the connected components of each type: clearly there is precisely one component of type (1), and there are $|G| - b - c - 1$ components of type (2), b components of types (3) and (4), and c components of type (5). From the above computations, our result follows. $\qquad\square$

Remark 6.2. Notice that since $-\mathrm{id}$ belongs to $ST(C^\xi)^0$, for every connected component M of $ST(C^\xi)$ there are two possible choices of Π_M, namely the ones we have used and their opposites. However, different choices lead (as they should) to the same result: this is clear for the case of Φ_2, which, being quadratic functions of the eigenvalues, take on the same value on a matrix x and on its opposite $-x$. It is also true for Φ_1 and Φ_3, because all the odd-indexed moments vanish, while all the expressions of the form Φ_1^{2k}, Φ_3^{2k} are again even functions of their argument, hence insensitive to our arbitrary choice of sign.

Remark 6.3. In Tables 2, 3, and 4, we present theoretical and numerical computations of the first few terms of the moment sequences of μ_1, μ_2, and μ_3. The algorithm used to compute the numerical data comes from [HS16].

Notice that the curves corresponding to subgroups 4, 5, and 6 in Table 1 all have the same μ_1 moments, but not the same Sato-Tate distribution. Indeed, the μ_2 moments provide a distinction between the curve corresponding to subgroup 4 and the curves corresponding to subgroups 5, and 6, where the latter two curves have the same Sato-Tate distribution by Lemma 4.5.

APPENDIX A. DETERMINATION OF SATO-TATE GROUP FROM THE FIRST MOMENT
SEQUENCE

In general, the sequence of Frobenius traces does not determine the Sato-Tate group. However, in the case where the Sato-Tate distribution is $3_*\phi$, as defined at the beginning of Section 5, we show that this distribution can only arise from the Sato-Tate group $SU(2)_3$. In fact we prove something stronger: the only Sato-Tate group (of a 3-dimensional abelian variety) whose associated trace distribution has the same first five moments as $3_*\phi$ is conjugate to $SU(2)_3$.

Proposition A.1. *Let* A/K *be a 3-dimensional abelian variety over some number field* K. *Suppose that the first five moments of the trace distribution* μ_1 *associated with* $ST(A)$ *coincide with the first five moments of* $3_*\phi$, *that is, we have* $\mathbb{E}_{\mu_1}[x^n] = \mathbb{E}_{3_*\phi}[x^n]$ *for* $n = 0,\ldots,4$. *Then* A *is* K-*isogenous to the cube of an elliptic curve without CM, and* $ST(A)$ *is conjugate to* $SU(2)_3$ *inside* $GSp(6)$.

The proof of this result occupies the remainder of the section. Notate $G := ST(A)$. Here, G is a (reductive) compact real Lie group, acting naturally on $\mathbb{R}^6 \subseteq \mathbb{C}^6$. Let W be $\mathbb{C}^6$ interpreted as a representation of G, and write $W = \bigoplus_{i=1}^k W_i^{\oplus n_i}$ for the decomposition of W into irreducible G-modules. Let $\chi = \sum_{i=1}^k n_i\chi_i$ be the character of this representation W. Observe that χ is real, and hence the assumption on the moments sequence implies

$$\langle \chi, \chi \rangle = \int_G \text{tr}(g)^2 dg = \mathbb{E}_{\mu_1}[x^2] = 9 \Rightarrow \sum_{i=1}^k n_i^2 = 9,$$

using $\mathbb{E}_{3_*\phi}[x^2] = 9$ (see Remark 5.1). On the other hand, we have that $\sum n_i \dim W_i = 6$, which leaves precisely two possibilities:

(1) either $k = 1$, $n_1 = 3$ and $\dim W_1 = 2$,
(2) or $k = 3$, $n_1 = n_2 = 2$, $n_3 = 1$, $\dim W_1 = \dim W_2 = 1$ and $\dim W_3 = 2$.

Let $\mathfrak{g}$ be the Lie algebra of $G_\mathbb{C}$, and write $\mathfrak{g} = \bigoplus_{j=1}^m \mathfrak{g}_j \oplus \mathfrak{c}$ with every $\mathfrak{g}_i$ simple and $\mathfrak{c}$ abelian. Each representation W_i can be written as $W_{i1} \boxtimes \cdots \boxtimes W_{im} \boxtimes \psi_i$, where W_{ij} is an irreducible representation of $\mathfrak{g}_j$ and ψ_i is a character of $\mathfrak{c}$. Notice that W is a faithful representation of G, so for each $j = 1,\ldots,m$ there exists an i such that W_i is a faithful representation of $\mathfrak{g}_j$. In particular, W_{ij} is a faithful representation of $\mathfrak{g}_j$, and since $\dim W_{ij} \leq 2$ we obtain that $\mathfrak{g}_j$ has a faithful representation of dimension at most 2. This is only possible if $\mathfrak{g}_j$ is $\mathfrak{sl}_2$ for all j, because no other simple Lie algebra admits an irreducible 2-dimensional faithful representation.

In both cases (1) and (2), up to isomorphism (of G-modules) there is only one irreducible submodule W_i of dimension 2, which implies that m (the number of copies of $\mathfrak{sl}_2$ appearing in $\mathfrak{g}$) is at most 1. Also observe that m cannot be zero, because an abelian Lie algebra does not admit any irreducible 2-dimensional faithful representation over $\mathbb{C}$. We can therefore write $\mathfrak{g} = \mathfrak{sl}_2 \oplus \mathfrak{c}$ and $W_i = W_{i1} \boxtimes \psi_i$, where W_{i1} is either trivial or isomorphic to the standard representation of $\mathfrak{sl}_2$ and ψ_i is a character of $\mathfrak{c}$. To complete the proof, we will now verify Proposition A.1 holds in both cases (1) and (2).

(1) Suppose that we are in case (1) above. We claim that $\mathfrak{c}$ is trivial. To show this, we restrict our attention to a maximal compact Lie subalgebra of $\mathfrak{g}$, which is necessarily of the form $\mathfrak{su}_2 \oplus \mathfrak{c}_\mathbb{R}$. By faithfulness, there exists i such that ψ_i is nontrivial; as W

26

comes from a real representation and $W_{i1} \boxtimes \psi_i \subseteq W$ we also have $\overline{W_{i1}} \boxtimes \overline{\psi_i} \subseteq W$. We have $\overline{W_{i1}} = W_{i1}$ both for the trivial and the standard representation of $\mathfrak{su}_2$, so $W_{i1} \boxtimes \overline{\psi_i} \subseteq W$. On the other hand we have $\overline{\psi_i} \neq \psi_i$: indeed, ψ_i is obtained (by differentiation and extension of scalars) from a real representation ρ_i of the maximal central torus $\mathbb{T}$ of $ST(A)$. As $ST(A)$ is compact, $\mathbb{T}$ is a product of copies of S^1, hence its representation ρ_i satisfies $\overline{\rho_i} = \rho_i^{-1}$, because all the eigenvalues of $\rho_i(x)$ lie on the unit circle, for all $x \in \mathbb{T}$. Extending scalars and differentiating we find $\overline{\psi_i} = -\psi_i$, so in particular $\overline{\psi_i} \neq \psi_i$ since ψ_i is nontrivial. This immediately leads to a contradiction, because on the one hand we have $W_{i1} \boxtimes \overline{\psi_i} \not\cong W_{i1} \boxtimes \psi_i$ and on the other all irreducible submodules of W are isomorphic. Hence $\mathfrak{c} = (0)$. Since $\mathfrak{c} = (0)$, we obtain that G^0 is abstractly isomorphic to $SU(2)$, which in turn implies that the Hodge group of A is (abstractly isomorphic to) $SL(2)$.

To complete this case, we will show that in fact $ST(A)$ is not only isomorphic to $SU(2)$, but in fact is conjugate to $SU(2)_3$ inside $GSp(6)$. Write $A_{\overline{K}}$ (up to isogeny) as a product of simple abelian varieties, $A_{\overline{K}} \sim \prod_{i=1}^{s} A_i^{t_i}$. If $s = 1$, this leads immediately to a contradiction, because no absolutely simple abelian threefold has Hodge group isomorphic to $SL(2)$. If instead A is nonsimple, all its absolutely simple factors are of dimension at most 2. By [Lom14, Corollary 1.2], we have

$$SL(2) \cong Hg(A) \cong \prod_{i=1}^{s} Hg(A_i),$$

where each factor on the right is nontrivial (because no abelian variety has trivial Hodge group). This clearly implies $s = 1$, $Hg(A_1) = SL(2)$, and $t_1 \dim A_1 = 3$: it is immediate to check that this is only possible if A_1 is an elliptic curve without CM and $t_1 = 3$. In turn, this means that A is *geometrically* isogenous to the cube of a non-CM elliptic curve, so that $ST(A)^0 = SU(2)_3$ (up to conjugacy in $GSp(6)$). Finally, Table 2 shows that for a Sato-Tate group with this identity component we can have $\mathbb{E}_{\mu_1}[x^2] = 9$ only when $ST(A)$ is connected. That is, if and only if $ST(A) = ST(A)^0 = SU(2)_3$ as claimed. Notice that the argument for this case only involves the first three moments of μ_1, and also shows that the equality $ST(A) = SU(2)_3$ is equivalent to A being K-isogenous to the cube of an elliptic curve without CM.

(2) In case (2), the same argument as above leads to the conclusion that $\overline{W_3} = W_3$, so that $W_1 = \overline{W_2}$ is given by a character ψ of $\mathfrak{c}$, while $\mathfrak{c}$ acts trivially on W_3 (which otherwise would not be self-conjugate). If $\mathfrak{c}$ is trivial, the same argument as in the previous case leads to the conclusion that A is K-isogenous to the cube of an elliptic curve. This is absurd under the hypotheses of case (2), because W would then be isomorphic to the direct sum of three identical copies of the same representation, which is incompatible with $W_1 \not\cong W_3$. To conclude the proof, we will assume $\mathfrak{c}$ is nontrivial and derive a contradiction with the assumption $\mathbb{E}_{\mu_1}[x^4] = 162$. Notice that there exist abelian threefolds for which we have $W_1 = \overline{W_2}$, $\overline{W_3} = W_3$, and $\mathfrak{c}$ nontrivial: an example is given by $A = E_1^2 \times E_2$, where E_1 is an elliptic curve admitting CM over K and E_2 is an elliptic curve without potential CM. As we now show, however, the Sato-Tate group of any such threefold does not satisfy $\mathbb{E}_{\mu_1}[x^4] = 162$.

We write the character χ of W as $2\psi + 2\overline{\psi} + \eta$, where ψ is a group morphism $G \to \mathbb{C}^\times$ and η is the character of an irreducible, 2-dimensional, real representation of G.

Lemma A.2. *The integrals $\int_G \psi^n \eta^k dg$ and $\int_G \overline{\psi}^n \eta^k dg$ vanish for all $n > 0$ and $k \geq 0$.*

Proof. Notice that the statements for ψ and $\overline{\psi}$ are clearly equivalent, so we only consider the former case. For the sake of simplicity, we identify representations with their characters; in particular, if ω is the character of a representation V, then ω^k is identified with $V^{\otimes k}$.

Recall that η is real, so the number $\int_G \psi^n \eta^k dg = \langle \psi^n, \eta^k \rangle$ is the multiplicity of the 1-dimensional representation ψ^n as a constituent of the representation η^k. We want to prove that this number is zero, so it suffices to show that ψ^n is not isomorphic to a G^0-submodule of η^k (a fortiori, this implies that there is no G-equivariant, nonzero map from ψ^n to η^k). It also suffices to show that ψ^n is not a subrepresentation of η^k for the action of the (real) Lie algebra $\mathfrak{g}_\mathbb{R}$ of G^0. We have already shown that $\mathfrak{g}_\mathbb{R} = \mathfrak{su}_2 \oplus \mathfrak{c}_\mathbb{R}$, and that $\eta = \mathrm{Std} \boxtimes 1$, where Std is the standard 2-dimensional representation of $\mathfrak{su}_2$ and 1 denotes the trivial representation of $\mathfrak{c}$. It follows easily that for $k \geq 0$ the only possible 1-dimensional constituents of $\eta^k = (\mathrm{Std})^{\otimes k} \boxtimes 1$ are copies of the trivial representation of $\mathfrak{g}_\mathbb{R}$, which, in particular, are not isomorphic to the non-trivial 1-dimensional representation ψ^n. It follows that $\langle \psi^n, \eta^k \rangle$ vanishes, as we wanted to show. $\square$

We now compute $\int_G \chi^4 dg$ in two different ways. On the one hand, this is the fourth moment of the Sato-Tate distribution of traces associated with G, so it is equal to $\mathbb{E}_{3_*\phi}[x^4] = 162$ (see Remark 5.1) by assumption. On the other hand, using Lemma A.2 and the equality $\psi\overline{\psi} = 1$, we find

$$\int_G \chi^4 dg = \int_G \left(48\eta^2 \psi\overline{\psi} + 96\psi^2\overline{\psi}^2 + \eta^4\right) dg$$

$$= \int_G \left(48\eta^2 + 96 + \eta^4\right) dg$$

$$= 96 + 48\langle \eta, \eta \rangle + \int_G \eta^4 dg$$

$$= 144 + \int_G \eta^4 dg.$$

Observe now that η is a 2-dimensional representation, so $|\eta(g)| \leq 2$ for all $g \in G$. It follows that $|\int_G \eta^4 dg| \leq \int_G 2^4 dg = 16$, whence $162 = \int_G \chi^4 dg \leq 144 + 16 = 160$. This is a contradiction, completing the proof of Proposition A.1.

APPENDIX B. TABLES

	Group	Generators	Equation of twist	Minimal field trivializing the twist	Normalized trace distributions
1	Trivial	$\{\mathrm{id}\}$	$\begin{cases} x^2+y^2+z^2=0 \\ -2t^2=x^4+y^4+z^4 \end{cases}$	$\mathbb{Q}$	$3_*\phi$
2	$\mathbb{Z}/2\mathbb{Z}$	$(1,2)$	$y^2=x^8-56x^4+16$	$\mathbb{Q}(i)$	$\frac{1}{2}(\phi)+\frac{1}{2}(3_*\phi)$
3	$\mathbb{Z}/2\mathbb{Z}$	$(1,4)(2,3)$	$y^2=-x^8-14x^4-1$	$\mathbb{Q}(i)$	$\frac{1}{2}(\phi)+\frac{1}{2}(3_*\phi)$
4	$\mathbb{Z}/4\mathbb{Z}$	$(1,2,3,4)$	$y^2=-x^8-x^7-7x^6+7x^5-7x^3-7x^2+x-1$	$\mathbb{Q}(\zeta_5)$	$\frac{3}{4}(\phi)+\frac{1}{4}(3_*\phi)$
5	$(\mathbb{Z}/2\mathbb{Z})^2$	$(1,2)(3,4),(1,3)(2,4)$	$y^2=-x^8-56x^4-16$	$\mathbb{Q}(\zeta_8)$	$\frac{3}{4}(\phi)+\frac{1}{4}(3_*\phi)$
6	$(\mathbb{Z}/2\mathbb{Z})^2$	$(1,2),(3,4)$	$y^2=x^8-14x^4+1$	$\mathbb{Q}(\zeta_8)$	$\frac{3}{4}(\phi)+\frac{1}{4}(3_*\phi)$
7	D_4	$(1,2,3,4),(1,3)$	$y^2=x^8+2x^7-14x^6+14x^5-14x^4+14x^3-14x^2+2x+1$	$\mathbb{Q}(i,\sqrt[4]{3})$	$\frac{7}{8}(\phi)+\frac{1}{8}(3_*\phi)$
8	$\mathbb{Z}/3\mathbb{Z}$	$(1,2,3)$	$\begin{cases} x^2+y^2+1=0 \\ 6t^2=-23(x^4+y^4+1)+16x-12x^2-20x^3 \\ \quad +20y-12xy-12x^2y-16x^3y-12y^2 \\ \quad +12xy^2-12x^2y^2-16y^3+20xy^3 \end{cases}$	$\mathbb{Q}(\zeta_9)^+$	$\frac{1}{3}(3_*\phi)+\frac{2}{3}(\delta_0)$
9	S_3	$(1,2,3),(1,2)$	$y^2=-6x^7+21x^4+12x$	$\mathbb{Q}(\zeta_3,\sqrt[3]{2})$	$\frac{1}{6}(3\phi)+\frac{3}{6}(\phi)+\frac{2}{6}(\delta_0)$
10	A_4	$(1,2,3),(1,2)(3,4)$	$y^2=-x^8+4x^7-28x^6+28x^5+14x^4+28x^3-196x^2+100x-61$	Splitting field of $x^4+2x^3+6x^2+6x+3$	$\frac{1}{12}(3\phi)+\frac{3}{12}(\phi)+\frac{8}{12}(\delta_0)$
11	S_4	$(1,2,3,4),(1,2)$	$y^2=x^8-14x^7+84x^6-294x^5+651x^4-882x^3+630x^2-126x-54$	Splitting field of x^4-6x^2+2x+6	$\frac{1}{24}(3_*\phi)+\frac{15}{24}(\phi)+\frac{8}{24}(\delta_0)$

TABLE 1. Explicit twists realizing all possible Sato-Tate groups

Subgroup	M_2	M_4	M_6	M_8	M_{10}
1 (theoretical)	9	162	3645	91854	2480058
1 (numerical)	8.999	161.988	3644.890	91854.573	2480122.102
2 (theoretical)	5	82	1825	45934	1240050
2 (numerical)	4.999	81.973	1824.235	45910.323	1239239.907
3 (theoretical)	5	82	1825	45934	1240050
3 (numerical)	4.999	81.973	1824.235	45910.326	1239239.988
4 (theoretical)	3	42	916	22974	620046
4 (numerical)	2.999	41.972	914.184	22949.933	619320.101
5 (theoretical)	3	42	916	22974	620046
5 (numerical)	2.999	41.973	914.37	22958.227	619599.349
6 (theoretical)	3	42	916	22974	620046
6 (numerical)	2.999	41.973	914.373	22958.228	619599.369
7 (theoretical)	2	22	460	11494	310044
7 (numerical)	1.999	21.978	459.311	11471.005	309269.022
8 (theoretical)	3	54	1215	30618	826686
8 (numerical)	2.999	53.972	1214.282	30600.607	826296.848
9 (theoretical)	2	28	610	153316	413364
9 (numerical)	1.999	27.987	609.764	15311.966	413302.154
10 (theoretical)	1	14	305	7658	206682
10 (numerical)	1.000	13.991	304.674	7647.112	206330.548
11 (theoretical)	1	8	155	3836	103362
11 (numerical)	1.000	7.983	154.585	3825.122	103074.236

TABLE 2. Table of μ_1 moment sequences

Subgroup	M_1	M_2	M_3	M_4	M_5
1 (theoretical)	6	45	405	4131	45684
1 (numerical)	6.000	44.997	404.978	4130.861	45683.553
2 (theoretical)	4	25	209	2083	22890
2 (numerical)	4.000	24.995	208.936	2082.168	22878.772
3 (theoretical)	4	25	209	2083	22890
3 (numerical)	4.000	24.995	208.936	2082.168	22878.773
4 (theoretical)	2	13	105	1043	11448
4 (numerical)	2.000	12.995	104.944	1042.139	11436.874
5 (theoretical)	3	15	111	1059	11493
5 (numerical)	3.000	14.995	110.941	1058.329	11485.207
6 (theoretical)	3	15	111	1059	11493
6 (numerical)	3.000	14.995	110.941	1058.329	11485.208
7 (theoretical)	2	9	59	539	5772
7 (numerical)	2.000	8.996	58.945	538.250	5761.490
8 (theoretical)	2	15	135	1377	15228
8 (numerical)	2.000	14.995	134.937	1376.264	15219.817
9 (theoretical)	2	10	74	706	7662
9 (numerical)	2.000	9.998	73.974	705.749	7659.752
10 (theoretical)	1	5	37	353	3831
10 (numerical)	1.000	4.999	36.977	352.657	3826.140
11 (theoretical)	1	4	22	186	1941
11 (numerical)	1.000	3.997	21.961	185.552	1935.804

TABLE 3. Table of μ_2 moment sequences

Subgroup	M_2	M_4	M_6	M_8
1 (theoretical)	65	11076	2561186	685324780
1 (numerical)	64.995	11075.733	2561214.275	685313387.267
2 (theoretical)	33	5540	1280610	342662572
2 (numerical)	32.991	5537.488	1279721.846	342293549.829
3 (theoretical)	33	5540	1280610	342662572
3 (numerical)	32.991	5537.488	1279721.927	342293572.882
4 (theoretical)	17	2772	640322	171331468
4 (numerical)	16.991	2769.460	639567.852	1171083665.383
5 (theoretical)	17	2772	640322	171331468
5 (numerical)	16.991	2770.097	639840.117	171172626.176
6 (theoretical)	17	2772	640322	171331468
6 (numerical)	16.991	2770.097	639840.145	171172628.271
7 (theoretical)	9	1388	320178	85665916
7 (numerical)	8.993	1385.715	319374.334	8537815.326
8 (theoretical)	23	3696	853742	228441640
8 (numerical)	22.991	3693.961	853369.706	228400307.404
9 (theoretical)	12	1850	426888	114221002
9 (numerical)	11.996	1849.356	42681.689	114211031.306
10 (theoretical)	7	928	213454	57110536
10 (numerical)	6.997	926.945	213098.809	56995860.860
11 (theoretical)	4	466	106744	28555450
11 (numerical)	3.994	464.747	106461.595	28497167.689

TABLE 4. Table of μ_3 moment sequences

REFERENCES

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[BK15] Grzegorz Banaszak and Kiran S. Kedlaya, *An algebraic Sato-Tate group and Sato-Tate conjecture*, Indiana university mathematics journal **64** (2015), no. 1, 245–274.

[BN15] Peter Bruin and Filip Najman, *Hyperelliptic modular curves and isogenies of elliptic curves over quadratic fields*, LMS Journal of Computation and Mathematics **18** (2015), no. 01, 578–602.

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Victor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compositio Mathematica **148** (2012), no. 05, 1390–1442.

[FKS16] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato-Tate groups of some weight 3 motives*, Contemporary Mathematics **663** (2016), no. 05, 66–112.

[FS14] Francesc Fité and Andrew 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, 543–585.

[FS16] ———, *Sato-Tate groups of $y^2 = x^8 + c$ and $y^3 = x^7 - cx$*, Contemporary Mathematics **663** (2016), no. 05, 112 – 136.

[GSS12] Jaime Gutierrez, David Sevilla, and Tanush Shaska, *Hyperelliptic curves of genus 3 with prescribed automorphism group*, arXiv:1209.2938 (2012).

[HS16] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time* II, Contemporary Mathematics **663** (2016), 127–148.

[Lom14] Davide Lombardo, *On the ℓ-adic Galois representations attached to nonsimple abelian varieties*, Annales de l'Institut Fourier **66** (2014), no. 3, 1217–1245.

[Lor14] Elisa Lorenzo, *Arithmetic properties of non-hyperelliptic genus 3 curves*, Ph.D. thesis, Universitat Politécnica de Catalunya, 2014.

[MM10] M. Ram Murty and V. Kumar Murty, *The Sato-Tate conjecture and generalizations*, Math. Newsl. **19** (2010), no. Sp. Number 1, 247–257. MR 3012726

[MT10] Stephen Meagher and Jaap Top, *Twists of genus three curves over finite fields*, Finite Fields Appl. **16** (2010), no. 5, 347–368. MR 2678623

[Ser12] Jean-Pierre Serre, *Lectures on $N_X(p)$*, CRC Press, 2012.

[Sha58] I.R. Shafarevich, *The imbedding problem for splitting extensions*, Dokl. Akad. Nauk SSR **120** (1958), no. 6, 1217–1219.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[Sut16] Andrew V. Sutherland, *Sato-Tate distributions*, arXiv:1604.01256 (2016).

DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802
E-mail address: `sza149@psu.edu`

INSTITUT DE MATHÉMATIQUES DE JUSSIEU - PARIS RIVE GAUCHE (IMJ-PRG) UP7D - BÂTIMENT SOPHIE GERMAIN - 75205 PARIS FRANCE
E-mail address: `victoria.cantoral-farfan@imj-prg.fr`

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CA 94305
E-mail address: `aaronlandesman@stanford.edu`

DÉPARTEMENT DE MATHÉMATIQUES D'ORSAY, UNIVERSITÉ PARIS-SUD, 91400 ORSAY (FRANCE)
E-mail address: `davide.lombardo@math.u-psud.fr`

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GA 30322
E-mail address: `jmorrow4692@gmail.com`