Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$.

Francesc Fité and Andrew V. Sutherland

Abstract. We consider the distribution of normalized Frobenius traces for two families of genus 3 hyperelliptic curves over $\mathbb{Q}$ that have large automorphism groups: $y^2 = x^8 + c$ and $y^2 = x^7 - cx$ with $c \in \mathbb{Q}^*$. We give efficient algorithms to compute the trace of Frobenius for curves in these families at primes of good reduction. Using data generated by these algorithms, we obtain a heuristic description of the Sato-Tate groups that arise, both generically and for particular values of $c$. We then prove that these heuristic descriptions are correct by explicitly computing the Sato-Tate groups via the correspondence between Sato-Tate groups and Galois endomorphism types.

Contents

1. Introduction
2. Background
3. Trace formulas
4. Guessing Sato-Tate groups
5. Determining Sato-Tate groups
6. Galois endomorphism types
References

1. Introduction

In this paper we consider two families of hyperelliptic curves over $\mathbb{Q}$:

$C_1: y^2 = x^8 + c, \quad C_2: y^2 = x^7 - cx.$

For $c \in \mathbb{Q}^*$, these equations define hyperelliptic curves of genus 3 with good reduction at primes $p > 3$ for which $v_p(c) = 0$ (in fact, $C_1$ also has good reduction at 3). For each such $p$ we have the trace of Frobenius

$$t_p(C_i) := p + 1 - \#C_i(\mathbb{F}_p),$$

2010 Mathematics Subject Classification. Primary 11M50; Secondary 11G10, 11G20, 14G10, and 14K15.

The first author received support from the German Research Council via SFB 701 and SFB/TR 45.

The second author received support from NSF grant DMS-1115455.

©2016 by the authors
where $\overline{C}_i$ denotes the reduction of $C_i$ modulo $p$. From the Weil bounds, we know that $t_p$ lies in the interval $[-6\sqrt{p}, 6\sqrt{p}]$. We wish to study the distribution of normalized Frobenius traces $t_p/\sqrt{p} \in [-6, 6]$, as $p$ varies over primes of good reduction up to a bound $N$.

The generalized Sato-Tate conjecture predicts that as $N \to \infty$ this distribution converges to the distribution of traces in the Sato-Tate group, a compact subgroup of USp(6) associated to the Jacobian of the curve. For the two families considered here, the curves $C_i$ have Jacobians that are $\mathbb{Q}$-isogenous to the product of an elliptic curve and an abelian surface. This allows us to apply the classification of Sato-Tate groups for abelian surfaces obtained in [FKRS12] to determine the Sato-Tate groups that arise. This is achieved in §5.

After recalling the definition of the Sato-Tate group of an abelian variety in §2, we begin in §3 by deriving formulas for the Frobenius trace $t_p(C_i)$ in terms of the Hasse-Witt matrix of $\overline{C}_i$. These formulas allow us to design particularly efficient algorithms for computing $t_p(C_i)$. In §4, under the assumption of the Sato-Tate conjecture, we use the numerical data obtained by applying these algorithms to heuristically guess the isomorphism class of the Sato-Tate groups of $C_1$ and $C_2$. The explicit computation in §5 proves that, in fact, these guesses are correct, without appealing to the Sato-Tate conjecture.

Strictly speaking, §4 and §5 are independent of each other. However, we should emphasize that in the process of achieving our results, there was a constant and mutually beneficial interplay between the two distinct approaches.

Up to dimension 3, the Sato-Tate group of an abelian variety defined over a number field $k$ is determined by its ring of endomorphisms over an algebraic closure of $k$. Although the Sato-Tate group does not capture the ring structure of the endomorphisms, it does codify the $\mathbb{R}$-algebra generated by the endomorphism ring, and the structure of this $\mathbb{R}$-algebra as a Galois module, what we refer to as the Galois endomorphism type of the abelian variety. As an example, in §6 we compute the Galois endomorphism type of the Jacobian of $C_2$.

The problem of analysing the Frobenius trace distributions and determining the Sato-Tate groups that arise in these two families was originally posed as part of a course given by the authors at the winter school Frobenius Distributions on Curves held in February, 2014, at the Centre International de Rencontres Mathématiques in Luminy. This problem turned out to be more challenging than we anticipated (the analogous question in genus 2 is quite straight-forward); this article represents a solution.

1.1. Acknowledgements. Both authors are grateful to the Centre International de Rencontres Mathématiques for the hospitality and financial support provided, and to the anonymous referee.

2. Background

We start by briefly recalling the definition of the Sato-Tate group of an abelian variety $A$ defined over a number field $k$, and set some notation. For a more detailed presentation we refer to [Ser12 Chap. 8] or [FKRS12 §2].

---

1 As we shall see, this abelian surface may itself be $\mathbb{Q}$-isogenous to a product of elliptic curves and is in any case never simple over $\mathbb{Q}$. 

---

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.
2.1. The Sato-Tate group of an abelian variety. Let \( \overline{k} \) denote a fixed algebraic closure of \( k \), and let \( g \) be the dimension of \( A \). For each prime \( \ell \) we have a continuous homomorphism

\[
g_{A,\ell} : \text{Gal}(\overline{k}/k) \to \text{GSp}_{2g}(\mathbb{Q}_\ell)
\]

arising from the action of \( \text{Gal}(\overline{k}/k) \) on the rational Tate module \((\varprojlim A[\ell^n]) \otimes \mathbb{Q}\). Here \( \text{GSp} \) denotes the group of symplectic similitudes, which preserve a symplectic form up to a scalar; in our setting the preserved symplectic form arises from the Weil pairing. Let \( G_\ell \) be the Zariski closure of the image of \( g_{A,\ell} \), and let \( G_1^\ell \) be the kernel of the similitude character \( G_\ell \to \mathbb{Q}_\ell^* \). We now choose an embedding \( \iota : \mathbb{Q}_\ell \to \mathbb{C} \), and for each prime ideal \( \mathfrak{p} \) of the ring of integers of \( k \), let \( \text{Frob}_\mathfrak{p} \) denote an arithmetic Frobenius at \( \mathfrak{p} \) and let \( N(\mathfrak{p}) \) be the cardinality of its residue field.

**Definition 2.1.** The Sato-Tate group of \( A \), denoted \( \text{ST}(A) \), is a maximal compact subgroup of \( G_1^\ell \otimes \iota \mathbb{C} \). For each prime \( \mathfrak{p} \) of good reduction for \( A \), let

\[
s(\mathfrak{p}) := g_{A,\ell}(\text{Frob}_\mathfrak{p}) \otimes \iota N(\mathfrak{p})^{-1/2}.
\]

Let \( \text{USp}(2g) \) denote the group of \( 2g \times 2g \) complex matrices that are unitary and preserve a fixed symplectic form; this is a real Lie group of dimension \( g(2g+1) \). One can show that \( \text{ST}(A) \) is well-defined up to conjugacy in \( \text{USp}(2g) \), and that \( s(\mathfrak{p}) \) determines a conjugacy class in \( \text{ST}(A) \).

**Conjecture 2.2** (generalized Sato-Tate). Let \( X \) denote the set of conjugacy classes of \( \text{ST}(A) \). Then:

(i) The conjugacy class of \( \text{ST}(A) \) in \( \text{USp}(2g) \) and the conjugacy classes \( s(\mathfrak{p}) \) in \( \text{ST}(A) \) are independent of the choice of the prime \( \ell \) and the embedding \( \iota \).

(ii) When the primes \( \mathfrak{p} \) are ordered by norm, the \( s(\mathfrak{p}) \) are equidistributed on \( X \) with respect to the projection of the Haar measure of \( \text{ST}(A) \) on \( X \).

It follows from [BK15] that part (i) of the above conjecture is true for \( g \leq 3 \). We next summarize some basic properties of the Sato-Tate group that we will need in our forthcoming discussion. If \( L/k \) is a field extension, we write \( A_L \) for the base change of \( A \) to \( L \). We denote by \( K_A \) the minimal extension \( L/k \) over which all the endomorphisms of \( A \) are defined, that is, the minimal extension for which \( \text{End}(A_L) \cong \text{End}(A_k) \).

The Sato-Tate group \( \text{ST}(A) \) is a compact real Lie group, but it need not be connected. We use \( \text{ST}^0(A) \) to denote the connected component of the identity.

**Proposition 2.3** (Prop. 2.17 of [FKRS12]). If \( g \leq 3 \), then the group of connected components \( \text{ST}(A)/\text{ST}^0(A) \) is isomorphic to \( \text{Gal}(K_A/k) \).

This proposition implies, in particular, that a prime \( \mathfrak{p} \) of good reduction for \( A \) splits completely in \( K_A \) if and only if \( s(\mathfrak{p}) \in \text{ST}^0(A) \). One can in fact show a little bit more: for any algebraic extension \( L/k \), the Sato-Tate group \( \text{ST}(A_L) \) is a subgroup of \( \text{ST}(A) \) with \( \text{ST}^0(A_L) = \text{ST}^0(A) \) and

\[
\text{ST}(A_L)/\text{ST}^0(A_L) \cong \text{Gal}(K_A/(K_A \cap L)) \subseteq \text{Gal}(K_A/k).
\]

2.2. Galois endomorphism types. We now work in the category \( \mathcal{C} \) 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 \( G \). A morphism \( \Phi : (G,E) \to (G',E') \) of \( \mathcal{C} \) consists of a pair \( \Phi := (\phi_1, \phi_2) \),
where $\phi_1: G \to G'$ is a morphism of groups and $\phi_2: E \to E'$ is an equivariant morphism of $\mathbb{R}$-algebras, that is,

$$\phi_2(\phi_1(g)e) = \phi_2(g)(\phi_1(e)) \quad \text{for all } g \in G \text{ and } e \in E.$$ 

**Definition 2.4.** The Galois endomorphism type of $A$ is the isomorphism class in $\mathcal{C}$ of the pair $(\Gal(K_A/k), \End(A_{K_A}) \otimes \mathbb{Z} \mathbb{R})$.

By [FKRS12] Prop. 2.19], for $g \leq 3$, the Galois endomorphism type is determined by the Sato-Tate group (in fact, the proof of this statement is effective, as we will illustrate in §6). This result admits a converse statement at least for $g \leq 2$.

**Theorem 2.5 (Thm. 4.3 of [FKRS12]).** For fixed $g \leq 2$, the Sato-Tate group and the Galois endomorphism type of an abelian variety $A$ defined over a number field $k$ uniquely determine each other. For $g = 1$ (resp. $g = 2$) there are $3$ (resp. $52$) possibilities for the Galois endomorphism type, all of which arise for some choice of $A$ and $k$.

For $g = 1$ the $3$ possible Sato-Tate groups are $SU(2) = USp(2)$, a copy of the unitary group $U(1)$ embedded in $SU(2)$, and its normalizer in $SU(2)$; these arise, respectively, for elliptic curves $E/k$ without CM, with CM by a field contained in $k$, and with CM by a field not contained in $k$. For $g = 2$ a complete list of the $52$ possible Sato-Tate groups can be found in [FKRS12].

In order to simplify the notation, when $C$ is a smooth projective curve defined over the number field $k$, we may simply write

$$\ST(C) := \ST(Jac(C)), \quad \ST^0(C) := \ST^0(Jac(C)), \quad \text{and} \quad K_C := K_{Jac(C)}.$$

### 3. Trace formulas

Let $p$ be an odd prime, and let $\overline{C}/\mathbb{F}_p$ be a smooth projective curve of genus $g \geq 1$ defined by an equation of the form $y^2 = f(x)$ with $f \in \mathbb{F}_p[x]$ squarefree. Let $n = (p - 1)/2$ and let $f^n_{ij}$ denote the coefficient of $x^k$ in the polynomial $f(x)^n$. The Hasse–Witt matrix of $\overline{C}$ is the $g \times g$ matrix $W_p := [w_{ij}]$ over $\mathbb{F}_p$, where

$$w_{ij} := f^n_{ip - j} \quad (1 \leq i, j \leq g).$$

It is shown in [Man61, Yui78] that the characteristic polynomial $\chi(\lambda)$ of the Frobenius endomorphism of $Jac(\overline{C})$ satisfies

$$\chi(\lambda) \equiv (-1)^g \lambda^g \det(W_p - \lambda I) \mod p.$$ 

In particular,

$$\tr W_p \equiv t_p \mod p,$$

where $t_p := p + 1 - \#\overline{C}(\mathbb{F}_p)$ is the trace of Frobenius. The Weil bounds imply $|t_p| \leq 2g\sqrt{p}$, which means that for all $p \geq 16g^2$, the trace of $W_p$ uniquely determines the integer $t_p$.

Let us now specialize to the case where $f(x)$ has the form

$$f(x) = ax^d + bx^e,$$

with $d \in \{2g + 1, 2g + 2\}$, $e \in \{0, 1\}$, and $a, b \in \mathbb{F}_p$; this includes the families $C_i$ defined in §1. Writing

$$f(x)^n = x^{en}(ax^{d-e} + b)^n$$
and applying the binomial theorem yields
\[ f_{e n + (d - e)r}^n = \binom{n}{r} a^r b^{n-r}, \]
and we have \( f_k^n = 0 \) whenever \( k \) is not of the form \( k = en + (d - e)r \). Setting \( k = ip - j = i(2n + 1) - j \) and solving for \( r = r_{ij} \) yields
\[ r_{ij} := \frac{(2i - e)n + i - j}{d - e} \quad (1 \leq i, j \leq g). \]

The entries of the Hasse-Witt matrix for \( y^2 = ax^d + bx^e \) are thus given by
\[
 w_{ij} = \begin{cases} 
 (r_{ij})a^r b^{n-r} & \text{if } r_{ij} \in \mathbb{Z}, \\
 0 & \text{otherwise}. 
\end{cases}
\]

For any fixed integer \( i \in [1, g] \), the quantity \( (2i - e)n + i - j \) lies in an interval of width \( g - 1 < (d - e)/2 \), as \( j \) varies over integers in \([1, g]\). This implies that at most one entry \( w_{ij} \) in each row of \( W_p \) is nonzero, and for this entry \( r_{ij} \) is simply the nearest integer to \((2i - e)n/(d - e)\).

We now specialize to the two families of interest and assume \( p > 3 \). For \( C_1: y^2 = x^8 + c \) we have \( d = 8, e = 0, a = 1, \) and \( b = \bar{c} \), where \( \bar{c} \) denotes the image of \( c \) in \( \mathbb{F}_p \). We thus have
\[ r_{ij} = \frac{2in + i - j}{8} = \frac{ip - j}{8}. \]

For integers \( i, j \in [1, 3] \), the integral values of \( r_{ij} \) that arise are listed below:
\[
\begin{align*}
 p \equiv 1 \mod 8 & : \quad r_{11} = \frac{n}{4}, \quad r_{22} = \frac{n}{2}, \quad r_{33} = \frac{3n}{4}; \\
 p \equiv 3 \mod 8 & : \quad r_{13} = \frac{n-1}{4}, \quad r_{31} = \frac{3n+1}{4}; \\
 p \equiv 5 \mod 8 & : \quad r_{22} = \frac{n}{2}; \\
 p \equiv 7 \mod 8 & : \quad \text{none.}
\end{align*}
\]

This yields the following formulas for the trace of Frobenius:
\[
 t_p(C_1) \equiv_p \begin{cases} 
 \left( \frac{n}{n/2} \right) \bar{c}^{n/2} + \left( \frac{n}{n/4} \right) \bar{c}^{n/4} + \left( \frac{n}{n/4} \right) \bar{c}^{3n/4} & \text{if } p \equiv 1 \mod 8, \\
 \left( \frac{n}{n/2} \right) \bar{c}^{n/2} & \text{if } p \equiv 5 \mod 8, \\
 0 & \text{otherwise.}
\end{cases}
\]

For \( C_2: y^2 = x^7 - cx \) we have \( d = 7, e = 1, a = 1, \) and \( b = -\bar{c} \). We thus have
\[ r_{ij} = \frac{(2i - 1)n + i - j}{6}. \]

For integers \( i, j \in [1, 3] \), the integral values of \( r_{ij} \) that arise are listed below:
\[
\begin{align*}
 p \equiv 1 \mod 12 & : \quad r_{11} = \frac{n}{6}, \quad r_{22} = \frac{n}{2}, \quad r_{33} = \frac{5n}{6}; \\
 p \equiv 5 \mod 12 & : \quad r_{13} = \frac{n-2}{6}, \quad r_{22} = \frac{n}{2}, \quad r_{31} = \frac{5n+2}{6}; \\
 p \equiv 7 \mod 12 & : \quad \text{none}; \\
 p \equiv 11 \mod 12 & : \quad \text{none.}
\end{align*}
\]

This yields the following formulas for the trace of Frobenius:
\[
 t_p(C_2) \equiv_p \begin{cases} 
 \left( \frac{n}{n/2} \right) (-\bar{c})^{n/2} + \left( \frac{n}{n/6} \right) (-\bar{c})^{n/6} + \left( \frac{n}{n/6} \right) (-\bar{c})^{5n/6} & \text{if } p \equiv 1 \mod 12, \\
 \left( \frac{n}{n/2} \right) (-\bar{c})^{n/2} & \text{if } p \equiv 5 \mod 12, \\
 0 & \text{otherwise.}
\end{cases}
\]
3.1. Algorithms. Computing the powers of \( \bar{c} \) that appear in the formulas (2) and (3) for \( t_p(C_i) \) is straight-forward; using binary exponentiation this requires just \( O(\log p) \) multiplication in \( \mathbb{F}_p \). The only potential difficulty is the computation of the binomial coefficients \( \binom{n}{n/2}, \binom{n}{n/4}, \binom{n}{n/6} \) modulo \( p \), where \( n = (p-1)/2 \) and \( p \) is known to lie in a suitable residue class. Fortunately, there are very efficient formulas for computing these particular binomial coefficients modulo suitable primes \( p \). These are given by the lemmas below, in which \( (\frac{2}{p}) \) denotes the Legendre symbol, and \( m, x, \) and \( y \) denote integers.

**Lemma 3.1.** Let \( p = 4m + 1 = x^2 + y^2 \) be prime, with \( x \equiv -(\frac{2}{p}) \mod 4 \). Then

\[
\binom{2m}{m} \equiv 2(-1)^{m+1} x \mod p.
\]

**Proof.** See [BEW98] Thm. 9.2.2].

**Lemma 3.2.** Let \( p = 8m + 1 = x^2 + 2y^2 \) be prime, with \( x \equiv -(\frac{2}{p}) \mod 4 \). Then

\[
\binom{4m}{m} \equiv 2(-1)^{m+1} x \mod p.
\]

**Proof.** See [BEW98] Thm. 9.2.8].

**Lemma 3.3.** Let \( p = 12m + 1 = x^2 + y^2 \) be prime, with \( x \equiv -(\frac{2}{p}) \mod 4 \), and define \( \epsilon \) to be 0 if \( x \equiv 0 \mod 3 \) and 1 otherwise. Then

\[
\binom{6m}{m} \equiv 2(-1)^{m+\epsilon} x \mod p.
\]

**Proof.** See [BEW98] Thm. 9.2.10] (replace \( p^2 \) with \( (-1)^{\epsilon-1} \)).

To apply these lemmas, one uses Cornacchia’s algorithm to find a solution \((x, y)\) to \( p = x^2 + dy^2 \), where \( d = 1 \) when computing \( \binom{n}{n/2} \mod p \) or \( \binom{n}{n/6} \mod p \), and \( d = 2 \) when computing \( \binom{n}{n/4} \). Cornacchia’s algorithm requires as input a square-root \( \delta \) of \(-d\) modulo \( p \) (if no such \( \delta \) exists then \( p = x^2 + dy^2 \) has no solutions).

**Cornacchia’s Algorithm**

Given integers \( 1 \leq d < m \) and an integer \( \delta \in [0, m/2] \) such that \( \delta^2 \equiv -d \mod m \), find a solution \((x, y)\) to \( x^2 + dy^2 = m \) or determine that none exist as follows:

1. Set \( x_0 := m, x_1 := \delta, \) and \( i = 1 \).
2. While \( x_i^2 \geq m \), set \( x_{i+1} := x_{i-1} \mod x_i \) with \( x_{i+1} \in [0, x_i] \) and increment \( i \).
3. If \( (m - x_i^2) / d = y_i^2 \) for some \( y_i \in \mathbb{Z} \), output the solution \((x_i, y_i)\).

Otherwise, report that no solution exists.

See [Bas04] for a simple proof of the correctness of this algorithm. We now consider its computational complexity, using \( M(n) \) to denote the time to multiply two \( n \)-bit integers; we may take \( M(n) = O(n \log n \log \log n) \) via [SS71]. The first two steps correspond to half of the standard Euclidean algorithm for computing the GCD of \( m \) and \( \delta \), whose bit-complexity is bounded by \( O(\log^2 m) \); see [GG13] Thm. 3.13]. The time required in step 3 to perform a division and check whether the result is a square integer is also \( O(M(\log m)) \); see [GG13] Thm. 9.8, Thm. 9.28]. Thus the overall complexity is \( O(\log^3 m) \), the same as the Euclidean algorithm.
REMARK 3.4. There is an asymptotically faster version of the Euclidean algorithm that allows one to compute any particular pair of remainders \((x_{i-1}, x_i)\), including the unique pair for which \(x_{i-1} \geq \sqrt{m} > x_i\), in \(O(M(\log m) \log \log m)\) time; see [PW03]. This yields a faster version of Cornacchia’s algorithm that runs in quasi-linear time, but we will not use this.

We now turn to the problem of computing the square-root \(\delta\) of \(-d\) mod \(m\) that is required by Cornacchia’s algorithm. There are two basic strategies for doing this:

1. (Cipolla-Lehmer) Use a probabilistic root-finding algorithm to factor \(x^2 + d\) in \(\mathbb{F}_p[x]\). This takes \(O(M(\log p) \log p)\) expected time.

2. (Tonelli-Shanks) Given a generator \(g\) for the 2-Sylow subgroup of \(\mathbb{F}^*_p\), compute the discrete logarithm \(e\) of \((-d)^e \in \langle g \rangle\) and let \(\delta = g^{-e/2}(-d)^{(s+1)/2}\), where \(p = 2^e s + 1\) with \(s\) odd. This takes \(O(M(\log p)(\log p + v \log v / \log \log v))\) time if the algorithm in [Sut11] is used to compute the discrete logarithm.

We will exploit both approaches. To obtain a generator for the 2-Sylow subgroup of \(\mathbb{F}^*_p\) one may take \(\alpha^8\) for any quadratic non-residue \(\alpha\). Half the elements of \(\mathbb{F}^*_p\) are non-residues, so randomly selecting elements and computing Legendre symbols will yield a non-residue after 2 attempts, on average, and each attempt takes \(O(M(\log p) \log p)\) time, via [BZ10]. Unfortunately, we know of no efficient way to deterministically obtain a quadratic non-residue modulo \(p\) without assuming the generalized Riemann hypothesis (GRH). Under the GRH the least non-residue is \(O((\log p)^2)\) [Bac90], thus if we simply test increasing integers \(2, 3, \ldots\) we can obtain a non-residue \(\alpha\) for a total cost of \(O(M(\log p) (\log^2 p / \log \log p))\).

But we are actually interested in computing \(t_p(C_i)\) for many primes \(p \leq N\), for some large bound \(N\); on average, this approach will find a non-residue very quickly. As \(N \to \infty\) the average value of the least non-residue converges to

\[
\sum_{k=1}^{\infty} \frac{p_k}{2^k} = 3.674643966\ldots,
\]

where \(p_k\) denotes the \(k\)th prime, as shown by Erdös [Erd61].

Finally, we should mention an alternative approach to solving \(p = x^2 + dy^2\) that is completely deterministic. Construct an elliptic curve \(E/\mathbb{F}_p\) with complex multiplication by the imaginary quadratic order \(\mathcal{O}\) with discriminant \(D = -d\) (or \(D = -4d\) if \(-d \equiv 0, 1 \pmod{4}\)) and then use Schoof’s algorithm [Sch85] to compute the trace of Frobenius \(t\) of \(E\). We then have \(4p = t^2 - \nu^2 D\), since the Frobenius endomorphism with trace \(t\) and norm \(p\) corresponds to \(\frac{t \pm \sqrt{D}}{2} \in \mathcal{O}\), and therefore \((t/\nu)^2 \equiv D \pmod{p}\). If \(D = -d\), we have a square root of \(-d\) modulo \(p\) and can use Cornacchia’s algorithm to solve \(p = x^2 + dy^2\). If \(D = -4d\), then \(t\) is even and \((t/2, 2\nu)\) is already a solution to \(p = x^2 + dy^2\). We are specifically interested in the cases \(D = -4\) and \(D = -8\). For \(D = -4\) we can take \(E\): \(y^2 = x^3 - x\), and for \(D = -8\) we can take \(E\): \(y^2 = x^4 + 4x^2 + 2x\); see §3 of Appendix A in [Sil94].

We collect all of these observations in the following theorem.

**Theorem 3.5.** Let \(C_1\): \(y^2 = x^8 + c\) and \(C_2\): \(y^2 = x^7 - cx\) be as above. Let \(p > 3\) be a prime with \(v_p(c) = 0\). We can compute \(t_p(C_i)\):

- probabilistically in \(O(M(\log p) \log p)\) expected time;
- deterministically in \(O(M(\log p) \log^2 p \log \log p)\) time, assuming GRH;
- deterministically in \(O(M(\log^4 p) \log^5 p / \log \log p)\) time.
For any positive integer \( N \), we can compute \( t_p(C_i) \) for all \( 3 < p \leq N \) with \( v_p(c) = 0 \) deterministically in \( O(N M (\log N)) \) time.

**Proof.** Since we are computing asymptotic bounds, we may assume \( p \geq 144 \) (if not, just count points naïvely). Then \( t_p(C_i) \mod p \) uniquely determines \( t_p(C_i) \in \mathbb{Z} \).

For the first bound we use the Cipolla-Lehmer approach to probabilistically compute the square root required by Cornacchia’s algorithm in \( O(M (\log p) \log p) \) time, matching the time required to apply any of Lemmas 2.1-4, and the time required by the exponentiations of \( \tau \) needed to compute \( t_p(C_i) \).

For the second bound we instead use the Tonelli-Shanks approach to computing square roots, relying on iteratively testing increasing integers to find a non-residue. Under the GRH this takes \( O(M (\log p) \log^2 p \log \log p) \) time, which dominates everything else.

For the third bound, we instead use Schoof’s approach to solve \( p = x^2 + dy^2 \). The analysis in \[SS14, \text{ Cor. 11}\] shows that Schoof’s algorithm can be implemented to run in \( O(M (\log^5 p) \log^2 p / \log \log p) \) time.

For the final bound we proceed as in the GRH bound but instead rely on the Erdös bound for the least non-residue modulo \( p \leq N \), on average. By the prime number theorem there are \( O(N / \log N) \) primes \( p \leq N \); the total number of quadratic residue tests is thus \( O(N / \log N) \). It takes \( O(M (\log N) \log \log N) \) time for each test, so the total time spent finding non-residues is \( O(N M (\log N) \log \log N / \log N) \). The average 2-adic valuation of \( p - 1 \) over primes \( p \leq N \) is \( O(1) \), so the total time spent computing square roots modulo primes \( p \leq N \) using the Tonelli-Shanks approach is \( O((N / \log N) M (\log N) \log N)) = O(N M (\log N)) \) which dominates the time spent finding non-residues and matches the time spent on everything else. \( \square \)

We note that the average time per prime \( p \leq N \) using a deterministic algorithm is \( O(M (\log p) \log p) \), which matches the expected time when applying our probabilistic approach for any particular prime \( p \leq N \); both bounds are quasi-quadratic \( O((\log p)^{2+o(1)}) \). For comparison, the average time per prime \( p \leq N \) achieved using the average polynomial time algorithm in \[HS14a, HS16\] is \( O((\log p)^{4+o(1)}) \).

**Remark 3.6.** Although Theorem 3.5 only addresses the computation of \( t_p(C_i) \), for \( p \not\equiv 3 \mod 8 \) (resp. \( p \not\equiv 5 \mod 12 \)) we can readily compute the entire Hasse-Witt matrix \( W_p \) for \( C_1 \) (resp. \( C_2 \)) using the same approach and within the same complexity bounds.

### 4. Guessing Sato-Tate groups

In this section we analyze the Sato-Tate distributions of the curves \( C_i \) and arrive at a heuristic characterization of their Sato-Tate groups up to isomorphism, based on statistics collected using the algorithm described in \[3.5\]. In \[3.5\] we will unconditionally prove that our heuristic characterizations are correct.

#### 4.1. The Sato-Tate distribution of \( C_1 \)

Before applying any heuristics we can derive some information about the structure of the Sato-Tate group directly from the formulas developed in the previous section. The possible shapes of the Hasse-Witt matrix for \( C_1 \) at a primes \( p \equiv 1, 3, 5, 7 \mod 8 \) are depicted below, with the residue class of \( p \mod 8 \) in parentheses:
SATO-TATE GROUPS OF $y^2 = x^8 + c$ AND $y^2 = x^7 - cx$. 111

\[
\begin{bmatrix}
0 & 0 & * \\
* & 0 & 0 \\
0 & * & 0 \\
\end{bmatrix}, \begin{bmatrix}
0 & 0 & * \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & * \\
0 & 0 & 0 \\
\end{bmatrix}, \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}
\] (1), (3), (5), (7).

From this we can (unconditionally) conclude the following:

(a) the component group $ST(C_1) / ST^0(C_1)$ has order divisible by 4;
(b) we have $s(p)$ in $ST^0(C_1)$ only if $p \equiv 1 \mod 8$;
(c) the field $K_{C_1}$ contains $\mathbb{Q}(i, \sqrt{2})$.

We note that (c) follows immediately from (b): a prime $p > 2$ splits completely in $\mathbb{Q}(i, \sqrt{2})$ if and only if $p \equiv 1 \mod 8$.

Table 1 lists moment statistics $M_n$ for the curve $C_1: y^2 = x^8 + c$ for selected values of $c$, where $M_n$ is the average value of the $n$th power of the normalized $L$-polynomial coefficient

$$a_1 := -t_p / \sqrt{p},$$

over odd primes $p \leq 2^{40}$ not dividing $c$. The moment statistics $M_n$ for odd $n$ are all close to zero, so we list $M_n$ only for even $n$.

| $c$ | $M_2$  | $M_4$  | $M_6$  | $M_8$  | $M_{10}$ |
|-----|--------|--------|--------|--------|---------|
| 1   | 3.000  | 50.999 | 1229.971 | 33634.058 | 978107.050 |
| 2   | 2.000  | 27.000 | 619.987  | 16834.560 | 489116.939 |
| 3   | 2.000  | 24.000 | 469.984  | 11234.520 | 297593.517 |
| 4   | 3.000  | 51.000 | 1229.990 | 33634.650 | 978125.742 |
| 5   | 2.000  | 23.999 | 469.976  | 11234.211 | 297585.653 |
| 6   | 2.000  | 23.999 | 469.979  | 11234.275 | 297587.173 |
| 7   | 2.000  | 23.999 | 469.968  | 11234.007 | 297579.866 |
| 8   | 2.000  | 27.000 | 619.987  | 16834.560 | 489116.939 |
| 9   | 2.000  | 27.000 | 619.991  | 16834.645 | 498118.664 |
| $2^4$ | 3.000 | 50.999 | 1229.971 | 33634.058 | 978107.050 |
| $3^3$ | 2.000 | 24.000 | 469.987  | 11234.520 | 297594.971 |
| $2^5$ | 2.000 | 27.000 | 619.987  | 16834.560 | 489116.939 |
| $2^6$ | 3.000 | 51.000 | 1229.990 | 33634.650 | 978125.742 |
| $3^4$ | 3.000 | 51.000 | 1229.990 | 33634.593 | 978121.494 |

Table 1. Trace moment statistics for $C_1: y^2 = x^8 + c$ for $p \leq 2^{40}$.

There appear to be three distinct trace distributions that arise, depending on whether the integer $c$ is in

$$\mathbb{Q}(i, \sqrt{2})^{*4}, \mathbb{Q}(i, \sqrt{2})^{*2} \setminus \mathbb{Q}(i, \sqrt{2})^{*4}, \text{ or } \mathbb{Q}(i, \sqrt{2})^{*} \setminus \mathbb{Q}(i, \sqrt{2})^{*2};$$

these can be distinguished by whether the nearest integer to $M_4$ is 51, 27, or 24, respectively. Histogram plots of representative examples are shown with $c = 1, 2, 3$ in Figure 1. We note that in each histogram the central spike at 0 has area 1/2, while the spikes at −2 and 2 have area zero.

Based on the data in Table 1 we expect $K_{C_1}$ to contain $\mathbb{Q}(i, \sqrt{2}, \sqrt{c})$. If we now require $c$ to be a fourth-power and restrict to primes $p \equiv 1 \mod 8$, we can
investigate the Sato-Tate distribution of $C_1$ over the number field $\mathbb{Q}(i, \sqrt{2}, \sqrt{c})$.
For $c = 1$ we obtain the moments listed below:

| $c$ | $M_2$  | $M_4$   | $M_6$  | $M_8$   | $M_{10}$ |
|-----|--------|---------|--------|---------|----------|
| 1   | 10.000 | 197.997 | 4899.892| 134466.452| 3912182.569|

The corresponding histogram is shown in Figure 2.

We claim that this distribution corresponds to a connected Sato-Tate group, namely, the group

$$U(1)_2 \times U(1) := \left\{ \begin{bmatrix} U(u) & 0 & 0 \\ 0 & U(u) & 0 \\ 0 & 0 & U(v) \end{bmatrix} : u, v \in U(1) \right\},$$

where for $u \in U(1) := \{ e^{i\theta} : \theta \in [0, 2\pi) \}$ the matrix $U(u)$ is defined by

$$U(u) := \begin{bmatrix} u & 0 \\ 0 & \overline{u} \end{bmatrix}.$$  

(4)

The $a_1$-moment sequence for $U(1)_2 \times U(1)$ can be computed as the binomial convolution of the $a_1$-moment sequences for $U(1)_2$ and $U(1)$ given in [FKRS12]. Explicitly,
SATO-TATE GROUPS OF $y^2 = x^8 + c$ AND $y^2 = x^7 - cx$.

if $M_n(G)$ denotes the $n$th moment of $a_1$ (or any class function), for $G = H_1 \times H_2$, we have

$$M_n(G) = \sum_{k=0}^{n} \binom{n}{k} M_k(H_1)M_{n-k}(H_2).$$

Applying this to $G = U(1)_2 \times U(1)$ yields:

| $M_0$ | $M_1$ | $M_2$ | $M_3$ | $M_4$ | $M_5$ | $M_6$ | $M_7$ | $M_8$ | $M_9$ | $M_{10}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|---------|
| U(1)  | 1     | 0     | 8     | 96    | 0     | 1280  | 0     | 17920 | 0     | 258048  |
| U(1)  | 1     | 0     | 2     | 0     | 6     | 20    | 70    | 0     | 252    |
| U(1)_2\times U(1) | 1 | 0 | 10 | 0 | 198 | 4900 | 0 | 1344700 | 0 | 3912300 |

This is in close agreement (within 0.1%) with the moment statistics for $y^2 = x^8 + 1$ over $\mathbb{Q}(i, \sqrt{2})$. We thus conjecture that the identity component is

$$\text{ST}^{0}(C_1) = U(1)_2 \times U(1),$$

up to conjugacy in $\text{USp}(6)$, and

$$K_{C_1} = \mathbb{Q}(i, \sqrt{2}, \sqrt{c}).$$

For generic $c$ the component group of $\text{ST}(C_1)$ is then isomorphic to

$$\text{Gal}(K_{C_1}/\mathbb{Q}) \simeq D_4 \times C_2,$$

where $D_4$ is the dihedral group of order 8 and $C_2$ is the cyclic group of order 2.

4.2. The Sato-Tate distribution of $C_2$. The possible shapes of the Hasse-Witt matrix for $C_2$ at a primes $p \equiv 1, 5, 7, 11 \mod 12$ are depicted below, with the residue class of $p \mod 12$ in parentheses:

$$\begin{bmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{bmatrix} \quad (1), \quad \begin{bmatrix} 0 & 0 & * \\ 0 & * & 0 \\ * & 0 & 0 \end{bmatrix} \quad (5), \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (7), \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (11).$$

From this information we can conclude that:

(a) the order of the component group $\text{ST}(C_2)/\text{ST}^{0}(C_2)$ is a multiple of 4;
(b) we have $s(p) \in \text{ST}^{0}(C_2)$ only if $p \equiv 1 \mod 12$;
(c) the field $K_{C_2}$ contains $\mathbb{Q}(i, \sqrt{3})$.

We note that (c) follows immediately from (b): a prime $p > 3$ splits completely in $\mathbb{Q}(i, \sqrt{3})$ if and only if $p \equiv 1 \mod 12$.

Table 2 lists moment statistics $M_n$ for the curve $C_2: y^2 = x^7 - cx$ for various values of $c$. There now appear to be just two distinct trace distributions that arise, depending on whether the integer $c$ is a cube or not; these can be distinguished by whether the nearest integer to $M_2$ is 2 or 3, respectively. Histogram plots of three representative examples are shown for $c = 1, 2$ in Figure 3. In the histogram for $c = 1$ the central spike at 0 has area 1/2 and the spikes at −2 and 2 have area zero, but in the histogram for $c = 2$ the central spike has area 7/12, while the spikes at −4, −2, 2, 4 have area zero. This gives us a further piece of information: the order of the component group $\text{ST}(C_2)/\text{ST}^{0}(C_2)$ should be divisible by 12.

Based on the data in Table 3 we expect $K_{C_2}$ to contain $\mathbb{Q}(i, \sqrt{3}, \sqrt{c})$. We now require $c$ to be a cube and restrict to primes $p \equiv 1 \mod 12$ in order to investigate
Table 2. Trace moment statistics for $C_2: y^2 = x^7 - cx$ for $p \leq 2^{40}$.

| $c$ | $M_2$   | $M_4$   | $M_6$   | $M_8$       | $M_{10}$    |
|-----|---------|---------|---------|-------------|-------------|
| 1   | 10.000  | 245.997 | 7299.909| 229666.846  | 7440189.620 |

Figure 3. $a_1$-histograms for two representative curves $C_2$.

The Sato-Tate distribution of $C_2$ over the number field $\mathbb{Q}(i, \sqrt{3}, \sqrt[4]{c})$. For $c = 1$ we obtain the moments listed below:

| $c$ | $M_2$   | $M_4$   | $M_6$   | $M_8$       | $M_{10}$    |
|-----|---------|---------|---------|-------------|-------------|
| 1   | 18.000  | 485.994 | 14579.770| 459261.673  | 14880044.545|

The corresponding histogram is shown in Figure 4 and is clearly not the distribution of the identity component; one can see directly that there are (at least) two components.

This suggests that we should try computing the Sato-Tate distribution over a quadratic extension of $\mathbb{Q}(i, \sqrt{3})$. After a bit of experimentation, one finds that $\mathbb{Q}(i, \sqrt{-3})$ works. With $c = 1$ we obtain the moments statistics:

| $c$ | $M_2$   | $M_4$   | $M_6$   | $M_8$       | $M_{10}$    |
|-----|---------|---------|---------|-------------|-------------|
| 1   | 18.000  | 485.994 | 14579.770| 459261.673  | 14880044.545|

The corresponding histogram is shown in Figure 5.
We claim that this distribution corresponds to a connected Sato-Tate group, namely, the group
\[ U(1)_3 := \left\langle \begin{bmatrix} U(u) & 0 & 0 \\ 0 & U(u) & 0 \\ 0 & 0 & U(u) \end{bmatrix} : u \in U(1) \right\rangle. \]

The \( a_1 \)-moment sequence for \( U(1)_3 \) can be computed as the \( 3a_1 \)-moment sequence for \( U(1) \), which simply scales the \( n \)th moment by \( 3^n \). This yields the moments:

\[
\begin{array}{cccccc}
M_2 & M_4 & M_6 & M_8 & M_{10} \\
U(1)_3 & 18 & 486 & 14580 & 459270 & 14880348 \\
\end{array}
\]
which are in close agreement (better than 0.1%) with the moment statistics for
\( y^2 = x^7 - x \) over the field \( \mathbb{Q}(i, \sqrt{-3}) \).

A complication arises if we repeat the experiment using a cube \( c \neq 1 \); we no
longer get a connected Sato-Tate group! Taking \( c \) to be a sixth-power works, but
we now need to ask whether, generically, the degree 48 extension \( \mathbb{Q}(i, \sqrt{-3}, \sqrt{c}) \)
is the minimal extension required to get a connected Sato-Tate group. We have
good reason to believe that a degree 24 extension is necessary, since \( K_{C_2} \)
appears
to properly contain the degree 12 field \( \mathbb{Q}(i, \sqrt{3}, \sqrt{c}) \), but it is not clear that a
degree 48 extension is required. We thus check various quadratic subextensions of
\( \mathbb{Q}(i, \sqrt{-3}, \sqrt{c}) \) and find that \( \mathbb{Q}(i, \sqrt{c}, \sqrt{c\sqrt{-3}}) \) works consistently.

We thus conjecture that
\[
K_{C_2} = \mathbb{Q}(i, \sqrt{c}, \sqrt{c\sqrt{-3}}).
\]

This implies that for generic \( c \), the component group of \( \text{ST}(C_2) \) is isomorphic to
\[\text{Gal}(K_{C_2}/\mathbb{Q}) \cong C_3 \rtimes D_4 \quad (\text{GAP id : } \langle 24, 8 \rangle).\]

As noted above, we conjecture that the identity component is
\[
\text{ST}^0(C_2) = U(1)_3,
\]
up to conjugacy in \( \text{USp}(6) \).

Remark 4.1. While we are able to give a general description of the Sato-Tate
group in both cases just by looking at the \( a_1 \)-distribution of the curves \( C_i \), it should
be noted that our characterization of the Sato-Tate group in terms of its identity
component and the isomorphism type of its component group is far from sufficient
to determine the Sato-Tate distribution. For this we need an explicit description of
the Sato-Tate group as a subgroup (up to conjugacy) of \( \text{USp}(6) \); this is addressed
in the next section.

5. Determining Sato-Tate groups

In this section we compute the Sato-Tate groups of the curves \( C_1 : y^2 = x^8 + c \)
and \( C_2 : y^2 = x^7 - cx \) for generic values of \( c \in \mathbb{Q}^* \). The meaning of generic will be
specified in each case, but it ensures that the order of the group of components of the
Sato-Tate group is as large as possible. The Sato-Tate groups for the non-generic
cases can then be obtained as subgroups.

The description of the Sato-Tate group in terms of the twisted Lefschetz group
introduced by Banaszak and Kedlaya [BK15] is a useful tool for explicitly deter-
mining Sato-Tate groups (see [FGL16], for example, where this is exploited), but
here we take a different approach that is better suited to our special situation. Our
strategy is to identify an elliptic quotient of each of the curves \( C_1 \) and \( C_2 \) and then
use the classification results of [FKRS12] to identify the Sato-Tate group of
the complement abelian surface. We then reconstruct the Sato-Tate group of
the curves \( C_1 \) and \( C_2 \) from this data.

To determine the splitting of the Jacobians of \( C_1 \) and \( C_2 \) we benefit from
the fact that these are curves with large automorphism groups. For generic \( c \),
the automorphism group of \( C_1 \) over \( K_{C_1} \) has order 32 (GAP id \( \langle 32, 9 \rangle \)), and the
automorphism group of \( C_2 \) over \( K_{C_2} \) has order 24 (GAP id \( \langle 24, 5 \rangle \)).
We start by fixing the following matrix notations:

\[
I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, J := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, K := \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, Z_n := \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix}.
\]

Also, for \( u \in U(1) \), recall the notation \( U(u) \) introduced in (4). Whenever we consider matrices of the unitary symplectic group \( USp(6) \), we do it with respect to the symplectic form given by the matrix

\[
H := \begin{bmatrix} J & 0 & 0 \\ 0 & J & 0 \\ 0 & 0 & J \end{bmatrix}.
\]

If \( A \) and \( A' \) are two abelian varieties defined over \( k \), we write \( A \sim A' \) to indicate that \( A \) and \( A' \) are related by an isogeny defined over \( k \). Finally, we let \( \zeta_3 \) denote a primitive third root of unity in \( \overline{\mathbb{Q}} \).

### 5.1. Sato-Tate group of \( C_1 : y^2 = x^8 + c \).

**Lemma 5.1.** Let \( c \in \mathbb{Q}^* \) and \( C_1 : y^2 = x^8 + c \). Then

\[
\text{Jac}(C_1) \sim E \times \text{Jac}(C),
\]

where \( E : y^2 = x^4 + c \) and \( C : y^2 = x^5 + cx \) over \( \mathbb{Q} \). Thus \( K_{C_1} = \mathbb{Q}(i, \sqrt{-2}, c^{1/4}) \).

**Proof.** First note that we can write nonconstant morphisms defined over \( \mathbb{Q} \):

\[
\begin{align*}
\phi_E : C_1 & \to E, \quad \phi_E(x, y) = (x^2, y), \\
\phi_C : C_1 & \to C, \quad \phi_C(x, y) = (x^2, xy).
\end{align*}
\]

We clearly have that \( K_E = \mathbb{Q}(i) \). To see that \( K_C = \mathbb{Q}(i, \sqrt{-2}, c^{1/4}) \), first set \( F = \mathbb{Q}(c^{1/4}) \), and consider the automorphism

\[
\alpha : C_F \to C_F, \quad \alpha(x, y) = \left( \frac{c^{1/2}}{x}, \frac{c^{3/4}}{x^3} y \right).
\]

Since \( \alpha \) has order 2 and is nonhyperelliptic, \( C_F/\langle \alpha \rangle \) is an elliptic curve \( E' \) defined over \( F \). Poincaré’s decomposition theorem implies that \( \text{Jac}(C) F \sim E' \times E'' \), where \( E'' \) is an elliptic curve defined over \( F \). Observe that we also have the automorphism

\[
\gamma : C_{F(i)} \to C_{F(i)}, \quad \gamma(x, y) = (-x, iy).
\]

Since \( \alpha \) and \( \gamma \) do not commute, we deduce that \( \text{End}(\text{Jac}(C) F(i)) \) is nonabelian. It follows that \( E'_F(i) \) and \( E''_F(i) \) are \( F(i) \)-isogenous and that \( \text{Jac}(C) F(i) \sim E'^2 F(i) \). One may readily find an equation for the quotient curve \( E' = C_F/\langle \alpha \rangle \), and, by computing its \( j \)-invariant, determine that \( E' \) has complex multiplication by \( \mathbb{Q}(\sqrt{-2}) \). From this we may conclude that \( K_C = F(i, \sqrt{-2}) \). The asserted splitting of the Jacobian \( \text{Jac}(C_1) \) follows from the existence of the morphisms of equation (7) and the fact that \( E \) and \( E' \) are not \( \overline{\mathbb{Q}} \)-isogenous. This latter fact also implies that \( K_{C_1} \) is the compositum of \( K_E \) and \( K_C \). \( \square \)

**Definition 5.2.** In this subsection, we say that \( c \in \mathbb{Q}^* \) is generic if \( [K_{C_1} : \mathbb{Q}] \) is maximal, that is, \( [K_{C_1} : \mathbb{Q}] = 16 \). Equivalently, \( c \not\in \mathbb{Q}(i, \sqrt{-2})^*2 \).
COROLLARY 5.3. For generic $c \in \mathbb{Q}^*$, the Sato-Tate group of $\text{Jac}(C_1)$ is

$$\left\langle \begin{bmatrix} J & 0 & 0 \\ 0 & J & 0 \\ 0 & 0 & J \end{bmatrix}, \begin{bmatrix} 0 & J & 0 \\ -J & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} U(u) & 0 & 0 \\ 0 & U(u) & 0 \\ 0 & 0 & U(v) \end{bmatrix} : u, v \in U(1) \right\rangle.$$

PROOF. Recall the notations of Lemma 5.1. It follows from the description of $\text{Jac}(C)$ given in the proof of the lemma and the results of [FKRS12] that $\text{ST}(C)$ can be presented as

$$\left\langle \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix}, S := \begin{bmatrix} 0 & J \\ -J & 0 \end{bmatrix}, T := \begin{bmatrix} Z_8 & 0 \\ 0 & Z_8 \end{bmatrix}, \begin{bmatrix} U(u) & 0 \\ 0 & U(u) \end{bmatrix} : u \in U(1) \right\rangle.$$

This is the group named $J(D_4)$ in [FKRS12]. Since $E/\mathbb{Q}$ has CM, we also have

$$\text{ST}(E) = \langle J, U(u) : u \in U(1) \rangle.$$  

Since $E$ is not a $\mathbb{Q}$-isogeny factor of $\text{Jac}(C)$, we have $\text{ST}^0(C_1) \simeq \text{ST}^0(E) \oplus \text{ST}^0(C)$, which proves the part of the corollary concerning the identity component. By Proposition 2.3 we have isomorphisms

$$\psi_E : \text{ST}(E)/\text{ST}^0(E) \xrightarrow{\sim} \text{Gal}(K_E/\mathbb{Q}),$$

$$\psi_C : \text{ST}(C)/\text{ST}^0(C) \xrightarrow{\sim} \text{Gal}(K_C/\mathbb{Q}),$$

$$\psi_{C_1} : \text{ST}(C_1)/\text{ST}^0(C_1) \xrightarrow{\sim} \text{Gal}(K_{C_1}/\mathbb{Q}).$$

The isomorphism $\psi_E$ identifies $J$ with the nontrivial automorphism of $K_E$, whereas the isomorphism $\psi_C$ identifies the images of the generators $g = R, S, T$ in

$$\text{ST}(C)/\text{ST}^0(C) \simeq \langle R, S, T \rangle / \langle -1 \rangle$$

with automorphisms $\sigma = r, s, t \in \text{Gal}(K_{C_1}/\mathbb{Q}) = \text{Gal}(K_C/\mathbb{Q})$ as indicated below:

| $g$ | $\sigma$ | $\sigma(i)$ | $\sigma(\sqrt{-2})$ | $\sigma(c^{1/4})$ |
|-----|----------|-------------|-------------------|-----------------|
| $R$ | $r$      | $-i$        | $\sqrt{-2}$      | $c^{1/4}$       |
| $S$ | $s$      | $i$         | $-\sqrt{-2}$     | $c^{1/4}$       |
| $T$ | $t$      | $i$         | $\sqrt{-2}$      | $ic^{1/4}$      |

Let $\mathcal{R}, S, T$ be the three first generators of $\text{ST}(C_1)$. To check the part of the theorem concerning the group of components of $\text{ST}(C_1)$, one only needs to verify that $\mathcal{R}, S, T$ generate a group of components isomorphic to

$$\text{Gal}(K_{C_1}/\mathbb{Q}) \simeq \langle \mathcal{R}, S, T | \mathcal{R}^2, S^2, T^4, \mathcal{R}S\mathcal{R}S, \mathcal{R}T\mathcal{R}T, STST^3 \rangle,$$

and that their natural projections onto $\text{ST}(E)/\text{ST}^0(E)$ and onto $\text{ST}(C)/\text{ST}^0(C)$ are compatible with the isomorphisms of [5]. In this case, this amounts to noting that $\mathcal{R}, S, T$ project onto $R, S, T$ in $\text{ST}(C)$; that the automorphism $r$ restricts to the non-trivial element of $\text{Gal}(K_E/\mathbb{Q})$, while $\mathcal{R}$ projects down to $J$ in $\text{ST}(E)$; and that the restrictions of $s$ and $t$ to $K_E$ are trivial, as are the projections of $S$ and $T$ to $\text{ST}(E)$.

REMARK 5.4. We note that even though $\text{Jac}(C_1) \sim E \times \text{Jac}(C)$, in the generic case the Sato-Tate group $\text{ST}(C_1)$ is not isomorphic to the direct sum of $\text{ST}(E)$ and $\text{ST}(C)$, because $\text{Gal}(K_{C_1}/\mathbb{Q})$ is not isomorphic to the direct product of $\text{Gal}(K_E/\mathbb{Q})$ and $\text{Gal}(K_C/\mathbb{Q})$. This highlights the importance of being able to write down an explicit description for $\text{ST}(C_1)$ in terms of generators.
Remark 5.5. To treat non-generic values of \(c\), one replaces \(Z_8\) in the third generator for \(\text{ST}(C_1)\) in Corollary 5.3 with \(Z_4\) or \(Z_2\) when \(c \in \mathbb{Q}(i, \sqrt{2})^{*2} \setminus \mathbb{Q}(i, \sqrt{2})^{*4}\) or \(c \in \mathbb{Q}(i, \sqrt{2})^{*4}\), respectively (in the latter case one can simply remove \(T\) since it is already realized by \(u = -1\) and \(v = 1\)).

Using the explicit representation of \(\text{ST}(C_1)\) given in Corollary 5.3 one may compute moment sequences using the techniques described in §3.2 of FKS16. The table below lists moments not only for \(a_1\), but also for \(a_2\) and \(a_3\), where \(a_i\) denotes the coefficient of \(T^i\) in the characteristic polynomial of a random element of \(\text{ST}(C_1)\) distributed according to the Haar measure (these correspond to normalized \(L\)-polynomial coefficients of \(\text{Jac}(C_1)\)):

| \(a_1\) | \(M_1\) | \(M_2\) | \(M_3\) | \(M_4\) | \(M_5\) | \(M_6\) | \(M_7\) | \(M_8\) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0      | 2      | 0      | 24     | 0      | 470    | 0      | 11235  |
| 2      | 9      | 56     | 492    | 5172   | 59691  | 726945 | 9178434|
| 0      | 9      | 0      | 1245   | 0      | 284880 | 0      | 79208745|

The \(a_1\) moments closely match the corresponding moment statistics listed in Table 1 in the cases where \(c\) is generic, as expected. For a further comparison, we computed moment statistics for \(a_1, a_2, a_3\) by applying the algorithm of FKS16 to the curve \(y^2 = x^8 + 3\) over primes \(p \leq 2^{40}\). The \(a_1\)-moment statistics listed below have less resolution than those in Table 1 which covers \(p \leq 2^{40}\) (with this higher bound we get \(M_8 \approx 11234\), an even better match to the value 11235 predicted by the Sato-Tate group \(\text{ST}(C_1)\)).

| \(a_1\) | \(M_1\) | \(M_2\) | \(M_3\) | \(M_4\) | \(M_5\) | \(M_6\) | \(M_7\) | \(M_8\) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0.00   | 2.00   | 0.00   | 23.98  | 0.04   | 469.26 | 1      | 11210  |
| 2.00   | 9.00   | 55.95  | 491.22 | 5160.77| 59527.55| 724556 | 9143413|
| 0.00   | 8.99   | 0.04   | 1242.59| 10.30  | 283980.23| 2972  | 78866094|

5.2. Sato-Tate group of \(C_2\): \(y^2 = x^7 - cx\).

Lemma 5.6. Let \(c \in \mathbb{Q}^*\) and \(C_2\): \(y^2 = x^7 - cx\). Set \(F := \mathbb{Q}(\zeta_3, c^{1/3})\). Then
\[
\text{Jac}(C_2) \sim E \times A,
\]
where \(E\): \(y^2 = x^3 - cx\) and \(A\) is an abelian surface defined over \(\mathbb{Q}\) for which \(A_F \sim E' \times E''\), where \(E'\) and \(E''\) are elliptic curves defined over \(F\) by the equations
\[
E': y^2 = x^3 + 3c^{1/3}x, \quad E'': y^2 = x^3 + 3\zeta_3 c^{1/3}x.
\]
Thus \(K_{C_2} = \mathbb{Q}(i, c^{1/3}, \sqrt{c\sqrt{3}})\).

Proof. We can write nonconstant morphisms:
\[
\phi_E: (C_2)_F \to E_F, \quad \phi_E(x, y) = (x^3, xy),
\]
\[
\phi_{E'}: (C_2)_F \to E', \quad \phi_{E'}(x, y) = \left(\frac{x^2 - c^{1/3}}{x}, \frac{y}{x^2}\right),
\]
\[
\phi_{E''}: (C_2)_F \to E'', \quad \phi_{E''}(x, y) = \left(\frac{x^2 - \zeta_3 c^{1/3}}{x}, \frac{y}{x^2}\right).
\]
Note that the morphisms $\phi_E$, $\phi_{E'}$, and $\phi_{E''}$ are quotient maps given by automorphisms $\alpha_E$, $\alpha_{E'}$, and $\alpha_{E''}$ of $(C_2)_F$:

$$
\alpha_E(x, y) := (\zeta_3 x, c^2 y) , \quad \alpha_{E'}(x, y) := \left( -\frac{c^{1/3}}{x}, \frac{c^{2/3} y}{x^4} \right) , \quad \alpha_{E''} := \alpha_E \circ \alpha_{E'} .
$$

To see that $\text{Jac}(C_2)_F \simeq E_F \times E' \times E''$, it is enough to check that we have an isomorphism of $F$-vector spaces of regular differential forms

$$
\Omega_{(C_2)_F} = \phi_E^*(\Omega_{E_F}) \oplus \phi_{E'}^*(\Omega_{E'}) \oplus \phi_{E''}^*(\Omega_{E''}) ,
$$

But this follows from the fact that $\omega_1 = dx/y$, $\omega_2 = x \cdot dx/y$, and $\omega_3 = x^2 \cdot dx/y$ constitute a basis for $\Omega_{(C_2)_F}$, together with the easy computation

$$
\phi_E^* \left( \frac{dx}{y} \right) = 3\omega_2 , \quad \phi_{E'}^* \left( \frac{dx}{y} \right) = c^{1/3}\omega_1 + \omega_3 , \quad \phi_{E''}^* \left( \frac{dx}{y} \right) = \zeta_3 c^{1/3}\omega_1 + \omega_3 .
$$

Since $E$ is defined over $\mathbb{Q}$, there exists an abelian surface $A$ defined over $\mathbb{Q}$ such that $A_F \simeq E' \times E''$. To see that $K_{C_2} = \mathbb{Q}(i, c^{1/3}, \sqrt{c\sqrt{-3}})$, first note that $F(i) \subseteq K_{C_2}$ and that $E' \simeq E''$. Therefore, $K_{C_2}$ is the minimal extension of $F(i)$ over which $E$ and $E'$ become isomorphic. Now observe that we have an isomorphism

$$
\psi : E_{F(i, \sqrt{c\sqrt{-3}})} \rightarrow E'_{F(i, \sqrt{c\sqrt{-3}})} , \quad \psi(x, y) = \left( \frac{\sqrt{-3}}{c^{1/3}} x, \frac{\sqrt{-3} \sqrt{c\sqrt{-3}}}{c} y \right) ,
$$

from which we see that $K_{C_2}$ is the extension of $F(i)$ obtained by adjoining the element $\sqrt{c\sqrt{-3}}$ to $F(i)$ (note: one needs to write formula in (9) carefully, otherwise one may be tempted to make $K_{C_2}$ too large).

\textbf{Definition 5.7.} In this subsection, we say that $c \in \mathbb{Q}^*$ is generic if $[K_{C_2} : \mathbb{Q}]$ is maximal, that is, $[K_{C_2} : \mathbb{Q}] = 24$. Equivalently, $c$ is not a cube in $\mathbb{Q}^*$.

\textbf{Corollary 5.8.} For generic $c \in \mathbb{Q}^*$, the Sato-Tate group of $\text{Jac}(C_2)$ is

$$
\left\langle \begin{bmatrix} J & 0 & 0 \\ 0 & K & 0 \\ 0 & 0 & J \end{bmatrix} , \begin{bmatrix} 0 & K & 0 \\ Z_3 & 0 & 0 \\ 0 & 0 & I \end{bmatrix} , \begin{bmatrix} U(u) & 0 & 0 \\ 0 & U(u) & 0 \\ 0 & 0 & U(u) \end{bmatrix} : u \in U(1) \right\rangle .
$$

\textbf{Proof.} We assume the notations of Lemma 5.6. Since $E$, $E'$, and $E''$ are $K_{C_2}$-isogenous, we have $\text{ST}^0(C_2) \simeq U(1)$. Note that $K_A = \mathbb{Q}(i, \zeta_3, c^{1/3})$. We claim that $\text{ST}(A)$ is the group named $D_{6,1}$ in [FKRS12]. As may be seen in [FKRS12] Table 8], there are three Sato-Tate groups with identity component $U(1)$ and group of components isomorphic to $\text{Gal}(K_A/\mathbb{Q}) \simeq D_6$, namely, $J(D_3)$, $D_{6,1}$, and $D_{6,2}$. We can rule out the latter option, since by [FKRS12] Table 2] this would imply that $\text{Gal}(K_A/\mathbb{Q}(i))$ is a cyclic group of order 6, which is false. To rule out $J(D_3)$, we need to argue along the lines of [FKRS12 §4.6]: Let $F$ denote $\mathbb{Q}(\zeta_3, c^{1/3})$ as in Lemma 5.6 if $\text{ST}(A) = J(D_3)$, then $\text{ST}(A_F) = J(C_1)$, whereas if $\text{ST}(A) = D_{6,1}$, then $\text{ST}(A_F) = C_{2,1}$. By the dictionary between Sato-Tate groups and Galois endomorphism types in dimension 2 given by Theorem 2.5 (see [FKRS12] Table 8]), the first option would imply that $\text{End}(A_F) \otimes \mathbb{Z} \mathbb{R} \simeq M_2(\mathbb{R})$. Since Lemma 5.6 ensures that we are in the latter case, we must have $\text{ST}(A) = D_{6,1}$. 

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.
For convenience, we take the following presentation of $D_{6,1}$, which is conjugate to the one given in [FKRS12]:

$$\left\langle R := \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix}, \ S := \begin{bmatrix} 0 & K \\ K & 0 \end{bmatrix}, \ T := \begin{bmatrix} Z_3 & 0 \\ 0 & Z_3 \end{bmatrix}, \ \begin{bmatrix} U(u) & 0 \\ 0 & U(u) \end{bmatrix} : u \in U(1) \right\rangle.$$  

Since $E/\mathbb{Q}$ has CM, we have

$$\text{ST}(E) = \langle J, U(u) : u \in U(1) \rangle.$$  

By Proposition 2.3 we have isomorphisms

$$\psi_E : \text{ST}(E)/\text{ST}^0(E) \xrightarrow{\sim} \text{Gal}(K_E/\mathbb{Q}),$$

$$\psi_A : \text{ST}(A)/\text{ST}^0(A) \xrightarrow{\sim} \text{Gal}(K_A/\mathbb{Q}),$$

$$\psi_{C_2} : \text{ST}(C_2)/\text{ST}^0(C_2) \xrightarrow{\sim} \text{Gal}(K_{C_2}/\mathbb{Q}).$$

To prove the corollary it suffices to make these isomorphisms explicit and show that they are compatible with the projections from ST($C_2$) to ST($E$) and ST($A$), and with the restriction maps from Gal($K_{C_2}/\mathbb{Q}$) to Gal($K_E/\mathbb{Q}$) and Gal($K_A/\mathbb{Q}$).

The isomorphism $\psi_E$ identifies the image of $J$ in ST($E$)/ST($E$) with the non-trivial element of Gal($K_E/\mathbb{Q}$), while the isomorphism $\psi_A$ identifies the images of the generators $g = R, S, T$ in

$$\text{ST}(A)/\text{ST}^0(A) \simeq \langle R, S, T \rangle / \langle -1 \rangle$$

with automorphisms $\sigma = r, s, t \in \text{Gal}(K_A/\mathbb{Q})$ as indicated below:

| $g$ | $\sigma = \psi_A(g)$ | $\sigma(i)$ | $\sigma(\zeta_3)$ | $\sigma(c^{1/3})$ |
|-----|-----------------|-------------|-----------------|-----------------|
| $R$  | $r$             | $-i$        | $\zeta_3^2$    | $c^{1/3}$       |
| $S$  | $s$             | $-i$        | $\zeta_3$      | $c^{1/3}$       |
| $T$  | $t$             | $i$         | $\zeta_3$      | $\zeta_3 c^{1/3}$ |

If we now let $\mathcal{R}, \mathcal{S}, \mathcal{T}$ denote the first three generators of ST($C_2$) listed in the corollary, $\psi_{C_2}$ identifies their images in ST($C_2$)/ST($C_2$) with elements of Gal($K_A/\mathbb{Q}$) as indicated below, where $\delta = \sqrt[c]{-3}$:

| $g$ | $\sigma = \psi_{C_2}(g)$ | $\sigma(i)$ | $\sigma(\zeta_3)$ | $\sigma(c^{1/3})$ | $\sigma(\delta)$ |
|-----|-----------------|-------------|-----------------|-----------------|----------------|
| $\mathcal{R}$ | $r$             | $-i$        | $\zeta_3^2$    | $c^{1/3}$       | $i\delta$      |
| $\mathcal{S}$ | $i$             | $-i$        | $\zeta_3$      | $c^{1/3}$       | $\delta$       |
| $\mathcal{T}$ | $t$             | $i$         | $\zeta_3$      | $\zeta_3 c^{1/3}$ | $\delta$       |

We note that, unlike their restrictions $r$ and $s$, the automorphisms $r$ and $s$ do not commute, they generate a dihedral group of order 8 inside Gal($K_{C_2}/\mathbb{Q}$). The three automorphisms $r, s, t$ together generate Gal($K_{C_2}/\mathbb{Q}$). Their restrictions to $K_A$ are the generators $r, s, t$ for $K_A$, and $R, S, T$ are the projections of $\mathcal{R}, \mathcal{S}, \mathcal{T}$ to ST($A$). The automorphisms $r$ and $s$ both restrict to the non-trivial element of Gal($K_E/\mathbb{Q}$), and both $\mathcal{R}$ and $\mathcal{S}$ project down to $J$ in ST($E$). The restriction of $t$ to $K_E$ is trivial, as is the projection of $\mathcal{T}$ to ST($E$). To complete the proof it suffices to verify that the map

$$\text{ST}(C_2)/\text{ST}^0(C_2) \simeq \langle \mathcal{R}, \mathcal{S}, \mathcal{T} \rangle / \langle -1 \rangle \xrightarrow{\psi_{C_2}} \langle r, s, t \rangle \simeq \text{Gal}(K_{C_2}/\mathbb{Q})$$
we have explicitly defined is indeed an isomorphism. One can check that both sides are isomorphic to the finitely presented group
\[ \langle R, S, T \mid R^2, S^2, T^3, RRSRSRSR, RT, STST \rangle, \]
via maps that send generators to corresponding generators (in the order shown). □

**Remark 5.9.** To treat non-generic values of \( c \), simply remove the third generator containing \( \mathbb{Z}_3 \) from the list of generators for \( \text{ST}(C_2) \) in Corollary 5.8 when \( c \) is a cube in \( \mathbb{Q}^\times \).

Using the explicit representation of \( \text{ST}(C_2) \) given in Corollary 5.8, one may compute moments sequences for the characteristic polynomial coefficients \( a_1, a_2, a_3 \) using the techniques described in §3.2 of [FKS16]; the first eight moments are listed below:

| \( M_1 \) | \( M_2 \) | \( M_3 \) | \( M_4 \) | \( M_5 \) | \( M_6 \) | \( M_7 \) | \( M_8 \) |
|---|---|---|---|---|---|---|---|
| \( a_1 \): | 0 | 2 | 0 | 30 | 0 | 720 | 0 | 20650 |
| \( a_2 \): | 2 | 10 | 75 | 784 | 9607 | 126378 | 1721715 | 23928108 |
| \( a_3 \): | 0 | 11 | 0 | 2181 | 0 | 660790 | 0 | 224864661 |

The \( a_1 \) moments closely match the corresponding moment statistics listed in Table 2 in the cases where \( c \) is generic, as expected. We also computed moment statistics for \( a_1, a_2, a_3 \) by applying the algorithm of [HS16] to the curve \( y^2 = x^7 - 2x \) over primes \( p \leq 2^{30} \). The \( a_1 \)-moment statistics listed below have less resolution than Table 2, which covers \( p \leq 2^{40} \) (with this higher bound we get \( M_8 \approx 20649 \), very close to the value 20650 predicted by \( \text{ST}(C_2) \)).

| \( M_1 \) | \( M_2 \) | \( M_3 \) | \( M_4 \) | \( M_5 \) | \( M_6 \) | \( M_7 \) | \( M_8 \) |
|---|---|---|---|---|---|---|---|
| \( a_1 \): | 0.00 | 2.00 | 0.00 | 30.00 | 0.04 | 719.62 | 2 | 20636 |
| \( a_2 \): | 2.00 | 10.00 | 74.97 | 783.59 | 9600.64 | 126281.75 | 1720266 | 23906297 |
| \( a_3 \): | 0.00 | 11.00 | 0.04 | 2179.67 | 19.68 | 660247.53 | 8549 | 224645654 |

### 6. Galois endomorphism types

As recalled in §2 up to dimension 3, the Galois endomorphism type of an abelian variety over a number field is determined by its Sato-Tate group. In this section, we derive the Galois endomorphism type of \( \text{Jac}(C_2) \) from \( \text{ST}(C_2) \) for generic values of \( c \) (in the sense of §5.2). The case of \( \text{Jac}(C_1) \), although leading to slightly larger diagrams, is completely analogous.

Let \( G := \text{ST}(C_2) \) and \( V := \text{End}(\text{Jac}(C_2)_{K_{C_2}}) \), and set \( V_C := V \otimes \mathbb{Z} \mathbb{C} \) and \( V_R := V \otimes \mathbb{Z} \mathbb{R} \). As described in the proof of [FKRS12] Prop. 2.19:

- \( V_C \) is the subspace of \( M_6(\mathbb{C}) \) fixed by the action of \( G^0 \);
- \( V_R \) is the subspace of \( V_C \), of half the dimension, over which the Rosati form is positive definite;
- If \( L/\mathbb{Q} \) is a subextension of \( K_{C_2}/\mathbb{Q} \), corresponding to the subgroup \( N \subseteq \text{Gal}(K_{C_2}/\mathbb{Q}) \simeq G/G^0 \), then \( \text{End}(\text{Jac}(C_2)_L) \otimes \mathbb{Z} \mathbb{R} \simeq V_R^N \).

The matrices \( \Phi \in M_6(\mathbb{C}) \) commuting with \( G^0 \simeq \text{U}(1) \), embedded in \( \text{USp}(6) \), are matrices of the form \( \Phi = (\phi_{i,j}) \) with \( i, j \in [1, 6] \) such that \( \phi_{i,j} \in \mathbb{C} \) is 0 unless \( i \equiv j \).
mod 2. The condition of the Rosati form being positive definite on $V_R$ amounts to requiring that
\[
\text{Trace}(\Phi^t H \Phi^t H) \geq 0
\]
for every $\Phi \in V_R$, where $H$ is the symplectic matrix given in (6). Imposing the above condition on $\Phi$, we find that
\[
\Phi = \begin{pmatrix}
\alpha & 0 & \beta & 0 & \gamma & 0 \\
0 & \pi & 0 & \beta & 0 & \gamma \\
\delta & 0 & \epsilon & 0 & \phi & 0 \\
0 & \delta & 0 & \tau & 0 & \phi \\
\lambda & 0 & \mu & 0 & \nu & 0 \\
0 & \lambda & 0 & \mu & 0 & \nu
\end{pmatrix}
\]
with $\alpha, \beta, \ldots, \mu, \nu \in \mathbb{C}$.

We thus deduce that $V_R \simeq M_3(\mathbb{C})$.

We now proceed to determine the sub-$\mathbb{R}$-algebras of $V_R$ fixed by each of the subgroups of $\text{Gal}(K_{C_2}/\mathbb{Q}) \simeq G/G^0$. With notations as in the proof of Corollary 5.8, these subgroups are listed (up to conjugation) in Figure 6, where normal subgroups are marked with a *. We can then reconstruct the Galois type of $\text{Jac}(C_2)$ (see Figure 7) from the information in Table 3.

24
\[
\langle r, t, s \rangle *
\]
12
\[
\langle t, r, (rs)^2 \rangle *
=\langle t, s, (rs)^2 \rangle *
\]
8
\[
\langle t, r \rangle 
=\langle t, s \rangle 
=\langle t, (rs)^2 \rangle *
\]
6
\[
\langle (rs)^2, r \rangle
=\langle rs \rangle
\]
4
\[
\langle (rs)^2, s \rangle *
=\langle t \rangle *
\]
3
\[
\langle (rs)^2 \rangle *
=\langle s \rangle
\]
2
\[
\langle r \rangle
=\langle (rs)^2 \rangle *
\]
1
\[
\langle 1 \rangle *
\]

Figure 6. Lattice of subgroups of $\text{Gal}(K_{C_2}/\mathbb{Q})$. 
This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.
Table 3. Some subgroups of $\text{Gal}(K_{C_2}/\mathbb{Q})$ with the respective fixed sub-$\mathbb{R}$-algebras of $V_{\mathbb{R}}$.

Obtaining the data in Table 3 is a straight-forward exercise, let us make just a few specific comments:

- $N = \langle \mathcal{R} \rangle$: One easily checks that the matrices $\Phi$ satisfying the required condition form a simple nondivision $\mathbb{R}$-algebra; by Wedderburn’s structure theorem, it is of the form $M_d(D)$, for some division algebra $D$ and $d > 1$; since its real dimension is 9, we must have $d = 3$ and $D = \mathbb{R}$.

- $N = \langle (\mathcal{R}S)^2, \mathcal{S} \rangle$: Note that the $\mathbb{R}$-algebra $\mathcal{H} := \left\{ A_{\alpha,\beta} := \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}$ is isomorphic to $M_2(\mathbb{R})$. Indeed, if $\alpha = \alpha_1 + i\alpha_2$ and $\beta = \beta_1 + i\beta_2$, then
  $$\psi: \mathcal{H} \to M_2(\mathbb{R}), \quad \psi(A_{\alpha,\beta}) = \begin{pmatrix} \alpha_1 + \beta_1 & -\alpha_2 + \beta_2 \\ \alpha_2 + \beta_2 & \alpha_1 - \beta_1 \end{pmatrix}$$
  provides the required isomorphism. Alternative, one can reach the same conclusion by noting that $\mathcal{H}$ is the only non-commutative $\mathbb{R}$-algebra of dimension 4 with zero divisors.

- $N = \langle \mathcal{R} \rangle$: Note that the $\mathbb{R}$-algebra $\mathcal{H} := \left\{ A_{\alpha,\beta} := \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}$ is isomorphic to $\mathbb{C} \times \mathbb{C}$ by means of
  $$\psi: \mathcal{H} \to \mathbb{C} \times \mathbb{C}, \quad \psi(A_{\alpha,\beta}) = (\alpha + \beta, \alpha - \beta).$$

References

[Bac90] Eric Bach, Explicit bounds for primality testing and related problems, Math. Comp. 55 (1990), no. 191, 355–380, DOI 10.2307/2008811. MR1023756 (91m:11096)

[Bas04] Julius Magalona Basilla, On the solution of $x^2 + dy^2 = m$, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), no. 5, 40–41. MR2062797 (2005c:11031)

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, Gauss and Jacobi sums, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication. MR1625181 (99d:11092)

[BK15] Grzegorz Banaszak and Kiran S. Kedlaya, An algebraic Sato-Tate group and Sato-Tate conjecture, Indiana Univ. Math. J. 64 (2015), no. 1, 245–274, DOI 10.1512/iumj.2015.64.5438. MR3320526
Figure 7. Galois endomorphism types of $\text{Jac}(C_2)$. Lattice of fixed sub-$\mathbb{R}$-algebras corresponding to the subgroups of Figure 6.
[HS14a] David Harvey and Andrew V. Sutherland, Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, LMS J. Comput. Math. 17 (2014), no. suppl. A, 257–273, DOI 10.1112/S1461157014000187. MR3240808

[HS16] David Harvey and Andrew V. Sutherland, Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II, Cont. Math. 663 (2016), 127–147.

[Man61] Ju. I. Manin, The Hasse-Witt matrix of an algebraic curve (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 25 (1961), 153–172. MR0124324 (23 #A1638)

[PW03] Xinmao Wang and Victor Y. Pan, Acceleration of Euclidean algorithm and rational number reconstruction, SIAM J. Comput. 32 (2003), no. 2, 548–556, DOI 10.1137/S0097539702408636. MR1969404 (2004a:68173)

[SS71] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen (German, with English summary), Computing (Arch. Elektron. Rechnen) 7 (1971), 281–292. MR0292344 (45 #1431)

[Sch85] René Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1985), no. 170, 483–494, DOI 10.2307/2007968. MR077280 (86e:11122)

[SS14] Igor E. Shparlinski and Andrew V. Sutherland, On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average, LMS J. Comput. Math. 18 (2015), no. 1, 308–322, DOI 10.1112/S1461157015000017. MR3349320

[Ser12] J.-P. Serre, Lectures on $\mathbb{N}^\times \left( p \right)$, A.K. Peters, CRC Research Notes in Mathematics 11 (2012), CRC Press. MR2920749

[Sil94] Joseph H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96h:11074)

[Sut11] Andrew V. Sutherland, Structure computation and discrete logarithms in finite abelian $p$-groups, Math. Comp. 80 (2011), no. 273, 477–500, DOI 10.1090/S0025-5718-10-02356-2. MR2728991 (2012d:11122)

[Yui78] Noriko Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, J. Algebra 52 (1978), no. 2, 378–410. MR0491717 (58 #10920)

Universität Duisburg-Essen/Institut für Experimentelle Mathematik, Fakultät für Mathematik, D-45127, Essen, Germany

E-mail address: francesc.fite@gmail.com

Department of Mathematics, Massachusetts Institute of Technology, 77 Mass. Ave., Cambridge, Massachusetts 02139

E-mail address: drew@math.mit.edu

URL: http://math.mit.edu/~drew