Algebra & Number Theory

Volume 8

2014

No. 3

Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$

Francesc Fité and Andrew V. Sutherland

msp

ALGEBRA AND NUMBER THEORY 8:3 (2014)
dx.doi.org/10.2140/ant.2014.8.543

Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$

Francesc Fité and Andrew V. Sutherland

We determine the limiting distribution of the normalized Euler factors of an abelian surface A defined over a number field k when A is $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve defined over k with complex multiplication. As an application, we prove the Sato–Tate conjecture for Jacobians of $\mathbb{Q}$-twists of the curves $y^2 = x^5 - x$ and $y^2 = x^6 + 1$, which give rise to 18 of the 34 possibilities for the Sato–Tate group of an abelian surface defined over $\mathbb{Q}$. With twists of these two curves, one encounters, in fact, all of the 18 possibilities for the Sato–Tate group of an abelian surface that is $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with complex multiplication. Key to these results is the *twisting Sato–Tate group* of a curve, which we introduce in order to study the effect of twisting on the Sato–Tate group of its Jacobian.

1. Introduction

Let A be an abelian variety of dimension g, defined over a number field k. The generalized *Sato–Tate conjecture* predicts that the Haar measure of a certain compact subgroup G of the unitary symplectic group $\mathrm{USp}(2g)$ governs the distribution of the normalized Euler factors $\bar{L}_{\mathfrak{p}}(A, T)$ as $\mathfrak{p}$ varies over the primes of k where A has good reduction. The normalized Euler factor at a prime $\mathfrak{p}$ is the polynomial $\bar{L}_{\mathfrak{p}}(A, T) = L_{\mathfrak{p}}(A, T/q^{1/2})$, where $q = \|\mathfrak{p}\|$ is the norm of $\mathfrak{p}$ and

$$L_{\mathfrak{p}}(A, T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$$

MSC2010: primary 11M50; secondary 14K15, 14G10, 11G20, 11G10.
Keywords: Sato–Tate, hyperelliptic curves, abelian surfaces, twists.

is the *L-polynomial* of A at $\mathfrak{p}$. The polynomial $L_{\mathfrak{p}}(A, T)$ has the defining property that for each positive integer n,

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

In order to give a precise statement of the Sato–Tate conjecture, we need to specify the group G and to define what it means for G to "govern" the distribution of the polynomials $L_{\mathfrak{p}}(A, T)$. Serre [2012] defined, in terms of ℓ-adic monodromy groups, a compact real Lie subgroup of $\mathrm{USp}(2g)$ associated to the abelian variety A, denoted by $\mathrm{ST}(A)$ and called the *Sato–Tate group* of A, satisfying the following property: for each prime $\mathfrak{p}$ at which A has good reduction, there exists a conjugacy class $s(\mathfrak{p})$ of $\mathrm{ST}(A)$ whose characteristic polynomial equals $\bar{L}_{\mathfrak{p}}(A, T) := \sum_{i=0}^{2g} a_i(A)(\mathfrak{p})T^i$.[1] For $i = 0, 1, \dots, 2g$, let I_i denote the interval

$$I_i = \left[-\binom{2g}{i}, \binom{2g}{i}\right],$$

and consider the map

$$\Phi_i : \mathrm{ST}(A) \subseteq \mathrm{USp}(2g) \to I_i \subseteq \mathbb{R} \tag{1-1}$$

that sends an element of $\mathrm{ST}(A)$ to the i-th coefficient of its characteristic polynomial. Let $\mu(\mathrm{ST}(A))$ denote the Haar measure of $\mathrm{ST}(A)$ and let $\Phi_{i,*}(\mu(\mathrm{ST}(A)))$ denote its image on I_i by Φ_i. We can now state the generalized Sato–Tate conjecture.

Conjecture 1.1. *For $i = 0, 1, \dots, 2g$, the $a_i(A)(\mathfrak{p})$ are equidistributed*[2] *on I_i with respect to $\Phi_{i,*}(\mu(\mathrm{ST}(A)))$.*[3]

The original Sato–Tate conjecture addresses the case where A is an elliptic curve $E/\mathbb{Q}$ without complex multiplication (CM), in which case $g = 1$ and $\mathrm{ST}(A) = \mathrm{USp}(2) = \mathrm{SU}(2)$. This case of the conjecture has recently been proved; see [Serre 2012, p. 105] for a complete list of references. For elliptic curves E/k with complex multiplication, there are two cases, depending on whether the CM field M is contained in k or not. In the former case, $\mathrm{ST}(E)$ is isomorphic to the unitary group $\mathrm{U}(1)$ (embedded in $\mathrm{SU}(2)$), and in the latter case, $\mathrm{ST}(E)$ is isomorphic to the normalizer of $\mathrm{U}(1)$ in $\mathrm{SU}(2)$. Both cases follow from classical results that we recall in Section 3B.

In all three cases arising for $g = 1$, it is easy to see that the Sato–Tate group of E is invariant under twisting: if E' is isomorphic to E over $\overline{\mathbb{Q}}$, then $\mathrm{ST}(E')$ is

[1] See also [Fité et al. 2012, §2] for a brief summary of this construction; there the Sato–Tate group of A is denoted by ST_A, rather than $\mathrm{ST}(A)$.

[2] When we make equidistribution statements, we sort primes in increasing order by norm.

[3] There is a slightly stronger form of Conjecture 1.1 which asserts that in fact the conjugacy classes $s(\mathfrak{p})$ are equidistributed with respect to the projection of $\mu(\mathrm{ST}(A))$ on the set of conjugacy classes of $\mathrm{ST}(A)$; see [Fité et al. 2012, Conjecture 1.1].

isomorphic to $\mathrm{ST}(E)$. However, when $g > 1$, this is no longer true.

In this article we study the possibilities for the Sato–Tate group of the Jacobians of twists of genus-2 curves defined over $\mathbb{Q}$ with many automorphisms (these arise for curves whose Jacobians are $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with complex multiplication), and to prove that in these cases Conjecture 1.1 is true.[4]

The curves we consider give rise to 18 of the 34 Sato–Tate groups that can occur for an abelian surface defined over $\mathbb{Q}$, yet they all lie in one of the two $\overline{\mathbb{Q}}$-isomorphism classes corresponding to the curves listed in the title of this article. This makes apparent the importance of understanding the effect of twisting on the Sato–Tate group.

In the remainder of this section, we describe the two points in the moduli space of genus-2 curves that are the object of our study, and state our main result (Theorem 1.4). We also describe the numerical computations used to obtain explicit examples that realize all the possibilities permitted by our main theorem.

Let us first fix some notation. Throughout this paper, $\overline{\mathbb{Q}}$ denotes a fixed algebraic closure of $\mathbb{Q}$ that is assumed to include the number field k and all of its algebraic extensions. Let $G_k = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ denote the absolute Galois group of k. For any algebraic variety X defined over k and any extension L/k, we use X_L to denote the algebraic variety defined over L obtained from X by the base change $k \hookrightarrow L$. For abelian varieties A and B defined over k, we write $A \sim B$ to indicate that there is an isogeny between A and B that is defined over k. We may write $A \sim_k B$ to emphasize the field of definition, but this is redundant (to indicate an isogeny defined over an extension L/k, we write $A_L \sim B_L$).

1A. ***Genus-2 curves with many automorphisms.*** Let C be a curve of genus $g \leq 3$ defined over k. In Section 2, we define the *twisting Sato–Tate group* $\mathrm{ST}_{\mathrm{Tw}}(C)$ of C, a compact Lie group with the property that the Sato–Tate group of the Jacobian of any twist of C is isomorphic to a subgroup of $\mathrm{ST}_{\mathrm{Tw}}(C)$. There is a well-known bijection between the set of twists of C up to k-isomorphism and the cohomology group $H^1(G_k, \mathrm{Aut}(C_{\overline{\mathbb{Q}}}))$, given by associating to a twist C' of C the class of the cocycle $\xi(\tau) := \phi({}^{\tau}\phi)^{-1}$, where ϕ is an isomorphism from $C'_{\overline{\mathbb{Q}}}$ to $C_{\overline{\mathbb{Q}}}$. Thus the group $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ is a good measure of how complicated the twists of C can be.

For the rest of Section 1, we let $k = \mathbb{Q}$ and $g = 2$. The automorphism group $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ is then one of the following seven groups:

$$\mathrm{C}_2,\ \mathrm{D}_2,\ \mathrm{D}_4,\ \mathrm{D}_6,\ \mathrm{C}_{10},\ 2\mathrm{D}_6,\ \tilde{\mathrm{S}}_4.$$

Here C_n denotes the cyclic group of n elements, D_n the dihedral group of order $2n$, and S_n the symmetric group on n letters. The groups $2\mathrm{D}_6$ and $\tilde{\mathrm{S}}_4$ are 2-coverings of

[4]Using the techniques of this article, one can obtain analogous results for genus-3 curves with many automorphisms, such as the Fermat and Klein quartics; see [Fité et al. $\geq$ 2014].

D_6 and S_4, isomorphic to $C_3 \rtimes D_4$ (with action kernel V_4) and $GL_2(\mathbb{F}_3)$, respectively. In the generic case, $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ is isomorphic to C_2. This implies that every twist C' of C is quadratic, and we have $\mathrm{ST}(\mathrm{Jac}(C')) = \mathrm{ST}(\mathrm{Jac}(C)) = \mathrm{ST}_{\mathrm{Tw}}(C)$.

We are interested in the opposite situation: the two exotic cases where $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ is as large as possible: $\tilde{S}_4$ and $2D_6$. All genus-2 curves C with $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ isomorphic to $\tilde{S}_4$ (resp. $2D_6$) are isomorphic to

$$y^2 = x^5 - x \quad (\text{resp. } y^2 = x^6 + 1), \tag{1-2}$$

and thus they constitute a single $\overline{\mathbb{Q}}$-isomorphism class $\mathscr{C}_2$ (resp. $\mathscr{C}_3$) of curves.

We shall choose representative curves C_2^0 and C_3^0 for $\mathscr{C}_2$ and $\mathscr{C}_3$ that are defined over $\mathbb{Q}$ and have particularly nice arithmetic properties. We write C^0 (resp. $\mathscr{C}$) to denote either C_2^0 or C_3^0 (resp. either $\mathscr{C}_2$ or $\mathscr{C}_3$). The key arithmetic property we require of C^0 is that its Jacobian be $\mathbb{Q}$-isogenous to E^2, where E is an elliptic curve defined over $\mathbb{Q}$ (with CM). This applies only to the curve $y^2 = x^6 + 1$ listed in (1-2), which we take as our representative C_3^0 for the class $\mathscr{C}_3$, but it also applies to the curve

$$y^2 = x^6 - 5x^4 - 5x^2 + 1, \tag{1-3}$$

which we take as a *better* representative C_2^0 for the class $\mathscr{C}_2$ of $y^2 = x^5 - x$.

The classification in [Fité et al. 2012] gives an explicit description of each of the 52 Sato–Tate groups that can and do arise in genus 2, as subgroups of $\mathrm{USp}(4)$, of which 32 have identity component (isomorphic to) $\mathrm{U}(1)$. The two curves listed in (1-2) both appear in [Fité et al. 2012], where they are shown to have Sato–Tate groups with identity component $\mathrm{U}(1)$. It follows that if C is a twist of either of these curves, then $\mathrm{ST}(\mathrm{Jac}(C))$ also has identity component $\mathrm{U}(1)$. In fact, the representative curves for all 32 of the $\mathrm{U}(1)$ cases listed in [Fité et al. 2012] are actually twists of one of the two curves in (1-2) (possibly using an extended field of definition).

Among the 32 genus-2 Sato–Tate groups with identity component $\mathrm{U}(1)$, two are maximal. The first has component group $S_4 \times C_2$ and is denoted by $J(O)$, while the second has component group $D_6 \times C_2$ and is denoted by $J(D_6)$. We will prove that $\mathrm{ST}_{\mathrm{Tw}}(C_2^0) = J(O)$ and $\mathrm{ST}_{\mathrm{Tw}}(C_3^0) = J(D_6)$, and, as a consequence, that the Sato–Tate group of any twist of C_2^0 (resp. C_3^0) is isomorphic to a subgroup of $J(O)$ (resp. $J(D_6)$). Conversely, we will show that every Sato–Tate group that can occur over $\mathbb{Q}$ and is isomorphic to a subgroup of $J(O)$ (resp. $J(D_6)$) arises for some $\mathbb{Q}$-twist C of C_2^0 (resp. C_3^0), by giving explicit examples in each case.[5] Most of the Sato–Tate groups G with identity component $\mathrm{U}(1)$ are actually subgroups of *both* $J(O)$ and $J(D_6)$. In such cases we exhibit $\mathbb{Q}$-twists of both C_2^0 and C_3^0 that have Sato–Tate group G.

[5] We call C a $\mathbb{Q}$-*twist* of C^0 if C is defined over $\mathbb{Q}$ and $C_{\overline{\mathbb{Q}}} \simeq C^0_{\overline{\mathbb{Q}}}$.

1B. *Main result.* Recall that C^0 denotes either C_2^0 or C_3^0. These are both genus-2 curves defined over $\mathbb{Q}$ whose Jacobians are $\mathbb{Q}$-isogenous to the square of an elliptic curve $E/\mathbb{Q}$ with CM by an imaginary quadratic field M equal to $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$, respectively. Our main result is that Conjecture 1.1 holds for the Jacobians of the $\mathbb{Q}$-twists C of C^0.

In order to state the theorem more precisely, we introduce some notation.

Definition 1.2. For any $\mathbb{Q}$-twist C of C^0, let $K/\mathbb{Q}$ (resp. $L/\mathbb{Q}$) denote the minimal extension over which all endomorphisms of $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ (resp. homomorphisms from $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ to $E_{\overline{\mathbb{Q}}}$) are defined. Then we write $T(C)$ for the isomorphism class

$$\big[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)\big].$$

We say that two triples of groups (H_1, H_2, H_3) and (H_1', H_2', H_3') are isomorphic if $H_i \simeq H_i'$ for $i = 1, 2, 3$. We write $[H_1, H_2, H_3]$ for the isomorphism class of (H_1, H_2, H_3), which we regard as a triple of abstract groups.

Definition 1.3. For any finite group H with a subgroup H_0 and a normal subgroup N, and any positive integers r and s with $r \mid s$, let $o(s, r)$ (resp. $\bar{o}(s, r)$) count the elements in H_0 (resp. $H \setminus H_0$) of order s whose projection in H/N has order r. Let $z(H, N, H_0)$ denote the vector $[z_1, z_2]$, where

$$z_1 = \big[o(1,1), o(2,1), o(2,2), o(3,3), o(4,2), o(6,3), o(6,6), o(8,4), o(12,6)\big],$$
$$z_2 = \big[\bar{o}(2,2), \bar{o}(4,2), \bar{o}(6,6), \bar{o}(8,4), \bar{o}(12,6)\big].$$

For any $\mathbb{Q}$-twist C of C^0, write

$$z(C) := [z_1(C), z_2(C)] := z\big(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(L/K), \mathrm{Gal}(L/M)\big).$$

We also define $o(r) = \sum_s o(s, r)$ and $\bar{o}(s) = \sum_r \bar{o}(s, r)$. We note that in the cases of interest, $z(H, N, H_0)$ is $z(C)$ for some $\mathbb{Q}$-twist C of C^0. In this situation, $o(r)$ is the number of elements in $\mathrm{Gal}(L/M)$ whose projection to $\mathrm{Gal}(K/M)$ has order r, and $\bar{o}(s)$ is the number of elements of order s in $\mathrm{Gal}(L/\mathbb{Q})$ that are not in $\mathrm{Gal}(L/M)$. Clearly

$$\sum_{r,s} o(s,r) = \sum_{r,s} \bar{o}(s,r) = \frac{|\mathrm{Gal}(L/\mathbb{Q})|}{2}.$$

Moreover, we prove in Proposition 4.9 that the only pairs (s, r) for which $o(s, r)$ or $\bar{o}(s, r)$ can be nonzero are those that appear in the vectors z_1 and z_2.

Finally, let $L_p(C, T)$ denote the Euler factor of C at a prime p of good reduction. We may write the normalized Euler factor $\bar{L}_p(C, T) = L_p(C, T/p^{1/2})$ as

$$\bar{L}_p(C, T) = T^4 + a_1(C)(p)T^3 + a_2(C)(p)T^2 + a_1(C)(p)T + 1.$$

We are now ready to state our main theorem.

Theorem 1.4. *Let C be a $\mathbb{Q}$-twist of C^0.*

(i) *There are exactly* 20 *possibilities for $T(C)$ if $C^0 = C_2^0$, and* 21 *if $C^0 = C_3^0$.*

(ii) *The triple $T(C)$ and the vector $z(C)$ uniquely determine each other.*

(iii) *The triple $T(C)$ (or $z(C)$) determines the Sato–Tate group* $\mathrm{ST}(\mathrm{Jac}(C))$.

(iv) *For $i = 1, 2$, the $a_i(C)(p)$ are equidistributed on $I_i = \left[-\binom{4}{i}, \binom{4}{i}\right]$ with respect to a measure $\mu(a_i(C))$ that is uniquely determined by the vector $z(C)$. More precisely, the density function of $\mu(a_i(C))$ is continuous up to a finite number of points, and it is therefore uniquely determined by its moments*:

$$\mathrm{M}_n[\mu(a_1(C))] = \frac{1}{[L:\mathbb{Q}]}\bigl(o(1)2^n + o(3) + o(4)2^{n/2} + o(6)3^{n/2}\bigr)b_{0,n},$$

$$\begin{aligned}\mathrm{M}_n[\mu(a_2(C))] = \frac{1}{[L:\mathbb{Q}]}\bigl(&o(1)b_{4,n} + o(2)b_{0,n} + o(3)b_{1,n} + o(4)b_{2,n} + o(6)b_{3,n}\\ &+ \bar{o}(2)2^n + \bar{o}(4)(-2)^n + \bar{o}(6)(-1)^n + \bar{o}(12)\bigr).\end{aligned}$$

Here $b_{m,n}$ denotes the coefficient[6] *of X^n in $(X^2 + mX + 1)^n$.*

(v) *Conjecture 1.1 holds for C.*

We actually prove statement (iv) in greater generality, for an abelian surface A defined over a number field k with $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over k with CM by a quadratic imaginary field M. This is accomplished in Section 3 via Corollary 3.12, whose proof relies on a study of the structure of $\mathrm{Hom}(E_L, A_L) \otimes_M \overline{\mathbb{Q}}$ as a Galois $\overline{\mathbb{Q}}[\mathrm{Gal}(L/M)]$-module and a refined equidistribution statement of Frobenius elements of a CM elliptic curve when restricted to certain Galois conjugacy classes (see Corollary 3.8). We compute the moments

$$\mathrm{M}_n[a_i(C)] := \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} a_i(C)(p)^n,$$

where p varies over primes of good reduction, and prove equidistribution of the $a_i(C)(p)$ with respect to a measure $\mu(a_i(C))$. It follows that $\mathrm{M}_n[\mu(a_1(C))] = \mathrm{M}_n[a_i(C)]$. We devote Section 4 to the proofs of assertions (i), (ii), and (iii), which follow from Corollary 4.18, Proposition 4.16, and Proposition 4.17, respectively. The final assertion (v) follows from (iii) and (iv): it is enough to check that for each of the 41 possibilities of $T(C)$, the formulas obtained for $\mu[a_i(C)]$ coincide with the ones obtained for $\Phi_{i,*}(\mu(\mathrm{ST}(\mathrm{Jac}(C))))$ in [Fité et al. 2012]. In fact, it has very recently been shown that the generalized Sato–Tate conjecture (in its strong form) holds in general for abelian surfaces with potential complex multiplication; see [Johansson 2013].

[6]For $m = 0, 1, 2, 3, 4$, the $b_{m,n}$ form the sequences A126869, A0002426, A000984, A026375, A081671, respectively, in the Online Encyclopedia of Integer Sequences [OEIS 2011].

1C. ***Numerical computations.*** In Section 5, we show that all 41 of the possible triples $T(C)$ determined in section Section 4 actually arise for some $\mathbb{Q}$-twist C of C^0 by exhibiting a provable example of each case. The example curves C were obtained by an extensive search that was made feasible by part (ii) of Theorem 1.4; it is computationally much easier to approximate $z(C)$ than it is to explicitly compute $T(C)$, which requires computing the Galois groups of number fields of fairly large degree (48 or 96 in the most typical cases).

For an elliptic curve E with CM, the values $a_1(E)(p)$ can be computed very quickly, and we show how to compute $a_1(C)(p)$ and $a_2(C)(p)$ from $a_1(E)(p)$ using the fact that $\mathrm{Jac}(C)$ is $\overline{\mathbb{Q}}$-isogenous to E^2 (see Proposition 4.9). This allows us to efficiently compute an approximation of $z(C)$ (using again Proposition 4.9) of precision sufficient to provisionally identify $T(C)$ (via part (ii) of Theorem 1.4). Many curves were analyzed (tens of thousands) in order to obtain 41 candidate examples, one for each possible triple $T(C)$. For each of these 41 candidates, we then proved that the provisional identification of $T(C)$ is correct by explicitly computing the Galois groups $\mathrm{Gal}(L/\mathbb{Q})$, $\mathrm{Gal}(K/\mathbb{Q})$, and $\mathrm{Gal}(L/M)$.

2. The twisting Sato–Tate group of a curve

In this section we define the *twisting Sato–Tate group*, which is our main object of study. We do so in terms of the *algebraic Sato–Tate group* defined by Banaszak and Kedlaya [2011]. Let A be an abelian variety of dimension $g\le 3$ defined over a number field k, and fix an embedding of k into $\mathbb{C}$. Fix a polarization on A and a symplectic basis for the singular homology group $H_1(A_{\mathbb{C}}^{\mathrm{top}},\mathbb{Q})$. Use it to equip this space with an action of $\mathrm{GSp}_{2g}(\mathbb{Q})$. For each $\tau\in G_k$, define

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

Here we view α as an endomorphism of $H_1(A_{\mathbb{C}}^{\mathrm{top}},\mathbb{Q})$. The *algebraic Sato–Tate group* of A is defined by

$$\mathrm{AST}(A):=\bigcup_{\tau\in G_k}\mathrm{L}(A,\tau).$$

The Sato–Tate group $\mathrm{ST}(A)$ is a maximal compact subgroup of $\mathrm{AST}(A)\otimes_{\mathbb{Q}}\mathbb{C}$; see [Banaszak and Kedlaya 2011, Theorems 6.1 and 6.10].

Remark 2.1. As noted in the introduction, $\mathrm{ST}(A)$ is invariant under twisting when $g=1$. This does not hold for $g>1$; however, $\mathrm{ST}(A)$ *is* invariant under quadratic twisting. For $g\le 3$, this follows easily from the definitions above. Indeed, let $\chi: G_k\to\mathbb{C}$ be a quadratic character. For every $\tau\in G_k$, one has $\mathrm{L}(A\otimes\chi,\tau)=\mathrm{L}(A,\tau)\otimes\chi(\tau)$ (see (2-2) for a more general relation). Invariance under quadratic twisting follows from the fact that $\mathrm{L}(A,\tau)\otimes\chi(\tau)=\mathrm{L}(A,\tau)$. For A of arbitrary dimension, the invariance of $\mathrm{ST}(A)$ under quadratic twisting follows easily from the definition of $\mathrm{ST}(A)$ given in [Serre 2012] (see also [Fité et al. 2012]), in terms of the image of the ℓ-adic representation attached to A.

We now assume that A is the Jacobian $\mathrm{Jac}(C)$ of a curve C defined over k, and view $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ as a subgroup of $\mathrm{GL}(H_1(\mathrm{Jac}(C)_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}))$.

Definition 2.2. The *twisting algebraic Sato–Tate group of C* is the algebraic subgroup of $\mathrm{Sp}_{2g}/\mathbb{Q}$ defined by

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

Observe that $\mathrm{AST}_{\mathrm{Tw}}(C)$ is indeed a group: for any $\gamma_1, \gamma_2 \in \mathrm{AST}(\mathrm{Jac}(C))$ and $\alpha_1, \alpha_2 \in \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$, we have

$$\gamma_1\alpha_1(\gamma_2\alpha_2)^{-1} = \gamma_1\gamma_2^{-1}\gamma_2[\alpha_1\alpha_2^{-1}]\gamma_2^{-1} = \gamma_1(\gamma_2^{-1})^{\tau_2^{-1}}(\alpha_1\alpha_2) \in \mathrm{AST}_{\mathrm{Tw}}(C).$$

We will make the notational convention that the τ_i are such that $\gamma_i \in \mathrm{L}(A, \tau_i)$ until the end of the section. Now let C' be a *twist* of C, a curve defined over k for which $C'_L \simeq C_L$ for some finite Galois extension L/k. Let $\phi : C'_L \to C_L$ be a fixed isomorphism. It is easy to check that

$$\mathrm{L}(\mathrm{Jac}(C'), \tau) = \phi^{-1}\,\mathrm{L}(\mathrm{Jac}(C), \tau)({}^{\tau}\phi). \tag{2-2}$$

Here ϕ is seen as a homomorphism from $H_1\big(\mathrm{Jac}(C')_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}\big)$ to $H_1\big(\mathrm{Jac}(C)_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}\big)$.

Lemma 2.3. *Let $\gamma' \in \mathrm{L}(\mathrm{Jac}(C'), \tau) \subseteq \mathrm{AST}(\mathrm{Jac}(C'))$. Write γ' as $\phi^{-1}\gamma({}^{\tau}\phi)$ with γ in $\mathrm{L}(\mathrm{Jac}(C), \tau)$ as in (2-2). The map*

$$\Lambda_\phi : \mathrm{AST}(\mathrm{Jac}(C')) \to \mathrm{AST}_{\mathrm{Tw}}(C), \quad \Lambda_\phi(\gamma') = \gamma({}^{\tau}\phi)\phi^{-1}$$

is a (well-defined) monomorphism of groups.

Proof. Let $\gamma'_1 = \phi^{-1}\gamma_1({}^{\tau_1}\phi)$ and $\gamma'_2 = \phi^{-1}\gamma_2({}^{\tau_2}\phi)$ be elements of $\mathrm{L}(\mathrm{Jac}(C'), \tau_1)$ and $\mathrm{L}(\mathrm{Jac}(C'), \tau_2)$, respectively. Then

$$\begin{aligned}
\Lambda_\phi(\gamma'_1\gamma'_2) &= \Lambda_\phi\big(\phi^{-1}\gamma_1\gamma_2\gamma_2^{-1}[({}^{\tau_1}\phi)\phi^{-1}]\gamma_2({}^{\tau_2}\phi)\big)\\
&= \Lambda_\phi\big(\phi^{-1}\gamma_1\gamma_2({}^{\tau_2\tau_1}\phi)({}^{\tau_2}\phi)^{-1}({}^{\tau_2}\phi)\big)\\
&= \Lambda_\phi\big(\phi^{-1}\gamma_1\gamma_2({}^{\tau_2\tau_1}\phi)\big) = \gamma_1\gamma_2({}^{\tau_2\tau_1}\phi)\phi^{-1}\\
&= \gamma_1\gamma_2\big[({}^{\tau_2\tau_1}\phi)({}^{\tau_2}\phi)^{-1}\big]\gamma_2^{-1}\gamma_2({}^{\tau_2}\phi)\phi^{-1}\\
&= \gamma_1({}^{\tau_1}\phi)\phi^{-1}\gamma_2({}^{\tau_2}\phi)\phi^{-1} = \Lambda_\phi(\gamma'_1)\Lambda_\phi(\gamma'_2).
\end{aligned}$$

It is clear that Λ_ϕ is both well-defined and injective: $\Lambda_\phi(\gamma'_1) = \Lambda_\phi(\gamma'_2)$ if and only if $\gamma'_1 = \gamma'_2$. □

We now define the *twisting Sato–Tate group* $\mathrm{ST}_{\mathrm{Tw}}(C)$ of C.

Definition 2.4. 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 2.5. It follows from the previous lemma that for any twist C' of C, the Sato–Tate group $\mathrm{ST}(\mathrm{Jac}(C))$ is isomorphic to a subgroup of $\mathrm{ST}_{\mathrm{Tw}}(C)$. We also note that the component groups of $\mathrm{ST}_{\mathrm{Tw}}(C)$ and $\mathrm{AST}_{\mathrm{Tw}}(C) \otimes \mathbb{C}$ must be isomorphic, and the identity components of $\mathrm{ST}_{\mathrm{Tw}}(C)$ and $\mathrm{ST}(\mathrm{Jac}(C))$ are equal.

Our next goal is to study the component group of $\mathrm{ST}_{\mathrm{Tw}}(C)$ when C is a hyperelliptic curve (of genus $g \leq 3$). Consider the group[7]

$$\big(\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \rtimes \mathrm{AST}(\mathrm{Jac}(C))\big)/Z,$$

where Z is the normal subgroup of $\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \rtimes \mathrm{AST}(\mathrm{Jac}(C))$ consisting of the pairs (α, γ) with $\alpha = \gamma$, where $\alpha \in \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ and $\gamma \in \mathrm{AST}(\mathrm{Jac}(C))$.

Lemma 2.6. *The map*

$$\Phi : \mathrm{AST}_{\mathrm{Tw}}(C) \to \big(\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \rtimes \mathrm{AST}(\mathrm{Jac}(C))\big)/Z, \quad \Phi(\gamma\alpha) = (\alpha^{-1}, \gamma)$$

is a (*well-defined*) *isomorphism.*

Proof. For any $\gamma_1, \gamma_2 \in \mathrm{AST}(\mathrm{Jac}(C))$ and $\alpha_1, \alpha_2 \in \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$, we have

$$\begin{aligned}\Phi(\gamma_1\alpha_1\gamma_2\alpha_2) &= \Phi\big(\gamma_1\gamma_2({}^{\tau_2}\alpha_1)\alpha_2\big) = \big(\alpha_2^{-1}({}^{\tau_2}\alpha_1)^{-1}, \gamma_1\gamma_2\big) \\ &= (\alpha_1^{-1}, \gamma_1)(\alpha_2^{-1}, \gamma_2) = \Phi(\gamma_1\alpha_1)\Phi(\alpha_2\gamma_2).\end{aligned}$$

The surjectivity of Φ is clear. It remains to prove that $\Phi(\gamma_1\alpha_1) = \Phi(\gamma_2\alpha_2)$ if and only if $\gamma_1\alpha_1 = \gamma_2\alpha_2$. On the one hand, $\Phi(\gamma_1\alpha_1) = \Phi(\gamma_2\alpha_2)$ if and only if

$$Z \ni (\alpha_2^{-1}, \gamma_2)(\alpha_1^{-1}, \gamma_1)^{-1} = \big({}^{\tau_1^{-1}}(\alpha_1\alpha_2^{-1}), \gamma_2\gamma_1^{-1}\big).$$

On the other hand, $\gamma_1\alpha_1 = \gamma_2\alpha_2$ if and only if $\alpha_1\alpha_2^{-1} = \gamma_1^{-1}\gamma_2$, or equivalently, ${}^{\tau_1^{-1}}(\alpha_1\alpha_2^{-1}) = \gamma_2\gamma_1^{-1}$. But then $\big({}^{\tau_1^{-1}}(\alpha_1\alpha_2^{-1}), \gamma_2\gamma_1^{-1}\big) \in Z$. □

We now assume C is a hyperelliptic curve (of genus $g \leq 3$). As an endomorphism of $H_1\big(\mathrm{Jac}(C)^{\mathrm{top}}_{\mathbb{C}}, \mathbb{Q}\big)$, the hyperelliptic involution w of C corresponds to the matrix $-1 \in \mathrm{Sp}_{2g}(\mathbb{Q})$. Recall that $\mathrm{AST}(\mathrm{Jac}(C))$ contains the matrix -1. Thus $(-1, -1) \in Z$, and Lemma 2.6 implies that $\mathrm{AST}_{\mathrm{Tw}}(C)$ is isomorphic to a subgroup of

$$\big(\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \rtimes \mathrm{AST}_{\mathrm{Jac}(C)}\big)/\langle(-1, -1)\rangle.$$

Let K/k denote the minimal field extension over which all the endomorphisms of $\mathrm{Jac}(C)$ are defined. Then, since the component group of $\mathrm{ST}(\mathrm{Jac}(C))$ is isomorphic to $\mathrm{Gal}(K/k)$ (see [Banaszak and Kedlaya 2011, Remark 6.4, Theorem 6.10]), and

[7]The product of elements (α_1, γ_1) and (α_2, γ_2) in $\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \rtimes \mathrm{AST}(\mathrm{Jac}(C))$ is defined to be $(\alpha_2\gamma_2^{-1}\alpha_1\gamma_2, \gamma_1\gamma_2) = (\alpha_2 \cdot {}^{\tau_2}\alpha_1, \gamma_1\gamma_2)$, where $\gamma_2 \in \mathrm{L}(A, \tau_2) \subset \mathrm{AST}(\mathrm{Jac}(C))$.

the identity component of $\mathrm{ST}(\mathrm{Jac}(C))$ contains the matrix -1, the component group of $\mathrm{ST}_{\mathrm{Tw}}(C)$ is isomorphic to a subgroup of

$$\mathrm{Aut}(C_{\overline{\mathbb{Q}}})/\langle w\rangle \rtimes \mathrm{Gal}(K/k).$$

By Lemma 2.3, for any twist C' of C, there exists a monomorphism of groups

$$\overline{\lambda}_\phi : \mathrm{Gal}(K/k) \to \mathrm{Aut}(C_{\overline{\mathbb{Q}}})/\langle w\rangle \rtimes \mathrm{Gal}(K/k). \tag{2-3}$$

It follows that if there exists a twist $\tilde{C}$ of C such that

$$|\mathrm{Gal}(\tilde{K}/k)| = |\mathrm{Aut}(C_{\overline{\mathbb{Q}}})| \cdot |\mathrm{Gal}(K/k)|/2, \tag{2-4}$$

where $\tilde{K}/k$ is the minimal extension over which all the endomorphisms of $\mathrm{Jac}(\tilde{C})$ are defined, then $\mathrm{ST}_{\mathrm{Tw}}(C) = \mathrm{ST}(\mathrm{Jac}(\tilde{C}))$, and for every twist C' of C, the Sato–Tate group $\mathrm{ST}(\mathrm{Jac}(C'))$ is a subgroup of $\mathrm{ST}(\mathrm{Jac}(\tilde{C}))$.

Remark 2.7. Let C_2^0 and C_3^0 be the two curves defined in Section 1A. If $\tilde{C}$ is a twist of C_2^0 (resp. C_3^0) such that $\mathrm{ST}(\tilde{C}) = J(O)$ (resp. $J(D_6)$), then (2-4) is satisfied. It follows that $\mathrm{ST}_{\mathrm{Tw}}(C_2^0) = J(O)$ and $\mathrm{ST}_{\mathrm{Tw}}(C_3^0) = J(D_6)$.

3. Squares of CM elliptic curves

We shall work in the category of abelian varieties up to isogeny, so we call the elements of $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$ homomorphisms, the elements of $\mathrm{End}(A) \otimes \mathbb{Q}$ endomorphisms, and the surjective elements in $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$ isogenies.

We henceforth assume that A is an abelian variety over k such that $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over k with CM by an imaginary quadratic field M (except in Section 3D, where we do not assume E has CM). Let L/k be the minimal extension over which all the homomorphisms from $E_{\overline{\mathbb{Q}}}$ to $A_{\overline{\mathbb{Q}}}$ are defined, and let K/k be the minimal extension over which all the endomorphisms of $A_{\overline{\mathbb{Q}}}$ are defined. We note that $kM \subseteq K \subseteq L$, and we have $\mathrm{Hom}(E_{\overline{\mathbb{Q}}}, A_{\overline{\mathbb{Q}}}) \simeq \mathrm{Hom}(E_L, A_L)$ and $A_L \sim E_L^2$.

3A. *The Galois modules* $\mathbf{Hom}(E_L, A_L)$ *and* $\mathbf{End}(A_L)$. Let σ and $\overline{\sigma}$ denote the two embeddings of M into $\overline{\mathbb{Q}}$. Consider

$$\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}} \quad \text{and} \quad \mathrm{End}(A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}},$$

where the tensor products are taken via the embedding $\sigma : M \hookrightarrow \overline{\mathbb{Q}}$. If we let $\mathrm{Gal}(L/kM)$ act trivially on $\overline{\mathbb{Q}}$ and naturally on $\mathrm{Hom}(E_L, A_L)$, these products become $\overline{\mathbb{Q}}[\mathrm{Gal}(L/kM)]$-modules of dimensions 2 and 4, respectively, over $\overline{\mathbb{Q}}$, and similarly for $\overline{\sigma}$.

Definition 3.1. Let $\theta := \theta_{M,\sigma}(E, A)$ (resp. $\theta_{M,\sigma}(A)$) denote the representation afforded by the module $\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$ (resp. $\mathrm{End}(A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$), and similarly define $\overline{\theta} := \theta_{M,\overline{\sigma}}(E, A)$ and $\theta_{M,\overline{\sigma}}(A)$. Let $\theta_{\mathbb{Q}} := \theta_{\mathbb{Q}}(E, A)$ (resp. $\theta_{\mathbb{Q}}(A)$) denote the representation afforded by the $\mathbb{Q}[\mathrm{Gal}(L/k)]$-module $\mathrm{Hom}(E_L, A_L) \otimes \mathbb{Q}$ (resp. $\mathrm{End}(A_L) \otimes \mathbb{Q}$).

For each $\tau \in \mathrm{Gal}(L/kM)$, we write

$$\det(1-\theta(\tau)T) = 1 + a_1(\theta)(\tau)T + a_2(\theta)(\tau)T^2,$$

where $a_1(\theta) = \mathrm{Tr}\,\theta$ and $a_2(\theta) = \det(\theta)$ are elements of M. Observe that

$$\mathrm{Tr}\,\theta_{\mathbb{Q}}(\tau) = \mathrm{Tr}_{M/\mathbb{Q}}\,\mathrm{Tr}\,\theta(\tau) \quad \text{if } \tau \in \mathrm{Gal}(L/kM). \tag{3-1}$$

For $z \in M$, let $|z| := \sqrt{\sigma(z)\overline{\sigma}(z)}$.

Proposition 3.2. *There is an isomorphism of* $\overline{\mathbb{Q}}[\mathrm{Gal}(L/kM)]$*-modules*

$$\mathrm{End}(A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}} \simeq \big(\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}\big)^* \otimes \mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}.$$

Thus $\mathrm{Tr}\,\theta_{M,\sigma}(A) = \mathrm{Tr}\,\theta_{M,\overline{\sigma}}(E, A) \cdot \mathrm{Tr}\,\theta_{M,\sigma}(E, A) = |\,\mathrm{Tr}(\theta)|^2 \in \mathbb{Q}$, *and therefore* $\theta_{M,\sigma}(A) \simeq \theta_{M,\overline{\sigma}}(A)$.

Proof. Consider the natural inclusion of $\overline{\mathbb{Q}}[\mathrm{Gal}(L/kM)]$-modules

$$\mathrm{End}(A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}} \hookrightarrow \mathrm{Hom}_{\overline{\mathbb{Q}}}\big(\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}, \mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}\big),$$

which sends an element ψ in $\mathrm{End}(A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$ to the linear map of $\overline{\mathbb{Q}}$-vector spaces that sends f in $\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$ to $\psi \circ f$ in $\mathrm{Hom}(E_L, A_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$. Both spaces have dimension 4 over $\overline{\mathbb{Q}}$, and thus must be isomorphic as $\overline{\mathbb{Q}}[\mathrm{Gal}(L/kM)]$-modules. □

Let $\pi : \mathrm{Gal}(L/kM) \to \mathrm{Gal}(K/kM)$ be the natural projection. For each τ in $\mathrm{Gal}(L/kM)$, let $s = s(\tau)$ denote the order of τ and let $r = r(\tau)$ denote the order of $\pi(\tau)$ in $\mathrm{Gal}(K/kM)$. The possible values of r are 1, 2, 3, 4, and 6; see [Fité et al. 2012, §4.5].

Proposition 3.3. *Suppose* $\tau \in \mathrm{Gal}(L/k)$ *does not lie in* $\mathrm{Gal}(L/kM)$. *Then the eigenvalues of* $\theta_{\mathbb{Q}}(E, A)(\tau)$ *are as follows*:

$$\begin{array}{llll} s=2: & -1, -1, 1, 1 & s=8: & \zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7 \\ s=4: & i, i, -i, -i & s=12: & \zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11} \\ s=6: & \zeta_3, \zeta_3^2, \zeta_6, \zeta_6^5 & & \end{array}$$

Here, ζ_r *stands for an* r*-th root of unity.*

Proof. We can assume that kM/k is quadratic; otherwise there is nothing to prove. We first show the following properties of $\theta_{\mathbb{Q}}(E, A)$:

(i) The least common multiple of the orders of the eigenvalues of $\theta_{\mathbb{Q}}(E, A)(\tau)$ is equal to s.

(ii) If $\tau \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/kM)$, then $\mathrm{Tr}\,\theta_{\mathbb{Q}}(E, A)(\tau) = 0$.

It follows from the definition of L/k that the representation $\theta_{\mathbb{Q}}(E, A)$ is faithful, which implies (i). Let χ be the quadratic character of $\mathrm{Gal}(L/k)$ associated to the quadratic extension kM/k. Then $E \otimes \chi \sim_k E$ (and, in fact, $A \otimes \chi \sim_k A$), which implies that $\mathrm{Hom}(E_L, A_L) = \mathrm{Hom}(E_L, A_L) \otimes \chi$ (by [Mazur et al. 2007, Proposition 1.6], for example). This proves (ii).

For $s = 2, 6, 8, 12$, the proposition follows from (i) and (ii). For $s = 4$, (i) implies that i is an eigenvalue of $\theta_{\mathbb{Q}}(E, A)(\tau)$, and (ii) leaves just two possibilities for the four eigenvalues: $i, -i, 1, -1$, or $i, -i, i, -i$. We now show that only the latter can arise. The eigenvalues of $\theta_{\mathbb{Q}}(E, A)(\tau)$ are quotients of roots of $\bar{L}_{\mathfrak{p}}(E, T)$ and roots of $\bar{L}_{\mathfrak{p}}(A, T)$, where $\mathfrak{p}$ is a prime of k, inert in kM, of good reduction for A and E. We can further assume that $\mathfrak{p}$ has absolute degree 1. Then $\bar{L}_{\mathfrak{p}}(E, T) = 1 + T^2$, and the polynomial $\bar{L}_{\mathfrak{p}}(A, T)$ is one of the following:

$$(1 - T^2)^2, \quad 1 - T^2 + T^4, \quad 1 + T^4, \quad 1 + T^2 + T^4, \quad (1 + T^2)^2. \tag{3-2}$$

In no case can both 1 and i arise as quotients of a root of $\bar{L}_{\mathfrak{p}}(E, T) = 1 + T^2$ and roots of $\bar{L}_{\mathfrak{p}}(A, T)$. □

In view of Proposition 3.2, we write $\theta_M(A)$ for $\theta_{M,\sigma}(A) \simeq \theta_{M,\bar{\sigma}}(A)$.

Proposition 3.4. *For each* $\tau \in \mathrm{Gal}(L/kM)$, *we have*

$$\mathrm{Tr}\,\theta_M(A)(\tau) = 2 + \zeta_r + \bar{\zeta}_r.$$

Proof. It follows from [Fité et al. 2012, Proposition 9] that the eigenvalues of $\theta_{\mathbb{Q}}(A)(\tau)$ are $1, 1, 1, 1, \zeta_r, \zeta_r, \bar{\zeta}_r, \bar{\zeta}_r$. Equation (3-1) leaves three possibilities for the eigenvalues of $\theta_M(A)$: they must be either $1, 1, \zeta_r, \bar{\zeta}_r$, or $1, 1, \zeta_r, \zeta_r$, or $1, 1, \bar{\zeta}_r, \bar{\zeta}_r$. By Proposition 3.2, $\mathrm{Tr}\,\theta_M(A)$ is rational, so only the first possibility can occur. □

3B. ***Equidistribution for Frobenius conjugacy classes.*** We first recall the well-known notion of equidistribution on a compact topological space X (see [Serre 1998, Chapter 1]). Let $\mathscr{C}(X)$ denote the Banach space of continuous, complex valued functions f on X, with norm $\|f\| = \sup_{x \in X} |f(x)|$. Let μ be a Radon measure on X, a continuous linear form on $\mathscr{C}(X)$. Let $\{x_i\}_{i \geq 1}$ be a sequence of points of X. The sequence $\{x_i\}_{i \geq 1}$ is said to be equidistributed with respect to μ if for every $f \in \mathscr{C}(X)$, we have

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

Note that if $\{x_i\}_{i \geq 1}$ is equidistributed with respect to μ, then μ is positive and has total mass 1. We are particularly interested in the case where X is an interval I of $\mathbb{R}$. In this case, the n-th moment $\mathrm{M}_n[\mu]$ of μ is the value $\mu(\varphi_n)$, where φ_n is the function of $\mathscr{C}(I)$ defined by $\varphi_n(z)=z^n$. Analogously, the n-th moment of a sequence $\{x_i\}_{i\geq 1}$ on I, if it exists, is defined by

$$\mathrm{M}_n[\{x_i\}_{i\geq 1}] = \lim_{m\to\infty} \frac{1}{m}\sum_{i=1}^{m} x_i^n.$$

Thus if the sequence $\{x_i\}_{i\geq 1}$ is equidistributed with respect to μ on I, then its n-th moment exists and is equal to $\mathrm{M}_n[\mu]$.

Let F/k be a field extension, and let P_{E_F} denote the set of primes of F at which the elliptic curve E_F has good reduction. We write the normalized L-polynomial for E_F at a prime $\mathfrak{p}$ of P_{E_F} as

$$\bar{L}_{\mathfrak{p}}(E_F,T) = 1 + a_1(E_F)(\mathfrak{p})T + T^2.$$

Choose an *ordering by norm* $\{\mathfrak{p}_i\}_{i\geq 1}$ of P_{E_F}, that is, an ordering for which $\|\mathfrak{p}\|_i \leq \|\mathfrak{p}\|_j$ for all $1\leq i\leq j$, and let $a_1(E_F)$ denote the sequence

$$\{a_1(E_F)(\mathfrak{p}_i)\}_{i\geq 1}$$

of real numbers in the interval $[-2,2]$. Equidistribution statements about $a_1(E_F)$ do not depend on the particular ordering by norm we have chosen.

Until the end of this section, we assume that F contains kM. We begin by recalling classical results of Hecke and Deuring that yield equidistribution for $a_1(E_F)$ with respect to the measure

$$\mu_{\mathrm{cm}} = \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}},$$

supported on $[2,-2]$. Here dz denotes the restriction of the Lebesgue measure on $\mathbb{R}$ to the interval $[-2,2]$. The measure μ_{cm} is uniquely characterized by the fact that it is continuous and its n-th moment is $b_n := b_{0,n}$ (as in Theorem 1.4).

We actually require a slightly stronger equidistribution statement than the one above. Let c be a Frobenius conjugacy class of an arbitrary finite Galois extension F'/F, and let P_c denote the set of primes in P_{E_F} that are unramified in F' and whose Frobenius conjugacy class is c. We will show that the subsequence $a_{1,c}(E_F)$ of $a_1(E_F)$ obtained by restricting to the primes in P_c is also equidistributed with respect to μ_{cm}.

Remark 3.5. Henceforth, for a compact group G, let $\mu(G)$ denote its Haar measure. In terms of the (generalized) Sato–Tate conjecture, the measure μ_{cm} is seen as $\Phi_{1,*}(\mu(\mathrm{ST}(E_F)))$, where Φ_1 is the trace map defined in (1-1) and $\mathrm{ST}(E_F)=\mathrm{U}(1)$. Recall that the Sato–Tate group $\mathrm{ST}(E)$ of an elliptic curve E defined over k with CM by M is $\mathrm{U}(1)$ (embedded in $\mathrm{SU}(2)$) if M is contained in k, and the normalizer of $\mathrm{U}(1)$ in $\mathrm{SU}(2)$ if M is not contained in k.

We follow the presentation in [Gross 1980, Chapter 1]. Let $\mathfrak{p}$ be a prime of F of good reduction for E_F. Let $\overline{\mathbb{F}}_{\mathfrak{p}}$ denote the algebraic closure of the residue field of F at $\mathfrak{p}$. The image of the injection

$$\mathrm{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q} = M \hookrightarrow \mathrm{End}(E_{\overline{\mathbb{F}}_{\mathfrak{p}}}) \otimes \mathbb{Q}$$

contains the Frobenius endomorphism $\mathrm{Fr}_{\mathfrak{p}} : E_{\overline{\mathbb{F}}_{\mathfrak{p}}} \to E_{\overline{\mathbb{F}}_{\mathfrak{p}}}$, which acts on a point by raising its coordinates to the q-th power, where $q = \|\mathfrak{p}\|$. Let $\alpha(\mathfrak{p}) := \alpha(E_F)(\mathfrak{p}) \in M^*$ denote the preimage of $\mathrm{Fr}_{\mathfrak{p}}$ under this injection. Since the characteristic polynomial of $\mathrm{Fr}_{\mathfrak{p}}$ is reciprocal to the L-polynomial of E_F at $\mathfrak{p}$, we have

$$a_1(E_F)(\mathfrak{p}) = -\frac{1}{\|\mathfrak{p}\|^{1/2}}\big(\sigma(\alpha(\mathfrak{p})) + \overline{\sigma}(\alpha(\mathfrak{p}))\big). \tag{3-3}$$

For any place v of F, let F_v denote the completion of F at v and let $\mathbb{O}_v$ denote the ring of integers of F_v. Let $I_F = \prod_v' F_v$ denote the group of idèles of F. Here the product runs over all places v of F, and the prime means that if $\mathfrak{s} = (\mathfrak{s}_v)$ belongs to I_F, then $\mathfrak{s}_v$ is in $\mathbb{O}_v^*$ for all but finitely many v. We write $v_{\mathfrak{p}}$ for the valuation associated to a finite prime $\mathfrak{p}$ of F. We then attach to E_F the group homomorphism

$$\chi_{E_F} : I_F \to M^*$$

uniquely characterized by the following three properties:

(i) $\mathrm{Ker}(\chi_{E_F})$ is an open subgroup of I_F.

(ii) If $\mathfrak{s} = (a)$ is a principal idèle ($a \in F^*$), then $\chi_{E_F}(\mathfrak{s}) = N_{F/M}(a)$.

(iii) If $\mathfrak{s} = (\mathfrak{s}_v)$ is an idèle with $\mathfrak{s}_v = 1$ at all infinite places of F and at those finite places where E_F has bad reduction, then

$$\chi_{E_F}(\mathfrak{s}) = \prod_{v_{\mathfrak{p}}} \alpha(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{s}_{\mathfrak{p}})}.$$

3B1. *The 1-dimensional ℓ-adic representation attached to E_F.* Fix a prime ℓ different from the characteristic of $\overline{\mathbb{F}}_{\mathfrak{p}}$ and an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_\ell$, and let $V_\ell(E_F)$ denote the (rational) ℓ-adic Tate module of E_F. Define

$$V_\sigma(E) := V_\ell(E_F) \otimes_{M,\sigma} \overline{\mathbb{Q}}_\ell, \tag{3-4}$$

where the tensor product is taken via the embedding $M \hookrightarrow \overline{\mathbb{Q}}_\ell$ induced by σ. Similarly define $V_{\overline{\sigma}}(E)$. We then have an isomorphism of $\overline{\mathbb{Q}}_\ell[G_F]$-modules:

$$V_\ell(E_F) \otimes \overline{\mathbb{Q}}_\ell \simeq V_\sigma(E) \oplus V_{\overline{\sigma}}(E). \tag{3-5}$$

Let $\varrho_{\ell,\sigma} : G_F \to \mathrm{Aut}(V_\sigma(E))$ denote the ℓ-adic character corresponding to the action of G_F on $V_\sigma(E)$. If $\mathrm{Frob}_{\mathfrak{p}}$ is an arithmetic Frobenius at $\mathfrak{p}$ in G_F, then the value of $\varrho_{\ell,\sigma}(\mathrm{Frob}_{\mathfrak{p}})$ is $\sigma(\alpha(\mathfrak{p}))$. Define

$$\psi_{\ell,\sigma} : I_F \to \left(M \otimes_{M,\sigma} \overline{\mathbb{Q}}_\ell\right)^*, \quad \psi_{\ell,\sigma}(\mathfrak{s}) = \chi_{E_F}(\mathfrak{s}) \otimes \left(N_{F/M}(\mathfrak{s}^{-1})\right)_\ell,$$

where for an idèle $\mathfrak{s}$ in I_F, the component of the idèle $N_{F/M}(\mathfrak{s})$ in I_M corresponding to the place w is $\prod_{v|w} N_{F_v/M_w}(\mathfrak{s}_v)$, where the product runs over all places v of F lying over w. We then have $\psi_{\ell,\sigma}(F^*) = 1$, by property (ii). Thus $\psi_{\ell,\sigma}$ is a continuous character on the group $C_F = I_F/F^*$ of classes of idèles. Since its image is totally disconnected, it is a character of C_F/C_F^0, where C_F^0 is the identity component of C_F. Artin reciprocity yields an isomorphism $\mathrm{Rec} : G_F^{\mathrm{ab}} \to C_F/C_F^0$. Property (iii) then implies that $\psi_{\ell,\sigma} \circ \mathrm{Rec}(\mathrm{Frob}_{\mathfrak{p}}) = \sigma(\alpha(\mathfrak{p}))$, and thus

$$\psi_{\ell,\sigma} \circ \mathrm{Rec}(\mathrm{Frob}_{\mathfrak{p}}) = \varrho_{\ell,\sigma} \tag{3-6}$$

as ℓ-adic characters of G_F.

3B2. *The Hecke character attached to E_F.* A *Hecke character* of F is a continuous homomorphism $\psi : I_F \to \mathbb{C}^*$ such that $\psi(F^*) = 1$. For primes $\mathfrak{p}$ where ψ is unramified, let $\psi(\mathfrak{p})$ denote $\psi(\mathfrak{s})$, where $\mathfrak{s}_{\mathfrak{p}}$ is a uniformizer of $\mathbb{O}_{\mathfrak{p}}$ and $\mathfrak{s}_v = 1$ for $v \neq \mathfrak{p}$, and let $\psi(\mathfrak{p}) = 0$ when ψ is ramified at $\mathfrak{p}$. The L-function of ψ is defined as

$$L(\psi, s) := \prod_{\mathfrak{p}} \left(1 - \psi(\mathfrak{p}) \|\mathfrak{p}\|^{-s}\right)^{-1}.$$

Hecke [1920] showed that if ψ is nontrivial and takes values in U(1), then $L(\psi, s)$ is a nonzero holomorphic function for $\Re(s) \geq 1$. Let us fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$, so that we may view σ and $\overline{\sigma}$ as embeddings of M into $\mathbb{C}$. Define

$$\psi_{\infty,\sigma} : I_F \to \left(M \otimes_{M,\sigma} \mathbb{C}\right)^*, \quad \psi_{\infty,\sigma}(\mathfrak{s}) = \chi_{E_F}(\mathfrak{s}) \otimes \left(N_{F/M}(\mathfrak{s}^{-1})\right)_\infty,$$

where ∞ denotes the only infinite place of M. Property (ii) of χ_{E_F} implies that $\psi_{\infty,\sigma}$ is a Hecke character. It is unramified at the primes of good reduction for E_F, and we note that $\overline{\psi}_{\infty,\sigma} = \psi_{\infty,\overline{\sigma}}$. Let $|z|$ denote the absolute value of a complex number z and define

$$\psi^1_{\infty,\sigma} : I_F \to \mathrm{U}(1), \quad \psi^1_{\infty,\sigma}(\mathfrak{s}) = \psi_{\infty,\sigma}(\mathfrak{s}) / |\psi_{\infty,\sigma}(\mathfrak{s})|.$$

For every prime $\mathfrak{p}$ of good reduction for E_F, let

$$\alpha_1(\mathfrak{p}) := \alpha_1(E_F)(\mathfrak{p}) := \psi^1_{\infty,\sigma} \circ \mathrm{Rec}(\mathrm{Frob}_{\mathfrak{p}}) = \sigma(\alpha(\mathfrak{p}))/\|\mathfrak{p}\|^{1/2}. \tag{3-7}$$

Let α_1 denote the sequence $\{\alpha_1(\mathfrak{p}_i)\}_{i \geq 1}$.

3B3. *Equidistribution statements.* For a finite Galois extension F'/F and a conjugacy class c of $\mathrm{Gal}(F'/F)$, let P_c be as above. Let $\alpha_{1,c} := \alpha_{1,c}(E_F)$ denote the subsequence of α_1 obtained by restricting to the primes of P_c. Our goal is to prove the following proposition.

Proposition 3.6. *Let c be any conjugacy class of* $\mathrm{Gal}(F'/F)$*. Then $\alpha_{1,c}$ is equidistributed with respect to $\mu(\mathrm{U}(1))$.*

We first recall a theorem of Serre. Let G be a compact group and X the set of its conjugacy classes. Let P be an infinite subset of the primes of F, and let $\{\mathfrak{p}_i\}_{i\geq 1}$ be an ordering by norm of P. Assume that each prime $\mathfrak{p}$ in P has been assigned a corresponding element $x_{\mathfrak{p}}$ in X.

Theorem 3.7 [Serre 1998, p. I-23]. *The sequence $\{x_{\mathfrak{p}_i}\}_{i\geq 1}$ is equidistributed over X with respect to the image on X of the Haar measure of G if and only if $L(\varrho, s)$ is holomorphic and nonzero for $\Re(s) \geq 1$ for every irreducible and nontrivial representation ϱ of G. Here $L(\varrho, s)$ stands for the infinite product*

$$\prod_{\mathfrak{p}\in P} \det\bigl(1-\varrho(x_{\mathfrak{p}})\|\mathfrak{p}\|^{-s}\bigr)^{-1}.$$

We now use Theorem 3.7 to prove Proposition 3.6.

Proof. We first reduce to the case that F'/F is abelian (in fact, cyclic). Let τ be an element of c, and let f denote its order. Define

$$I(\tau) = \bigl\{i \in \{0, 1, \ldots, f-1\} \mid [\tau^i] = c\bigr\}.$$

Let H be the subfield of F' fixed by $\langle\tau\rangle$. The residue degree over F of a prime $\mathfrak{P}$ of H lying over $\mathfrak{p} \in P_c$ is 1, and thus $\alpha_1(E_H)(\mathfrak{P}) = \alpha_1(E_F)(\mathfrak{p})$. Then $\alpha_{1,c}(E_F)$ is the disjoint union

$$\bigsqcup_{i\in I(\tau)} \alpha_{1,\tau^i}(E_H),$$

where we identify τ^i with its conjugacy class in the cyclic group $\mathrm{Gal}(F'/H)$. To show that $\alpha_{1,c} = \alpha_{1,c}(E_F)$ is $\mu(\mathrm{U}(1))$-equidistributed, it suffices to show that all its subsequences $\alpha_{1,\tau^i}(E_H)$ are (any sequence that can be partitioned into a finite set of subsequences that are all equidistributed with respect to a fixed common measure is clearly equidistributed with respect to the same measure), and if we assume the proposition holds for abelian extensions, then this is true.

So suppose that F'/F is abelian, and define $G := \mathrm{U}(1)\times \mathrm{Gal}(F'/F)$ and $x_{\mathfrak{p}} := \alpha_1(\mathfrak{p}) \times \mathrm{Frob}_{\mathfrak{p}}$ for each prime in P_{E_F} unramified in F'/F. Since for such a prime, $x_{\mathfrak{p}} \in \mathrm{U}(1) \times \{c\}$ if and only if $\mathfrak{p} \in P_c$, proving the proposition is equivalent to showing that $\{x_{\mathfrak{p}_i}\}_{i\geq 1}$ is equidistributed over the set X of conjugacy classes of G with respect to the measure induced by the Haar measure of G. The irreducible characters of G are of the form $\phi_a \otimes \chi$, where $\phi_a : \mathrm{U}(1) \to \mathbb{C}^*$ is a character of $\mathrm{U}(1)$, which is of the form $\phi_a(z) = z^a$ for some integer a, and χ is an irreducible character of $\mathrm{Gal}(F'/F)$, which is 1-dimensional since $\mathrm{Gal}(F'/F)$ is abelian. By

Theorem 3.7, it is enough to show that if $\phi_a \otimes \chi$ is nontrivial, then

$$L(\phi_a \otimes \chi, s) = \prod_{\mathfrak{p}} \bigl(1 - \psi^1_{\infty,\sigma}(\mathfrak{p})^a \chi(\mathfrak{p}) \|\mathfrak{p}\|^{-s}\bigr)^{-1}$$

is holomorphic and nonzero for $\Re(s) \geq 1$. Via Artin reciprocity, we may view $(\psi^1_{\infty,\sigma})^a \otimes \chi$ as a Hecke character (with values in U(1)), and then $L(\phi_a \otimes \chi, s)$ is equal, up to a finite number of factors, to the Hecke L-function $L((\psi^1_{\infty,\sigma})^a \otimes \chi, s)$, which is holomorphic and nonzero for $\Re(s) \geq 1$. □

Recalling that

$$\mu_{\mathrm{cm}} = \frac{1}{\pi} \frac{dz}{\sqrt{4 - z^2}}$$

supported on $[-2, 2]$ is the image by Φ_1 of the Haar measure of U(1), we obtain the following.

Corollary 3.8. *Let E be an elliptic curve defined over k with CM by an imaginary quadratic field M. Let F be any field containing kM, let F'/F be a finite Galois extension, and let c be a conjugacy class of* $\mathrm{Gal}(F'/F)$. *Then*:

(i) *The sequence $a_{1,c}(E_F)$ is equidistributed with respect to the measure μ_{cm}.*

(ii) $\mathrm{M}_n[a_{1,c}(E_F)] = \mathrm{M}_n[a_1(E_F)]$.

3C. ***Equidistribution of $a_1(A)$ and $a_2(A)$.*** As in Section 3A, A is an abelian surface defined over k with $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over k with CM by M, and we have the tower of fields $kM \subseteq K \subseteq L$, where L/k is the minimal extension over which all the homomorphisms from $A_{\overline{\mathbb{Q}}}$ to $E_{\overline{\mathbb{Q}}}$ are defined, and K/k is the minimal extension over which all the endomorphisms of $A_{\overline{\mathbb{Q}}}$ are defined.

For any field extension F/k, let P_{A_F} denote the set of primes of F at which A_F has good reduction. For $\mathfrak{p}$ in P_{A_F}, we write the normalized L-polynomial for A_F at $\mathfrak{p}$ as

$$\bar{L}_{\mathfrak{p}}(A_F, T) = 1 + a_1(A_F)(\mathfrak{p})T + a_2(A_F)(\mathfrak{p})T^2 + a_1(A_F)(\mathfrak{p})T^3 + T^4.$$

Let P be the set of primes lying in P_{A_F} and P_{E_F} that are unramified in FL. Choose an ordering by norm $\{\mathfrak{p}_i\}_{i\geq 1}$ of P, and let $a_1(A_F)$ and $a_2(A_F)$ denote the sequences

$$\{a_1(A_F)(\mathfrak{p}_i)\}_{i\geq 1}, \quad \{a_2(A_F)(\mathfrak{p}_i)\}_{i\geq 1},$$

respectively. In this section, we use the results in Sections 3A and 3B to prove equidistribution for $a_1(A)$ and $a_2(A)$.

Lemma 3.9. *Let $\mathfrak{p}$ be a prime of good reduction for A and E that splits in kM and is unramified in L.*

(i) *With* $u_1 = \operatorname{Re} a_1(\theta)(\mathrm{Frob}_{\mathfrak{p}})$ *and* $u_2 = \operatorname{Im} a_1(\theta)(\mathrm{Frob}_{\mathfrak{p}})$, *we have*

$$a_1(A)(\mathfrak{p}) = u_1 a_1(E)(\mathfrak{p}) \pm u_2\sqrt{4 - a_1(E)(\mathfrak{p})^2}.$$

(ii) *With* $v_1 = \operatorname{Re} a_2(\theta)(\mathrm{Frob}_{\mathfrak{p}})$ *and* $v_2 = \operatorname{Im} a_2(\theta)(\mathrm{Frob}_{\mathfrak{p}})$, *we have*

$$a_2(A)(\mathfrak{p}) = v_1 a_1(E)(\mathfrak{p})^2 - 2v_1 + |a_1(\theta)(\mathrm{Frob}_{\mathfrak{p}})|^2 \mp v_2 a_1(E)(\mathfrak{p})\sqrt{4 - a_1(E)(\mathfrak{p})^2}.$$

Proof. Define $V_\sigma(A)$ and $V_{\overline{\sigma}}(A)$ as in (3-4). We then have the following isomorphism of $\overline{\mathbb{Q}}_\ell[G_{kM}]$-modules:

$$V_\ell(A_{kM}) \otimes \overline{\mathbb{Q}}_\ell \simeq V_\sigma(A) \oplus V_{\overline{\sigma}}(A).$$

By arguments analogous to those in [Fité 2013, Theorem 3.1], we have

$$V_\sigma(A) \simeq \theta_{M,\sigma}(E, A) \otimes V_\sigma(E), \qquad V_{\overline{\sigma}}(A) \simeq \theta_{M,\overline{\sigma}}(E, A) \otimes V_{\overline{\sigma}}(E).$$

Thus there is an isomorphism of $\overline{\mathbb{Q}}_\ell[G_{kM}]$-modules:

$$V_\ell(A) \otimes \overline{\mathbb{Q}}_\ell \simeq \theta_{M,\sigma}(E, A) \otimes V_\sigma(E) \oplus \theta_{M,\overline{\sigma}}(E, A) \otimes V_{\overline{\sigma}}(E). \tag{3-8}$$

To shorten notation, we write $\alpha_1(\mathfrak{p})$ for $\alpha_1(E_{kM})(\mathfrak{p}) = \sigma(\alpha(E_{kM})(\mathfrak{p}))/\|\mathfrak{p}\|^{1/2}$, as defined in (3-7). Then $\overline{\alpha_1(\mathfrak{p})} = \overline{\sigma}(\alpha(E_{kM})(\mathfrak{p}))/\|\mathfrak{p}\|^{1/2}$, and (3-8) implies that

$$\begin{aligned} a_1(A_{kM})(\mathfrak{p}) &= -a_1(\mathfrak{p})\alpha_1(\mathfrak{p}) - \overline{a_1(\mathfrak{p})\alpha_1(\mathfrak{p})}, \\ a_2(A_{kM})(\mathfrak{p}) &= a_2(\mathfrak{p})\alpha_1(\mathfrak{p})^2 + \overline{a_2(\mathfrak{p})\alpha_1(\mathfrak{p})^2} + a_1(\mathfrak{p})\overline{a_1(\mathfrak{p})}, \end{aligned} \tag{3-9}$$

where $a_i(\mathfrak{p})$ denotes $a_i(\theta)(\mathrm{Frob}_{\mathfrak{p}})$. The proposition then follows from the fact that $a_1(E_{kM})(\mathfrak{p}) = -\alpha_1(\mathfrak{p}) - \overline{\alpha_1(\mathfrak{p})}$. □

Proposition 3.10. *For* $\tau \in \mathrm{Gal}(L/kM)$, *let* $u(\tau) = |a_1(\theta)(\tau)|$. *Then* $a_1(A_{kM})$ *and* $a_2(A_{kM})$ *are equidistributed with respect to the measures*

(i) $\displaystyle \mu(a_1(A_{kM})) := \frac{1}{[L:kM]}\frac{1}{\pi}\sum_\tau \frac{dz}{\sqrt{4u(\tau)^2 - z^2}}\mathbf{1}_{[-2u(\tau),2u(\tau)]},$

(ii) $\displaystyle \mu(a_2(A_{kM})) := \frac{1}{[L:kM]}\frac{1}{\pi}\sum_\tau \frac{dz}{\sqrt{4 - (u(\tau)^2 - z)^2}}\mathbf{1}_{[u(\tau)^2-2,u(\tau)^2+2]},$

whose support lies in the intervals $I_1 = [-4, 4]$ *and* $I_2 = [-6, 6]$, *respectively. In each sum,* τ *ranges over* $\mathrm{Gal}(L/kM)$ *and* $\mathbf{1}_{[a,b]}$ *is the characteristic function of the interval* $[a, b] \subseteq \mathbb{R}$. *Moreover, we have*

(i) $\displaystyle \mathrm{M}_n[a_1(A_{kM})] = \frac{1}{[L:kM]}\sum_\tau b_{0,n}u(\tau)^n,$

(ii) $\displaystyle \mathrm{M}_n[a_2(A_{kM})] = \frac{1}{[L:kM]}\sum_\tau b_{u(\tau)^2,n},$

where the integer $b_{m,n}$ *is the coefficient of* X^n *in* $(X^2 + mX + 1)^n$.

Proof. We can rewrite the equations in (3-9) as follows:

$$a_1(A_{kM})(\mathfrak{p}) = |a_1(\mathfrak{p})|\left(\frac{-a_1(\mathfrak{p})}{|a_1(\mathfrak{p})|}\alpha_1(\mathfrak{p}) + \frac{-\overline{a_1(\mathfrak{p})}}{|a_1(\mathfrak{p})|}\overline{\alpha_1(\mathfrak{p})}\right),$$

$$\begin{aligned} a_2(A_{kM})(\mathfrak{p}) &= |a_2(\mathfrak{p})|\left(\frac{a_2(\mathfrak{p})^{1/2}}{|a_2(\mathfrak{p})|^{1/2}}\alpha_1(\mathfrak{p}) + \frac{\overline{a_2(\theta)}^{1/2}}{|a_2(\mathfrak{p})|^{1/2}}\overline{\alpha_1(\mathfrak{p})}\right)^2 - 2|a_2(\mathfrak{p})| + |a_1(\mathfrak{p})|^2 \\ &= \left(a_2(\mathfrak{p})^{1/2}\alpha_1(\mathfrak{p}) + \overline{a_2(\mathfrak{p})}^{1/2}\overline{\alpha_1(\mathfrak{p})}\right)^2 - 2 + |a_1(\mathfrak{p})|^2, \end{aligned}$$

where $a_i(\mathfrak{p})$ denotes $a_i(\theta)(\mathrm{Frob}_{\mathfrak{p}})$, and we have used $|a_2(\mathfrak{p})| = 1$. The equidistribution statements now follow from the Chebotarev density theorem and two facts below:

(1) For any $z \in \mathrm{U}(1)$ and any conjugacy class c of $\mathrm{Gal}(L/kM)$, the sequence $z\alpha_{1,c}$ is $\mu(\mathrm{U}(1))$-equidistributed on $\mathrm{U}(1)$. Indeed, Proposition 3.6 ensures equidistribution of $\alpha_{1,c}$, and invariance under translations is in fact the defining property of the Haar measure. Thus the sequence $z\alpha_{1,c} + \overline{z}\overline{\alpha}_{1,c}$ is μ_{cm}-equidistributed on $I_1(E_{kM}) = [-2, 2]$.

(2) If a sequence $\beta = \{\beta_i\}_{i\geq 1}$ is μ_{cm}-equidistributed on $[-2, 2]$, then for $u \in \mathbb{R}_{>0}$:

- The sequence $u\beta$ is equidistributed on $[-2u, 2u]$ with respect to the measure
$$\frac{1}{\pi}\frac{dz}{\sqrt{4u^2 - z^2}}.$$
- The sequence $\{\beta_i^2 - 2 + u^2\}_{i\geq 1}$ is equidistributed on $[u^2 - 2, u^2 + 2]$ with respect to the measure
$$\frac{1}{\pi}\frac{dz}{\sqrt{4 - (u^2 - z)^2}}.$$

Regarding the moments, the Chebotarev density theorem implies that

$$\mathrm{M}_n[a_1(A_{kM})] = \frac{1}{[L : kM]}\sum_{\tau} |a_1(\theta)(\tau)|^n \cdot \mathrm{M}_n\left[z([\tau])\alpha_1 + \overline{z([\tau])}\overline{\alpha}_1 \mid P_{[\tau]}\right],$$

where $z([\tau]) = -a_1(\theta)(\tau)/|a_1(\theta)(\tau)|$. But now (1) implies that

$$\mathrm{M}_n\left[z([\tau])\alpha_1 + \overline{z([\tau])}\overline{\alpha}_1 \mid P_{[\tau]}\right] = b_{0,n}.$$

The same argument is used to compute

$$\mathrm{M}_n[a_2(A_{kM})] = \frac{1}{[L : kM]}\sum_{\tau}\sum_{i=0}^{n}\binom{n}{i}\binom{2i}{i}\left(|a_1(\theta)(\tau)|^2 - 2\right)^{n-i}.$$

One then applies

$$\begin{aligned}\sum_{i=0}^{n}\binom{n}{i}\binom{2i}{i}(m-2)^{n-i} &= [X^n]\big((X+1)^2+(m-2)X\big)^n \\ &= [X^n](X^2+mX+1)^n = b_{m,n},\end{aligned}$$

where $[X^n]f(X)$ denotes the coefficient of X^n in the polynomial $f(X)$. □

We now generalize the definitions of $o(r)$ and $\overline{o}(s)$ given in Section 1B for $k=\mathbb{Q}$.

Definition 3.11. Let $o(r)$ count the elements in $\mathrm{Gal}(L/kM)$ whose projection in $\mathrm{Gal}(K/kM)$ has order r. Let $\overline{o}(s)$ count the elements in $\mathrm{Gal}(L/k)\setminus\mathrm{Gal}(L/kM)$ of order s.

If $k=kM$, the sequence $a_i(A)$ is equidistributed with respect to $\mu(a_i(A_{kM}))$ and $\mathrm{M}_n[a_i(A)]=\mathrm{M}_n[a_i(A_{kM})]$, for $i=1,2$.

Corollary 3.12. *Suppose $k\neq kM$. Then $a_1(A)$ and $a_2(A)$ are equidistributed with respect to the measures*

(i) $\mu(a_1(A)) := \frac{1}{2}\mu(a_1(A_{kM}))+\frac{1}{2}\delta_0$,

(ii) $$\mu(a_2(A)) := \tfrac{1}{2}\mu(a_1(A_{kM})) + \frac{1}{2[L:kM]}\big(\bar{o}(2)\delta_2+\bar{o}(4)\delta_{-2}+\bar{o}(6)\delta_{-1}+\bar{o}(12)\delta_1\big),$$

whose support lies in the intervals $I_1=[-4,4]$ and $I_2=[-6,6]$, respectively. Here δ_z denotes the Dirac measure at z. We also have

(i) $$\mathrm{M}_n[a_1(A)] = \frac{1}{[L:k]}\big(o(1)2^n+o(3)+o(4)2^{n/2}+o(6)3^{n/2}\big)b_{0,n},$$

(ii) $$\begin{aligned}\mathrm{M}_n[a_2(A)] = \frac{1}{[L:k]}\big(&o(1)b_{4,n}+o(2)b_{0,n}+o(3)b_{1,n}+o(4)b_{2,n}+o(6)b_{3,n}\\ &+\bar{o}(2)2^n+\bar{o}(4)(-2)^n+\bar{o}(6)(-1)^n+\bar{o}(12)\big).\end{aligned}$$

Proof. We focus on the proof of the statements about the moments, since the arguments involved suffice to deduce the statements about the measures. Statement (i) follows from Propositions 3.2, 3.4, and 3.10, and the equality

$$\mathrm{M}_{2n}[a_1(A_{kM})] = 2\cdot\mathrm{M}_{2n}[a_1(A)],$$

which follows from the fact that if $\mathfrak{p}$ is a prime of k, where A has good reduction and $\mathfrak{p}$ is inert in kM, then A is supersingular at $\mathfrak{p}$ and $a_1(A)(\mathfrak{p})=0$.

For (ii), let ν denote the nontrivial conjugacy class of $\mathrm{Gal}(kM/k)$. Note that

$$\mathrm{M}_n[a_2(A)] = \tfrac{1}{2}\mathrm{M}_n[a_2(A)\mid P_1]+\tfrac{1}{2}\mathrm{M}_n[a_2(A)\mid P_\nu].$$

To compute $\mathrm{M}_n[a_2(A) \mid P_1] = \mathrm{M}_n[a_2(A_{kM})]$, we apply Proposition 3.10. We then claim that

$$\mathrm{M}_n[a_2(A_k) \mid P_\nu] = \frac{1}{[L : kM]}\big(\bar{o}(2)2^n + \bar{o}(4)(-2)^n + \bar{o}(6)(-1)^n + \bar{o}(12)\big).$$

We may restrict to primes $\mathfrak{p}$ of k that are inert in kM, of absolute residue degree 1, and of good reduction for both A and E. The polynomial $\bar{L}_\mathfrak{p}(A, T)$ must then be one of the five listed in (3-2).

We now consider the Rankin–Selberg polynomial $\bar{L}_\mathfrak{p}\big(E, \theta_\mathbb{Q}(E, A), T\big)$, whose roots are all products of roots of $\bar{L}_\mathfrak{p}(E, T) = 1 + T^2$, and all roots of the polynomial $\det\big(1 - \theta_\mathbb{Q}(E, A)(\mathrm{Frob}_\mathfrak{p})T\big)$. More explicitly, if s is the order of $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(L/k)$, one may apply Proposition 3.3 to compute $\bar{L}_\mathfrak{p}\big(E, \theta_\mathbb{Q}(E, A), T\big)$. This yields:

$$\begin{array}{lll} s = 2\colon\ (1 + T^2)^4 & s = 6\colon\ (1 - T^2 + T^4)^2 & s = 12\colon\ (1 + T^2 + T^4)^2 \\ s = 4\colon\ (1 - T^2)^4 & s = 8\colon\ (1 + T^4)^2 & \end{array}$$

By arguments analogous to those of [Fité 2013, Theorem 3.1], there is an inclusion of $\mathbb{Q}_\ell[G_k]$-modules

$$V_\ell(A) \subseteq V_\ell(E) \otimes \theta_\mathbb{Q}(E, A).$$

This implies that $\bar{L}_\mathfrak{p}(A, T)$ divides $\bar{L}_\mathfrak{p}(E, \theta_\mathbb{Q}(E, A), T)$. It immediately follows that $\bar{L}_\mathfrak{p}(A, T)$ is

$$\begin{array}{lll} s = 2\colon\ (1 + T^2)^2 & s = 6\colon\ 1 - T^2 + T^4 & s = 12\colon\ 1 + T^2 + T^4 \\ s = 4\colon\ (1 - T^2)^2 & s = 8\colon\ 1 + T^4 & \end{array}$$

Finally, we observe that the condition $\bar{L}_\mathfrak{p}(A, T)$ divides $\bar{L}_\mathfrak{p}(E, \theta_\mathbb{Q}(E, A), T)$ implies that s can not attain any value other than the ones considered. □

3D. ***Additional remarks.*** As noted in the introduction, all 32 of the genus-2 Sato–Tate groups with identity component isomorphic to $\mathrm{U}(1)$ can arise as the Sato–Tate group of an abelian variety A defined over k with $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over k (with CM).

However, not all 10 of the genus-2 Sato–Tate groups with identity component isomorphic to $\mathrm{SU}(2)$ can arise as the Sato–Tate group of an abelian variety A defined over k such that $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over k (without CM).[8] The Sato–Tate groups for which this is not true are the four whose component group contains an element of order 4 or 6. Indeed, recall that $\theta_\mathbb{Q}(E, A)$ and $\theta_\mathbb{Q}(A)$ are the representations afforded by $\mathrm{Hom}(E_L, A_L) \otimes \mathbb{Q}$ and $\mathrm{End}(A_L) \otimes \mathbb{Q}$. As in the proof of Proposition 3.2, one can then show that $\theta_\mathbb{Q}(A) = \theta_\mathbb{Q}(E, A)^{\otimes 2}$,

[8] All Sato–Tate groups with identity component $\mathrm{SU}(2)$ can occur for an A over k such that $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$ for *some* elliptic curve E, but this curve need not be defined over k.

that is, $a_1(\theta_{\mathbb{Q}}(A)) = a_1(\theta_{\mathbb{Q}}(E, A))^2$. But if $\tau \in \mathrm{Gal}(K/k)$ has order 4 or 6, then $a_1(\theta_{\mathbb{Q}}(A))(\tau) = 2$ or 3, which are not squares in $\mathbb{Q}$.

We end this section by computing the density $z_1(A_k)$ of zero traces of an abelian variety A defined over k such that $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$ for some elliptic curve E defined over $\overline{\mathbb{Q}}$.

Lemma 3.13. *Let A be an abelian variety defined over k such that $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$, where E is an elliptic curve defined over $\overline{\mathbb{Q}}$ (not necessarily over k). Let M denote the CM field if E has CM, and let $M = \mathbb{Q}$ otherwise. Then*

$$z_1(A_k) = \begin{cases} \dfrac{o(2)}{|\mathrm{Gal}(L/kM)|} & \textit{if } [kM:k] = 1, \\[2ex] \dfrac{1}{2} + \dfrac{1}{2}\dfrac{o(2)}{|\mathrm{Gal}(L/kM)|} & \textit{if } [kM:k] = 2. \end{cases}$$

Proof. Except for a set of density zero, any prime $\mathfrak{p}$ of k that does not split in kM is supersingular, in which case $a_1(A)(\mathfrak{p}) = 0$. This gives density 0 in the first case and density $\frac{1}{2}$ in the second case. Among the primes that split in kM, we wish to show that exactly the proportion $o(2)/|\mathrm{Gal}(L/kM)|$ have trace 0. Among these primes, the density of the supersingular primes is zero. Let $\mathfrak{p}$ be a nonsupersingular prime of good reduction for A that splits in kM. From Remark 4.8 in [Fité et al. 2012] in the non-CM case, and from Proposition 3.4 in the CM case, the roots of $L_{\mathfrak{p}}(A, T)$ are α, $\overline{\alpha}$, $\zeta_r\alpha$, $\overline{\zeta}_r\overline{\alpha}$, where r is the order of $\mathrm{Frob}_{\mathfrak{p}}$ in $\mathrm{Gal}(K/k)$ and where $\alpha/\overline{\alpha}$ is not a root of unity. It follows that $\alpha + \overline{\alpha} + \zeta_r\alpha + \overline{\zeta}_r\overline{\alpha} = 0$ if and only if $r = 2$. One then applies the Chebotarev density theorem. □

4. Twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$

In this section, we strengthen the results of Section 3 in the particular case that $k = \mathbb{Q}$ and $A \sim_{\mathbb{Q}} \mathrm{Jac}(C)$, where C is a twist of the curve $y^2 = x^5 - x$ or $y^2 = x^6 + 1$. We first introduce some convenient notation. Let C_2^0 and C_3^0 denote the curves defined over $\mathbb{Q}$ by the equations

$$C_2^0\colon\ y^2 = x^6 - 5x^4 - 5x^2 + 1, \qquad C_3^0\colon\ y^2 = x^6 + 1.$$

The curve C_2^0 is a twist of $y^2 = x^5 - x$, as one may verify by computing their respective Igusa invariants, as defined in [Igusa 1960]. As shown below, the Jacobian of C_2^0 is $\mathbb{Q}$-isogenous to the square of an elliptic curve defined over $\mathbb{Q}$, a property that the curve $y^2 = x^5 - x$ does not enjoy. We also note that the minimal field of definition of the endomorphisms of the Jacobian of C_2^0 is $\mathbb{Q}(\sqrt{-2})$, but for $y^2 = x^5 - x$ it is $\mathbb{Q}(i, \sqrt{-2})$.

Let E_2^0 and E_3^0 denote the elliptic curves defined over $\mathbb{Q}$ by the equations

$$E_2^0\colon\ Y^2 = X^3 - 5X^2 - 5X + 1, \qquad E_3^0\colon\ Y^2 = X^3 + 1.$$

We note that $j(E_2^0) = 2^6 5^3$ and $j(E_3^0) = 0$, and thus E_2^0 has CM by $\mathbb{Q}(\sqrt{-2})$ and E_3^0 has CM by $\mathbb{Q}(\sqrt{-3})$.

To simplify notation, throughout this section d denotes either 2 or 3, and we write C^0 for C_d^0, E^0 for E_d^0, and M for $\mathbb{Q}(\sqrt{-d})$. We use C to denote a twist of C^0 defined over $\mathbb{Q}$. In the context of Section 3, we are specializing $A_{\overline{\mathbb{Q}}} \sim E^2_{\overline{\mathbb{Q}}}$ to the case where $A = \mathrm{Jac}(C)$ and $E = E^0$, as we now show.

4A. *Fields of definition of isomorphisms.*

Lemma 4.1. $\mathrm{Jac}(C_d^0)$ *is* $\mathbb{Q}$*-isogenous to* $(E_d^0)^2$.

Proof. We proceed as in the proof of Lemma 4.1 in [Fité and Lario 2013]. The quotient of C_d^0 by the nonhyperelliptic involution $\alpha(x, y) = (-x, y)$ is precisely the elliptic curve E_d^0, and thus $\mathrm{Jac}(C_d^0) \sim_{\mathbb{Q}} E_d^0 \times E$, where E is also an elliptic curve defined over $\mathbb{Q}$. The automorphism $\gamma(x, y) = (1/x, y/x^3)$ does not commute with α, which implies that $\mathrm{End}(\mathrm{Jac}(C^0))$ is nonabelian, and therefore $\mathrm{Jac}(C_d^0) \sim_{\mathbb{Q}} (E_d^0)^2$. □

Lemma 4.2. *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 endomorphisms of* $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ *are defined.*

Proof. Let K_a (resp. K_e) denote the minimal number field over which all the automorphisms of $C_{\overline{\mathbb{Q}}}$ (resp. all the endomorphisms of $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$) are defined. The fact that $\mathrm{Aut}(C_{K_a})$ is nonabelian and contains a nonhyperelliptic involution implies that $\mathrm{Jac}(C)_{K_a} \sim E^2$, where E is an elliptic curve defined over K_a. Since E has CM by M, it follows that $K_e = K_a M$. But [Cardona 2001, Proposition 7.3.1] asserts that $M = \mathbb{Q}(\sqrt{-3})$ is already contained in K_a if C is a twist of C_3^0, whereas [Cardona 2006, Proposition 8] states that $M = \mathbb{Q}(\sqrt{-2})$ is already contained in K_a if C is a twist of C_2^0. □

We use K to denote the field given by Lemma 4.2. We note that K is a Galois extension of $\mathbb{Q}$, and we have $M \subseteq K$, with equality in the case $C = C^0$.

Lemma 4.3. *Let* ϕ *be an isomorphism from* $C^0_{\overline{\mathbb{Q}}}$ *to* $C_{\overline{\mathbb{Q}}}$. *The following number fields coincide*:

(i) *the minimal field over which all isomorphisms from* $C^0_{\overline{\mathbb{Q}}}$ *to* $C_{\overline{\mathbb{Q}}}$ *are defined*;

(ii) *the compositum of* K (*or even just* M) *and the minimal field* L_ϕ *over which* ϕ *is defined*;

(iii) *the minimal field over which all homomorphisms from* $\mathrm{Jac}(C^0)_{\overline{\mathbb{Q}}}$ *to* $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ *are defined*;

(iv) *the minimal field over which all homomorphisms from* $E^0_{\overline{\mathbb{Q}}}$ *to* $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ *are defined.*

Proof. Let L_1, L_2, L_3, and L_4 denote the fields defined by (i), (ii), (iii), and (iv), respectively. Any isomorphism ψ from $C^0_{\overline{\mathbb{Q}}}$ to $C_{\overline{\mathbb{Q}}}$ can be written as $\psi = \alpha \circ \phi$ and $\phi \circ \alpha^0$ for some $\alpha \in \mathrm{Aut}(C_K)$ and some $\alpha^0 \in \mathrm{Aut}(C^0_M)$. This implies that $L_1 \subseteq ML_\phi \subseteq KL_\phi = L_2$. Conversely, for any $\alpha^0 \in \mathrm{Aut}(C^0_M)$ and $\alpha \in \mathrm{Aut}(C_K)$, the compositions $\alpha \circ \phi$ and $\phi \circ \alpha^0$ are isomorphisms from $C^0_{\overline{\mathbb{Q}}}$ to $C_{\overline{\mathbb{Q}}}$. It follows that $L_2 \subseteq L_1$. Thus we have shown $L_1 = ML_\phi = KL_\phi = L_2$.

The isomorphism from $C^0_{L_\phi}$ to C_{L_ϕ} induces an isogeny $\mathrm{Jac}(C^0)_{L_\phi} \sim \mathrm{Jac}(C)_{L_\phi}$, which we also denote by ϕ. Any homomorphism from $\mathrm{Jac}(C^0)_{\overline{\mathbb{Q}}}$ to $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ can be written as $\psi \circ \phi$ for some $\psi \in \mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$. This implies that $L_3 \subseteq L_\phi K, L_\phi M = L_2$. Conversely, it is clear that L_1 is contained in L_3.

Any endomorphism ϕ from $\mathrm{Jac}(C^0)_{\overline{\mathbb{Q}}}$ to $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ can be written as $\phi_2 \circ \phi_1$, where $\phi_1 \in \mathrm{Hom}(\mathrm{Jac}(C^0), (E^0)^2) \otimes \mathbb{Q}$ and $\phi_2 \in (\mathrm{Hom}(E^0_{L_4}, \mathrm{Jac}(C)_{L_4}) \otimes \mathbb{Q})^2$. Thus $L_3 \subseteq L_4$. Conversely, any homomorphism from $E^0_{\overline{\mathbb{Q}}}$ to $\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}$ can be written as $\phi_2 \circ \phi_1$, where $\phi_1 \in \mathrm{Hom}(E^0, \mathrm{Jac}(C^0)) \otimes \mathbb{Q}$ and ϕ_2 is an element of $\mathrm{Hom}(\mathrm{Jac}(C^0)_{L_3}, \mathrm{Jac}(C)_{L_3}) \otimes \mathbb{Q}$. Thus $L_4 \subseteq L_3$. □

We use L to denote the field given by Lemma 4.3, and we note that L is a Galois extension of $\mathbb{Q}$ that contains K.

Remark 4.4. If A is the abelian three-fold $E^0 \times \mathrm{Jac}(C)$, we observe that L coincides with the minimal field over which all the endomorphisms of $A_{\overline{\mathbb{Q}}}$ are defined. It follows that the component group of $\mathrm{ST}(A)$ is isomorphic to $\mathrm{Gal}(L/\mathbb{Q})$.

4B. ***The Galois module*** $\mathbf{Hom}(E^0_L, \mathbf{Jac}(C)_L)$**.** We now compute $\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))$, strengthening Lemma 3.9 in the case where $A \sim_{\mathbb{Q}} \mathrm{Jac}(C)$. We take advantage of the following fact: the group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of $G_{C^0} := \mathrm{Aut}(C^0_M) \rtimes \mathrm{Gal}(M/\mathbb{Q})$. Here the action of $\mathrm{Gal}(M/\mathbb{Q})$ on $\mathrm{Aut}(C^0_M)$ is the natural one (see [Fité and Lario 2013, §2]).

More precisely, let $\phi : C_L \to C^0_L$ be an isomorphism. Then

$$\lambda_\phi : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow G_{C^0}, \quad \lambda_\phi(\sigma) = \big(\phi({}^\sigma\phi)^{-1}, \pi_{L/M}(\sigma)\big)$$

is a monomorphism of groups, where $\pi_{L/M} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(M/\mathbb{Q})$ is the natural projection, as in [Fité and Lario 2013, Lemma 2.1]. Now let

$$\mathrm{Res}^{\mathbb{Q}}_M \lambda_\phi : \mathrm{Gal}(L/M) \hookrightarrow \mathrm{Aut}(C^0_M)$$

be the restriction of λ_ϕ at $\mathrm{Gal}(L/M)$. Consider the 2-dimensional M-rational representation

$$\theta_{E^0,C^0} : \mathrm{Aut}(C^0_M) \to \mathrm{Aut}_{\overline{\mathbb{Q}}}\big(\mathrm{Hom}(E^0_M, \mathrm{Jac}(C^0)_M) \otimes_{M,\sigma} \overline{\mathbb{Q}}\big)$$

defined by $\theta_{E^0,C^0}(\alpha)(\psi) = \alpha \circ \psi$. As in [Fité and Lario 2013, Theorem 2.1], one then has

$$\theta_{E^0,C^0} \circ \mathrm{Res}^{\mathbb{Q}}_M \lambda_\phi \simeq \theta_{M,\sigma}(E^0, \mathrm{Jac}(C)), \tag{4-1}$$

Class	1a	2a	2b	3a	4a	6a	8a	8b
Size	1	1	12	8	6	8	6	6
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	-1	1	1	1	-1	-1
χ_3	2	2	0	-1	2	-1	0	0
χ_4	2	-2	0	-1	0	1	$\sqrt{-2}$	$-\sqrt{-2}$
χ_5	2	-2	0	-1	0	1	$-\sqrt{-2}$	$\sqrt{-2}$
χ_6	3	3	1	0	-1	0	-1	-1
χ_7	3	3	-1	0	-1	0	1	1
χ_8	4	-4	0	1	0	-1	0	0

Table 1. Character table of $\mathrm{Aut}((C_2^0)_M) \simeq \langle 48, 29\rangle$.

Class	1a	2a	2b	2c	3a	4a	6a	6b	6c
Size	1	1	2	6	2	6	2	2	2
χ_1	1	1	1	1	1	1	1	1	1
χ_2	1	1	1	-1	1	-1	1	1	1
χ_3	1	1	-1	-1	1	1	-1	-1	1
χ_4	1	1	-1	1	1	-1	-1	-1	1
χ_5	2	2	-2	0	-1	0	1	1	-1
χ_6	2	-2	0	0	2	0	0	0	-2
χ_7	2	2	2	0	-1	0	-1	-1	-1
χ_8	2	-2	0	0	-1	0	$-\sqrt{-3}$	$\sqrt{-3}$	1
χ_9	2	-2	0	0	-1	0	$\sqrt{-3}$	$-\sqrt{-3}$	1

Table 2. Character table of $\mathrm{Aut}((C_3^0)_M) \simeq \langle 24, 8\rangle$.

where $\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))$ is the representation of $\mathrm{Gal}(L/M)$ in Definition 3.1.

Lemma 4.5. *Let C be a twist of C^0. Then*

$$\mathrm{Tr}\,\theta_{E^0,C^0} = \begin{cases} \chi_4 \text{ or } \chi_5 & \text{if } C^0 = C_2^0 \text{ (see Table 1)}, \\ \chi_8 \text{ or } \chi_9 & \text{if } C^0 = C_3^0 \text{ (see Table 2)}. \end{cases}$$

Proof. A glance at Tables 1 and 2 tells us that any M-rational faithful representation of degree 2 must have trace χ_4 or χ_5 when $C^0 = C_2^0$, or trace χ_8 or χ_9 when $C^0 = C_3^0$. The two possibilities in each case correspond to the two different embeddings of M into $\overline{\mathbb{Q}}$. □

Proposition 4.6. *The index of K in L is at most* 2.

Proof. As in Lemma 4.1, let α be the nonhyperelliptic involution $\alpha(x, y) = (-x, y)$ of C^0. Let E be the elliptic curve $C_K/\langle\phi^{-1}\alpha\phi\rangle$ defined over K (note that $\phi^{-1}\alpha\phi$ is an automorphism of C, all of which are defined over K). The isomorphism $\phi : C_L \to C_L^0$ induces an isomorphism $\tilde{\phi} : E_L \to E_L^0$. Thus E is a K-twist of E^0.

From characterization (iii) of L in Lemma 4.3, it is clear that L is the compositum of K and the minimal field $L_{\tilde\phi}$ over which $\tilde\phi$ is defined.

When $C^0 = C_2^0$, we have $j(E) \neq 0, 1728$, and by [Silverman 2009, p. 304], it follows that $\tilde\phi$ is then defined over a quadratic extension of K and $[L:K] \leq 2$. When $C^0 = C_3^0$, we have $j(E) = 0$, and in this case $L = K(\sqrt[6]{\gamma})$, for some $\gamma \in K$. Let $L_0 = K(\sqrt{\gamma})$. It suffices to show that $\sqrt[3]{\gamma} \in L_0$.

Suppose for the sake of contradiction that $\sqrt[3]{\gamma} \notin L_0$. Then $\mathrm{Gal}(L/L_0) \simeq \mathrm{C}_3$. Lemma 4.5 then implies that if τ is a nontrivial element of $\mathrm{Gal}(L/L_0)$, then $\mathrm{Tr}\,\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))(\tau) = -1$. Therefore, the restriction of the representation afforded by the $\mathrm{Gal}(L/M)$-module $\mathrm{Hom}(E_L^0, \mathrm{Jac}(C)_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$ to $\mathrm{Gal}(L/L_0)$ is

$$\mathrm{Res}^M_{L_0}\, \theta_{M,\sigma}(E^0, \mathrm{Jac}(C)) \simeq \chi \oplus \overline{\chi},$$

where χ is any of the two nontrivial characters of $\mathrm{Gal}(L/L_0)$. As in [Fité 2013, Theorem 3.1], we have

$$\mathrm{Res}^M_{L_0}\, \theta_{M,\sigma}(E^0, \mathrm{Jac}(C)) \otimes V_\sigma(E^0) \simeq V_\sigma(\mathrm{Jac}(C)),$$

as $\overline{\mathbb{Q}}_\ell[G_{L_0}]$-modules. This implies that

$$V_\sigma(\mathrm{Jac}(C)) \simeq \bigl(\chi \otimes V_\sigma(E^0)\bigr) \oplus \bigl(\overline{\chi} \otimes V_\sigma(E^0)\bigr), \tag{4-2}$$

as $\overline{\mathbb{Q}}_\ell[G_{L_0}]$-modules. However, as seen in Lemma 4.2, $\mathrm{Jac}(C)_{L_0} \sim E^2_{L_0}$, which implies the following isomorphism of $\overline{\mathbb{Q}}_\ell[G_{L_0}]$-modules:

$$V_\sigma(\mathrm{Jac}(C)) \simeq V_\sigma(E)^{2\oplus}. \tag{4-3}$$

But now (4-2) and (4-3) together imply $V_\sigma(E^0) \simeq \chi \otimes V_\sigma(E^0)$, which is impossible. (We remark that if $\mathrm{Res}^M_{L_0}\, \theta_{M,\sigma}(E^0, \mathrm{Jac}(C)) \simeq \chi^{2\oplus}$, one does not reach a contradiction; see Example 4.12). □

Proposition 4.7. *Let w be the hyperelliptic involution of C^0. Then $[L:K] = 2$ if and only if $(w, 1) \in G_{C^0}$ lies in the image of λ_ϕ. If $[L:K] = 2$, then the preimage of $(w, 1)$ by λ_ϕ is the nontrivial element ω of $\mathrm{Gal}(L/K)$.*

Proof. We first suppose that $[L:K] = 2$. Observe that for both C_2^0 and C_3^0, if $\alpha \in \mathrm{Aut}(C_M^0)$ and $\mathrm{Tr}\,\theta_{E^0,C^0}(\alpha) = -2$, then $\alpha = w$. In view of the isomorphism in (4-1), it thus suffices to prove that $\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))(\omega) = -2$. From the proof of Proposition 4.6, we know that $\mathrm{Jac}(C)_K \sim E^2$, where E is an elliptic curve defined over K with CM by M. Fix an isomorphism $\psi_1 : E_L^0 \to E_L$. Fix an isogeny $\psi_2 : E_K \times E_K \to \mathrm{Jac}(C)_K$. For $i = 1, 2$, let $\iota_i : E_K \to E_K \times E_K$ denote the natural injection to the i-th factor. Then $\psi_2 \circ \iota_1 \circ \psi_1$ and $\psi_2 \circ \iota_2 \circ \psi_1$ constitute a basis of the $\overline{\mathbb{Q}}[\mathrm{Gal}(L/M)]$-module $\mathrm{Hom}(E_L^0, \mathrm{Jac}(C)_L) \otimes_{M,\sigma} \overline{\mathbb{Q}}$. The claim follows from the fact that ${}^\omega\psi_1 = -\psi_1$, ${}^\omega\psi_2 = \psi_2$, and ${}^\omega\iota_i = \iota_i$.

Now suppose that $[L:K]=1$. Recall the monomorphism

$$\overline{\lambda}_\phi : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(C^0_M)/\langle w\rangle \rtimes \mathrm{Gal}(M/\mathbb{Q})$$

of (2-3). The commutativity of the diagram

$$\begin{tikzcd} & & G_{C^0} \arrow[dr] & \\ \mathrm{Gal}(L/\mathbb{Q}) \arrow[urr, hook, "\lambda_\phi"] \arrow[r, equal] & \mathrm{Gal}(K/\mathbb{Q}) \arrow[rr, hook, "\overline{\lambda}_\phi"] & & G_{C^0}/\langle (w,1)\rangle \end{tikzcd}$$

implies that $(w,1)$ does not lie in the image of λ_ϕ. □

Remark 4.8. Let $H_0 := \lambda_\phi(\mathrm{Gal}(L/M))$. If $(1,\tau)$ lies in the image of λ_ϕ, then $\lambda_\phi(\mathrm{Gal}(L/\mathbb{Q})) = H_0 \rtimes \langle (1,\tau)\rangle$; indeed, H_0 is normal in $\lambda_\phi(\mathrm{Gal}(L/\mathbb{Q}))$, since its index is 2, and $H_0 \cap \langle (1,\tau)\rangle$ is trivial. In this case, H_0 is stable under the action of $\mathrm{Gal}(M/\mathbb{Q})$. However, it is not true in general that $\mathrm{Gal}(L/\mathbb{Q}) \simeq H_0 \rtimes \langle (1,\tau)\rangle$ or that H_0 is stable under the action of $\mathrm{Gal}(M/\mathbb{Q})$.

Proposition 4.9. *For τ in $\mathrm{Gal}(L/\mathbb{Q})$, let $s=s(\tau)$, $r=r(\tau)$, and $t=t(\tau)$ denote the orders of τ, the projection of τ on $\mathrm{Gal}(K/\mathbb{Q})$, and the projection of τ on $\mathrm{Gal}(M/\mathbb{Q})$, respectively. The following hold*:

(i) *The triple (s,r,t) is one of the 13 triples listed in Table 3.*

(ii) *If τ fixes M, then the triple $(s,r,1)$ determines, up to sign, the quantities*

$$a_1(\theta)(\tau) = \mathrm{Tr}\,\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))(\tau), \tag{4-4}$$

$$a_2(\theta)(\tau) = \det\theta_{M,\sigma}(E^0, \mathrm{Jac}(C))(\tau), \tag{4-5}$$

as specified in Table 3.

(iii) *For each triple (s,r,t), let $F_{(s,r,t)} : [-2,2] \to [-4,4]\times[-2,6]$ be the map defined in Table 3. For every prime $p>3$ unramified in L of good reduction for both $\mathrm{Jac}(C)$ and E^0, there exists a unique triple (s,r,t) such that*

$$F_{(s,r,t)}\big(a_1(E^0)(p)\big) = \big(u\cdot a_1(\mathrm{Jac}(C))(p), a_2(\mathrm{Jac}(C))(p)\big), \tag{4-6}$$

with $u=\pm 1$ (in fact, $u=1$ for $(s,r,t)\neq (6,6,1)$ and $(8,4,1)$). Moreover, the unique triple (s,r,t) for which (4-6) holds is $(f_L(p), f_K(p), f_M(p))$, where $f_F(p)$ is the residue degree of p in F.

Remark 4.10. For a prime p unramified in L such that $f_M(p)=1$, we have

$$a_2(\mathrm{Jac}(C))(p) = a_2(\theta)(\mathrm{Frob}_p)\cdot a_1(E^0)(p)^2 + |a_1(\theta)(\mathrm{Frob}_p)|^2 - 2a_2(\theta)(\mathrm{Frob}_p),$$

where $a_2(\theta)(\mathrm{Frob}_p)=\pm 1$. It follows that for any two twists C and C' of C^0, we have

$$\hat{a}_2(\mathrm{Jac}(C))(p) \equiv \pm\hat{a}_2(\mathrm{Jac}(C'))(p) \pmod{p},$$

(s,r,t)	$F_{(s,r,t)}(x)$	$a_1(\theta)(\tau)$	$a_2(\theta)(\tau)$
$(1,1,1)$	$(2x, x^2+2)$	2	1
$(2,1,1)$	$(-2x, x^2+2)$	-2	1
$(2,2,1)$	$(0, -x^2+2)$	0	-1
$(3,3,1)$	$(-x, x^2-1)$	-1	1
$(4,2,1)$	$(0, x^2-2)$	0	1
$(6,3,1)$	(x, x^2-1)	1	1
$(6,6,1)$	$\left(\sqrt{3(4-x^2)}, -x^2+5\right)$	$\pm\sqrt{-3}$	-1
$(8,4,1)$	$\left(\sqrt{2(4-x^2)}, -x^2+4\right)$	$\pm\sqrt{-2}$	-1
$(2,2,2)$	$(0, 2)$	$-$	$-$
$(4,2,2)$	$(0, -2)$	$-$	$-$
$(6,6,2)$	$(0, -1)$	$-$	$-$
$(8,4,2)$	$(0, 0)$	$-$	$-$
$(12,6,2)$	$(0, 1)$	$-$	$-$

Table 3. The triples for (s,r,t) associated to $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ (as defined in Proposition 4.9), and corresponding values of $F_{(s,r,t)}(x)$, $a_1(\theta)(\tau)$, and $a_2(\theta)(\tau)$.

where $\hat{a}_i(A)(p) = p^{i/2}a_i(A)(p)$ is the integer that appears as the coefficient of T^i in the (unnormalized) L-polynomial $L_p(A,T)$.

Proof. For assertion (i), assume first that $t=1$. Observe that s is the order of $\lambda_\phi(\tau)$ in $\mathrm{Aut}(C_M^0)$, and r is the order of the projection of $\lambda_\phi(\tau)$ in $\mathrm{Aut}(C_M^0)/\langle w\rangle$. Let c denote the conjugacy class of $\lambda_\phi(\tau)$ in $\mathrm{Aut}(C_M^0)$. One finds that the pairs (s,r) are determined by the conjugacy class of τ as follows:

$$\text{if } C^0 = C_3^0, \quad \begin{cases} c: & 1a & 2a & 2b,2c & 3a & 4a & 6a,6b & 6c \\ (r,s): & (1,1) & (2,1) & (2,2) & (3,3) & (4,2) & (6,6) & (6,3) \end{cases}$$

$$\text{if } C^0 = C_2^0, \quad \begin{cases} c: & 1a & 2a & 2b & 3a & 4a & 6a & 8a \\ (r,s): & (1,1) & (2,1) & (2,2) & (3,3) & (4,2) & (6,3) & (8,4) \end{cases}$$

(see Tables 2 and 1 for the names of the conjugacy classes). Assertion (ii) now follows immediately by applying the isomorphism in (4-1) and Lemma 4.5. If $t=2$, then r must be 2, 4, or 6, and the fact that $[L:K] \le 2$ limits (s,r,t) to either one of the last 5 triples in Table 3, or $(4,4,2)$. The latter possibility is ruled out by Proposition 3.3: if $s=4$, then for every prime p for which Frob_p lies in the same conjugacy class of τ in $\mathrm{Gal}(L/\mathbb{Q})$, we have $\bar{L}_p(\mathrm{Jac}(C),T) = (1-T^2)^2$, and the only quotients of roots of this polynomial are 1 and -1. This implies that $\theta_M(\mathrm{Jac}(C))(\tau)$ has order 2, and since $\theta_M(\mathrm{Jac}(C))$ is faithful, we must have $r = r(\tau) = 2$, not 4.

For $t=1$, the existence statement in (iii) follows from combining Lemma 3.9 with statement (ii), and for $t=2$, it follows from the proof of Corollary 3.12.

The uniqueness of the map $F_{(s,r,t)}$ satisfying (4-6) at a prime $p > 3$ may be verified by noting that the graphs of the 13 functions $F_{(s,r,t)}$ intersect in only finitely many points in $\mathbb{R}^3$, none of which corresponds to a possible value of $\big(a_1(E^0)(p), a_1(\mathrm{Jac}(C))(p), a_2(\mathrm{Jac}(C))(p)\big)$ for any prime $p > 3$. Finally, we note that if $\tau = \mathrm{Frob}_p$, then $\big(s(\tau), r(\tau), t(\tau)\big) = \big(f_L(p), f_K(p), f_M(p)\big)$. □

We now give two examples of abelian varieties A such that $A_{\overline{\mathbb{Q}}} \sim (E^0_{\overline{\mathbb{Q}}})^2$ for which the conclusions of Propositions 4.6 and 4.9 do not hold because A is not $\mathbb{Q}$-isogenous to the Jacobian of a twist of C^0. In the two examples below, we use the elliptic curve

$$\tilde{E}^0_3\colon\ y^2 = x^3 + 2$$

defined over $\mathbb{Q}$, which is a twist of E^0_3.

Example 4.11. Let $A = E^0_3 \times \tilde{E}^0_3$. Then $K = L = \mathbb{Q}(\sqrt[6]{2}, \zeta_3)$. If $\tau \in \mathrm{Gal}(L/M)$ and $s(\tau) = 3$, then $a_1(\theta)(\tau) = 1 + \zeta_3$ or $1 + \overline{\zeta}_3$ and $a_2(\theta)(\tau) = \zeta_3$ or $\overline{\zeta}_3$, which do not lie in $\mathbb{Q}$. Thus by Proposition 4.9, A is not $\mathbb{Q}$-isogenous to the Jacobian of any $\mathbb{Q}$-twist of C^0_3. Moreover, for $p = 7$, one can compute that $\hat{a}_2(A)(7) = 30$, while $\hat{a}_2((E^0_3)^2)(7) = \hat{a}_2(\mathrm{Jac}(C^0_3))(7) = 18$. Thus

$$\hat{a}_2(A)(7) \not\equiv \pm\hat{a}_2(\mathrm{Jac}(C^0))(7) \pmod 7.$$

Example 4.12. Let $A = (\tilde{E}^0_3)^2$; then $L = \mathbb{Q}(\sqrt[6]{2}, \zeta_3)$ and $K = \mathbb{Q}(\zeta_3)$; we have $[L : K] = 6$, and, by Proposition 4.6, A is not $\mathbb{Q}$-isogenous to the Jacobian of any $\mathbb{Q}$-twist of C^0_3. In the context of the proof of Proposition 4.6, $L_0 = \mathbb{Q}(\sqrt{2}, \zeta_3)$ and $\mathrm{Res}^{\mathbb{Q}}_{L_0}\, \theta(E^0, A) \simeq \chi^{2\oplus}$, rather than $\mathrm{Res}^{\mathbb{Q}}_{L_0}\, \theta(E^0, A) \simeq \chi \oplus \overline{\chi}$, which avoids the contradiction used in the proof. Moreover, for A we may have $s(\tau) = 3$ and $r(\tau) = 1$, which gives a pair (s, r) that cannot occur for the Jacobian of any $\mathbb{Q}$-twist of C^0_3, by part (ii) of Proposition 4.9.

4C. ***The triples $T(C)$.*** We determine the possible values of the triple $T(C)$, which denotes the isomorphism class $\big[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)\big]$. To specify triples explicitly, we use identifiers from the Small Groups Library [Besche et al. 2002] found in computer algebra systems such as GAP and Magma. These identifiers consist of a pair of positive integers $\langle n, m\rangle$, where n is the order of the group and m distinguishes the group from other groups of order n but otherwise has no meaning. We also recall from Section 4B the embeddings

$$\lambda_\phi : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow G_{C^0}, \qquad \mathrm{Res}\,\lambda_\phi : \mathrm{Gal}(L/M) \hookrightarrow \mathrm{Aut}(C^0_M),$$
$$\overline{\lambda}_\phi : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow G_{C^0}/\langle (w, 1)\rangle, \quad \mathrm{Res}\,\overline{\lambda}_\phi : \mathrm{Gal}(K/M) \hookrightarrow \mathrm{Aut}(C^0_M)/\langle w\rangle,$$

where w denotes the hyperelliptic involution of C^0.

Lemma 4.13. *The groups* G_{C^0}, $G_{C^0}/\langle (w, 1)\rangle$, $\mathrm{Aut}(C^0_M)$, *and* $\mathrm{Aut}(C^0_M)/\langle w\rangle$ *are as follows*:

C^0	G_{C^0}	$G_{C^0}/\langle(w,1)\rangle$	$\mathrm{Aut}(C^0_M)$	$\mathrm{Aut}(C^0_M)/\langle w\rangle$
C^0_2	$\langle 96, 193\rangle$	$\langle 48, 48\rangle$	$\langle 48, 29\rangle$	$\langle 24, 12\rangle$
C^0_3	$\langle 48, 38\rangle$	$\langle 24, 14\rangle$	$\langle 24, 8\rangle$	$\langle 12, 4\rangle$

Proof. We show how to compute G_{C^0} and $\mathrm{Aut}(C^0_M)$; the respective quotients are then easily obtained. Recall that if $C/\mathbb{Q}$ is a genus-2 curve, given by a hyperelliptic equation $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$, then for any $\alpha \in \mathrm{Aut}(C_{\overline{\mathbb{Q}}})$, there exist $m, n, p, q \in \overline{\mathbb{Q}}$ such that

$$\alpha(x, y) = \left(\frac{mx+n}{px+q}, \frac{mq-np}{(px+q)^3}y\right); \tag{4-7}$$

see, for example, [Cardona 2006]. Let

$$\iota(\alpha) := \begin{pmatrix} m & n \\ p & q \end{pmatrix}.$$

The map $\iota : \mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \to \mathrm{GL}_2(\overline{\mathbb{Q}})$ that sends α to $\iota(\alpha)$ is a $G_{\mathbb{Q}}$-equivariant monomorphism. For $d = 2, 3$, we have $\mathrm{Aut}((C^0_d)_M) = \langle U_d, V_d\rangle$, where

$$U_2 = \frac{1}{2}\begin{pmatrix} \sqrt{-2}-1 & 1 \\ 1 & 1+\sqrt{-2} \end{pmatrix}, \quad V_2 = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{-2}+1 \\ -1-\sqrt{-2} & 1 \end{pmatrix}.$$

$$U_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad V_3 = \frac{1}{2}\begin{pmatrix} 0 & -1+\sqrt{-3} \\ 1+\sqrt{-3} & 0 \end{pmatrix},$$

One can readily check that U_d and V_d represent automorphisms of $(C^0_d)_M$, and that they generate a group of order 48 if $d = 2$ and of order 24 if $d = 3$, which are known to be the orders of $\mathrm{Aut}((C^0_d)_M)$. With this explicit representation, the isomorphism type of $\langle U_d, V_d\rangle$ is then easily determined by a computer algebra system. The group $G_{C^0_d}$ is then determined by explicitly computing the semidirect product $\langle U_d, V_d\rangle \rtimes \mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$. □

Remark 4.14. We note that $\langle 48, 29\rangle \simeq \tilde{\mathrm{S}}_4 \simeq \mathrm{GL}_2(\mathbb{F}_3)$ and $\langle 24, 8\rangle \simeq 2\mathrm{D}_6 \simeq \mathrm{C}_3 \rtimes \mathrm{D}_4$ are the two automorphism groups mentioned in the introduction, with quotients $\langle 24, 12\rangle \simeq \mathrm{S}_4$ and $\langle 12, 4\rangle \simeq \mathrm{D}_6$, respectively. The group $\langle 24, 14\rangle$ is isomorphic to $\mathrm{D}_6 \times \mathrm{C}_2$, while the groups $\langle 48, 38\rangle$ and $\langle 48, 48\rangle$ are both degree-3 extensions of $\mathrm{D}_4 \times \mathrm{C}_2$ and $\langle 96, 193\rangle$ is a degree-3 extension of $\mathrm{C}_8 \rtimes \mathrm{Aut}(\mathrm{C}_8)$.

Let $\tilde{T}(C)$ denote the triple

$$\big(\lambda_\phi(\mathrm{Gal}(L/\mathbb{Q})), \lambda_\phi(\mathrm{Gal}(L/M)), \lambda_\phi(\mathrm{Gal}(L/M))\big)$$

in $G_{C^0} \times G_{C^0} \times G_{C^0}$. Since λ_ϕ is injective, the conjugacy class of $\tilde{T}(C)$ determines $T(C)$ and $z(C)$, where $z(C)$ is the vector in Definition 1.3. In order to bound the number of possibilities for $T(C)$ and $z(C)$, we first bound the number of possible triples $\tilde{T}(C)$, up to conjugation.

Lemma 4.15. *Let H, N, and H_0 be subgroups of G_{C^0}. If $\tilde{T}(C)=(H, N, H_0)$, then the following conditions must be satisfied*:

(i) *H_0 and $H\cap \mathrm{Aut}(C^0_M)\times\langle 1\rangle$ coincide and have order $|H|/2$.*

(ii) *N and $\langle(w, 1)\rangle\cap H_0$ coincide.*

Proof. Let $\mathrm{Gal}(M/\mathbb{Q})=\{1, \tau\}$. Then

$$H_0=\lambda_\phi(\mathrm{Gal}(L/M))\subseteq(\mathrm{Aut}(C^0_M)\times\{1\})\cap H,$$
$$H_1:=\lambda_\phi\big(\mathrm{Gal}(L/\mathbb{Q})\setminus\mathrm{Gal}(L/M)\big)\subseteq(\mathrm{Aut}(C^0_M)\times\{\tau\})\cap H.$$

The injectivity of λ_ϕ implies that $|H_0|=|H_1|=|H|/2$, and (i) follows from the fact that $H=H_0\sqcup H_1$.

Proving (ii) is equivalent to showing that $(w, 1)$ lies in the image of λ_ϕ if and only if $[L:K]=2$. But this has already been proved; see Proposition 4.7. □

Proposition 4.16. *Let H, N, and H_0 be subgroups of G_{C^0} that satisfy conditions (i) and (ii) of Lemma 4.15.*

(i) *For $C^0=C^0_2$ (resp. $C^0=C^0_3$), there are 27 (resp. 38) possibilities for the conjugacy class of (H, N, H_0) in $G_{C^0}\times G_{C^0}\times G_{C^0}$.*

(ii) *For $C^0=C^0_2$ (resp. $C^0=C^0_3$), the 27 (resp. 38) possibilities for the conjugacy class of (H, N, H_0) give rise to the 23 (resp. 23) isomorphism classes $[H, H/N, H_0]$ and vectors $z(H, N, H_0)$ listed in the top (resp. bottom) half of Table 4. Moreover, $[H, H/N, H_0]$ and $z(H, N, H_0)$ determine each other uniquely.*

(iii) *For $C^0=C^0_2$ (resp. $C^0=C^0_3$), the triple $T(C)$ and the vector $z(C)$ must be among those listed in the corresponding half of Table 4, and $T(C)$ and $z(C)$ determine each other uniquely.*

Proof. For (i), recall that $G_{C^0_3}\simeq\langle 48, 38\rangle$ and $\mathrm{Aut}((C^0_3)_M)\simeq\langle 24, 8\rangle$. The following three facts permit us to work with $G_{C^0_3}$ and $\mathrm{Aut}((C^0_3)_M)$ as abstract groups. First, there are exactly two subgroups A_1 and A_2 of $\langle 48, 38\rangle$ isomorphic to $\langle 24, 8\rangle$. Second, there is a unique nontrivial central involution $\hat{w}$ in $\langle 48, 38\rangle$, and it lies in both A_1 and A_2. Third, consider the two lists of triples of groups, up to conjugation,

$$\mathcal{L}_i=\big\{\big(H, \langle\hat{w}\rangle\cap H, H\cap A_i\big)\mid H\subseteq\langle 48, 38\rangle, |H\cap A_i|=|H|/2\big\}\big/\!\sim,\quad i=1,2,$$

where $(H, \langle\hat{w}\rangle\cap H, H\cap A_i)\sim(H', \langle\hat{w}\rangle\cap H', H'\cap A_i)$ if H and H' are conjugated in $\langle 48, 38\rangle$. Then the lists $\mathcal{L}_1$ and $\mathcal{L}_2$ coincide; write $\mathcal{L}$ for this list. For $C^0=C^0_2$, the three previous facts can be checked to hold *verbatim* when replacing $\langle 48, 38\rangle$ and $\langle 24, 8\rangle$ by $\langle 96, 193\rangle$ and $\langle 48, 29\rangle$, respectively. For $C^0=C^0_3$, $\mathcal{L}$ has 38 elements and, for $C^0=C^0_2$, it has 27 elements.

For (ii), for each of C_2^0 and C_3^0, we enumerate the triples (H, N, H_0) in $\mathscr{L}$ and explicitly compute $[H, H/N, H_0]$ and $z(H, N, H_0)$ in each case using a computer algebra system (we used Magma), obtaining the values listed in Table 4. One then checks that $[H, H/N, H_0] = [H', H'/N', H_0']$ if and only if $z(H, H/N, H_0) = z(H', H'/N', H_0')$.

Statement (iii) follows immediately from (ii) and Lemma 4.15. □

Proposition 4.17. *The vector $z(C)$ and the triple $T(C)$ both uniquely determine the Sato–Tate group* $\mathrm{ST}(\mathrm{Jac}(C))$.

Proof. The 18 Sato–Tate groups G that can occur over $\mathbb{Q}$ with $G^0 \simeq \mathrm{U}(1)$ (see [Fité et al. 2012, Theorem 4.3]) are uniquely determined by the combination of:

(a) the isomorphism classes of the groups G/G^0 and $G^{ns}/G^{ns,0}$,

(b) the vector $z_2(G) = \big(z_{2,2}(G), z_{2,-2}(G), z_{2,-1}(G), z_{2,0}(G), z_{2,1}(G)\big)$,[9]

where G^{ns} is the index-2 subgroup of G obtained by removing from G those components all of whose elements have a constant characteristic polynomial.

On the one hand, the isomorphism classes of the groups G/G^0 and $G^{ns}/G^{ns,0}$ are determined by $T(C)$, since $G/G^0 \simeq \mathrm{Gal}(K/\mathbb{Q})$ and $G^{ns}/G^{ns,0} \simeq \mathrm{Gal}(K/M)$. On the other hand, $z_2(G)$ is determined by $z(C)$; indeed, it follows from the construction of the Sato–Tate group in terms of the image of the ℓ-adic representation attached to $\mathrm{Jac}(C)$ and from assertion (iii) of Proposition 4.9, that $z_2(G)\cdot[L:K] = z_2(C)$. □

Corollary 4.18. *For each triple $[H, H/N, H_0]$ in Table 4, there exists a twist C of C^0 such that $T(C) = [H, H/N, H_0]$ if and only if the corresponding row in the table is not marked with an asterisk. Thus, for $C^0 = C_2^0$ (resp. for $C^0 = C_3^0$) there are exactly* 20 (*resp.* 21) *possibilities for $T(C)$.*

Proof. Observe that the triples marked with an asterisk in Table 4 correspond to Sato–Tate groups (equivalently, Galois types) that cannot arise for abelian surfaces defined over $\mathbb{Q}$ (see [Fité et al. 2012, Proposition 4.11]). For each of the triples $[H, H/N, H_0]$ that is not marked with an asterisk, a curve C with $T(C) = [H, H/N, H_0]$ is exhibited in Tables 5 and 6 (for details on how the curves have been found, see Section 5A; for details on how $T(C)$ is computed for each of the curves, see Section 5C.) □

Remark 4.19. If the triple $[H, H, H_0]$ appears in either half of Table 4, then so does the triple $[H \times \mathrm{C}_2, H, H_0 \times \mathrm{C}_2]$. In other words, if there exists a twist C of C^0 such that $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$, then there exists a twist C' of C^0 such that $\mathrm{Gal}(K'/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{C}_2$. Here K' (resp. L') is

[9]Following the notation of [Fité et al. 2012], recall that $z_{2,i}(G)$ denotes the number of connected components of G all of whose elements have a constant characteristic polynomial, for which the coefficient of the quadratic term is equal to i. Note that the components of the vector $z_2(G)$ have been permuted with respect to the definition of $z_2(G)$ given in [Fité et al. 2012].

the minimal field over which all the automorphisms of C' (resp. all the isomorphisms between C' and C^0) are defined. Indeed, if C is given by the hyperelliptic equation $y^2 = f(x)$, let C' be the curve given by $dy^2 = f(x)$, where $d \in \mathbb{Q}^*$ is not a square in K. We will use this remark in Section 5 for the computation of some of the curves.

Remark 4.20. Among the 18 Sato–Tate groups with identity component U(1) that can occur over $\mathbb{Q}$, there are 13 that are subgroups of $J(O)$ and 11 that are subgroups of $J(D_6)$ (6 are subgroups of both). From Table 6, we see that the 13 that are subgroups of $J(O)$ can all occur as $\mathbb{Q}$-twists of C_2^0, and the 11 that are subgroups of $J(D_6)$ can all occur as $\mathbb{Q}$-twists of C_3^0.

5. Numerical computations

We now describe the methods used to obtain the example curves C listed in Tables 5 and 6. As in Section 4, each curve C is a $\mathbb{Q}$-twist of $C^0 = C_d^0$, for $d = 2, 3$, where $\mathrm{Jac}(C_d^0) \sim (E_d^0)^2$ and E_d^0 is an elliptic curve with CM by $M = \mathbb{Q}(\sqrt{-d})$. For $d = 2$, we list 20 curves C that are $\mathbb{Q}$-twists of the curve C_2^0 defined by $y^2 = x^6 - 5x^4 - 5x^2 + 1$, realizing every possible triple

$$T(C) = \bigl[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)\bigr]$$

that can occur when C is a $\mathbb{Q}$-twist of C_2^0. Recall that the fields K and L are the minimal fields of definition $\mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}})$ and $\mathrm{Hom}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}}, E_{\overline{\mathbb{Q}}})$, respectively, as in Definition 1.2. Similarly, for $d = 3$, we list 21 curves C that are twists of the curve C_3^0 defined by $y^2 = x^6 + 1$, realizing every possible triple $T(C)$ that can occur when C is a $\mathbb{Q}$-twist of C_3^0.

For each of the two curves C^0, we followed the procedure outlined below:

(1) Generate a large set S of $\mathbb{Q}$-twists of C^0.

(2) For each $C \in S$, compute a provisional value of the triple $T(C)$.

(3) Select a single representative C for each distinct triple $T(C)$ and then verify the provisional value of $T(C)$ by explicitly computing the fields K and L and the triple $T(C) = \bigl[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)\bigr]$.

The purpose of the "provisional" computation of $T(C)$ in step (2) is to avoid computing the fields K and L for all of the curves in S, which would have been infeasible. Explicit computation of the fields K and L (and their Galois groups) for even a single curve C can be quite time-consuming, taking hours or even days of computer time, and the sets S that we used contained tens of thousands of curves.

In the rest of this section we fill in some of the details of the three steps listed above.

5A. ***Generating twists of C^0.*** Explicit parametrizations of the families of twists of C_2^0 and C_3^0 are given in [Cardona 2001; 2006]. One can easily obtain a large set S using these parametrizations. However, the resulting curves tend to have large coefficients, making the computation of K and L more difficult, and the vast majority of curves in S are likely to represent the generic case, where $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ are as large as possible. In principle, one can control the isomorphism type of $\mathrm{Gal}(K/\mathbb{Q})$ by placing appropriate constraints on the input parameters, but this is not enough to determine the Sato–Tate group, and it gives no control over $\mathrm{Gal}(L/\mathbb{Q})$.

We instead adapted the search method used in [Fité et al. 2012], generating S by enumerating all curves of the form $y^2 = \sum_{i=0}^{6} c_i x^i$ satisfying coefficient bounds $|c_i| \le B_i$. To quickly identify curves C that are twists of C^0, we first compute $a_1(C)(p)$ for a handful of small primes p that are inert in M, and immediately discard C if $a_1(C)(p) \ne 0$ for any such p. We then compute the absolute Igusa invariants of C, and compare them to the corresponding values for C^0. With the bounds B_i chosen to encompass some 2^{50} curves with small coefficients, we obtain a set S containing tens of thousands of twists of C^0 in each case.

After applying the method in Section 5B below to all of the curves in S, we had several candidate curves C for every possible triple $T(C)$ that can arise when C is defined over $\mathbb{Q}$ (the triples listed in Table 4 that are not marked with an asterisk). We then selected a single representative C for each triple and computed K and L for each of these C, as described in Section 5C, and then computed the Galois groups $\mathrm{Gal}(L/\mathbb{Q})$, $\mathrm{Gal}(K/\mathbb{Q})$, and $\mathrm{Gal}(L/M)$, using the Magma computer algebra system, to obtain the true value of the triple $T(C)$. As expected, this computation confirmed the provisional value in every case. Indeed, in all but the most time-consuming cases we were able to repeat the computations using several different candidate curves C and always obtained the expected value of $T(C)$.

Remark 5.1. The computation of the triple $T(C)$ in Magma is completely independent of the calculations used to obtain a provisional value for $T(C)$, which were performed using the `smalljac` software library [Sutherland 2011]; the purpose of the provisional computations was simply to obtain a set of candidate curves that is much smaller than the initial set S. The fact that in every case we obtained the same value for $T(C)$ using two completely different methods gives us a high degree of confidence in our numerical computations.

5B. ***Provisional computation of $T(C)$.*** To provisionally identify the triple $T(C)$, we compute an approximation of the vector $z(C)$ (see Definition 1.3), which, by Theorem 1.4, uniquely determines $T(C)$. To do this, it suffices to determine the triples (s, r, t) of residue degrees $(f_L(p), f_K(p), f_M(p))$ for a sample set of primes p (say, primes $p \le 2^{16}$ of good reduction for C), and then count how often each triple appears. The components $o(s, r)$ and $\bar{o}(s, r)$ of the vector $z(C)$ may be approximated by computing the relative frequencies of the triples $(s, r, 1)$ and $(s, r, 2)$, respectively, and normalizing so that $o(1, 1) = 1$.

We can easily compute $t = f_M(p) \in \{1, 2\}$ by checking whether p splits in M, but we also need to compute $r = f_K(p)$ and $s = f_L(p)$, and we would like to do so *without knowing K or L*. This can be achieved as follows: we first compute $a_1(E^0)(p)$ and the values $a_1(C)(p)$ and $a_2(C)(p)$, as described in Section 5B1, and then determine the unique map $F_{(s,r,t)}$ from Proposition 4.9 for which

$$F_{(s,r,t)}(a_1(E^0)(p)) = \big(\pm a_1(C)(p), a_2(C)(p)\big). \tag{5-1}$$

5B1. *Computation of $a_1(C)(p)$ and $a_2(C)(p)$.* For an arbitrary genus-2 curve, efficient computation of $a_1(C)(p)$ and $a_2(C)(p)$ is addressed in [Kedlaya and Sutherland 2008], but in the special case of interest here, where C is a $\mathbb{Q}$-twist of C^0, we use a faster approach. The Jacobian of C^0 is $\mathbb{Q}$-isogenous to the square of E^0, an elliptic curve defined over $\mathbb{Q}$. Because E^0 has complex multiplication, we can very efficiently determine $a_1(E)(p)$. Taking C_2^0 as an example, E_2^0 is defined by the Weierstrass equation $y^2 = x^3 - 5x^2 - 5x + 1$. This curve has CM by $M = \mathbb{Q}(\sqrt{-2})$, and for any prime $p > 2$ we may compute $a = a_1(E_2^0)(p)$ as follows: $a = 0$ if p is inert in M and otherwise $a = 4x/\sqrt{p}$, where the integer x satisfies $p = x^2 + 2y^2$ for some integer y. The positive integer $z = |x|$ may be determined via Cornacchia's algorithm, and then $x = (-1)^\epsilon z$, where $\epsilon = (z-1)/2 + (p-1)(p+5)/16$; see [Rubin and Silverberg 2010] for details. The computation for C_3^0 is similar: in this case E_3^0 is defined by $y^2 = x^3 + 1$, with CM by $M = \mathbb{Q}(\sqrt{-3})$.

With $a_1(E^0)(p)$ computed, there are only a handful of pairs (a_1, a_2) that are compatible with (5-1), that is, for which there exists a triple (s, r, t) such that $F_{(s,r,t)}(a_1(E^0)(p)) = (\pm a_1, a_2)$. Taking into account whether C is a twist of C_2^0 or C_3^0, whether p splits in M or not, and that the sign of a_1 is actually ambiguous in only 2 cases, there are at most 8 possibilities. Each compatible pair (a_1, a_2) determines an integer

$$n = p^2 + p^{3/2}a_1 + pa_2 + p^{1/2}a_1 + 1,$$

one of which is equal to $\#\operatorname{Jac}(C)(\mathbb{F}_p)$. In most cases, if we pick a random point $P \in \operatorname{Jac}(C)(\mathbb{F}_p)$, the equation $nP = 0$ will hold for exactly one n and uniquely determine a_1 and a_2. Even when this is not the case, after factoring the integers n, we can determine the order of any point P in $\operatorname{Jac}(C)(\mathbb{F}_p)$, using just $\tilde{O}(\log p)$ operations in $\mathbb{F}_p$; see [Sutherland 2007, Chapter 7]. This allows us to compute the order of $\operatorname{Jac}(C)(\mathbb{F}_p)$ using a probabilistic generic group algorithm (of Las Vegas type) that runs in $O(p^{1/4})$ expected time; see [Sutherland 2007; Kedlaya and Sutherland 2008, Proposition 1].[10] This compares to an $O(p^{3/4})$ expected running

[10] The $O(p^{1/4})$ bound is a worst-case estimate; it is faster than this for most p.

time for an arbitrary genus-2 curve using a generic group algorithm.[11]

Having computed $L_p(C, 1) = \#\,\mathrm{Jac}(C)(\mathbb{F}_p)$, we use the same method to determine $L_p(C, -1) = \#\,\mathrm{Jac}(\tilde{C})(\mathbb{F}_p)$, where $\tilde{C}$ is any nontrivial quadratic twist of C over $\mathbb{F}_p$, and these two values uniquely determine a_1 and a_2.

The algorithm described above is included in the most recent version of the `smalljac` software library, whose source code is available at [Sutherland 2011].

5C. *Computation of K and L.* In this section, we describe the procedure used to compute the fields K and L for the curves C listed in Tables 5 and 6.

For the field K, its characterization in Lemma 4.2 as the minimal field over which all the automorphisms of C are defined turns out to be the most computationally effective. For all 41 curves $C\colon y^2 = f(x)$ listed in Tables 5 and 6, one readily checks that $\mathrm{Aut}(C^0_{\overline{\mathbb{Q}}}) \simeq \mathrm{Aut}(C_{\overline{\mathbb{Q}}}) = \mathrm{Aut}(C_{F(\zeta_{24})})$, where F is the splitting field of $f(x)$ (see Remark 5.2 below). It is then a finite problem to identify the minimal subfield K of $F(\zeta_{24})$ for which $\mathrm{Aut}(C_K) = \mathrm{Aut}(C_{F(\zeta_{24})})$.

Having computed K, we determine L as follows. For any nonhyperelliptic involution $\beta \in \mathrm{Aut}(C^0_M)$, the elliptic quotient $C^0/\langle\beta\rangle$ is defined over M. If β_1 and β_2 are conjugate in $\mathrm{Aut}(C^0_M)$, then $C^0/\langle\beta_1\rangle \simeq C^0/\langle\beta_2\rangle$. For C^0_2 there is just one conjugacy class of nonhyperelliptic involutions; hence in this case every elliptic quotient $C^0/\langle\beta\rangle$ is isomorphic to E^0_M. For C^0_3 there are two conjugacy classes of nonhyperelliptic involutions, of size 2 and 6 (see Table 2). The first corresponds to the M-isomorphism class of E^0_3, and the second corresponds to the M-isomorphism class of the elliptic curve $y^2 = x^3 - 15x + 22$.

Since we know K explicitly, we can compute $\mathrm{Aut}(C_K)$ and enumerate all the nonhyperelliptic involutions α (there are 12 when $d = 2$ and 8 when $d = 3$). For $d = 2$ we pick any α, and for $d = 3$ we pick α from the conjugacy class of size 2. Define $\tilde{E} := C_K/\langle\alpha\rangle$ and $\tilde{E}^0 := C^0_M/\langle\phi\alpha\phi^{-1}\rangle$. The isomorphism ϕ induces an isomorphism $\tilde{\phi}: \tilde{E}_L \to \tilde{E}^0_L$. As in the proof of Proposition 4.6, L is the compositum of K and the minimal field over which $\tilde{\phi}$ is defined. Our choice of α ensures that $\tilde{E}^0 \simeq E^0_M$; thus $\tilde{E}_L \simeq E^0_L$.

By applying [Cardona et al. 1999, Lemma 2.2], we can compute an explicit Weierstrass equation for $\tilde{E}$ of the form

$$\tilde{E}\colon\; Y^2 = X^3 + AX + B, \quad \text{with } A, B \in K.$$

Writing E^0 in the form $Y^2 = X^3 + UX + V$, there then exists $\gamma \in L$ such that $U = \gamma^4 A$ and $V = \gamma^6 B$, and γ generates L as an (at most quadratic) extension of K. We can easily derive γ from the coefficients A, B, U, and V.

[11] As noted in [Kedlaya and Sutherland 2008], the asymptotically faster polynomial-time algorithm of Pila [1990] is not practically useful in the range of p relevant to the computations considered here.

Remark 5.2. In fact, it is true in general that for any twist C of C_2^0 (resp. C_3^0), the field K is contained in $F(\sqrt{-2})$ (resp. $F(\sqrt{-3},i)$). We thank J. Quer for kindly providing the following argument.

Let $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})^*$ denote the subgroup of $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ generated by those elements α such that $\mathrm{Trace}(\iota(\alpha))$ is nonzero. We claim that

$$\mathrm{Aut}(C_{\overline{\mathbb{Q}}})^* = \mathrm{Aut}(C_{FM})^*.$$

Let $\mathrm{WP}(C)$ denote the set of Weierstrass points of C and let σ be an element of G_{FM}. It suffices to show that ${}^\sigma\alpha=\alpha$ for every α in $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})^*$ such that $\mathrm{Trace}(\iota(\alpha))$ is nonzero. Observe that for every P in $\mathrm{WP}(C)$, one has ${}^\sigma P = P$. Then, writing $Q=\alpha^{-1}(P)$, we have

$${}^\sigma\alpha\circ\alpha^{-1}(P) = ({}^\sigma\alpha)(Q) = {}^\sigma(\alpha(Q)) = {}^\sigma P = P,$$

which implies that ${}^\sigma\alpha$ is either α or $w\alpha$, since the action of $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})/\langle w\rangle$ on $\mathrm{WP}(C)$ is faithful. Provided that $\mathrm{Trace}(\iota(\alpha))$ is in M, the latter option is not possible, since otherwise we would have

$$\mathrm{Trace}(\iota(\alpha)) = {}^\sigma\,\mathrm{Trace}(\iota(\alpha)) = \mathrm{Trace}(\iota(w\alpha)) = -\,\mathrm{Trace}(\iota(\alpha)),$$

contradicting the fact that $\mathrm{Trace}(\iota(\alpha))$ is nonzero. Since $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$ and $\mathrm{Aut}(C^0_{\overline{\mathbb{Q}}})$ are conjugated, the groups $\mathrm{Aut}(C_{\overline{\mathbb{Q}}})^*$ and $\mathrm{Aut}(C^0_{\overline{\mathbb{Q}}})^*$ are isomorphic. It is straightforward to check that

$$\mathrm{Aut}\big((C_2^0)_{\overline{\mathbb{Q}}}\big)^* \simeq \tilde{\mathrm{S}}_4 \quad\text{and}\quad \mathrm{Aut}\big((C_3^0)_{\overline{\mathbb{Q}}}\big)^* \simeq \mathrm{C}_2\times\mathrm{C}_6.$$

Thus, for every twist C of C_2^0, the field K is contained in $F(\sqrt{-2})$; but for a twist C of C_3^0, the order of $\mathrm{Aut}\big((C_3^0)_{F(\sqrt{-3})}\big)$ can be 12 or 24. By considering the parametrizations given in [Cardona 2001, Proposition 7.4.1] of all the twists C of C_3^0 as well as of the corresponding embeddings $\iota(\mathrm{Aut}(C_{\overline{\mathbb{Q}}}))$ in $\mathrm{GL}_2(\overline{\mathbb{Q}})$, one may explicitly verify that K is always contained in $F(\sqrt{-3},i)$.

5C1. *An example.* Consider the twist C of C_3^0 defined by the hyperelliptic equation

$$y^2 = f(x) = x^6+15x^4+20x^3+30x^2+18x+5$$

over $\mathbb{Q}$. This curve is listed in Table 6 for the triple $[\langle 24,5\rangle,\langle 12,4\rangle,\langle 12,1\rangle]$. Let us prove that this is in fact the triple $T(C)=\big[\mathrm{Gal}(L/\mathbb{Q}),\mathrm{Gal}(K/\mathbb{Q}),\mathrm{Gal}(L/M)\big]$.

We first compute K. Let F denote the splitting field of $f(x)$. One checks (via Magma) that $|\mathrm{Aut}(C_{MF})|=24$, where $M=\mathbb{Q}(\sqrt{-3})$, and therefore $K\subseteq MF$ (since we know *a priori* that $|\mathrm{Aut}(C_K)| = |\mathrm{Aut}((C_3^0)_{\overline{\mathbb{Q}}})| = 24$). By enumerating the various subfields of MF, we find that the minimal subfield K of MF for which $|\mathrm{Aut}(C_K)|=24$ is $K=M(\sqrt{5},a)$, where $a^3+3a-1=0$.

To compute L, we choose the nonhyperelliptic involution α of $\mathrm{Aut}(C_K)$ whose image under the map $\iota:\mathrm{Aut}(C_{\overline{\mathbb{Q}}})\to \mathrm{GL}_2(\overline{\mathbb{Q}})$ defined in (4-7) is

$$\iota(\alpha)=\frac{1}{5}\begin{pmatrix}\sqrt{5} & -2\sqrt{5}\\ -2\sqrt{5} & -\sqrt{5}\end{pmatrix}.$$

Applying [Cardona et al. 1999, Lemma 2.2] yields a Weierstrass equation for $\tilde{E}=C/\langle\alpha\rangle$:

$$\tilde{E}:\ Y^2=X^3+B,\quad \text{with } B=-\frac{11}{97656250}\sqrt{5}+\frac{1}{3906250}.$$

Since E^0 is the curve $y^2=x^3+1$, we have $U=0$ and $V=1$, so $\gamma^6=1/B$. This implies that

$$\gamma^2-\left(\frac{125}{2}\sqrt{5}+\frac{375}{2}\right)a^2+\left(\frac{125}{2}\sqrt{5}+\frac{125}{2}\right)a-125\sqrt{5}-375=0,$$

and one finds that $L=K\big(\sqrt{2\sqrt{5}+10}\big)$.

Having explicitly computed the fields K and L, it is then straightforward to verify that $\mathrm{Gal}(L/\mathbb{Q})\simeq\langle 24,5\rangle$, $\mathrm{Gal}(K/\mathbb{Q})\simeq\langle 12,4\rangle$, and $\mathrm{Gal}(L/M)\simeq\langle 12,1\rangle$ using Magma.

6. Tables

This section contains the remaining tables described earlier, whose definitions we briefly recall. Remember that C^0 is one of the two curves $C_2^0\colon y^2=x^6-5x^4-5x^2+1$ (in which case $M=\mathbb{Q}(\sqrt{-2})$) or $C_3^0\colon y^2=x^6+1$ (in which case $M=\mathbb{Q}(\sqrt{-3})$). Table 4 lists (up to isomorphism) the possible values of the triples $T(C)$ that can arise when C is a $\mathbb{Q}$-twist of the curve C^0.

Section 4C describes the computation of these tables. Each triple $[H, H/N, H_0]$ is a possible value for $T(C)=\big[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}, \mathrm{Gal}(L/M)\big]$, and is determined by a subgroup $H\subset G_{C^0}$ whose intersection with $\mathrm{Aut}(C_M^0)$ is an index-2 subgroup H_0 of H, where $N=H\cap Z(G_{C^0})$.

For each triple $T(C)$ we list the corresponding Sato–Tate group G and its matching Galois type, as defined in [Fité et al. 2012], as well as the vector $z(C)$ given by Definition 1.3, all of which are uniquely determined by $T(C)$, by Theorem 1.4. As proven in [Fité et al. 2012], the Sato–Tate groups $J(C_1)$, $J(C_3)$, and $C_{4,1}$ cannot arise for a genus-2 curve defined over $\mathbb{Q}$, and the corresponding rows in Table 4 are marked with an asterisk.

In Tables 5 and 6, we list representative curves that realize every triple $T(C)$ that can occur when C is defined over $\mathbb{Q}$. For each curve, we also give an explicit description of the fields K and L, where K is the minimal field for which $\mathrm{Aut}(C_K)=\mathrm{Aut}(C_{\overline{\mathbb{Q}}})$, and L is the minimal extension of K over which C is isomorphic to C^0.

G	H	H/N	H_0	Galois type	$z(H, N, H_0)$
$*J(C_1)$	$\langle 4, 1\rangle$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathbb{H}]$	$[1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0]$
$J(C_2)$	$\langle 8, 2\rangle$	$\langle 4, 2\rangle$	$\langle 4, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathbb{H}]$	$[1, 1, 0, 0, 2, 0, 0, 0, 0, 2, 2, 0, 0, 0]$
$J(C_2)$	$\langle 8, 3\rangle$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathbb{H}]$	$[1, 1, 2, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0]$
$*J(C_3)$	$\langle 12, 2\rangle$	$\langle 6, 2\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathbb{H}]$	$[1, 1, 0, 2, 0, 2, 0, 0, 0, 0, 2, 0, 0, 4]$
$J(C_4)$	$\langle 16, 6\rangle$	$\langle 8, 2\rangle$	$\langle 8, 1\rangle$	$\mathbf{F}[\mathrm{C}_4 \times \mathrm{C}_2, \mathrm{C}_4]$	$[1, 1, 0, 0, 2, 0, 0, 4, 0, 2, 2, 0, 4, 0]$
$J(D_2)$	$\langle 16, 11\rangle$	$\langle 8, 5\rangle$	$\langle 8, 3\rangle$	$\mathbf{F}[\mathrm{D}_2 \times \mathrm{C}_2, \mathrm{D}_2]$	$[1, 1, 4, 0, 2, 0, 0, 0, 0, 6, 2, 0, 0, 0]$
$J(D_2)$	$\langle 16, 13\rangle$	$\langle 8, 5\rangle$	$\langle 8, 4\rangle$	$\mathbf{F}[\mathrm{D}_2 \times \mathrm{C}_2, \mathrm{D}_2]$	$[1, 1, 0, 0, 6, 0, 0, 0, 0, 6, 2, 0, 0, 0]$
$J(D_3)$	$\langle 24, 6\rangle$	$\langle 12, 4\rangle$	$\langle 12, 4\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathbb{H}]$	$[1, 1, 6, 2, 0, 2, 0, 0, 0, 6, 2, 0, 0, 4]$
$J(D_4)$	$\langle 32, 43\rangle$	$\langle 16, 11\rangle$	$\langle 16, 8\rangle$	$\mathbf{F}[\mathrm{D}_4 \times \mathrm{C}_2, \mathrm{D}_4]$	$[1, 1, 4, 0, 6, 0, 0, 4, 0, 10, 2, 0, 4, 0]$
$J(T)$	$\langle 48, 33\rangle$	$\langle 24, 13\rangle$	$\langle 24, 3\rangle$	$\mathbf{F}[\mathrm{A}_4 \times \mathrm{C}_2, \mathrm{A}_4]$	$[1, 1, 0, 8, 6, 8, 0, 0, 0, 6, 2, 0, 0, 16]$
$J(O)$	$\langle 96, 193\rangle$	$\langle 48, 48\rangle$	$\langle 48, 29\rangle$	$\mathbf{F}[\mathrm{S}_4 \times \mathrm{C}_2, \mathrm{S}_4]$	$[1,1,12,8,6,8,0,12,0,18,2,0,12,16]$
$C_{2,1}$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\langle 1, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0]$
$C_{2,1}$	$\langle 4, 2\rangle$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0]$
$*C_{4,1}$	$\langle 8, 1\rangle$	$\langle 4, 1\rangle$	$\langle 4, 1\rangle$	$\mathbf{F}[\mathrm{C}_4, \mathrm{C}_2]$	$[1, 1, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 4, 0]$
$D_{2,1}$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 1, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0]$
$D_{2,1}$	$\langle 8, 3\rangle$	$\langle 4, 2\rangle$	$\langle 4, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 0, 2, 0, 0, 0, 0, 4, 0, 0, 0, 0]$
$D_{2,1}$	$\langle 8, 5\rangle$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 2, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0]$
$D_{3,2}$	$\langle 6, 1\rangle$	$\langle 6, 1\rangle$	$\langle 3, 1\rangle$	$\mathbf{F}[\mathrm{D}_3, \mathrm{C}_3]$	$[1, 0, 0, 2, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0]$
$D_{3,2}$	$\langle 12, 4\rangle$	$\langle 6, 1\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{D}_3, \mathrm{C}_3]$	$[1, 1, 0, 2, 0, 2, 0, 0, 0, 6, 0, 0, 0, 0]$
$D_{4,1}$	$\langle 16, 7\rangle$	$\langle 8, 3\rangle$	$\langle 8, 3\rangle$	$\mathbf{F}[\mathrm{D}_4, \mathrm{D}_2]$	$[1, 1, 4, 0, 2, 0, 0, 0, 0, 4, 0, 0, 4, 0]$
$D_{4,1}$	$\langle 16, 8\rangle$	$\langle 8, 3\rangle$	$\langle 8, 4\rangle$	$\mathbf{F}[\mathrm{D}_4, \mathrm{D}_2]$	$[1, 1, 0, 0, 6, 0, 0, 0, 0, 4, 0, 0, 4, 0]$
$D_{4,2}$	$\langle 16, 7\rangle$	$\langle 8, 3\rangle$	$\langle 8, 1\rangle$	$\mathbf{F}[\mathrm{D}_4, \mathrm{C}_4]$	$[1, 1, 0, 0, 2, 0, 0, 4, 0, 8, 0, 0, 0, 0]$
O_1	$\langle 48, 29\rangle$	$\langle 24, 12\rangle$	$\langle 24, 3\rangle$	$\mathbf{F}[\mathrm{S}_4, \mathrm{A}_4]$	$[1, 1, 0, 8, 6, 8, 0, 0, 0, 12, 0, 0, 12, 0]$
$*J(C_1)$	$\langle 4, 1\rangle$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathbb{H}]$	$[1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0]$
$J(C_2)$	$\langle 8, 2\rangle$	$\langle 4, 2\rangle$	$\langle 4, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathbb{H}]$	$[1, 1, 0, 0, 2, 0, 0, 0, 0, 2, 2, 0, 0, 0]$
$J(C_2)$	$\langle 8, 3\rangle$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathbb{H}]$	$[1, 1, 2, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0]$
$*J(C_3)$	$\langle 12, 2\rangle$	$\langle 6, 2\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathbb{H}]$	$[1, 1, 0, 2, 0, 2, 0, 0, 0, 0, 2, 0, 0, 4]$
$J(C_6)$	$\langle 24, 10\rangle$	$\langle 12, 5\rangle$	$\langle 12, 5\rangle$	$\mathbf{F}[\mathrm{C}_6 \times \mathrm{C}_2, \mathrm{C}_6]$	$[1, 1, 2, 2, 0, 2, 4, 0, 0, 2, 2, 4, 0, 4]$
$J(D_2)$	$\langle 16, 11\rangle$	$\langle 8, 5\rangle$	$\langle 8, 3\rangle$	$\mathbf{F}[\mathrm{D}_2 \times \mathrm{C}_2, \mathrm{D}_2]$	$[1, 1, 4, 0, 2, 0, 0, 0, 0, 6, 2, 0, 0, 0]$
$J(D_3)$	$\langle 24, 5\rangle$	$\langle 12, 4\rangle$	$\langle 12, 1\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathbb{H}]$	$[1, 1, 0, 2, 6, 2, 0, 0, 0, 6, 2, 0, 0, 4]$
$J(D_3)$	$\langle 24, 6\rangle$	$\langle 12, 4\rangle$	$\langle 12, 4\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathbb{H}]$	$[1, 1, 6, 2, 0, 2, 0, 0, 0, 6, 2, 0, 0, 4]$
$J(D_6)$	$\langle 48, 38\rangle$	$\langle 24, 14\rangle$	$\langle 24, 8\rangle$	$\mathbf{F}[\mathrm{D}_6 \times \mathrm{C}_2, \mathrm{D}_6]$	$[1, 1, 8, 2, 6, 2, 4, 0, 0, 14, 2, 4, 0, 4]$
$C_{2,1}$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\langle 1, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0]$
$C_{2,1}$	$\langle 4, 2\rangle$	$\langle 2, 1\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0]$
$C_{6,1}$	$\langle 6, 2\rangle$	$\langle 6, 2\rangle$	$\langle 3, 1\rangle$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 0, 2, 0, 0, 0, 0, 0, 1, 0, 2, 0, 0]$
$C_{6,1}$	$\langle 12, 5\rangle$	$\langle 6, 2\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 2, 0, 2, 0, 0, 0, 2, 0, 4, 0, 0]$
$D_{2,1}$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\langle 2, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 1, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0]$
$D_{2,1}$	$\langle 8, 3\rangle$	$\langle 4, 2\rangle$	$\langle 4, 1\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 0, 2, 0, 0, 0, 0, 4, 0, 0, 0, 0]$
$D_{2,1}$	$\langle 8, 5\rangle$	$\langle 4, 2\rangle$	$\langle 4, 2\rangle$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 2, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0]$
$D_{3,2}$	$\langle 6, 1\rangle$	$\langle 6, 1\rangle$	$\langle 3, 1\rangle$	$\mathbf{F}[\mathrm{D}_3, \mathrm{C}_3]$	$[1, 0, 0, 2, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0]$
$D_{3,2}$	$\langle 12, 4\rangle$	$\langle 6, 1\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{D}_3, \mathrm{C}_3]$	$[1, 1, 0, 2, 0, 2, 0, 0, 0, 6, 0, 0, 0, 0]$
$D_{6,1}$	$\langle 12, 4\rangle$	$\langle 12, 4\rangle$	$\langle 6, 1\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathrm{M}_2(\mathbb{R})]$	$[1, 0, 3, 2, 0, 0, 0, 0, 0, 4, 0, 2, 0, 0]$
$D_{6,1}$	$\langle 24, 8\rangle$	$\langle 12, 4\rangle$	$\langle 12, 1\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 0, 2, 6, 2, 0, 0, 0, 8, 0, 4, 0, 0]$
$D_{6,1}$	$\langle 24, 14\rangle$	$\langle 12, 4\rangle$	$\langle 12, 4\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathrm{M}_2(\mathbb{R})]$	$[1, 1, 6, 2, 0, 2, 0, 0, 0, 8, 0, 4, 0, 0]$
$D_{6,2}$	$\langle 12, 4\rangle$	$\langle 12, 4\rangle$	$\langle 6, 2\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{C}_6]$	$[1, 0, 1, 2, 0, 0, 2, 0, 0, 6, 0, 0, 0, 0]$
$D_{6,2}$	$\langle 24, 14\rangle$	$\langle 12, 4\rangle$	$\langle 12, 5\rangle$	$\mathbf{F}[\mathrm{D}_6, \mathrm{C}_6]$	$[1, 1, 2, 2, 0, 2, 4, 0, 0, 12, 0, 0, 0, 0]$

Table 4. Triples for twists of C_2^0 (top) and C_3^0 (bottom).

G	$[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)]$	K	L
$\boldsymbol{y^2 = x^5 - x}$			
$J(C_2)$	$\langle 8, 2\rangle, \langle 4, 2\rangle, \langle 4, 1\rangle$	$M(i)$	$K\big(\sqrt{\sqrt{2}+2}\,\big)$
$\boldsymbol{y^2 = x^5 + 4x}$			
$J(C_2)$	$\langle 8, 3\rangle, \langle 4, 2\rangle, \langle 4, 2\rangle$	$M(i)$	$K(\sqrt[4]{2})$
$\boldsymbol{y^2 = x^6 + x^5 - 5x^4 - 5x^2 - x + 1}$			
$J(C_4)$	$\langle 16, 6\rangle, \langle 8, 2\rangle, \langle 8, 1\rangle$	$M(\sqrt{\sqrt{17}+17})$	$K\big(\sqrt{(\sqrt{17}+3)\sqrt{\sqrt{17}+17} - 8\sqrt{17}}\,\big)$
$\boldsymbol{y^2 = x^5 + 9x}$			
$J(D_2)$	$\langle 16, 11\rangle, \langle 8, 5\rangle, \langle 8, 3\rangle$	$M(i, \sqrt{3})$	$K(\sqrt[4]{3})$
$\boldsymbol{y^2 = x^5 - 9x}$			
$J(D_2)$	$\langle 16, 13\rangle, \langle 8, 5\rangle, \langle 8, 4\rangle$	$M(i, \sqrt{3})$	$K(\sqrt[4]{3i})$
$\boldsymbol{y^2 = x^6 + 10x^3 - 2}$			
$J(D_3)$	$\langle 24, 6\rangle, \langle 12, 4\rangle, \langle 12, 4\rangle$	$M(\sqrt{-3},\ \sqrt[3]{-2})$	$K\big(\sqrt{\sqrt{6}-2}\,\big)$
$\boldsymbol{y^2 = x^5 + 3x}$			
$J(D_4)$	$\langle 32, 43\rangle, \langle 16, 11\rangle, \langle 16, 8\rangle$	$M(i,\ \sqrt[4]{3})$	$K(\sqrt[8]{3})$
$\boldsymbol{y^2 = x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8}$			
$J(T)$	$\langle 48, 33\rangle, \langle 24, 13\rangle, \langle 24, 3\rangle$	$M(u_1, u_2)$	$K(\sqrt{v_1})$
$\boldsymbol{y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1}$			
$J(O)$	$\langle 96, 193\rangle, \langle 48, 48\rangle, \langle 48, 29\rangle$	$M(\sqrt{-11}, u_3, u_4)$,	$K(\sqrt{v_2})$
$\boldsymbol{y^2 = x^6 - 5x^4 - 5x^2 + 1}$			
$C_{2,1}$	$\langle 2, 1\rangle, \langle 2, 1\rangle, \langle 1, 1\rangle$	M	K
$\boldsymbol{y^2 = -x^6 + 5x^4 + 5x^2 - 1}$			
$C_{2,1}$	$\langle 4, 2\rangle, \langle 2, 1\rangle, \langle 2, 1\rangle$	M	$K(i)$
$\boldsymbol{y^2 = x^5 + x}$			
$D_{2,1}$	$\langle 4, 2\rangle, \langle 4, 2\rangle, \langle 2, 1\rangle$	$M(i)$	K
$\boldsymbol{y^2 = x^6 + 3x^5 - 20x^4 + 30x^3 - 35x^2 + 3x + 10}$			
$D_{2,1}$	$\langle 8, 3\rangle, \langle 4, 2\rangle, \langle 4, 1\rangle$	$M(\sqrt{7})$	$K\big(\sqrt{3\sqrt{7}+7}\,\big)$
$\boldsymbol{y^2 = x^5 + 81x}$			
$D_{2,1}$	$\langle 8, 5\rangle, \langle 4, 2\rangle, \langle 4, 2\rangle$	$M(i)$	$K(\sqrt{3})$
$\boldsymbol{y^2 = x^6 - 18x^5 - 15x^4 - 20x^3 + 135x^2 - 498x - 89}$			
$D_{3,2}$	$\langle 6, 1\rangle, \langle 6, 1\rangle, \langle 3, 1\rangle$	$M(u_5)$	K
$\boldsymbol{y^2 = x^6 + 4x^5 - 10x^4 + 80x^3 + 140x^2 + 144x - 184}$			
$D_{3,2}$	$\langle 12, 4\rangle, \langle 6, 1\rangle, \langle 6, 2\rangle$	$M(u_6)$	$K(i)$
$\boldsymbol{y^2 = x^5 - 2x}$			
$D_{4,1}$	$\langle 16, 7\rangle, \langle 8, 3\rangle, \langle 8, 3\rangle$	$M(i\sqrt[4]{-2})$	$K(\sqrt[8]{-2})$
$\boldsymbol{y^2 = x^5 + 2x}$			
$D_{4,1}$	$\langle 16, 8\rangle, \langle 8, 3\rangle, \langle 8, 4\rangle$	$M(i\sqrt[4]{2})$	$K(\sqrt[8]{2})$
$\boldsymbol{y^2 = x^6 + x^5 + 10x^3 + 5x^2 + x - 2}$			
$D_{4,2}$	$\langle 16, 7\rangle, \langle 8, 3\rangle, \langle 8, 1\rangle$	$M\big(\sqrt{\sqrt{-7}+7}\,\big)$	$K\big(\sqrt{-\sqrt{-2}\sqrt{\sqrt{-7}-7}+2\sqrt{-7}}\,\big)$
$\boldsymbol{y^2 = x^6 + 7x^5 + 10x^4 + 10x^3 + 15x^2 + 17x + 4}$			
O_1	$\langle 48, 29\rangle, \langle 24, 12\rangle, \langle 24, 3\rangle$	$M(u_7, u_8)$	$K\big(\sqrt{-u_8^3 + u_8^2 + 5u_8 + 4}\,\big)$

$u_1^3 - 7u_1 + 7 = 0 \qquad u_2^4 + 4u_2^2 + 8u_2 + 8 = 0 \qquad u_3^3 - 4u_3 + 4 = 0 \qquad u_4^4 + 22u_4 + 22 = 0$

$u_5^3 + 6u_5 - 8 = 0 \qquad u_6^3 + 5u_6 - 10 = 0 \qquad u_7^3 + 5u_7 + 10 = 0 \qquad u_9^4 + 4u_9^2 + 8u_9 + 2 = 0$

$$v_1^{12} - 12v_1^{11} + 70v_1^{10} - 236v_1^9 + 337v_1^8 - 40v_1^7 - 420v_1^6 + 452v_1^5 - 150v_1^4 + 16v_1^3 - 28v_1^2 + 8v_1 + 1 = 0$$

$$v_2^{12} + 44v_2^{11} + 682v_2^{10} + 4048v_2^9 + 3135v_2^8 - 19844v_2^7 + 306614v_2^6 + 1783540v_2^5 \\ - 5571929v_2^4 + 85184v_2^3 + 1269774v_2^2 - 1293732v_2 - 970299 = 0$$

Table 5. Twists of C_2^0: $y^2 = x^6 - 5x^4 - 5x^2 + 1$ realizing each triple.

G	$[\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(L/M)]$	K	L
$\boldsymbol{y^2=x^6+6x^5+30x^4+120x^2-96x+64}$			
$J(C_2)$	$\langle 8, 2\rangle, \langle 4, 2\rangle, \langle 4, 1\rangle$	$M(\sqrt{5})$	$K\left(\sqrt{\sqrt{5}+5}\right)$
$\boldsymbol{y^2=x^5+10x^3+9x}$			
$J(C_2)$	$\langle 8, 3\rangle, \langle 4, 2\rangle, \langle 4, 2\rangle$	$M(i)$	$K(\sqrt[4]{3})$
$\boldsymbol{y^2=x^6-15x^4-20x^3+6x+1}$			
$J(C_6)$	$\langle 24, 10\rangle, \langle 12, 5\rangle, \langle 12, 5\rangle$	$M(i, u_1)$	$K(\sqrt[4]{3})$
$\boldsymbol{y^2=x^5+20x^3+36x}$			
$J(D_2)$	$\langle 16, 11\rangle, \langle 8, 5\rangle, \langle 8, 3\rangle$	$M(i, \sqrt{2})$	$K(\sqrt[4]{6})$
$\boldsymbol{y^2=x^6+15x^4+20x^3+30x^2+18x+5}$			
$J(D_3)$	$\langle 24, 5\rangle, \langle 12, 4\rangle, \langle 12, 1\rangle$	$M(\sqrt{5}, u_1)$	$K\left(\sqrt{2\sqrt{5}+10}\right)$
$\boldsymbol{y^2=x^6+6x^5+40x^3-60x^2+72x-32}$			
$J(D_3)$	$\langle 24, 6\rangle, \langle 12, 4\rangle, \langle 12, 4\rangle$	$M(i, u_2)$	$K(\sqrt[4]{3})$
$\boldsymbol{y^2=x^6+3x^5+10x^3-15x^2+15x-6}$			
$J(D_6)$	$\langle 48, 38\rangle, \langle 24, 14\rangle, \langle 24, 8\rangle$	$M(i, \sqrt{2}, u_3)$	$K(\sqrt[4]{2})$
$\boldsymbol{y^2=x^6+1}$			
$C_{2,1}$	$\langle 2, 1\rangle, \langle 2, 1\rangle, \langle 1, 1\rangle$	M	K
$\boldsymbol{y^2=x^6+15x^4+15x^2+1}$			
$C_{2,1}$	$\langle 4, 2\rangle, \langle 2, 1\rangle, \langle 2, 1\rangle$	M	$K(\sqrt{2})$
$\boldsymbol{y^2=-x^6-6x^5+30x^4-20x^3-15x^2+12x-1}$			
$C_{6,1}$	$\langle 6, 2\rangle, \langle 6, 2\rangle, \langle 3, 1\rangle$	$M(u_1)$	K
$\boldsymbol{y^2=x^6+6x^5-30x^4+20x^3+15x^2-12x+1}$			
$C_{6,1}$	$\langle 12, 5\rangle, \langle 6, 2\rangle, \langle 6, 2\rangle$	$M(u_1)$	$K(i)$
$\boldsymbol{y^2=x^6-1}$			
$D_{2,1}$	$\langle 4, 2\rangle, \langle 4, 2\rangle, \langle 2, 1\rangle$	$M(i)$	K
$\boldsymbol{y^2=11x^6+30x^5+30x^4+40x^3-60x^2+120x-88}$			
$D_{2,1}$	$\langle 8, 3\rangle, \langle 4, 2\rangle, \langle 4, 1\rangle$	$M(\sqrt{-2})$	$K\left(\sqrt{\sqrt{6}-2}\right)$
$\boldsymbol{y^2=x^6-15x^4+15x^2-1}$			
$D_{2,1}$	$\langle 8, 5\rangle, \langle 4, 2\rangle, \langle 4, 2\rangle$	$M(i)$	$K(\sqrt{2})$
$\boldsymbol{y^2=x^6+4}$			
$D_{3,2}$	$\langle 6, 1\rangle, \langle 6, 1\rangle, \langle 3, 1\rangle$	$M(\sqrt[3]{2})$	K
$\boldsymbol{y^2=x^6+12x^5+15x^4+40x^3+15x^2+12x+1}$			
$D_{3,2}$	$\langle 12, 4\rangle, \langle 6, 1\rangle, \langle 6, 2\rangle$	$M(\sqrt[3]{3})$	$K(\sqrt{-2})$
$\boldsymbol{y^2=x^6+9x^5-60x^4-120x^3+240x^2+144x-64}$			
$D_{6,1}$	$\langle 12, 4\rangle, \langle 12, 4\rangle, \langle 6, 1\rangle$	$M(i, u_4)$	K
$\boldsymbol{y^2=x^6+6x^5-30x^4-40x^3+60x^2+24x-8}$			
$D_{6,1}$	$\langle 24, 8\rangle, \langle 12, 4\rangle, \langle 12, 1\rangle$	$M(\sqrt{-2}, u_5)$	$K\left(\sqrt{\sqrt{6}-2}\right)$
$\boldsymbol{y^2=x^6+3x^5+15x^4-20x^3+60x^2-60x+28}$			
$D_{6,1}$	$\langle 24, 14\rangle, \langle 12, 4\rangle, \langle 12, 4\rangle$	$M(\sqrt{-2}, u_2)$	$K(\sqrt{2})$
$\boldsymbol{y^2=x^6+2}$			
$D_{6,2}$	$\langle 12, 4\rangle, \langle 12, 4\rangle, \langle 6, 2\rangle$	$M(\sqrt[6]{2})$	K
$\boldsymbol{y^2=x^6+6x^5-15x^4+20x^3-15x^2+6x-1}$			
$D_{6,2}$	$\langle 24, 14\rangle, \langle 12, 4\rangle, \langle 12, 5\rangle$	$M(\sqrt{-2}, u_6)$	$K(i)$

$$u_1^3-3u_1+1=0 \qquad u_2^3-3u_2+4=0 \qquad u_3^3+3u_3-2=0$$
$$u_4^3-15u_4-10\ =0 \qquad u_5^3-9u_5-6\ =0 \qquad u_7^3-6u_7-6$$

Table 6. Twists of C_3^0: $y^2=x^6+1$ realizing each triple.

The methods used to obtain these curves and the computation of K and L are described in Section 5.

Acknowledgements

We thank Joan-C. Lario and Jordi Quer for helpful comments, and we are grateful to Kiran S. Kedlaya for indicating the way to prove Proposition 3.6. Fité thanks the Massachusetts Institute of Technology for its warm hospitality from September to December 2011, the period in which this project was realized. Fité is also grateful to the University of Cambridge for its welcome in the period May-July 2011, when some of the ideas of this article originated. Fité received financial support from DGICYT grant MTM2009-13060-C02-01 and from NSF grant DMS-0545904. Sutherland received financial support from NSF grant DMS-1115455.

References

[Banaszak and Kedlaya 2011] G. Banaszak and K. S. Kedlaya, "An algebraic Sato–Tate group and Sato–Tate conjecture", preprint, 2011. To appear in *Indiana Univ. Math. J.* arXiv 1109.4449v1

[Besche et al. 2002] H. U. Besche, B. Eick, and E. A. O'Brien, "A millennium project: Constructing small groups", *Internat. J. Algebra Comput.* **12**:5 (2002), 623–644. MR 2003h:20042 Zbl 1020.20013

[Cardona 2001] G. Cardona, *Models racionals de corbes de gènere* 2, Tesi Doctoral, Universitat Politècnica de Catalunya, 2001, http://dmi.uib.es/∼gcardona/tesi.pdf.

[Cardona 2006] G. Cardona, "Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$", *J. Algebra* **303**:2 (2006), 707–721. MR 2007e:14049 Zbl 1149.14023

[Cardona et al. 1999] G. Cardona, J. González, J. C. Lario, and A. Rio, "On curves of genus 2 with Jacobian of GL_2-type", *Manuscripta Math.* **98**:1 (1999), 37–54. MR 99j:11068 Zbl 0998.11032

[Fité 2013] F. Fité, "Artin representations attached to pairs of isogenous abelian varieties", *J. Number Theory* **133**:4 (2013), 1331–1345. MR 3004003 Zbl 1275.11100

[Fité and Lario 2013] F. Fité and J.-C. Lario, "The twisting representation of the L-function of a curve", *Rev. Mat. Iberoam.* **29**:3 (2013), 749–764. MR 3089761 Zbl 06216017

[Fité et al. 2012] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland, "Sato–Tate distributions and Galois endomorphism modules in genus 2", *Compos. Math.* **148**:5 (2012), 1390–1442. MR 2982436 Zbl 1269.11094

[Fité et al. ≥ 2014] F. Fité, E. Lorenzo, and A. Sutherland, "Sato–Tate distributions of twists of the Fermat and Klein quartics". In preparation.

[Gross 1980] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics **776**, Springer, Berlin, 1980. MR 81f:10041 Zbl 0433.14032

[Hecke 1920] E. Hecke, "Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen", *Math. Z.* **6**:1-2 (1920), 11–51. MR 1544392 JFM 47.0152.01

[Igusa 1960] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math.* (2) **72** (1960), 612–649. MR 22 #5637 Zbl 0122.39002

[Johansson 2013] C. Johansson, "On the Sato–Tate conjecture for non-generic abelian surfaces", preprint, 2013. arXiv 1307.6478

[Kedlaya and Sutherland 2008] K. S. Kedlaya and A. V. Sutherland, "Computing L-series of hyperelliptic curves", pp. 312–326 in *Algorithmic number theory* (Banff, AB, 2008), edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010d:11070 Zbl 1232.11078

[Mazur et al. 2007] B. Mazur, K. Rubin, and A. Silverberg, "Twisting commutative algebraic groups", *J. Algebra* **314**:1 (2007), 419–438. MR 2008j:14089 Zbl 1128.14034

[OEIS 2011] OEIS, "The On-Line Encyclopedia of Integer Sequences", 2011, http://oeis.org.

[Pila 1990] J. Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields", *Math. Comp.* **55**:192 (1990), 745–763. MR 91a:11071 Zbl 0724.11070

[Rubin and Silverberg 2010] K. Rubin and A. Silverberg, "Choosing the correct elliptic curve in the CM method", *Math. Comp.* **79**:269 (2010), 545–561. MR 2010i:11091 Zbl 1213.11127

[Serre 1998] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics **7**, A K Peters, Wellesley, MA, 1998. MR 98g:11066 Zbl 0902.14016

[Serre 2012] J.-P. Serre, *Lectures on $N_X(p)$*, Research Notes in Mathematics **11**, CRC Press, Boca Raton, FL, 2012. MR 2920749 Zbl 1238.11001

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2010i:11005 Zbl 1194.11005

[Sutherland 2007] A. V. Sutherland, *Order computations in generic groups*, Ph.D. thesis, Massachusetts Institute of Technology, 2007, http://groups.csail.mit.edu/cis/theses/sutherland-phd.pdf.

[Sutherland 2011] A. V. Sutherland, "`smalljac` software library, v. 4.0", 2011, http://math.mit.edu/~drew.

Communicated by Peter Sarnak
Received 2012-11-20 Revised 2013-08-22 Accepted 2013-09-23

francesc.fite@gmail.com *Fakultät für Mathematik, Bielefeld Universität, P.O. Box 100131, D-33501 Bielefeld, Germany*

drew@math.mit.edu *Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 8 No. 3 2014