OXFORD

International Mathematics Research Notices, 2024, **2024**(16), 11989–12020

https://doi.org/10.1093/imrn/rnae148
Advance access publication date 8 July 2024
Article

Frobenius Distributions of Low Dimensional Abelian Varieties Over Finite Fields

Santiago Arango-Piñeros[1,*], Deewang Bhamidipati[2], and Soumya Sankar[3]

[1]Department of Mathematics, Emory University, Atlanta, GA 30322, USA
[2]Mathematics Department, University of California, Santa Cruz, CA 95064, USA
[3]Mathematical Institute, Utrecht University, Hans Freudenthal building, Budapest 6, 3584 CD Utrecht, The Netherlands
[*]Correspondence to be sent to: e-mail: santiago.arango@emory.edu
Communicated by Prof. Barry Mazur

Given a g-dimensional abelian variety A over a finite field $\mathbf{F}_q$, the Weil conjectures imply that the normalized Frobenius eigenvalues generate a multiplicative group of rank at most g. The Pontryagin dual of this group is a compact abelian Lie group that controls the distribution of high powers of the Frobenius endomorphism. This group, which we call the Serre–Frobenius group, encodes the possible multiplicative relations between the Frobenius eigenvalues. In this article, we classify all possible Serre–Frobenius groups that occur for $g \leq 3$. We also give a partial classification for simple ordinary abelian varieties of prime dimension $g \geq 3$.

1 Introduction

Let E be an elliptic curve over a finite field $\mathbf{F}_q$ of characteristic $p > 0$. The zeros $\alpha_1, \overline{\alpha}_1$ of the characteristic polynomial of Frobenius acting on the Tate module of E are complex numbers of absolute value $\sqrt{q}$. Consider $u_1 := \alpha_1/\sqrt{q}$ and $\overline{u}_1$ the normalized zeros in the unit circle U(1). The curve E is *ordinary* if and only if u_1 is not a root of unity, and in this case, the sequence $(u_1^r)_{r=1}^{\infty}$ is equidistributed in U(1). Further, the normalized Frobenius traces $x_r := u_1^r + \overline{u}_1^r$ are equidistributed on the interval $[-2, 2]$ with respect to the pushforward of the probability Haar measure on U(1) via $u \mapsto u + \overline{u}$, namely

$$\lambda_1(x) := \frac{dx}{\pi\sqrt{4 - x^2}}, \tag{1}$$

where dx is the restriction of the Lebesgue measure to $[-2, 2]$ (see [10, Proposition 2.2]).

In contrast, if E is supersingular, the sequence $(u_1^r)_{r=1}^{\infty}$ generates a finite cyclic subgroup of order m, $C_m \subset$ U(1). In this case, the normalized Frobenius traces are equidistributed with respect to the pushforward of the uniform measure on C_m.

This dichotomy branches out in an interesting way for abelian varieties of higher dimension $g >$ 1: potential non-trivial multiplicative relations between the Frobenius eigenvalues $\alpha_1, \overline{\alpha}_1, \ldots, \alpha_g, \overline{\alpha}_g$

Received: June 19, 2023. **Revised:** May 27, 2024. **Accepted:** June 20, 2024

increase the complexity of the problem of classifying the distribution of normalized traces of high powers of Frobenius,

$$x_r := (\alpha_1^r + \overline{\alpha}_1^r + \cdots + \alpha_g^r + \overline{\alpha}_g^r)/q^{r/2} \in [-2g, 2g], \text{ for } r \geq 1. \tag{2}$$

In analogy with the case of elliptic curves, we identify a compact abelian subgroup of $\mathrm{USp}_{2g}(\mathbf{C})$ controlling the distribution of Sequence (2) via pushforward of the Haar measure. In this article, we provide a complete classification of the conjugacy class of this subgroup, which we call the *Serre–Frobenius group*, for abelian varieties of dimension up to 3. We do this by classifying the possible multiplicative relations between the Frobenius eigenvalues. This classification provides a description of all the possible distributions of Frobenius traces in these cases (see Corollary 1.1.1). We also provide a partial classification for simple ordinary abelian varieties of odd prime dimension.

Definition 1.0.1. (Serre–Frobenius group). Let A be an abelian variety of dimension g over $\mathbf{F}_q$. Let $\alpha_1, \alpha_2 \ldots, \alpha_g, \overline{\alpha}_1, \overline{\alpha}_2 \ldots \overline{\alpha}_g$ denote the eigenvalues of Frobenius. Let $u_i = \alpha_i/\sqrt{q}$ denote the normalized Frobenius eigenvalues. The **Serre–Frobenius group of** A, denoted by $\mathrm{SF}(A)$, is the closure of the subgroup of $\mathrm{USp}_{2g}(\mathbf{C})$ generated by the diagonal matrix $\mathrm{diag}(u_1, \ldots, u_g, \overline{u}_1, \ldots, \overline{u}_g)$. This group is well defined up to relabelling of the eigenvalues of Frobenius (see Remark 2.3.1).

The classification of Serre–Frobenius groups relies crucially on the relation between the Serre–Frobenius group and the multiplicative subgroup of $U_A \subset \mathbf{C}^\times$ generated by the normalized eigenvalues $u_1, \ldots, u_g$. Indeed, the isomorphism class of the former is determined by the Pontryagin dual of the latter (see Lemma 2.3.2). The rank of the group U_A is called the **angle rank** of the abelian variety and the order of the torsion subgroup is called the **angle torsion order**. The relation between $\mathrm{SF}(A)$ and the group generated by the normalized eigenvalues gives us the following structure theorem.

Theorem 1.0.2. Let A be an abelian variety defined over $\mathbf{F}_q$. Then

$$\mathrm{SF}(A) \cong \mathrm{U}(1)^\delta \times C_m,$$

where $\delta = \delta_A$ is the angle rank and $m = m_A$ is the angle torsion order. Furthermore, the connected component of the identity is $\mathrm{SF}(A)^\circ = \mathrm{SF}(A \times_{\mathbf{F}_q} \mathbf{F}_{q^m})$.

By definition, the Serre–Frobenius group carries the data of the embedding into the $\mathrm{USp}_{2g}(\mathbf{C})$, which in turn is captured by the relations among the Frobenius eigenvalues. While in general these relations can be hard to pin down (see, for instance, [8, Theorem 3.25]), in our cases, we are able to write them down explicitly and use them to deduce the angle torsion order. In particular, we classify the Serre–Frobenius groups of abelian varieties of dimension $g \leq 3$.

Theorem 1.0.3. (Elliptic curves). Let E be an elliptic curve defined over $\mathbf{F}_q$. Then,

(1) E is ordinary if and only if $\mathrm{SF}(E) = \mathrm{U}(1)$; and
(2) E is supersingular if and only if $\mathrm{SF}(E) \in \{C_1, C_2, C_3, C_4, C_6, C_8, C_{12}\}$.

Here, C_m is the subgroup of $\mathrm{USp}_2(\mathbf{C}) = \mathrm{SL}_2(\mathbf{C})$ generated by $\left(\begin{smallmatrix} \zeta_m & 0 \\ 0 & \zeta_m^{-1} \end{smallmatrix}\right)$ for ζ_m a primitive m-th root, and $\mathrm{U}(1) = \left\{\left(\begin{smallmatrix} u & 0 \\ 0 & \overline{u} \end{smallmatrix}\right) : u \in \mathbf{C}^\times, |u| = 1\right\}$. Moreover, each one of these groups is realized for some prime power q.

We note that the classification of supersingular Serre–Frobenius groups of elliptic curves follows from Deuring [5] and Waterhouse's [33] classification of Frobenius traces (see also [22, Section 14.6] and [28, Theorem 2.6.1]).

Theorem 1.0.4. (Abelian surfaces). Let S be an abelian surface over $\mathbf{F}_q$. Then S has Serre–Frobenius group according to Figure 3. In particular, the possible options for the connected component of the identity $\mathrm{SF}(S)^\circ$, and the size of the cyclic component group $\mathrm{SF}(S)/\mathrm{SF}(S)^\circ \cong C_m$

are given below. Moreover, each one of these groups is realized for some prime power q.

$\mathrm{SF}(S)^\circ$	m
1	1, 2, 3, 4, 5, 6, 8, 10, 12, 24
U(1)	1, 2, 3, 4, 6, 8, 12
$\mathrm{U}(1)^2$	1

Theorem 1.0.5. (Abelian threefolds). Let X be an abelian threefold over $\mathbf{F}_q$. Then, X has Serre–Frobenius group according to Figure 7. In particular, the possible options for the connected component of the identity, $\mathrm{SF}(X)^\circ$, and the size of the cyclic component group $\mathrm{SF}(X)/\mathrm{SF}(X)^\circ \cong C_m$ are given below. Moreover, each one of these groups is realized for some prime power q.

$\mathrm{SF}(X)^\circ$	m
1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 20, 24, 28, 30, 36
U(1)	1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 24
$\mathrm{U}(1)^2$	1, 2, 3, 4, 6, 8, 12, 24
$\mathrm{U}(1)^3$	1

If g is an odd prime, we have the following classification for simple ordinary abelian varieties; in the following theorem, we say that an abelian variety A **splits** over a field extension $\mathbf{F}_{q^m}$ if A is isogenous over $\mathbf{F}_{q^m}$ to a product of proper abelian subvarieties.

Theorem 1.0.6. (Prime dimension). Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of **prime** dimension $g > 2$. Then, exactly one of the following conditions holds:

(1) A is absolutely simple;
(2) A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$; and
(3) A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$. This case only occurs if $2g+1$ is also a prime, that is, if g is a Sophie Germain prime.

1.1 Application to distributions of Frobenius traces

Our results can be applied to understanding the distribution of Frobenius traces of an abelian variety over $\mathbf{F}_q$ as we range over finite extensions of the base field. Indeed, for each integer $r \geq 1$, we may rewrite Equation (2) as

$$x_r = u_1^r + \overline{u}_1^r + \cdots + u_g^r + \overline{u}_g^r \in [-2g, 2g]$$

denote the **normalized Frobenius trace** of the base change of an abelian variety A to $\mathbf{F}_{q^r}$.

In [1], the authors study Jacobians of smooth projective genus g curves with maximal angle rank and show that the sequence $(x_r/2g)_{r=1}^\infty$ is equidistributed on $[-1, 1]$ with respect to an explicit measure. (In their notation, this is the condition that the Frobenius angles are linearly independent modulo 1.) The Serre–Frobenius group enables us to remove the assumption of maximal angle rank.

Corollary 1.1.1. Let A be a g-dimensional abelian variety defined over $\mathbf{F}_q$. Then, the sequence $(x_r)_{r=1}^\infty$ of normalized traces of Frobenius is equidistributed in $[-2g, 2g]$ with respect to the pushforward of the Haar measure on $\mathrm{SF}(A) \subseteq \mathrm{USp}_{2g}(\mathbf{C})$ via the trace

$$\mathrm{SF}(A) \subseteq \mathrm{USp}_{2g}(\mathbf{C}) \to [-2g, 2g], \quad M \mapsto \mathbf{Tr}(M). \tag{3}$$

The classification of the Serre–Frobenius groups in our theorems can be used to distinguish between the different Frobenius trace distributions occurring in each dimension.

Fig. 1. a_1-histograms for 2.5.a_ab and 2.25.ac_bz.

Example 1.1.2. Let S be a simple abelian surface over $\mathbf{F}_q$ with Frobenius eigenvalues $R_S = \{\alpha_1, \alpha_2, \overline{\alpha}_1, \overline{\alpha}_2\}$ and suppose that $S_{(2)} := S \times_{\mathbf{F}_q} \mathbf{F}_{q^2}$ is isogenous to E^2 for some ordinary elliptic curve $E/\mathbf{F}_{q^2}$. In this case, $\{\alpha_1^2, \overline{\alpha}_1^2\} = R_E = \{\alpha_2^2, \overline{\alpha}_2^2\}$. Normalizing, and possibly after re-indexing, we see that either $u_2 = u_1$ or $u_2 = -u_1$. Since S is simple and ordinary, the characteristic polynomial of Frobenius of S is irreducible (see Remark 2.1.1), and we must have $u_2 = -u_1$. The Serre–Frobenius groups of S and $S_{(2)}$ are calculated as follows:

$$\mathrm{SF}(S) = \overline{\left\{ \begin{bmatrix} u_1^r & & & \\ & (-u_1)^r & & \\ & & \overline{u}_1^r & \\ & & & (-\overline{u}_1)^r \end{bmatrix} : r \in \mathbf{Z} \right\}} = \left\{ \begin{bmatrix} u & & & \\ & -u & & \\ & & \overline{u} & \\ & & & -\overline{u} \end{bmatrix} : u \in \mathrm{U}(1) \right\},$$

$$\mathrm{SF}(S_{(2)}) = \overline{\left\{ \begin{bmatrix} u_1^{2r} & & & \\ & (-u_1)^{2r} & & \\ & & \overline{u}_1^{2r} & \\ & & & (-\overline{u}_1)^{2r} \end{bmatrix} : r \in \mathbf{Z} \right\}} = \left\{ \begin{bmatrix} u & & & \\ & u & & \\ & & \overline{u} & \\ & & & \overline{u} \end{bmatrix} : u \in \mathrm{U}(1) \right\}.$$

The sequence of normalized traces, henceforth referred to as the a_1-sequence, is given by $x_r(S) = 0$ when r is odd, and $x_r(S) = 2u_1^r + 2\overline{u}_1^r$ when r is even. Extending the base field to $\mathbf{F}_{q^2}$ yields the sequence of normalized traces $x_r(S_{(2)}) = x_{2r}(S) = 2x_r(E)$. The data of the embedding $\mathrm{SF}(S) \subseteq \mathrm{USp}_4(\mathbf{C})$ precisely captures the (non-trivial) multiplicative relations between the Frobenius eigenvalues.

The sequence of normalized traces $x_r(S)$ is equidistributed with respect to the pushforward of the Haar measure under the trace map $\mathrm{SF}(S) \subseteq \mathrm{USp}_4(\mathbf{C}) \to [-4, 4]$ given by $\mathbf{diag}(z_1, z_2, \overline{z}_1, \overline{z}_2) \mapsto z_1 + z_2 + \overline{z}_1 + \overline{z}_2$, and similarly for $S_{(2)}$. These can be computed explicitly for S and $S_{(2)}$ as

$$\tfrac{1}{2}\delta_0 + \frac{\mathrm{d}x}{2\pi\sqrt{16 - x^2}} \quad \text{and} \quad \frac{\mathrm{d}x}{\pi\sqrt{16 - x^2}}, \tag{4}$$

where $\mathrm{d}x$ is the restriction of the Haar measure to $[-4, 4]$, and δ_0 is the Dirac measure supported at 0.

For instance, choose the surface S to be in the isogeny class with LMFDB [17] label 2.5.a_ab and Weil polynomial $P(T) = T^4 - T^2 + 25$. (Recall the labellingconvention for isogeny classes of abelian varieties over finite fields in the LMFDB is `g.q.iso` where `g` is the dimension, `q` is the cardinality of the base field, and `iso` specifies the isogeny class by writing the coefficients of the Frobenius polynomial in base 26.) This isogeny class is ordinary and simple, but not geometrically simple. Indeed, $S_{(2)}$ is in the isogeny class $\texttt{1.25.ab}^2$ = 2.25.ac_bz corresponding to the square of an ordinary elliptic curve. The corresponding a_1-histograms describing the frequency of the sequence $(x_r)_{r=1}^{\infty}$ are depicted in Figure 1. Each graph represents a histogram of $16^6 = 16777216$ samples placed into $4^6 = 4096$ buckets partitioning the interval $[-2g, 2g]$. The vertical axis has been suitably scaled, with the height of the uniform distribution, $1/4g$, indicated by a gray line.

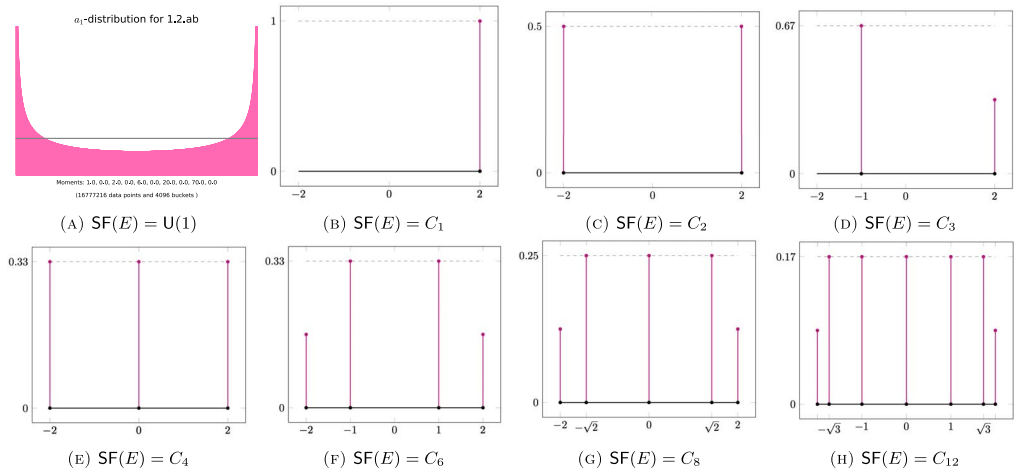


Fig. 2. a_1-histograms of elliptic curves.

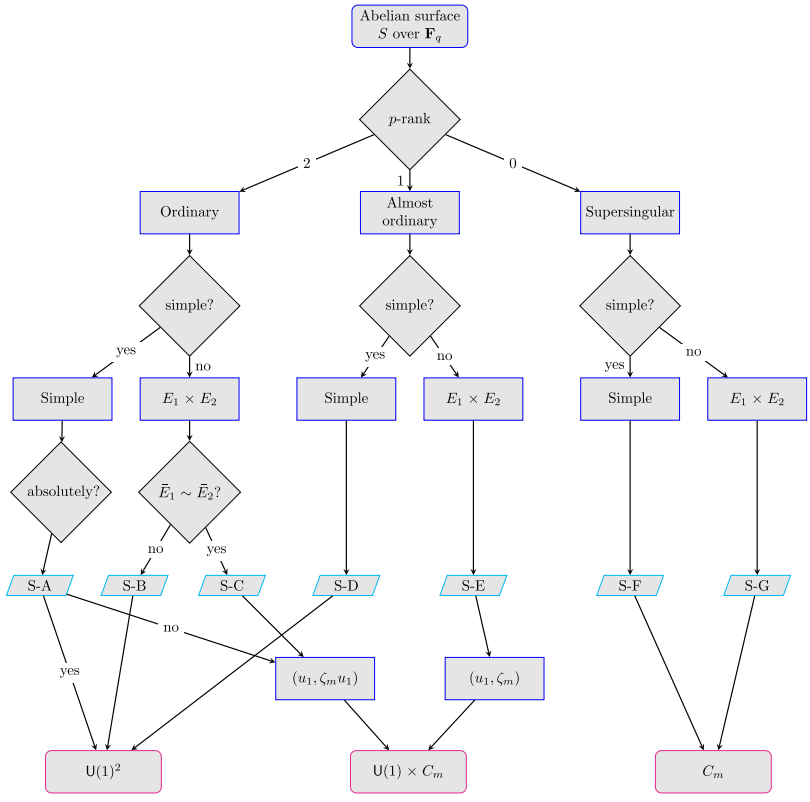


Fig. 3. Theorem 1.0.4: Classification in dimension 2.

1.2 Relation to other work

The reason for adopting the name "Serre–Frobenius group" is that the Lie group SF(A) is closely related to Serre's **Frobenius torus** [27], as explained in Remark 2.3.4.

1.2.1 *Angle rank*

In this article, we study multiplicative relations between Frobenius eigenvalues, a subject studied extensively by Zarhin [16, 37–40]. Our classification relies heavily on being able to understand multiplicative

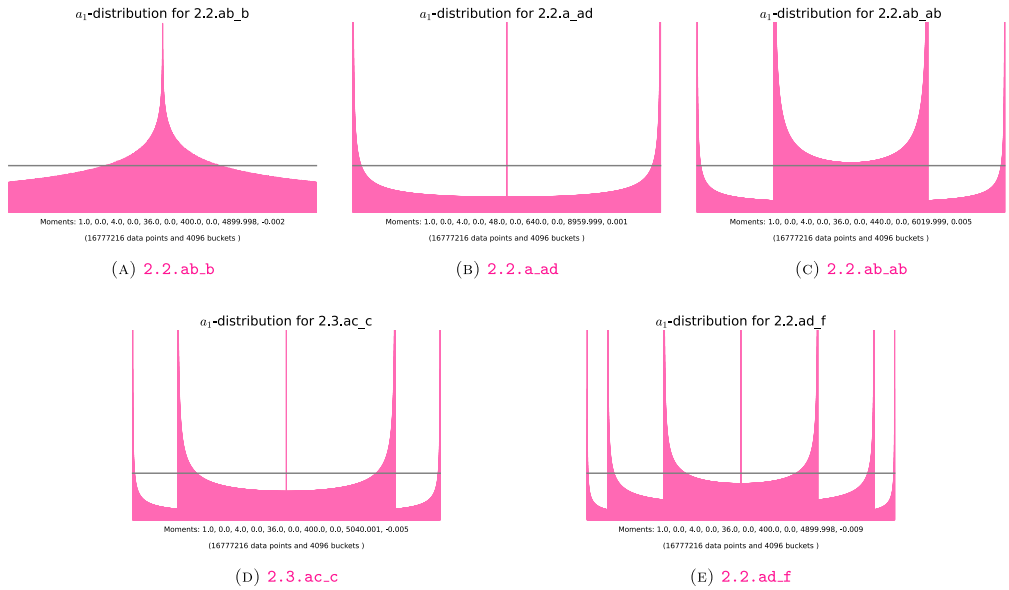


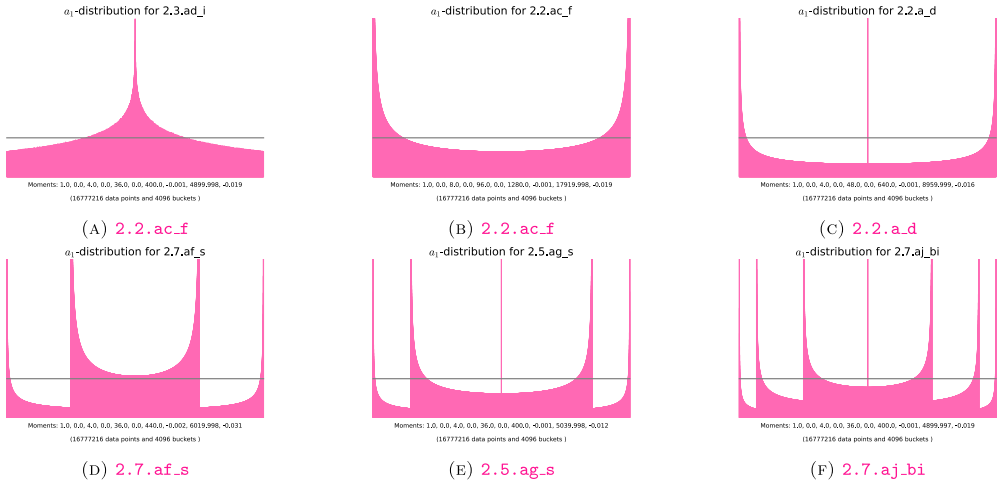
Fig. 4. a_1-histograms for simple ordinary abelian surfaces.

relations in low dimension, and we use results of Zarhin in completing parts of it. The number of multiplicative relations is quantified by the angle rank, an invariant studied in [7, 8] for absolutely simple abelian varieties by elucidating its interactions with the Galois group and Newton polygon of the Frobenius polynomial. We study the angle rank as a stepping stone to classifying the full Serre–Frobenius group. While our perspective differs from that in [8], the same theme is continued here: the Serre–Frobenius groups depend heavily on the Galois group of the Frobenius polynomial. It is worth noting that here that the results about the angle rank in the non-absolutely simple case cannot be pieced together by knowing the results in the absolutely simple cases (for instance, see Zywina's exposition of Shioda's example [42, Remark 1.16]).

1.2.2 *Sato–Tate groups*

The Sato–Tate group of an abelian variety defined over a number field controls the distribution of the Frobenius of the reduction modulo prime ideals, and it is defined via its ℓ-adic Galois representation (see [30, Section 3.2]). The Serre–Frobenius group can also be defined via ℓ-adic representations in an analogous way: it is conjugate to a maximal compact subgroup of the image of Galois representation $\rho_{A,\ell}\colon \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to \mathrm{Aut}(V_\ell A) \otimes \mathbf{C}$, where $V_\ell A$ is the ℓ-adic Tate vector space. Therefore, it is natural to expect that the Sato–Tate and the Serre–Frobenius group are related to each other. The following observations support this claim:

- Assuming standard conjectures, the connected component of the identity of the Sato–Tate group can be recovered from knowing the Frobenius polynomial at two suitably chosen primes [42, Theorem 1.6].
- Several abelian Sato–Tate groups (see [9, 11]) appear as Serre–Frobenius groups of abelian varieties over finite fields. The ones with maximal angle rank are as below.
  - U(1) is the Sato–Tate group of an elliptic curve with complex multiplication over any number field that contains the CM field (see 1.2.B.1.1a). It is also the Serre–Frobenius group of any ordinary elliptic curve (see Figure 2a), and the a_1-moments coincide.
  - $\mathrm{U}(1)^2$ is the Sato–Tate group of weight 1 and degree 4 (see 1.4.D.1.1a). It is also the Serre–Frobenius group of an abelian surface with maximal angle rank (see Figure 4a), and the a_1-moments coincide.
  - $\mathrm{U}(1)^3$ is the Sato–Tate group of weight 1 and degree 6 (see 1.6.H.1.1a). It is also the Serre–Frobenius group of abelian threefolds with maximal angle rank (see Figure 8), and the a_1-moments coincide.



(A) 2.2.ac_f (B) 2.2.ac_f (C) 2.2.a_d

(D) 2.7.af_s (E) 2.5.ag_s (F) 2.7.aj_bi

Fig. 5. a_1-histograms of non-simple ordinary abelian surfaces.

1.3 Outline

In Section 2, we give some background on abelian varieties over finite fields, expand on the definition of the Serre–Frobenius group, and describe how it controls the distribution of traces of high powers of Frobenius. In Section 3, we prove some preliminary results on the geometric isogeny types of abelian varieties of dimension $g \leq 3$ and g odd prime. We also recall some results about Weil polynomials of supersingular abelian varieties, and Zarhin's notion of neatness. In Section 3.2, we discuss the classification in the case of simple ordinary abelian varieties of odd prime dimension. In Section 4, Section 5, and Section 6, we give a complete classification of the Serre–Frobenius group for dimensions 1, 2, and 3, respectively. A list of tables containing different pieces of the classification follows this section.

1.4 Notation

Throughout this paper, A will denote a g-dimensional abelian variety over a finite field $\mathbf{F}_q$ of characteristic p. The polynomial $P_A(T) = \sum_{i=0}^{2g} a_i T^{2g-i}$ will denote the characteristic polynomial of the q-Frobenius endomorphism π_A acting on the Tate module of A, and $h_A(T)$ its minimal polynomial. The set of roots of $P_A(T)$ is denoted by R_A. We usually write $\alpha_1, \overline{\alpha}_1 \ldots, \alpha_g, \overline{\alpha}_g \in R_A$ for the Frobenius eigenvalues, where $\overline{\alpha}_i = q/\alpha_i$. In the case that $P_A(T)$ is a power of $h_A(T)$, we will denote this power by e_A (See 2.1). The subscript $(\cdot)_{(r)}$ will denote the base change of any object or map to $\mathbf{F}_{q^r}$. The group U_A will denote the multiplicative group generated by the normalized eigenvalues of Frobenius, δ_A its rank and m_A the order of its torsion subgroup. The group Γ_A will denote the multiplicative group generated by $\{\alpha_1, \alpha_2 \ldots \alpha_g, q\}$. In Section 5, S will be used to denote an abelian surface, while in Section 6, X will be used to denote a threefold.

2 Frobenius Multiplicative Groups

In this section we introduce the Serre–Frobenius group of A and explain how it is related to Serre's theory of Frobenius tori [27]. We do this from the perspective of the theory of algebraic groups of multiplicative type, as in [19, Chapter 12]. We start by recalling some facts about abelian varieties over finite fields.

2.1 Background on Abelian varieties over finite fields

Fix A a g dimensional abelian variety over $\mathbf{F}_q$. A q-**Weil number** is an algebraic integer α such that $|\phi(\alpha)| = \sqrt{q}$ for every embedding $\phi\colon \mathbf{Q}(\alpha) \to \mathbf{C}$. Let $P_A(T)$ denote the characteristic polynomial of the Frobenius endomorphism acting on the ℓ-adic Tate module of A. The polynomial $P_A(T)$ is monic of degree $2g$, and Weil [34] showed that its roots are q-Weil numbers; we denote the set of roots of $P_A(T)$

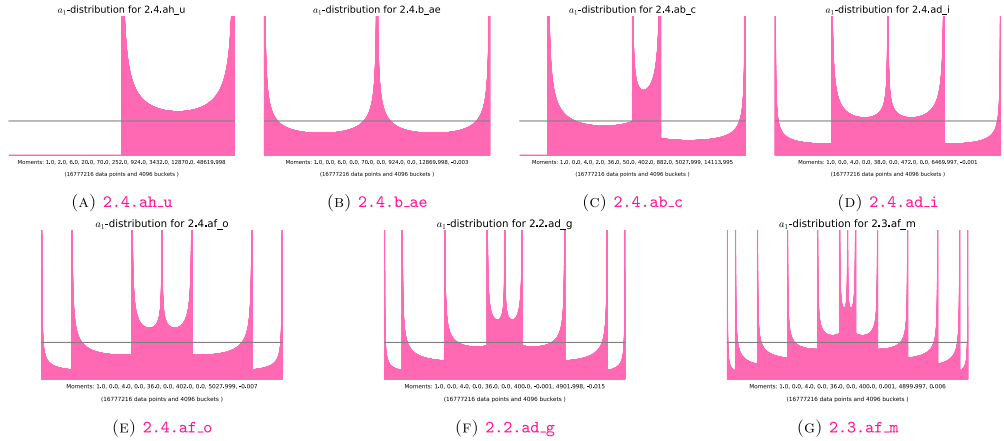


Fig. 6. a_1-distributions of non-simple almost ordinary abelian surfaces.

by $R_A := \{\alpha_1, \alpha_2 \ldots, \alpha_g, \alpha_{g+1}, \ldots, \alpha_{2g}\}$ with $\overline{\alpha}_j := \alpha_{g+j} = q/\alpha_j$ for $j \in \{1, \ldots, g\}$. The seminal work of Honda [13] and Tate [31, 32] classifies the isogeny decomposition type of A in terms of the factorization of $P_A(T)$. In particular, if A is simple, we have that $P_A(T) = h_A(T)^{e_A}$ where $h_A(T)$ is the **minimal polynomial** of the Frobenius endomorphism and e_A is the degree, that is, the square root of the dimension of the central simple algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbf{Q}$ over its center. The Honda–Tate theorem gives a bijective correspondence between isogeny classes of simple abelian varieties over $\mathbf{F}_q$ and conjugacy classes of q-Weil numbers, sending the isogeny class determined by A to the set of roots R_A. Further, the isogeny decomposition $A \sim A_1 \times A_2 \ldots \times A_k$ can be read from the factorization $P_A(T) = \prod_{i=1}^{k} P_{A_i}(T)$.

Writing $P_A(T) = \sum_{i=0}^{2g} a_i T^{2g-i}$, the q-**Newton polygon** of A is the lower convex hull of the set of points $\{(i, \nu(a_i)) \in \mathbf{R}^2 : a_i \neq 0\}$ where ν is the p-adic valuation normalized so that $\nu(q) = 1$. The Newton polygon is isogeny invariant. Define the p-**rank** of A as the number of slope 0 segments of the Newton polygon. An abelian variety is called **ordinary** if it has maximal p-rank, that is, its p-rank is equal to g. It is called **almost ordinary** if it has p-rank $g - 1$; equivalently, the set of slopes of its Newton polygon is $\{0, 1/2, 1\}$ and the slope $1/2$ has length 2. An abelian variety is called **supersingular** if all the slopes of the Newton polygon are equal to $1/2$. The field $L = L_A := \mathbf{Q}(\alpha_1, \ldots, \alpha_g)$ is the splitting field of the Frobenius polynomial. By definition, the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ acts on the roots R_A by permuting them.

Remark 2.1.1. When an abelian variety A over $\mathbf{F}_q$ is simple and ordinary, then $P_A(T)$ is irreducible and its endomorphism algebra is a field [33, Theorem 7.2].

Notation. Whenever A is fixed or clear from context, we will omit the subscript corresponding to it from the notation described above. In particular, we will use $P(T), h(T)$ and e instead of $P_A(T), h_A(T)$ and e_A.

2.2 Angle groups

Denote by $\Gamma := \Gamma_A$ the multiplicative subgroup of $\mathbf{C}^\times$ generated by the set of Frobenius eigenvalues R_A, and let $\Gamma_{(r)} := \Gamma_{A_{(r)}}$ for every $r \geq 1$. Since $\alpha \mapsto q/\alpha$ is a permutation of R_A, the set $\{\alpha_1, \ldots, \alpha_g, q\}$ is a set of generators for Γ; that is, every $\gamma \in \Gamma$ can be written as

$$\gamma = q^k \prod_{j=1}^{g} \alpha_j^{k_j} \tag{5}$$

for some $(k, k_1, \ldots, k_g) \in \mathbf{Z}^{g+1}$.

Since Γ is a subgroup of $\overline{\mathbf{Q}}^\times$, it is naturally a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module. However, this perspective is not necessary for our applications. This group is denoted as Φ_A in [42].

Definition 2.2.1. We define the **angle group** of A to be $U := U_A$, the multiplicative subgroup of $U(1)$ generated by the unitarized eigenvalues $\{u_j := \alpha_j/\sqrt{q} : j = 1, \dots, g\}$. When A is fixed, for every $r \geq 1$ we abbreviate $U_{(r)} := U_{A_{(r)}}$.

Definition 2.2.2. The **angle rank** of an abelian variety $A/\mathbf{F}_q$ is the rank of the finitely generated abelian group U_A. It is denoted by $\delta_A := \mathbf{rk}\, U_A$. The **angle torsion order** m_A is the order of the torsion subgroup of U_A, so that $U_A \cong \mathbf{Z}^{\delta_A} \oplus \mathbf{Z}/m_A\mathbf{Z}$.

The angle rank δ is by definition an integer between 0 and g. When $\delta = g$, there are no multiplicative relations among the normalized eigenvalues. In other words, there are no additional relations among the generators of Γ_A apart from the ones imposed by the Weil conjectures. If A is absolutely simple, the maximal angle rank condition also implies that the Tate conjecture holds for all powers of A (see Remark 1.3 in [8]). On the other extreme, $\delta = 0$ if and only if A is supersingular (see Example 5.1 [7]).

Remark 2.2.3. The angle rank is invariant under base extension: $\delta(A) = \delta(A_{(r)})$ for every $r \geq 1$. Indeed, any multiplicative relation between $\left\{u_1^r, \dots, u_g^r\right\}$ is a multiplicative relation between $\left\{u_1, \dots, u_g\right\}$. We have that $U_A/\mathrm{Tors}(U_A) \cong U_{A_{(r)}}/\mathrm{Tors}(U_{A_{(r)}})$ for every positive integer r. In particular, $U_A/\mathrm{Tors}(U_A) \cong U_{A_{(m)}}$ where $m = m_A$ is the angle torsion order of A.

Example 2.2.4. (Extension and restriction of scalars). Let $A/\mathbf{F}_q$ be an abelian variety with Frobenius polynomial $P_A(T) = \prod(T - \alpha_i) \in \mathbf{C}[T]$ and angle group $U_A = \langle u_1, \dots, u_g \rangle$. Then, the extension of scalars $A_{(r)}$ has Frobenius polynomial $P_{(r)}(T) = \prod(T - \alpha_i^r)$ and angle group $U_{A_{(r)}} = \langle u_1^r, \dots, u_g^r \rangle \subset U_A$. On the other hand, if $B/\mathbf{F}_{q^r}$ is an abelian variety for some $r \geq 1$, and $A/\mathbf{F}_q$ is the Weil restriction of B to $\mathbf{F}_q$, then $P_A(T) = P_B(T^r)$ and $U_A = \langle U_B, \zeta_r \rangle \supset U_B$. See [6].

2.3 The Serre–Frobenius group

For every locally compact abelian group G, denote by $\widehat{G}$ its **Pontryagin dual**; this is the topological group of continuous group homomorphisms $G \to U(1)$. It is well known that $G \mapsto \widehat{G}$ gives an anti-equivalence of categories from the category of locally compact abelian groups to itself. Moreover, this equivalence preserves exact sequences, and every such G is canonically isomorphic to its double dual via the evaluation isomorphism. See [23] for the original reference and [20] for a gentle introduction.

Recall that we defined the Serre–Frobenius group of A as the topological group generated by the matrix $\mathbf{diag}(u_1, \dots, u_g, \overline{u}_1, \dots, \overline{u}_g)$ inside of $\mathrm{USp}_{2g}(\mathbf{C})$ (see Definition 1.0.1).

Remark 2.3.1. The group $U(1)^g$ embeds into $\mathrm{USp}_{2g}(\mathbf{C})$ as a maximal torus via $\mathbf{z} \mapsto \mathrm{diag}(\mathbf{z}, \overline{\mathbf{z}})$, so a different choice of indexing of the Frobenius eigenvalues yields a conjugate subgroup $g^{-1}\mathrm{SF}(A)g$, where g is an element of the Weyl group $N_{\mathrm{USp}_{2g}(\mathbf{C})}(U(1)^g)/U(1)^g$. This Weyl group is isomorphic to the group $S_g^{\pm}$ of signed permutation matrices; the generic Galois group of a complex multiplication polynomial of degree $2g$.

Notation. In light of Remark 2.3.1, we identify $U(1)^g$ with the group

$$\begin{bmatrix} \mathbf{diag}(z_1, \dots, z_g) & \\ & \mathbf{diag}(\overline{z}_1, \dots, \overline{z}_g) \end{bmatrix} \subset \mathrm{USp}_{2g}(\mathbf{C}),$$

and the vector $\mathbf{u} := (u_1, \cdots, u_g)$ with the matrix $\mathbf{diag}(\mathbf{u}, \overline{\mathbf{u}})$. The embedding of $\mathrm{SF}(A)$ into $\mathrm{USp}_{2g}(\mathbf{C})$ is completely determined by the topological generator of $(u_1, \dots, u_g)$, a vector of normalized Frobenius eigenvalues. We will represent the embedding of $\mathrm{SF}(A)$ into $\mathrm{USp}_{2g}(\mathbf{C})$ (up to conjugation) by giving the topological generator of the Serre–Frobenius group.

The following lemma will help us identify the isomorphism class of $\mathrm{SF}(A)$ as a compact abelian group.

Lemma 2.3.2. The Serre–Frobenius group of an abelian variety A has character group U_A. In particular, $\mathrm{SF}(A) \cong \widehat{U}_A$ canonically via the evaluation isomorphism.

Proof. We have an injection $U_A \to \widehat{\mathrm{SF}(A)}$ given by mapping γ to the character ϕ_γ that maps the topological generator $\mathbf{u}$ to γ. To see that this map is surjective, observe that by the exactness of Pontryagin duality, the inclusion $\mathrm{SF}(A) \hookrightarrow \mathrm{U}(1)^g$ induces a surjection $\mathbf{Z}^g = \widehat{\mathrm{U}(1)}^g \to \widehat{\mathrm{SF}(A)}$. Explicitly, this tells us that every character of $\mathrm{SF}(A)$ is given by $\phi(z_1, \dots, z_g) = z_1^{m_1} \cdots z_g^{m_g}$ for some $(m_1, \dots, m_g) \in \mathbf{Z}^g$. By continuity, every character ϕ of $\mathrm{SF}(A)$ is completely determined by $\phi(\mathbf{u})$. In particular, we have that $\phi(\mathbf{u}) = u_1^{m_1} \cdots u_g^{m_g} \in U_A$. ■

The following theorem should be compared to [30, Theorem 3.12]

Theorem 2.3.3. (Theorem 1.0.2). Let A be an abelian variety defined over $\mathbf{F}_q$. Then

$$\mathrm{SF}(A) \cong \mathrm{U}(1)^\delta \times C_m,$$

where $\delta = \delta_A$ is the angle rank and $m = m_A$ is the angle torsion order. Furthermore, the connected component of the identity is

$$\mathrm{SF}(A)^\circ = \mathrm{SF}(A_{(m)}).$$

Proof. Since every finite subgroup of $\mathrm{U}(1)$ is cyclic, the torsion part of the finitely generated group U_A is generated by some primitive m-th root of unity ζ_m. The group $U_{(m)}$ is torsion free by Remark 2.2.3. We thus have the split short exact sequence

$$1 \longrightarrow \langle \zeta_m \rangle \longrightarrow U_A \xrightarrow{u \mapsto u^m} U_{(m)} \longrightarrow 1. \tag{6}$$

After dualizing, we get:

$$1 \longrightarrow \mathsf{SF}(A_{(m)}) \longrightarrow \mathsf{SF}(A) \longrightarrow \langle \zeta_m \rangle \longrightarrow 1. \tag{7}$$

We conclude that $\mathrm{SF}(A)^\circ = \mathrm{SF}(A_{(m)})$ and $\mathrm{SF}(A)/\mathrm{SF}(A)^\circ \cong \langle \zeta_m \rangle$. ■

Remark 2.3.4. By definition, U_A is the image of Γ_A under the radial projection $\psi : \mathbf{C}^\times \to \mathrm{U}(1), z \mapsto z/|z|$. Thus, we have a short exact sequence

$$1 \longrightarrow \Gamma_A \cap \mathbf{R}_{>0} \longrightarrow \Gamma_A \xrightarrow{\psi|_\Gamma} U_A \longrightarrow 1, \tag{8}$$

which is split by the section $u_j \mapsto \alpha_j$. The kernel $\Gamma \cap \mathbf{R}_{>0}$ is free of rank 1 and contains the group $q^{\mathbf{Z}}$. The relation between the Serre–Frobenius group $\mathrm{SF}(A)$ and Serre's Frobenius Torus (see [27, Volume IV, 133.], [4, Section 3]) can be understood via their character groups.

- The (Pontryagin) character group of $\mathrm{SF}(A)$ is U_A.
- The (algebraic) character group of the Frobenius torus of A is the torsion free part of Γ_A.

2.4 Equidistribution results

Let (Y, μ) be a measure space in the sense of Serre (see Appendix A.1 in [26]). Recall that a sequence $(y_r)_{r=1}^\infty \subset Y$ is μ-equidistributed if for every continuous function $f : Y \to \mathbf{C}$ we have that

$$\int_Y f\mu = \lim_{n \to \infty} \frac{1}{n} \sum_{r=1}^{n} f(y_r). \tag{9}$$

In our setting, Y will be a compact abelian Lie group with probability Haar measure μ. We have the following lemma.

Lemma 2.4.1. Let G be a compact group, and $h \in G$. Let H be the closure of the group generated by h. Then, the sequence $(h^r)_{r=1}^{\infty}$ is equidistributed in H with respect to the Haar measure μ_H.

Proof. For a non-trivial character $\phi\colon H \to \mathbf{C}^\times$, the image of the generator $\phi(h) = u \in \mathrm{U}(1)$ is non-trivial. We see that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{r=1}^{n} \phi(h^r) = \lim_{n\to\infty} \frac{1}{n}\sum_{r=1}^{n} u^r = 0,$$

both when u has finite or infinite order. The latter case follows from Weyl's equidistribution theorem in $\mathrm{U}(1)$. The result follows from Lemma 1 in [26, I-19] and the Peter–Weyl theorem. ∎

Corollary 2.4.2. (Corollary 1.1.1). Let A be a g-dimensional abelian variety defined over $\mathbf{F}_q$. Then, the sequence $(x_r)_{r=1}^{\infty}$ of normalized traces of Frobenius is equidistributed in $[-2g, 2g]$ with respect to the pushforward of the Haar measure on $\mathrm{SF}(A) \subseteq \mathrm{USp}_{2g}(\mathbf{C})$ via

$$\mathrm{SF}(A) \subseteq \mathrm{USp}_{2g}(\mathbf{C}) \to [-2g, 2g], \quad M \mapsto \mathbf{Tr}(M).$$

Proof. By Lemma 2.4.1, the sequence $(\mathbf{u}^r)_{r=1}^{\infty}$ is equidistributed in $\mathrm{SF}(A)$ with respect to the Haar measure $\mu_{\mathrm{SF}(A)}$. By definition, the sequence $(x_r)_{r=1}^{\infty}$ is equidistributed with respect to the pushforward measure, and it is invariant under relabelling of the Frobenius eigenvalues. ∎

Remark 2.4.3. (Maximal angle rank). When A has maximal angle rank $\delta = g$, the Serre–Frobenius group is the full torus $\mathrm{U}(1)^g$, and the sequence of normalized traces of Frobenius is equidistributed with respect to the pushforward of the measure $\mu_{\mathrm{U}(1)^g}$; which we denote by $\lambda_g(x)$ following the notation in [1]. (Beware of the different choice of normalization. We chose to use the interval $[-2g, 2g]$ instead of $[-1, 1]$ to be able to compare our distributions with the Sato–Tate distributions of abelian varieties defined over number fields.)

3 Preliminary Results

For this entire section, we let A be an abelian variety over $\mathbf{F}_q$, where $q = p^d$ for some prime p. Recall from Section 1 that an abelian variety A splits over a field extension $\mathbf{F}_{q^m}$ if $A_{(m)} \sim A_1 \times A_2$ and $\dim A_1, \dim A_2 < \dim A$, that is, if A obtains at least one isogeny factor after extending scalars to $\mathbf{F}_{q^m}$. We say that A **splits completely** over $\mathbf{F}_{q^m}$ if $A_{(m)} \sim A_1 \times A_2 \times \ldots \times A_k$, where each A_i is an absolutely simple abelian variety defined over $\mathbf{F}_{q^m}$. In other words, A acquires its geometric isogeny decomposition over $\mathbf{F}_{q^m}$. We define the **splitting degree** of A to be the minimal positive integer m such that A splits completely over $\mathbf{F}_{q^m}$.

3.1 Geometric products of elliptic curves

We begin by stating an important lemma, attributed to Bjorn Poonen in [15].

Lemma 3.1.1. (Poonen). If $E_1, \ldots, E_n$ are n pairwise geometrically non-isogenous elliptic curves over $\mathbf{F}_q$, then their eigenvalues of Frobenius $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent.

In fact, for abelian varieties that split completely as products of elliptic curves, we can explicitly describe the Serre–Frobenius group.

Lemma 3.1.2. Let $B/\mathbf{F}_q$ be an abelian variety that splits over $\mathbf{F}_{q^m}$ as a power of an ordinary elliptic curve, where $m \geq 1$ is the splitting degree of B. Then, $\mathrm{SF}(B) \cong \mathrm{U}(1) \times C_m$. Furthermore, if $m > 1$, then

$$\mathrm{SF}(B) = \left\{(u, \xi_1^v u, \xi_2^v u, \ldots, \xi_{g-1}^v u) : u \in \mathrm{U}(1), v \in \mathbf{Z}/m\mathbf{Z}\right\} \subset \mathrm{U}(1)^g,$$

with $\xi_1, \ldots, \xi_{g-1}$ m-th roots of unity whose orders have least common multiple m. In particular, when B is simple then all the ξ_j are distinct, primitive and $g - 1 \leq \varphi(m)$.

Proof. Angle rank is invariant under base change, so $\delta_B = \delta_{E^g} = 1$. It remains to show that the angle torsion order m_B equals m. If $m = 1$, then $B = E^g$ and there is nothing to show. Assume that $m > 1$. Since $B_{(m)} \sim E^g$, we have that $P_{B,(m)}(T) = P_E(T)^g$. If we denote by $\gamma_1, \overline{\gamma}_1, \dots \gamma_g, \overline{\gamma}_g$ and $\pi_1, \overline{\pi}_1$ the Frobenius eigenvalues of B and E respectively, we have that $\left\{\gamma_1^m, \overline{\gamma}_1^m, \dots, \gamma_g^m, \overline{\gamma}_g^m\right\} = \{\pi_1, \overline{\pi}_1\}$. Possibly after relabelling, we have that $\gamma_{j+1} = \xi_j \gamma_1$ for $j = 1, \dots, g-1$, where the ξ_j's are m-th roots of unity and the minimality of m ensures that the lcm of the orders of the ξ_j's is m. This shows that $C_m \subset U_B$, so that $m \mid m_B$. On the other hand, we have that $\mathrm{SF}(B_{(m)}) = \mathrm{SF}(E^g) \cong \mathrm{U}(1)$ is connected. This implies that $m_B \mid m$ and we conclude that $\mathrm{SF}(B) \cong \mathrm{U}(1) \times C_m$. Assume now B is simple, then $P_B(T)$ is irreducible and hence has no repeated roots, and thus $\xi_j \neq \xi_i$ for every $0 < j < i < g$, and every ξ_i is primitive. This shows that the set $\left\{\xi_j : j = 1, \dots, g-1\right\}$ has $g-1$ elements, and therefore $g - 1 \leq \varphi(m)$. ■

Lemma 3.1.3. Let $A = B \times A_1$ be an abelian variety over $\mathbf{F}_q$ such that A_1 is supersingular with angle torsion order $m_{A_1} = m_1$ and B splits over $\mathbf{F}_{q^m}$ as the power of an ordinary elliptic curve, where $m \geq 1$ is the splitting degree of B. Then, $\mathrm{SF}(A)^\circ \cong \mathrm{U}(1)$ and $m_A = \mathbf{lcm}(m_1, m)$. Furthermore,

$$\mathrm{SF}(A) = \mathbf{diag}(\mathrm{SF}(B), \mathrm{SF}(A_1), \overline{\mathrm{SF}(B)}, \overline{\mathrm{SF}(A_1)}) \subset \mathrm{USp}_{2g}(\mathbf{C}),$$

where $\overline{\mathrm{SF}(B)}$ denotes the (pointwise) complex conjugate of $\mathrm{SF}(B)$, and similarly for A_1.

Proof. From Lemma 3.1.2, we see that $U_A = \langle \zeta_{m_1}, \zeta_m, \upsilon_1 \rangle$, where $\upsilon_1 = \gamma_1/\sqrt{q}$ is a normalized Frobenius eigenvalue of B and all the other roots γ_j can be written as $\zeta_m^{\nu_j}\gamma_1$ with $\mathbf{lcm}_j(\mathbf{ord}(\zeta_m^{\nu_j})) = m$. It follows that $U_A = C_{\mathbf{lcm}(m_1,m)} \oplus \langle \upsilon_1 \rangle$ so that $\delta_A = 1$ and $m_A = \mathbf{lcm}(m_1, m)$. Furthermore, $\mathrm{SF}(A)$ is generated by $(\upsilon_1, \xi_1\upsilon_1, \dots, \xi_{\dim B - 1}\upsilon_1, \eta_1, \dots, \eta_{g_1})$ for some $\xi_j \in \mu_m$ with $\mathbf{lcm}_j(\mathbf{ord}(\xi_j)) = m$ and $\eta_i \in \mu_{m_1}$. ■

Lemma 3.1.4. Let B be an ordinary abelian variety defined over $\mathbf{F}_q$ such that B is geometrically isogenous to a product of elliptic curves. Let m be the splitting degree of B, and write $B_{(m)} \sim E_1^{g_1} \times \cdots \times E_n^{g_n}$ with E_j not geometrically isogenous to E_i for $j \neq i$. Then $\mathrm{SF}(B) \cong \mathrm{U}(1)^n \times C_m$. Moreover, we can describe the embedding of $\mathrm{SF}(B) \hookrightarrow \mathrm{U}(1)^g$ as follows:

(1) Let $r \geq 1$ be the smallest positive integer such that $B_{(r)} \sim B_1 \times \cdots \times B_n$ decomposes into pairwise non-geometrically isogenous factors.
(2) Let m_j be the splitting degree of B_j, so that $(B_j)_{(m_j)} \sim E_j^{g_j}$.

Then, $m = r\,\mathbf{lcm}(m_1, \dots, m_n)$ and

$$\mathrm{SF}(B_{(r)}) = \mathbf{diag}(\mathrm{SF}(B_1), \dots, \mathrm{SF}(B_n), \overline{\mathrm{SF}(B_1)}, \dots, \overline{\mathrm{SF}(B_n)}) \subset \mathrm{USp}_{2g}(\mathbf{C}),$$

where each $\mathrm{SF}(B_j)$ is as in Lemma 3.1.2, and $\overline{\mathrm{SF}(B_i)}$ denotes the (pointwise) complex conjugate of $\mathrm{SF}(B_i)$.

Proof. This follows from combining Lemma 3.1.1 with the fact that the Serre–Frobenius group of B is connected over an extension of degree m. The proof then proceeds as in Lemma 3.1.2. ■

3.2 Splitting of simple ordinary abelian varieties of odd prime dimension

In this section, we analyze the splitting behavior of simple ordinary abelian varieties of *prime dimension* $g > 2$. Our first result is analogous to [14, Theorem 6] for odd primes.

Theorem 3.2.1. (Theorem 1.0.6). Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of **prime** dimension $g > 2$. Then, exactly one of the following conditions holds:

(1) A is absolutely simple.
(2) A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_g$.
(3) A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathrm{SF}(A) \cong \mathrm{U}(1) \times C_{2g+1}$. This case only occurs if $2g+1$ is also a prime, that is, if g is a Sophie Germain prime.

Furthermore, in (2) and (3), we have that

$$\mathrm{SF}(A) = \left\{(u, \xi_1^v u, \xi_2^v u, \ldots, \xi_{g-1}^v u) : u \in \mathrm{U}(1), v \in \mathbf{Z}/m\mathbf{Z}\right\},$$

with $\xi_1, \ldots, \xi_{g-1}$ distinct primitive m-th roots of unity, for $m = g$ and $m = 2g+1$ respectively.

Proof. Let $\alpha = \alpha_1$ be a Frobenius eigenvalue of A, and denote by $K = \mathbf{Q}(\alpha) \cong \mathbf{Q}[T]/P(T)$ the number field generated by α. Since A is ordinary, $\mathbf{Q}(\alpha^n) \neq \mathbf{Q}$ is a CM-field over $\mathbf{Q}$ for every positive integer n, and $P(T)$ is irreducible and therefore $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2g$. Suppose that A is not absolutely simple, and let m be the smallest positive integer such that $A_{(m)}$ splits; by [14, Lemma 4] this is also the smallest m such that $\mathbf{Q}(\alpha^m) \subsetneq \mathbf{Q}(\alpha)$. Since $\mathbf{Q}(\alpha^m)$ is also a CM field, it is necessarily an imaginary quadratic number field.

Observe first that m must be odd. Indeed, if m was even, then $\mathbf{Q}(\alpha^{m/2}) = \mathbf{Q}(\alpha)$ and $[\mathbf{Q}(\alpha^{m/2}) : \mathbf{Q}(\alpha^m)] = 2$. This contradicts the fact that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2g$, since g is an odd prime. By [14, Lemma 5], there are two possibilities:

(i) $P(T) \in \mathbf{Q}[T^m]$,
(ii) $K = \mathbf{Q}(\alpha^m, \zeta_m)$.

If (i) holds and $P(T) = T^{2m} + bT^m + q^g$, we conclude that $m = g$ and $b = a_g$. In this case, the minimal polynomial of α^g has degree 2 and is of the form $h_{(g)}(T) = (T - \alpha^g)(T - \overline{\alpha}^g)$. Note that α^g and $\overline{\alpha}^g$ are distinct, since A is ordinary. Thus, $P_{(g)}(T) = h_{(g)}(T)^g$ and A must split over a degree g extension as the power of an ordinary elliptic curve.

If (ii) holds, we have that $\varphi(m) \mid 2g$. Since $m > 1$ is odd and $\varphi(m)$ takes even values, we have two possible options: either $\varphi(m) = 2$ or $\varphi(m) = 2g$. If $\varphi(m) = 2$, then $[K : \mathbf{Q}(\alpha^m)] \leq 2$ which contradicts the fact that $K = \mathbf{Q}(\alpha)$ is a degree $2g$ extension of $\mathbf{Q}$. Therefore, necessarily, $\varphi(m) = 2g$, and $\mathbf{Q}(\alpha) = \mathbf{Q}(\zeta_m)$. Recall from elementary number theory that the solutions to this equation are $(m, g) = (9, 3)$ or $(m, g) = (2g+1, g)$ for g a Sophie Germain prime.

- ($g > 3$) In this case, (ii) only occurs when $2g + 1$ is prime.
- ($g = 3$) In this case, either $m = 7$ or $m = 9$. To conclude the proof, we show that $m = 9$ does not occur. More precisely, we will show that if A splits over a degree 9 extension, it splits over a degree 3 extension as well. In fact, suppose that $K = \mathbf{Q}(\zeta) = \mathbf{Q}(\alpha)$ for ζ a primitive 9th root of unity. The subfield $F = \mathbf{Q}(\zeta^3)$ is the only imaginary quadratic subfield of K, so if a power of α does not generate K, it must lie in F. Suppose α^9 lies in F. Let σ be the generator of $\mathbf{Gal}(K/F)$ sending ζ to ζ^4. The minimal polynomial of α over F divides $T^9 - \alpha^9$, so $\sigma(\alpha) = \alpha \cdot \zeta^j$ for some j, and $\sigma^2(\alpha) = \alpha\zeta^{5j}$. Since the product of the three conjugates of α over F must lie in F, we have that $\alpha^3 \cdot \zeta^{6j} = (\alpha)(\alpha \cdot \zeta^j)(\alpha \cdot \zeta^{5j}) \in F$, which implies that $\alpha^3 \in F$ and we conclude that A splits over a degree-3 extension of the base field.

The statement about the structure of the Serre–Frobenius group follows from Lemma 3.1.2. ∎

We thank Everett Howe for explaining to us why the case $m = 9$ above does not occur.

3.3 Zarhin's notion of neatness

In this section we discuss Zarhin's notion of *neatness*, a useful technical definition closely related to the angle rank. Define

$$\mathrm{R}'_A := \left\{u_j^2 : \alpha_j \in \mathrm{R}_A\right\}. \tag{10}$$

Note that according to our numbering convention, we have that $u_j^{-1} = \overline{u}_j = u_{j+g}$ for every $j \in \{1, \ldots, g\}$.

Definition 3.3.1. (Zarhin). Let A be an abelian variety defined over $\mathbf{F}_q$. We say that A is **neat** if it satisfies the following conditions:

(Na) Γ_A is torsion free.

Table 1. Minimal polynomial of a supersingular q-Weil number α.

Type	d		$h(T)$	Roots
Z-1	Even	-	$\Phi_m^{[\sqrt{q}]}(T) := \sqrt{q}^{\varphi(m)}\Phi_m(T/\sqrt{q})$	$\zeta_m^j\sqrt{q}$ for $j \in (\mathbf{Z}/m\mathbf{Z})^\times$
Z-2	Odd	$\mathbf{Q}(\alpha) \neq \mathbf{Q}(\alpha^2)$	$\Phi_n^{[q]}(T^2) := q^{\varphi(n)}\Phi_n(T^2/q)$	$\pm\zeta_{2n}^j\sqrt{q}$ for $j \in (\mathbf{Z}/n\mathbf{Z})^\times$
Z-3	Odd	$\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha^2)$	$\prod_{\substack{1\le j\le n \\ \gcd(j,n)=1}} \left(T - \left(\frac{q}{j}\right)\zeta_m^{vj}\sqrt{q}\right)$	$\left(\frac{q}{j}\right)\zeta_m^j\sqrt{q}$ for $j \in (\mathbf{Z}/n\mathbf{Z})^\times$

(Nb) For every function $e\colon R'_A \to \mathbf{Z}$ satisfying

$$\prod_{\beta\in R'_A} \beta^{e(\beta)} = 1,$$

then $e(\beta) = e(\beta^{-1})$ for every $\beta \in R'_A$.

Remarks 3.3.2.

- If A is supersingular and Γ_A is torsion free, then A is neat. Indeed, in this case we have that $R'_A = \{1\}$ and condition NB is trivially satisfied.
- Suppose that the Frobenius eigenvalues of A are distinct and not supersingular. Some base extension of A is neat if and only if A has maximal angle rank.
- In general, maximal angle rank always implies neatness.

3.4 Supersingular Serre–Frobenius groups

Recall that a q-Weil number α is called **supersingular** if $\alpha/\sqrt{q}$ is a root of unity. In [41, Proposition 3.1], Zhu classified the minimal polynomials $h(T)$ of supersingular q-Weil numbers. Let $\Phi_r(T)$ denote the r-th cyclotomic polynomial, $\varphi(r) := \deg\Phi_r(T)$ the Euler totient function, and $\left(\frac{a}{b}\right)$ the Jacobi symbol. Then the possibilities for the minimal polynomials of supersingular q-Weil numbers are given in Table 1.

(Table 1). In case (Z-1), m is any positive integer. In cases (Z-2) and (Z-3), m additionally satisfies $m \not\equiv 2 \bmod 4$, and $n := m/\gcd(2,m)$. The symbol ζ_m denotes the a primitive m-th root of unity. Note that in this case, $\varphi(n) = \varphi(m)/\gcd(2,m)$. Following the notation in [29], given a polynomial $f(T) \in K[T]$ for some field K, and a constant $a \in K^\times$, let

$$f^{[a]}(T) := a^{\deg f} f(T/a).$$

Given any supersingular abelian variety A defined over $\mathbf{F}_q$, the Frobenius polynomial $P_A(T)$ is a power of the minimal polynomial $h_A(T)$, and this minimal polynomial is of type (Z-1), (Z-2), or (Z-3) as above. We say that A is of **type Z-i** if the minimal polynomial $h_A(T)$ is of type (Z-i) for $i = 1, 2, 3$.

Since U_A is finite in the supersingular case, we have that $\mathrm{SF}(A) \cong U_A \cong C_{m_A}$. Furthermore, we have that

$$\mathrm{SF}(A) = \left\{(\xi_1^\nu, \xi_2^\nu, \ldots, \xi_g^\nu) : \nu \in \mathbf{Z}/m_A\mathbf{Z}\right\} \subset \mathrm{U}(1)^g,$$

with ξ_i's being m_A-th roots of unity, whose orders have least common multiple m_A. In particular, we can read off the character group U_A from the fourth column in Table 1. For instance, if $m = 3$ and d is even, then we have a polynomial of type Z-1, and the Serre–Frobenius group is isomorphic to C_3. On the other hand, if $m = 3$ and we have a polynomial of type Z-2, then the Serre–Frobenius group is isomorphic to C_6. Given a q-Weil polynomial $f(T) \in \mathbf{Q}[T]$ with roots $\alpha_1, \cdots, \alpha_{2n}$, the associated **normalized polynomial** $\tilde{f}(T) \in \mathbf{R}[T]$ is the monic polynomial with roots $u_1 = \alpha_1/\sqrt{q}, \ldots, u_{2n} = \alpha_{2n}/\sqrt{q}$. Table 1 allows us to go back and forth between q-Weil polynomials $f(T)$ and the normalized polynomials $\tilde{f}(T)$.

- If $h(T)$ is the minimal polynomial of a supersingular q-Weil number of type Z-1, the normalized polynomial $\tilde{h}(T)$ is the cyclotomic polynomial $\Phi_m(T)$. Conversely, we have that $h(T) = \tilde{h}^{[\sqrt{q}]}(T)$.

Table 2. Serre–Frobenius groups of elliptic curves.

Theorem 4.0.1	p	d	a	SF(E)	Generator	Example	Figure 2
(1)	-	-	$p \nmid a$	U(1)	u_1	1.2.ab	2a
2-(i)	-	Even	$2\sqrt{q}$	C_1	1	1.4.ae	2b
2-(i)	-	Even	$-2\sqrt{q}$	C_2	-1	1.4.e	2c
2-(iii)	$p \not\equiv 1 \bmod 3$	Even	$-\sqrt{q}$	C_3	ζ_3	1.4.c	2d
2-(iv)	$p \not\equiv 1 \bmod 4$	Even	0	C_4	ζ_4	1.4.a	2e
2–(v)	-	Odd	0	C_4	ζ_4	1.2.a	2e
2–(ii)	$p \not\equiv 1 \bmod 3$	Even	$\sqrt{q}$	C_6	ζ_6	1.4.ac	2f
2–(vi)	2	Odd	$\pm\sqrt{2q}$	C_8	ζ_8	1.2.ac	2g
2–(vii)	3	Odd	$\pm\sqrt{3q}$	C_{12}	ζ_{12}	1.3.ad	2h

- If $h(T)$ is the minimal polynomial of a supersingular q-Weil number of type Z-2, the normalized polynomial $\tilde{h}(T)$ is the polynomial $\Phi_n(T^2)$. Conversely, $h(T) = \tilde{h}^{[q]}(T)$.

4 Elliptic Curves

The goal of this section is to prove Theorem 1.0.3. Furthermore, we give a thorough description of the set of possible orders m for the supersingular Serre–Frobenius groups $\mathrm{SF}(E) = C_m$ in terms of p and $q = p^d$.

The isogeny classes of elliptic curves over $\mathbf{F}_q$ were classified by Deuring [5] and Waterhouse [33, Theorem 4.1]. Writing the characteristic polynomial of Frobenius as $P(T) = T^2 + a_1 T + q$, the Weil bounds give $|a_1| \leq 2\sqrt{q}$. Conversely, the integers a satisfying $|a| \leq 2\sqrt{q}$ that correspond to the isogeny class of an elliptic curve are the following.

Theorem 4.0.1. ([28, Theorem 2.6.1]). Let p be a prime and $q = p^d$. Let $a \in \mathbf{Z}$ satisfy $|a| \leq 2\sqrt{q}$.

(1) If $p \nmid a$, then a is the trace of Frobenius of an elliptic curve over $\mathbf{F}_q$. This is the ordinary case.
(2) If $p \mid a$, then a is the trace of Frobenius of an elliptic curve over $\mathbf{F}_q$ if and only if one of the following holds:
  (i) d is even and $a = \pm 2\sqrt{q}$,
  (ii) d is even and $a = \sqrt{q}$ with $p \not\equiv 1 \bmod 3$,
  (iii) labelcase:SS-p d is even and $a = -\sqrt{q}$ with $p \not\equiv 1 \bmod 3$,
  (iv) d is even and $a = 0$ with $p \not\equiv 1 \bmod 4$,
  (v) d is odd and $a = 0$,
  (vi) d is odd, $a = \pm\sqrt{2q}$ with $p = 2$.
  (vii) d is odd, $a = \pm\sqrt{3q}$ with $p = 3$.
(vii) This is the supersingular case.

In the ordinary case, the normalized Frobenius eigenvalue u_1 is not a root of unity, and thus $\mathrm{SF}(E) = \mathrm{U}(1)$. In the supersingular case, the normalized Frobenius eigenvalue u_1 is a root of unity, and thus $\mathrm{SF}(E) = C_m$ is cyclic, with m equal to the order of u_1. For each value of q and a in Theorem 4.0.1 part (2), we get a right triangle of hypotenuse of length $\sqrt{q}$ and base $a/2$, from which we can deduce the angle ϑ_1 and thus the order m of the corresponding root of unity u_1. We thus obtain Theorem 1.0.3 as a restatement of Theorem 4.0.1.

There are eight Serre–Frobenius groups for elliptic curves, summarized in Table 2, and they correspond to eight possible Frobenius distributions of elliptic curves over finite fields. For ordinary elliptic curves (as explained in Section 1), the sequence of normalized traces $(x_r)_{r=1}^{\infty}$ is equidistributed in the interval $[-2, 2]$ with respect to the measure $\lambda_1(x)$ (1) obtained as the pushforward of the Haar measure $\mu_{\mathrm{U}(1)}$ under $z \mapsto z + \bar{z}$. See Figure 2a.

The remaining seven Serre–Frobenius groups are finite and cyclic; they correspond to supersingular elliptic curves. For a given $C_m = \langle \zeta_m \rangle \subset \mathrm{U}(1)$, denote by δ_m the measure obtained by pushforward along

$z \mapsto z + \overline{z}$ of the normalized counting measure,

$$\mu_{C_m}(f) := \int f \, \mu_{C_m} := \frac{1}{m} \sum_{j=1}^{m} f(\zeta_m^j).$$

5 Abelian Surfaces

The goal of this section is to classify the possible Serre–Frobenius groups of abelian surfaces (Theorem 1.0.4). The proof is a careful case-by-case analysis, described by Flowchart 3.

We separate our cases first according to p-rank, and then according to simplicity. In the supersingular and almost ordinary cases this stratification is enough. In the ordinary case, we have to further consider the geometric isogeny type of the surface. When the angle rank is 2, the Serre–Frobenius group is the full torus $U(1)^2$. When the angle rank is 1, the Serre–Frobenius group is isomorphic to $U(1) \times C_m$ but there are two non-conjugate ways to embed $SF(S)$ into $U(1)^2$; these are determined by the topological generator of the group, which can be either $(u_1, \zeta_m u_1)$ or (u_1, ζ_m).

5.1 Simple ordinary surfaces

We restate a theorem of Howe and Zhu in our notation.

Theorem 5.1.1. ([14, Theorem 6]). Suppose that $P(T) = T^4 + a_1 T^3 + a_2 T^2 + q a_1 T + q^2$ is the Frobenius polynomial of a simple ordinary abelian surface S defined over $\mathbf{F}_q$. Then, exactly one of the following conditions holds.

(a) S is absolutely simple.
(b) $a_1 = 0$ and S splits over a quadratic extension.
(c) $a_1^2 = q + a_2$ and S splits over a cubic extension.
(d) $a_1^2 = 2a_2$ and S splits over a quartic extension.
(e) $a_1^2 = 3a_2 - 3q$ and S splits over a sextic extension.

Lemma 5.1.2. (Node S-A in Figure 3). Let S be a simple ordinary abelian surface over $\mathbf{F}_q$. Then, exactly one of the following conditions holds.

(a) S is absolutely simple and $SF(S) = U(1)^2$.
(b) S splits over a quadratic extension and $SF(S) \cong U(1) \times C_2$.
(c) S splits over a cubic extension and $SF(S) \cong U(1) \times C_3$.
(d) S splits over a quartic extension and $SF(S) \cong U(1) \times C_4$.
(e) S splits over a sextic extension and $SF(S) \cong U(1) \times C_6$.

In cases (b)–(e), we have that $SF(A) = \left\{(u, \zeta_m^v u) : u \in U(1),\ v \in (\mathbf{Z}/m\mathbf{Z})\right\}$, for some primitive m-th root of unity ζ_m.

Proof.

(a) From [40, Theorem 1.1], we conclude that some finite base extension of an absolutely simple abelian surface is neat and therefore has maximal angle rank by Remark (3.3.2.c). Alternatively, this also follows from the proof of [1, Theorem 2] for Jacobians of genus 2 curves, which generalizes to any abelian surface. Theorem 1.0.2 then implies that $SF(S) = U(1)^2$.

(b,c,d,e) Denote by m the splitting degree of S. By Theorem 5.1.1 we know that $m \in \{2, 3, 4, 6\}$. Let $\alpha \in \{\alpha_1, \overline{\alpha}_1, \alpha_2, \overline{\alpha}_2\}$ be a Frobenius eigenvalue of S. From [14, Lemma 4] and since S is ordinary, we have that $[\mathbf{Q}(\alpha) : \mathbf{Q}(\alpha^m)] = [\mathbf{Q}(\alpha^m) : \mathbf{Q}] = 2$. In particular, the minimal polynomial $h_{(m)}(T)$ of α^m is quadratic, and $P_{(m)}(T) = h_{(m)}(T)^2$. This implies that $\left\{\alpha_1^m, \overline{\alpha}_1^m\right\} = \left\{\alpha_2^m, \overline{\alpha}_2^m\right\}$, so that (up to relabelling) there is a primitive m-th root of unity ζ_m such that $\alpha_2 = \zeta_m \alpha_1$. (Note that ζ_m must be primitive, since otherwise, $P_{(n)}(T)$ would split for some $n \leq m$, contradicting the minimality of

Table 3. Serre–Frobenius groups of simple ordinary surfaces.

Splitting type	≅ class	Generator	Example	Figure 4
Absolutely simple	$U(1)^2$	(u_1, u_2)	2.2.ab_b	4a
$S_{(2)} \sim E^2$	$U(1) \times C_2$	$(u_1, -u_1)$	2.2.a_ad	4b
$S_{(3)} \sim E^2$	$U(1) \times C_3$	$(u_1, \zeta_3 u_1)$	2.2.ab_ab	4c
$S_{(4)} \sim E^2$	$U(1) \times C_4$	$(u_1, \zeta_4 u_1)$	2.3.ac_c	4d
$S_{(6)} \sim E^2$	$U(1) \times C_6$	$(u_1, \zeta_6 u_1)$	2.2.ad_f	4e

Table 4. Serre–Frobenius groups of non-simple ordinary surfaces $S = E_1 \times E_2$.

Splitting type	≅ class	Generator	Example	Figure 5
$(E_1)_{\overline{\mathbf{F}}_p} \not\sim (E_2)_{\overline{\mathbf{F}}_p}$	$U(1)^2$	(u_1, u_2)	2.3.ad_i	5a
$E_1 \sim E_2$	$U(1)$	(u_1, u_1)	2.2.ac_f	5b
$(E_1)_{(2)} \sim (E_2)_{(2)}$	$U(1) \times C_2$	$(u_1, -u_1)$	2.2.a_d	5c
$(E_1)_{(3)} \sim (E_2)_{(3)}$	$U(1) \times C_3$	$(u_1, \zeta_3 u_1)$	2.7.af_s	5d
$(E_1)_{(4)} \sim (E_2)_{(4)}$	$U(1) \times C_4$	$(u_1, \zeta_4 u_1)$	2.5.ag_s	5e
$(E_1)_{(6)} \sim (E_2)_{(6)}$	$U(1) \times C_6$	$(u_1, \zeta_6 u_1)$	2.7.aj_bi	5f

m.) It follows that

$$\mathrm{SF}(S) = \overline{\langle (u_1, \zeta_m u_1) \rangle} = \left\{ (u, \zeta_m^\nu u) : u \in U(1),\ \nu \in \mathbf{Z}/m\mathbf{Z} \right\} \cong U(1) \times C_m$$

and $\mathrm{SF}(S)^\circ$ embeds diagonally in $U(1)^2$. ∎

Notation. In Table 3, the *Splitting type* title refers to that of the abelian variety S, the ≅ *class* title refers to the Serre–Frobenius group $\mathrm{SF}(S)$, and the *Generator* title refers to the topological generator of $\mathrm{SF}(S)$, which precisely and succinctly captures the data of the embedding of the Serre–Frobenius group into the ambient unitary symplectic group. We will follow the same conventions in the following tables.

5.2 Non-simple ordinary surfaces

Let S be a non-simple ordinary abelian surface defined over $\mathbf{F}_q$. Then S is isogenous to a product of two ordinary elliptic curves $E_1 \times E_2$. As depicted in Figure 3, we consider two cases:

(S-B) E_1 and E_2 are not isogenous over $\overline{\mathbf{F}}_q$.
(S-C) E_1 and E_2 become isogenous over some base extension $\mathbf{F}_{q^{m_1}} \supseteq \mathbf{F}_q$, for $m_1 \geq 1$.

The Serre-Frobenius groups corresponding to these isogeny decomposition types are sumarized in Table 4. The proof of the following lemma is a straightforward application of Lemma 3.1.1.

Lemma 5.2.1. (Node S-B in Figure 3). Let S be an abelian surface defined over $\mathbf{F}_q$ such that S is isogenous to $E_1 \times E_2$, for E_1 and E_2 geometrically non-isogenous ordinary elliptic curves. Then S has maximal angle rank $\delta = 2$ and $\mathrm{SF}(S) = U(1)^2$.

Lemma 5.2.2. (Node S-C in Figure 3). Let S be an abelian surface defined over $\mathbf{F}_q$ such that S is isogenous to $E_1 \times E_2$, for E_1 and E_2 geometrically isogenous ordinary elliptic curves. Then S has angle rank $\delta = 1$ and $\mathrm{SF}(S) = U(1) \times C_m$ for $m \in \{1, 2, 3, 4, 6\}$. Furthermore, m is precisely the degree of the extension of $\mathbf{F}_q$ over which E_1 and E_2 become isogenous.

Proof. Let $\alpha_1, \overline{\alpha}_1$ and $\alpha_2, \overline{\alpha}_2$ denote the Frobenius eigenvalues of E_1 and E_2 respectively. Let m_1 be the smallest positive integer such that $(E_1)_{(m_1)} \sim (E_2)_{(m_1)}$. From Lemma 3.1.2, we immediately have that $\mathrm{SF}(S) \cong U(1) \times C_m$, where $m = m_1$. In order to find the value of m, observe that $\{\alpha_1^m, \overline{\alpha}_1^m\} = \{\alpha_2^m, \overline{\alpha}_2^m\}$, from which we may assume, possibly after relabelling, that $\alpha_2 = \zeta_m \alpha_1$ for some primitive m-th root

Table 5. Serre–Frobenius groups of non-simple almost ordinary surfaces.

≅class	Generator	Example	Figure 6
$U(1)$	$(u_1, 1)$	2.4.ah_u	6a
$U(1) \times C_2$	$(u_1, -1)$	2.4.b_ae	6b
$U(1) \times C_3$	(u_1, ζ_3)	2.4.ab_c	6c
$U(1) \times C_4$	(u_1, ζ_4)	2.4.ad_i	6d
$U(1) \times C_6$	(u_1, ζ_6)	2.4.af_o	6e
$U(1) \times C_8$	(u_1, ζ_8)	2.2.ad_g	6f
$U(1) \times C_{12}$	(u_1, ζ_{12})	2.3.af_m	6g

of unity ζ_m. Since the curves E_1 and E_2 are ordinary, the number fields $\mathbf{Q}(\alpha_1)$ and $\mathbf{Q}(\alpha_2)$ are imaginary quadratic and $\mathbf{Q}(\alpha_1) = \mathbf{Q}(\alpha_1^m) = \mathbf{Q}(\alpha_2^m) = \mathbf{Q}(\alpha_2)$. Hence, $\zeta_m \in \mathbf{Q}(\alpha_1)$ and thus $\varphi(m) = [\mathbf{Q}(\zeta_m) : \mathbf{Q}] \in \{1, 2\}$; therefore $m \in \{1, 2, 3, 4, 6\}$. Finally, we have by definition that $\mathrm{SF}(S) = \left\{(u, \zeta_m^v u) : u \in U(1),\ v \in \mathbf{Z}/m\mathbf{Z}\right\} \cong U(1) \times C_m$. ■

5.3 Simple almost ordinary surfaces

In [16] Lenstra and Zarhin carried out a careful study of the multiplicative relations of Frobenius eigenvalues of simple almost ordinary varieties (see Section 2.1 for the definition), which was later generalized in [8]. In particular, they prove that even dimensional simple almost ordinary abelian varieties have maximal angle rank [16, Theorem 5.8]. Since every abelian surface of p-rank 1 is almost ordinary, their result allows us to deduce the following.

Lemma 5.3.1. (Node S-D in Figure 3). Let S be a simple and almost ordinary abelian surface defined over $\mathbf{F}_q$. Then S has maximal angle rank $\delta = 2$ and $\mathrm{SF}(S) = U(1)^2$.

5.4 Non-simple almost ordinary surfaces

If S is almost ordinary and not simple, then S is isogenous to the product of an ordinary elliptic curve E_1 and a supersingular elliptic curve E_2. The corresponding Serre-Frobenius groups are sumarized in Table 5.

Lemma 5.4.1. (Node S-E in Figure 3). Let S be a non-simple almost ordinary abelian surface defined over $\mathbf{F}_q$. Then S has angle rank $\delta = 1$ and angle torsion order $m \in \{1, 2, 3, 4, 6, 8, 12\}$. Furthermore, $\mathrm{SF}(S) = \left\{(u, \zeta_m^v) : u \in U(1),\ v \in \mathbf{Z}/m\mathbf{Z}\right\} \cong U(1) \times C_m$.

Proof. Let E_1 be an ordinary elliptic curve and E_2 a supersingular elliptic curve such that $S \sim E_1 \times E_2$. By Lemma 3.1.3, $\mathrm{SF}(S) = \mathrm{SF}(E_1) \times \mathrm{SF}(E_2) \cong U(1) \times C_m$ with m in the list of possible orders of Serre–Frobenius groups of supersingular elliptic curves. ■

5.5 Simple supersingular surfaces

Since every supersingular abelian variety is geometrically isogenous to a power of an elliptic curve, the Serre–Frobenius group only depends on the splitting degree. We separate our analysis into the simple and non-simple cases.

The classification of Frobenius polynomials of supersingular abelian surfaces over finite fields was completed by Maisner and Nart [18, Theorem 2.9] building on work of Xing [36] and Rück [24]. Denoting by (a_1, a_2) the isogeny class of abelian surfaces over $\mathbf{F}_q$ with Frobenius polynomial $P_S(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$, the following lemma gives the classification of Serre–Frobenius groups of simple supersingular surfaces.

Lemma 5.5.1. (Node S-F in Figure 3). Let S be a simple supersingular abelian surface defined over $\mathbf{F}_q$. The Serre–Frobenius group of S is classified according to Table 6.

Table 6. Serre–Frobenius groups of simple supersingular surfaces.

(a_1, a_2)	p	d	e	**Type**	$\tilde{h}(T)$	**SF**(S)	**Example**
$(0,0)$	$\not\equiv 1 \bmod 8$	even	1	Z-1	$\Phi_8(T)$	C_8	2.4.a_a
$(0,0)$	$\neq 2$	odd	1	Z-2	$\Phi_8(T)$	C_8	2.3.a_a
$(0,q)$	-	odd	1	Z-2	$\Phi_3(T^2)$	C_6	2.2.a_c
$(0,-q)$	$\not\equiv 1 \bmod 12$	even	1	Z-1	$\Phi_{12}(T)$	C_{12}	2.4.a_ae
$(0,-q)$	$\neq 3$	odd	1	Z-2	$\Phi_6(T^2) = \Phi_{12}(T)$	C_{12}	2.2.a_ac
$(\sqrt{q},q)$	$\not\equiv 1 \bmod 5$	even	1	Z-1	$\Phi_5(T)$	C_5	2.4.c_e
$(-\sqrt{q},q)$	$\not\equiv 1 \bmod 5$	even	1	Z-1	$\Phi_{10}(T) = \Phi_5(-T)$	C_{10}	2.4.ac_e
$(\sqrt{5q},3q)$	$= 5$	odd	1	Z-3	$\Psi_{5,1}(T)$	C_{10}	2.5.f_p
$(-\sqrt{5q},3q)$	$= 5$	odd	1	Z-3	$\Psi_{5,1}(-T)$	C_{10}	2.5.af_p
$(\sqrt{2q},q)$	$= 2$	odd	1	Z-3	$\Psi_{2,3}(T)$	C_{24}	2.2.c_c
$(-\sqrt{2q},q)$	$= 2$	odd	1	Z-3	$\Psi_{2,3}(-T)$	C_{24}	2.2.ac_c
$(0,-2q)$	-	odd	2	Z-2	$\Phi_1(T^2)$	C_2	2.2.a_ae
$(0,2q)$	$\equiv 1 \bmod 4$	even	2	Z-1	$\Phi_4(T)$	C_4	2.25.a_by
$(2\sqrt{q},3q)$	$\equiv 1 \bmod 3$	even	2	Z-1	$\Phi_3(T)$	C_3	2.49.o_fr
$(-2\sqrt{q},3q)$	$\equiv 1 \bmod 3$	even	2	Z-1	$\Phi_6(T) = \Phi_3(-T)$	C_6	2.49.ao_fr

Table 7. Angle torsion set for non-simple supersingular surfaces defined over $\mathbf{F}_q$, with $q = p^d$.

d	p	$M(p,d)$
Even	-	$\{1,2\}$
Even	$p \not\equiv 1 \bmod 3$	$\{1,2,3,6\}$
Even	$p \not\equiv 1 \bmod 4$	$\{1,2,4\}$
Odd	-	$\{4\}$
Odd	$p = 2$	$\{4,8\}$
Odd	$p = 3$	$\{4,12\}$

The notation for polynomials of type Z-3 is taken from [29], where the authors classify simple supersingular Frobenius polynomials for $g \leq 7$. We have

$$\Psi_{5,1}(T) := \prod_{a \in (\mathbf{Z}/5)^\times} \left(T - \left(\tfrac{a}{5}\right)\zeta_5^a\right) = T^4 + \sqrt{5}T^3 + 3T^2 + \sqrt{5}T + 1, \tag{13}$$

$$\Psi_{2,3}(T) := \prod_{a \in (\mathbf{Z}/3)^\times} \left(T - \zeta_8\zeta_3^a\right)\left(T - \overline{\zeta}_8\zeta_3^a\right) = T^4 + \sqrt{2}T^3 + T^2 + \sqrt{2}T + 1. \tag{12}$$

We exhibit the proof of the second line in Table 6 for exposition. The remaining cases can be checked similarly. If $(a_1, a_2) = (0,0)$, $p \neq 2$ and q is an odd power of p: then, $P(T) = T^4 + q^2 = \sqrt{q}^4\Phi_8(T/\sqrt{q}) = q^2\Phi_4(T^2/q)$ and $\tilde{h}(T) = \Phi_8(T)$. Thus U_S is generated by a primitive 8th root of unity.

5.6 Non-simple supersingular surfaces

If S is a non-simple supersingular surface, then S is isogenous to a product of two supersingular elliptic curves E_1 and E_2. If m_{E_1} and m_{E_2} denote the torsion orders of E_1 and E_2 respectively, then the extension over which E_1 and E_2 become isogenous is precisely $\mathbf{lcm}(m_{E_1}, m_{E_2})$. Thus, we have the following result, depending on the values of $q = p^d$ as in Table 2.

Lemma 5.6.1. (Node S-G in Figure 3). Let S be a non-simple supersingular abelian surface defined over $\mathbf{F}_q$. Then S has angle rank $\delta = 0$ and $\mathrm{SF}(S) = C_m$ for m in the set $M = M(p,d)$ described in Table 7.

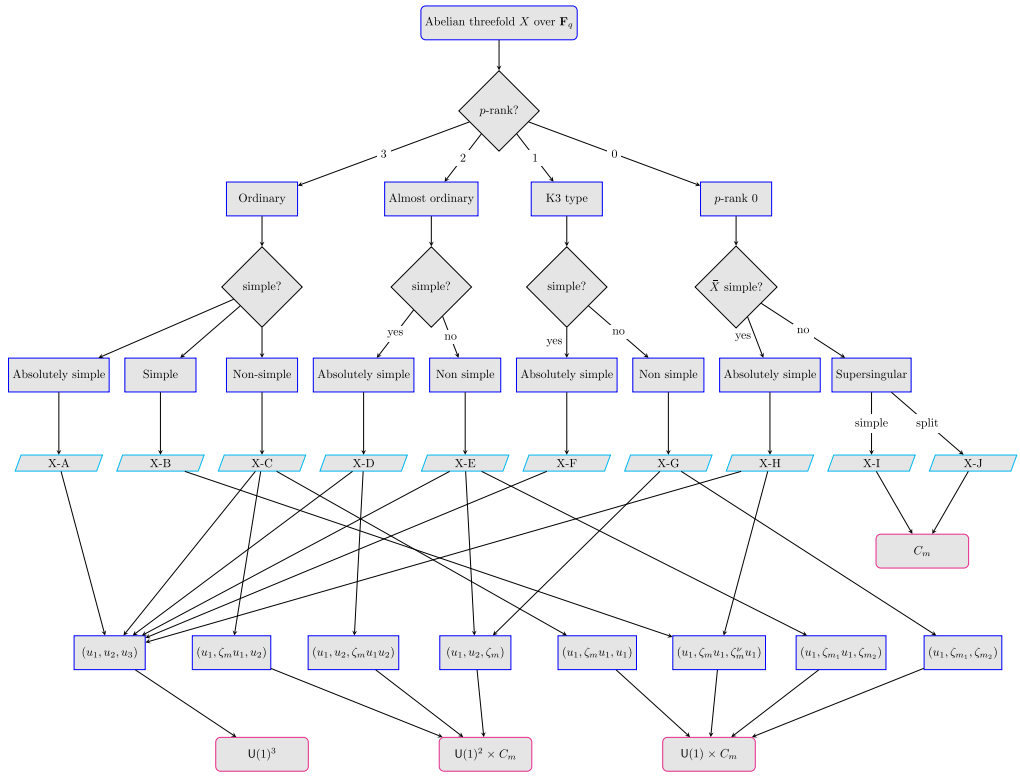


Fig. 7. Theorem 1.0.5: Classification in dimension 3.

6 Abelian Threefolds

In this section, we classify the Serre–Frobenius groups of abelian threefolds (see Figure 7). Let X be an abelian variety of dimension 3 defined over $\mathbf{F}_q$. For our analysis, we will first stratify the cases by p-rank and then by simplicity. Before we proceed, we make some observations about simple threefolds that will be useful later.

6.1 Simple abelian threefolds

If X is a simple abelian threefold, there are only two possibilities for the Frobenius polynomial $P_X(T) = h_X(T)^e$:

$$P_X(T) = h_X(T) \tag{13}$$

$$P_X(T) = h_X(T)^3. \tag{14}$$

Indeed, if $h_X(T)$ were a linear or cubic polynomial, it would have a real root $\pm\sqrt{q}$. By an argument of Waterhouse [33, Chapter 2], the q-Weil numbers $\pm\sqrt{q}$ must come from simple abelian varieties of dimension 1 or 2. Further, Xing [35] showed that (14) can only occur in very special cases.

Theorem 6.1.1. ([35], [12, Proposition 1.2]). Let X be a simple abelian threefold over $\mathbf{F}_q$. Then, $P_X(T) = h_X(T)^3$ if and only if 3 divides $d = \mathbf{log}_p(q)$ and $h_X(T) = T^2 + aq^{1/3}T + q$ with $\mathbf{gcd}(a, p) = 1$.

When $P_X(T)$ is a cube as above, since $\mathbf{gcd}(a, p) = 1$, the q-adic valuation of its middle coefficient is the same as that of aq, which in turn is 1. Thus, X is non-supersingular of p-rank 0 and its Newton Polygon has slopes $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3})$. Furthermore, every simple abelian threefold is either absolutely simple or geometrically isogenous to the cube of an elliptic curve. Thus, we have the following.

Table 8. Serre–Frobenius groups of simple ordinary threefolds X.

Splitting type	$\cong$ class	Generator	Example	Figure 8
Absolutely simple	$U(1)^3$	(u_1, u_2, u_3)	3.2.ad_f_ah	8a
$X_{(3)} \sim E^3$	$U(1) \times C_3$	$(u_1, \zeta_3 u_1, \zeta_3^\nu u_1)$	3.2.a_a_ad	8b
$X_{(7)} \sim E^3$	$U(1) \times C_7$	$(u_1, \zeta_7 u_1, \zeta_7^\nu u_1)$	3.2.ae_j_ap	8c

Lemma 6.1.2. If X is an abelian threefold defined over $\mathbf{F}_q$ that is not ordinary or supersingular, then X is simple if and only if it is absolutely simple.

Proof. Assume X is a simple abelian threefold that is not ordinary or supersingular. Assume also that X is not absolutely simple. Let $r > 1$ be the splitting degree of X. Recall that since X is simple, one either has $P_X(T) = h_X(T)$ or $P_X(T) = h_X(T)^3$, where $h_X(T)$ is irreducible of even degree. We will show that in each case $X_{(r)} \sim E^3$, contradicting the assumption that X is not ordinary or supersingular.

Assume $P_X(T) = h_X(T)^3$, then $P_{X_{(r)}}(T) = h_{X,(r)}(T)^3$. Observe that necessarily $X_{(r)}$ has an elliptic curve $E/\mathbf{F}_{q^r}$ as an isogeny factor. Then $P_E(T)$, a quadratic polynomial, must divide $P_{X_{(r)}}(T)$, and we conclude $P_E(T) = h_{X,(r)}(T)$. Thus, $X_{(r)} \sim E^3$.

Assume instead that $P_X(T) = h_X(T)$, that is, $P_X(T)$ is irreducible. Therefore $\mathbf{Q}(\pi_X)$ is a degree 6 extension and $\mathbf{Q}(\pi_X) \hookrightarrow \mathrm{End}^0(X) \hookrightarrow \mathrm{End}^0(X_{(r)})$. Then by [3, Theorem 1.3.1.1] $X_{(r)}$ is isotypic, so that $X_{(r)} \sim E^3$. ∎

In each case of the classification that follows, we will denote by M, the set of possible angle torsion orders that occur for that case. When we want to emphasize the dependence on the prime p and the power d, we will denote this by $M(p, d)$.

6.2 Simple ordinary threefolds

In this section, X will denote a simple ordinary abelian threefold defined over $\mathbf{F}_q$. The corresponding Serre-Frobenius groups are summarized in Table 8.

As a corollary to Theorem 3.2.1, we have the following.

Proposition 6.2.1. Let X be a simple ordinary abelian threefold defined over $\mathbf{F}_q$. Then, exactly one of the following conditions is satisfied.

(1) X is absolutely simple.
(2) X splits over a degree 3 extension and $P_X(T) = T^6 + a_3 T^3 + q^3$.
(3) X splits over a degree 7 extension and the number field of $P_X(T)$ is $\mathbf{Q}(\zeta_7)$.

Lemma 6.2.2. (Node X-A in Figure 7). Let X be an absolutely simple abelian threefold defined over $\mathbf{F}_q$. Then X has maximal angle rank $\delta = 3$ and $\mathrm{SF}(X) = U(1)^3$.

Proof. Let $m = m_X$ be the order of the torsion subgroup of Γ_X. By [40, Theorem 1.1], we have that $X_{(m)}$ is neat. Since $X_{(m)}$ is ordinary and simple, its Frobenius eigenvalues are distinct and non-real. Remark (3.3.2.b) implies that $X_{(m)}$ has maximal angle rank. Since angle rank is invariant under base extension (Remark 2.2.3) we have that $\delta(X) = \delta(X_{(m)}) = 3$ as we wanted to show. ∎

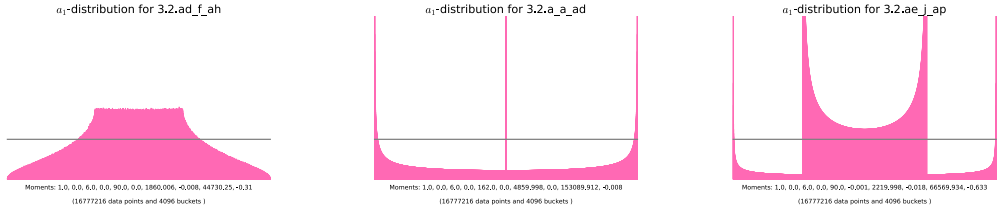
Lemma 6.2.3. (Node X-B in Figure 7). Let X be a simple ordinary abelian threefold over $\mathbf{F}_q$ that is not absolutely simple. Then X has angle rank 1 and

(a) $\mathrm{SF}(X) \cong U(1) \times C_3$ if X splits over a degree 3 extension, or
(b) $\mathrm{SF}(X) \cong U(1) \times C_7$ if X splits over a degree 7 extension.

Furthermore, in (a) and (b), we have that

$$\mathrm{SF}(X) = \left\{(u, \xi_1^\nu u, \xi_2^\nu u) : u \in U(1), \nu \in \mathbf{Z}/m\mathbf{Z}\right\},$$

with ξ_1, ξ_2 distinct primitive m-th roots of unity, for $m = 3$ and $m = 7$, respectively.



(A) 3.2.ad_f_ah (B) 3.2.a_a_ad (C) 3.2.ae_j_ap

Fig. 8. a_1-distributions for simple ordinary threefolds.

Table 9. Serre–Frobenius groups of non-simple ordinary threefolds $X = S \times E$.

Splitting type	$\cong$ class SF(X)	Generator	$m \in M$	Examples
(6.3-a)	$\mathrm{U}(1) \times C_m$	$(u_1, \zeta_m u_1, u_1)$	$\{1, 2, 3, 4, 6\}$	Example 6.3.2
(6.3-b)	$\mathrm{U}(1)^2 \times C_m$	$(u_1, \zeta_m u_1, u_2)$	$\{1, 2, 3, 4, 6\}$	Example 6.3.3
(6.3-c)	$\mathrm{U}(1)^3$	(u_1, u_2, u_3)	$\{1\}$	3.5.ai_bi_ado
(6.3-d)	$\mathrm{U}(1)^3$	(u_1, u_2, u_3)	$\{1\}$	3.2.ad_h_al

Proof. From the proof of Theorem 3.2.1, we have that the torsion free part of U_X is generated by a fixed normalized root $u_1 = \alpha_1/\sqrt{q}$, and all other roots u_j for $1 < j \leq g$ are related to u_1 by a primitive root of unity of order 3 or 7, respectively; $u_2 = \xi_1 u_1$ and $u_3 = \xi_2 u_1$ with $\xi_1 \neq \xi_2$. ■

6.3 Non-simple ordinary threefolds

Let X be a non-simple ordinary abelian threefold defined over $\mathbf{F}_q$. Then X is isogenous to a product $S \times E$, for some ordinary surface S and some ordinary elliptic curve E.

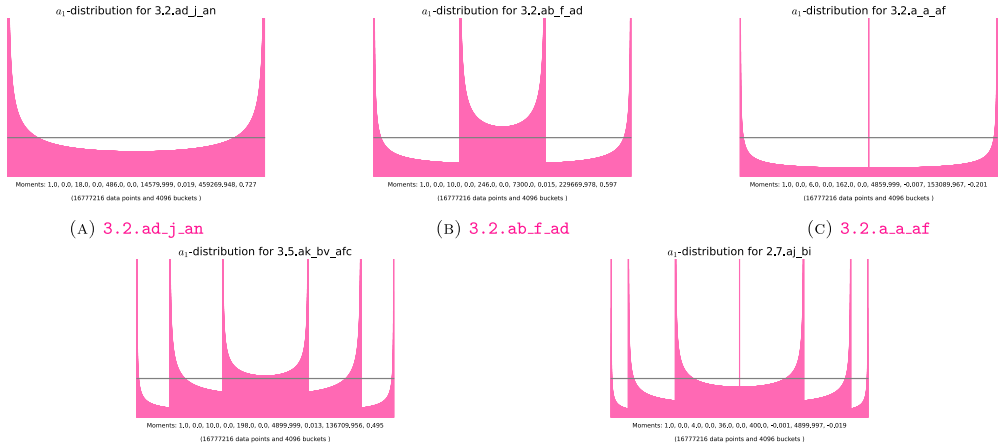
The Frobenius polynomial of X is the product of those of S and E. Further, exactly one of the following is true for S: either it is absolutely simple, or it is simple and geometrically isogenous to the power of a single elliptic curve, or it is not simple (see observation after Lemma 5.1.2). The Serre–Frobenius group of X depends on its geometric isogeny decomposition, of which there are the following four possibilities.

(6.3-a) X is geometrically isogenous to E^3.
(6.3-b) X is geometrically isogenous to $E_1^2 \times E$, for some ordinary elliptic curve E_1, with $(E_1)_{\overline{\mathbf{F}}_q} \not\sim (E)_{\overline{\mathbf{F}}_q}$.
(6.3-c) X is geometrically isogenous to $E_1 \times E_2 \times E$, for ordinary and pairwise geometrically non-isogenous elliptic curves E_1, E_2 and E.
(6.3-d) X is geometrically isogenous to $S \times E$ for an absolutely simple ordinary surface S and an ordinary elliptic curve E.

Lemma 6.3.1. (Node X-C in Figure 7). Let X be a non-simple ordinary abelian threefold over $\mathbf{F}_q$. The possible Serre–Frobenius groups of X are given in Table 9.

Proof. Recall that $X \sim S \times E$ over $\mathbf{F}_q$. (6.3-a) If X is geometrically isogenous to E^3, then S is geometrically isogenous to E^2. By Lemma 3.1.4 SF$(X) \cong \mathrm{U}(1) \times C_m$, where m is the splitting degree of S, and so $S_{(m)} \sim E^2$. By [14, Theorem 6], we have that $m \in \{1, 2, 3, 4, 6\}$. (6.3-b) In this case, by Lemma 3.1.4, SF$(X) \cong \mathrm{U}(1)^2 \times C_m$, where m is the splitting degree of S and $S_{(m)} \sim E_1^2$. As in the previous case, $m \in \{1, 2, 3, 4, 6\}$. (6.3-c) In this case $S \sim E_1 \times E_2$ over the base field. Lemma 3.1.1 implies $\delta_X = 3$. (6.3-d) In this case, $X \sim S \times E$ with S absolutely simple. By [40, Theorem 1.1], we know that X is neat. Since X is ordinary and S is simple, all Frobenius eigenvalues are distinct and not supersingular. By Remark (3.3.2.b), we conclude that $\delta_X = 3$. ■

Example 6.3.2. (Non-simple ordinary threefolds of splitting type (6.3-a)).

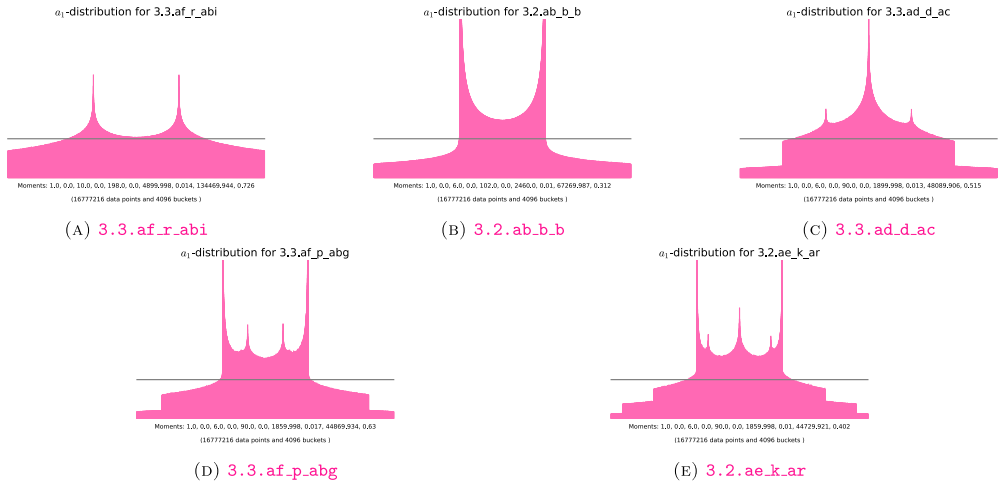


(A) 3.2.ad_j_an (B) 3.2.ab_f_ad (C) 3.2.a_a_af

(D) 3.5.ak_bv_afc (E) 3.7.ao_di_alk

Fig. 9. a_1-distributions for non-simple ordinary abelian threefolds of splitting type (6.3-a).

Example 6.3.3. (Non-simple ordinary threefolds of splitting type (6.3-b)).



(A) 3.3.af_r_abi (B) 3.2.ab_b_b (C) 3.3.ad_d_ac

(D) 3.3.af_p_abg (E) 3.2.ae_k_ar

Fig. 10. a_1-distributions for non-simple ordinary abelian threefolds of splitting type (6.3-b).

6.4 Simple almost ordinary threefolds

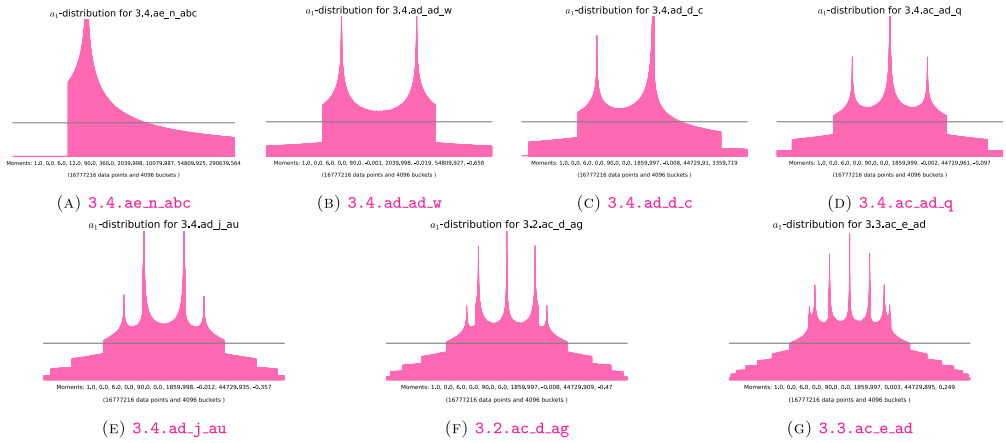
Let X be a simple and almost ordinary abelian threefold over $\mathbf{F}_q$. Recall that X is in fact absolutely simple, so that the Frobenius polynomial $P_{(r)}(T)$ is irreducible for every positive integer r.

Lemma 6.4.1. (Node X-D in Figure 7). Let X be a simple almost ordinary abelian threefold over $\mathbf{F}_q$. The Serre–Frobenius group of X can be read from Table 10.

Proof. Let $m := m_X$ be the torsion order of U_X, and consider the base extension $Y := X_{(m)}$. By [16, Theorem 5.7], we know that $\delta_X = \delta_Y \geq 2$. Furthermore, since Y is absolutely simple, by the discussion in Section 6.1, the roots of $P_Y(T) = P_{(m)}(T)$ are distinct and non-supersingular. If Y is neat, Remark (3.3.2.b) implies that $\delta_X = \delta_Y = 3$. Assume then that Y is not neat, so that $\delta_X = 2$. Let $\boldsymbol{\alpha} = \boldsymbol{\alpha}_1$ be a Frobenius eigenvalue of X. By [40, Theorem 1.1] and the discussion thereafter, we have that the sextic CM-field $\mathbf{Q}(\boldsymbol{\alpha}) = \mathbf{Q}(\alpha^m)$ contains

Table 10. Serre–Frobenius groups of simple almost ordinary threefolds.

Def. 3.3.1	$\sqrt{q} \in \mathbf{Q}(\pi_X)$	$\cong$ class	Generator	$m \in M$	Example
Neat	-	$U(1)^3$	(u_1, u_2, u_3)	$\{1\}$	3.2.ab_ab_c
Not neat	Yes	$U(1)^2 \times C_m$	$(u_1, u_2, \zeta_m u_1 u_2)$	$\{1, 2, 3, 4, 6\}$	Example 6.4.2
Not neat	No	$U(1)^2 \times C_m$	$(u_1, u_2, \zeta_m u_1 u_2)$	$\{4, 6, 8, 12\}$	Example 6.4.2



(A) 3.4.ae_n_abc (B) 3.4.ad_ad_w (C) 3.4.ad_d_c (D) 3.4.ac_ad_q

(E) 3.4.ad_j_au (F) 3.2.ac_d_ag (G) 3.3.ac_e_ad

Fig. 11. a_1-distributions of simple almost ordinary abelian threefolds of angle rank 2.

an imaginary quadratic field B, and $(u_1u_2u_3)^{2m} = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1^{2m}) = 1$. Further, $\mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(\alpha_1) = \alpha_1\alpha_2\alpha_3$. Since U_Y has no torsion, this implies that $(u_1u_2u_3)^m = 1$. Moreover, this means that $u_1u_2u_3 = \zeta$ for some primitive m-th root of unity ζ. (The primitivity of ζ follows from the fact that m is the minimal positive integer such that $U_Y = U_{(m)}$ is torsion free.) Therefore,

$$\zeta^2 = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1^2) \in B. \tag{15}$$

If m is odd, ζ^2 is also primitive, so that $\varphi(m) \leq 2$ and $m \in \{1, 3\}$. If m is even, then we may distinguish between two cases. If $\sqrt{q} \in \mathbf{Q}(\alpha)$, we know that $u_1 \in \mathbf{Q}(\alpha)$ so that in fact $\pm\zeta = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1) \in B$ and $\varphi(m) \leq 2$ implies that $m \in \{2, 4, 6\}$. If $\sqrt{q} \notin \mathbf{Q}(\alpha)$, then ζ^2 is a primitive $m/2$-root of unity and $m/2 \in \{1, 2, 3, 4, 6\}$.

In the setting where Y is not neat and $\sqrt{q} \notin \mathbf{Q}(\alpha)$, we notice that $u_1u_2u_3 = \pm 1$ implies that $\sqrt{q} = \pm\alpha_1\alpha_2\alpha_3/q \in \mathbf{Q}(\alpha)$, so the cases $m = 1, 2$ don't occur when $\sqrt{q} \notin \mathbf{Q}(\alpha)$. Similarly, if $u_1u_2u_3 = \zeta_3$, then $\sqrt{q} = (\alpha_1\alpha_2\alpha_3)^3/q^4 \in \mathbf{Q}(\alpha)$. Thus, the torsion orders $m = 1, 2, 3$ do not occur in this case. ■

Example 6.4.2. (a_1-distributions of simple almost ordinary abelian threefolds with angle rank 2). The histograms corresponding to the following examples are presented in Figure 11. In these examples we use SageMath [25] to initialize the degree-6 number field $K = \mathbf{Q}(\alpha)$ corresponding to the Frobenius polynomial, find the corresponding quadratic subfield B, and check that $\mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1)$ is the root of unity in question. The code for generating the histograms is available on the GitHub repository [2].

6.5 Non-simple almost ordinary threefolds

Since X is not simple, we have that $X \sim S \times E$ for some surface S and some elliptic curve E. For this section, we let $\pi_1, \overline{\pi}_1, \pi_2, \overline{\pi}_2$ and $\alpha, \overline{\alpha}$ be the Frobenius eigenvalues of S and E respectively. The normalized eigenvalues will be denoted by $u_1 := \pi_1/\sqrt{q}, u_2 = \pi_2/\sqrt{q}$ and $u := \alpha/\sqrt{q}$. If X has a geometric supersingular factor, by Honda–Tate theory, it must have a supersingular factor over the base field; and without loss of generality we may assume that this factor is E.

Table 11. Serre–Frobenius groups of non-simple almost ordinary threefolds $X = S \times E$.

δ_E	$\cong$ **class**	**Generator**	$d = \log_p(q)$	$m \in M(p,d)$	**Example**
1	$U(1)^3$	(u_1, u_2, u_3)	-	$\{1\}$	3.3.ac_d_ae
0	$U(1)^2 \times C_m$	(u_1, u_2, ζ_{m_E})	-	$m = m_E \in \{1,2,3,4,6,8,12\}$	Figure 13
0	$U(1) \times C_m$	$(u_1, \zeta_{m_S} u_1, \zeta_{m_E})$	even	$m = \mathrm{lcm}(m_S, m_E) \in \{1,2,3,4,6,12\}$	Figure 14
0	$U(1) \times C_m$	$(u_1, \zeta_{m_S} u_1, \zeta_{m_E})$	odd	$m = \mathrm{lcm}(m_S, m_E) \in \{4,8,12,24\}$	Figure 14

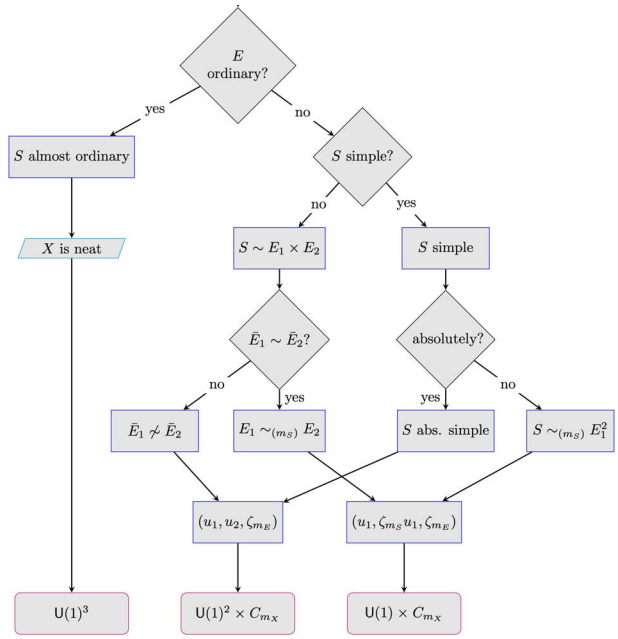


Fig. 12. Serre–Frobenius groups of non-simple almost ordinary threefolds.

Lemma 6.5.1. (Node X-E in Figure 7). Let $X \sim S \times E$ be a non-simple almost ordinary abelian threefold over $\mathbf{F}_q$. The Serre–Frobenius group of X can be read from Flowchart 12. In particular, if X has no supersingular factor, then $\delta_X = 3$. If E is supersingular, then $\delta_X \in \{1,2\}$ and $m_X = \mathrm{lcm}(m_S, m_E)$. The list of possible torsion orders m_X in this case is given Table 11.

Proof. First, suppose that X has no supersingular factor. Thus E is ordinary and S is almost ordinary and absolutely simple. This implies that $\mathbf{Q}(\pi_1^r)$ and $\mathbf{Q}(\alpha^r)$ are CM-fields of degrees 4 and 2, respectively, for every positive integer r. In particular, $\#\left\{\pi_1^r, \overline{\pi}_1^r, \pi_2^r, \overline{\pi}_2^r, \alpha^r, \overline{\alpha}^r\right\} = 6$ for every r. Let $m = m_X$ and consider the base extension $X_{(m)}$. Since $X_{(m)}$ is not simple, [40, Theorem 1.1] implies that $X_{(m)}$ is neat. The eigenvalues of $X_{(m)}$ are all distinct and not supersingular, so that $\delta(X) = \delta(X_{(m)}) = 3$ by Remark (3.3.2.b). The case where X has a supersingular factor follows from Lemma 3.1.3. ∎

6.6 Abelian threefolds of K3-type

In this section X will be an abelian threefold defined over $\mathbf{F}_q$ of p-rank 1. The q-Newton polygon of such a variety has slopes $(0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1)$. This is the three-dimensional instance of abelian varieties of K3 type, which were studied by Zarhin in [39] and [38].

Definition 6.6.1. An abelian variety A defined over $\mathbf{F}_q$ is said to be of **K3-type** if the set of Newton slopes is either $\{0,1\}$ or $\{0,1/2,1\}$, and the segments of slope 0 and 1 have length one.

By [38, Theorem 5.9], simple abelian varieties of K3-type have maximal angle rank. As a corollary, we have another piece of the classification.

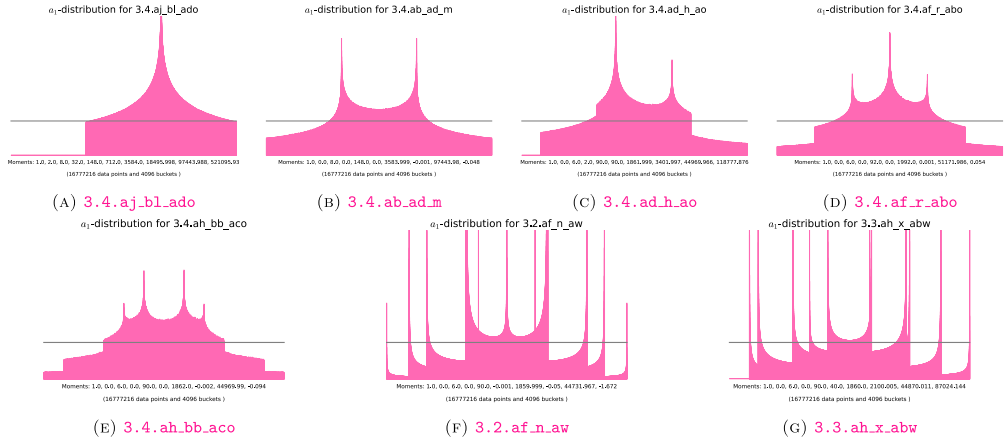


Fig. 13. a_1-distributions of non-simple almost ordinary abelian threefolds of angle rank 2.

Table 12. Serre–Frobenius groups of abelian threefolds of p-rank 1.

Splitting type	$\cong$ class	Generator	$m \in M$	Example
Absolutely simple	$\mathrm{U}(1)^3$	(u_1, u_2, u_3)	$\{1\}$	3.2.ab_a_a
(6.3-a)	$\mathrm{U}(1)^2 \times C_m$	(u_1, u_2, ζ_{m_E})	$m = m_E \in \{1, 2, 3, 4, 6, 8, 12\}$	-
(6.3-b)	$\mathrm{U}(1) \times C_m$	$(u_1, \zeta_{m_1}, \zeta_{m_2})$	$m = \mathrm{lcm}(m_1, m_2)$ in Table 7	-
(6.3-c)	$\mathrm{U}(1) \times C_m$	$(u_1, \zeta_{m_1}, \zeta_{m_2})$	$m = \mathrm{lcm}(m_1, m_2) \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 24\}$	Figure 15

Lemma 6.6.2. (Node X-F in Figure 7). Let X be a simple abelian threefold over $\mathbf{F}_q$ of p-rank 1. Then X has maximal angle rank and $\mathrm{SF}(X) \cong \mathrm{U}(1)^3$.

There are several examples of such X, one of them being 3.2.ab_a_a. Now assume that X is not simple, so that $X \sim S \times E$ for some surface S and elliptic curve E.

Lemma 6.6.3. (Node X-G in Figure 7). Let $X \sim S \times E$ be a non-simple abelian threefold over $\mathbf{F}_q$ of p-rank 1. The Serre–Frobenius group of X is given by Table 12.

We consider three cases:

(6.6.3-a) S is simple and almost ordinary, and E is supersingular.
(6.6.3-b) S is non-simple and almost ordinary, and E is supersingular.
(6.6.3-c) S is supersingular and E is ordinary.

Proof. As in Section 6.3, we let $\pi_1, \overline{\pi}_1, \pi_2, \overline{\pi}_2$ and $\alpha, \overline{\alpha}$ be the Frobenius eigenvalues of S and E respectively. Denote the normalized eigenvalues by $u_1 := \pi_1/\sqrt{q}, u_2 := \pi_2/\sqrt{q}$ and $u := \alpha/\sqrt{q}$.

Suppose first that X is of type (6.6.3-a). By Lemma 5.3.1, the set $\{u_1, u_2\}$ is multiplicatively independent. Since u is a root of unity, $U_X = \langle u_1, u_2, u\rangle = U_S \oplus U_E \cong \mathbf{Z}^2 \oplus C_m$ for $m \in M = \{1, 2, 3, 4, 6, 8, 12\}$ the set of possible torsion orders for supersingular elliptic curves. Thus, in this case, $\mathrm{SF}(X) \cong \mathrm{U}(1)^2 \times C_m$ and is generated by (u_1, u_2, ζ_m).

If X is of type (6.6.3-b), then $S \sim E_1 \times E_2$ with E_1 ordinary and E_2 supersingular. By Lemma 3.1.3, $\mathrm{SF}(X) \cong \mathrm{U}(1) \times C_m$, with m in the set of possible torsion orders of non-simple supersingular surfaces.

If X is of type (6.6.3-c), we have $U_X = U_E \oplus U_S \cong \mathbf{Z} \oplus C_m$ for m in the set $M = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 24\}$ of possible torsion orders of supersingular surfaces from Lemma 5.5.1 and Lemma 5.6.1. ■

The following examples are all of splitting type (6.6.3-c), since this splitting type contains all the new Serre–Frobenius groups appearing in Table 12. The histograms corresponding to these examples are presented in Figure 15.

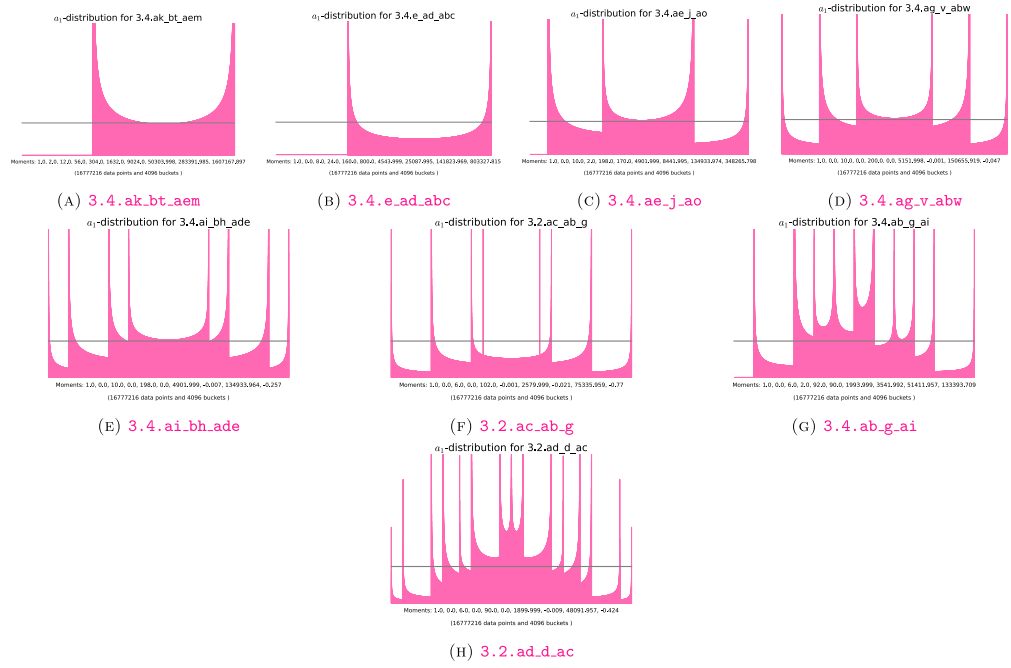


Fig. 14. a_1-distributions of non-simple almost ordinary abelian threefolds of angle rank 1.

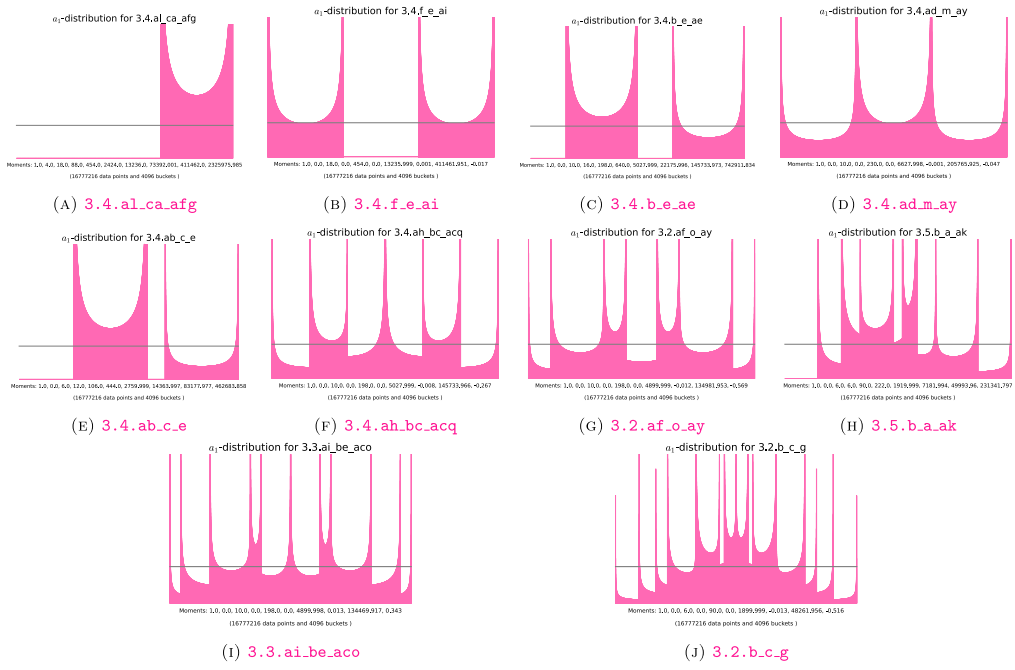


Fig. 15. a_1-distributions of p-rank 1 threefolds with angle rank 1

6.7 Absolutely simple p-rank 0 threefolds

In this section, X will be a non-supersingular p-rank 0 abelian threefold over $\mathbf{F}_q$. Since the q-Newton polygon of the Frobenius polynomial $P(T) = P_X(T)$ has slopes $\frac{1}{3}$ and $\frac{2}{3}$, each with multiplicity three, it follows that X is absolutely simple, since the slope 1/3 does not occur for abelian varieties of smaller dimension. Let e_r^2 denote the dimension of $\mathrm{End}^0(X_{(r)})$ over its center. We consider two cases:

Table 13. Serre–Frobenius groups of absolutely simple abelian threefolds of p-rank 0.

Case	$q = p^d$	$\cong$ class	Generator	$m \in M$
(6.7-a)	$3 \mid m_X \cdot d$	$\mathrm{U}(1) \times C_m$	$(u_1, \zeta_m u_1, \zeta_m^v u_1)$	$\{1, 3, 7\}$
(6.7-b)	-	$\mathrm{U}(1)^3$	(u_1, u_2, u_3)	$\{1\}$

(6.7-a) There exists $r \geq 1$ such that $e_r = 3$. In this case we have $P_{(r)}(T) = h_{(r)}(T)^3$ and $h_{(r)}(T)$ is as in Theorem 6.1.1, so that 3 divides $r \cdot \log_p(q)$.
(6.7-a) $e_r = 1$ for every positive integer r.

Lemma 6.7.1. (Node X-H in Figure 7). Let X be an absolutely simple abelian threefold of p-rank 0 defined over $\mathbf{F}_q$. Then, the Serre–Frobenius group of X is classified according to Table 13. Furthermore, X is of type (6.7-a), m_X is the smallest positive integer r such that $e_r = 3$.

Remark 6.7.2. The techniques for proving the Generalized Lenstra–Zarhin result in [8, Theorem 1.5], cannot be applied to this case. Thus, even the angle rank analysis in this case is particularly interesting.

Proof. Suppose first that X is of type (6.7-a), and let m be the minimal positive integer such that $e_m = 3$. Maintaining previous notation, $P_{(m)}(T) = h_{(m)}(T)^3$ implies that $\alpha_2 = \zeta \cdot \alpha_1$ and $\alpha_3 = \xi \cdot \alpha_1$ for m-th roots of unity ζ and ξ, whose orders have lcm m. By Lemma 2.3.2, this implies that $\mathrm{SF}(X) \cong \mathrm{U}(1) \times C_m$. We conclude that $\delta_X = 1$ and $m = m_X$. To calculate the set M of possible torsion orders, assume that $m_X = m > 1$. Then $\mathbf{Q}(\alpha_1^m)$ is a quadratic imaginary subextension of $\mathbf{Q}(\alpha_1) \supset \mathbf{Q}$, and we can argue as in the proof of Theorem 3.2.1 (with $\ell = 3$) to conclude that $m \in \{3, 7\}$.

Assume now that X is of type (6.7-b). This implies that $\mathbf{Q}(\alpha_1^r)$ is a degree 6 CM-field for every positive integer r. If $m := m_X$, the base extension $X_{(m)}$ is neat and the Frobenius eigenvalues are distinct and not supersingular. By Remark (3.3.2.b) we have that $\delta_X = 3$ and $m = 1$. ■

Example 6.7.3. (a_1-distribution for p-rank 0 non-supersingular threefolds of splitting type (6.7-a)). The histograms corresponding to these examples are presented in Figure 16. Note that the first one already showed up in Figure 9, while the other ones appeared in Figure 8.

(A) ($m = 1$) The isogeny class 3.8.ag_bk_aea satisfies $m_X = 1$. Note that 3 divides $m_X \cdot \log_2(8)$.
(B) ($m = 3$) The isogeny class 3.2.a_a_ac has angle rank 1 and irreducible Frobenius polynomial $P(T) = T^6 - 2T^3 + 8$. The cubic base extension gives the isogeny class 3.8.ag_bk_aea with reducible Frobenius polynomial $P_{(3)}(T) = (T^6 - 2T^3 + 8)^3$. Note that 3 divides $m_X \cdot \log_2(2)$.
(C) ($m = 7$) The isogeny class 3.8.ai_bk_aeq has angle rank 1 and irreducible Frobenius polynomial $P(T) = T^6 - 8T^5 + 36T^4 - 120T^3 + 288T^2 - 512T + 512$. Its base change over a degree $m_X = 7$ extension is the isogeny class `3.2097152.ahka_bfyoxc_adesazpwa` with Frobenius polynomial

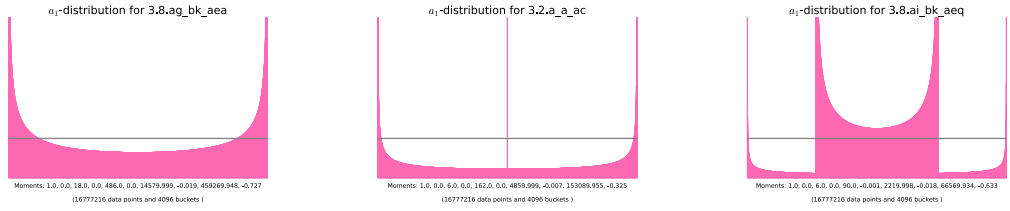
$$P_{(7)}(T) = (T^2 - 1664T + 2097152)^3.$$

In this example, $q = 8$, so that 3 divides $m_X \cdot \log_2(8)$.

6.8 Simple supersingular threefolds

Nart and Ritzenthaler [21] showed that the only degree 6 supersingular q-Weil numbers are the conjugates of

$$\pm\sqrt{q}\zeta_7, \pm\sqrt{q}\zeta_9, \quad \text{when } q \text{ is a square, and}$$
$$7^{d/2}\zeta_{28}, 3^{d/2}\zeta_{36}, \quad \text{when } q \text{ is not a square.}$$



(A) 3.8.ag_bk_aea (B) 3.2.a_a_ac (C) 3.8.ai_bk_aeq

Fig. 16. a_1-distribution for p-rank 0 non-supersingular threefolds of splitting type (6.7-a).

Table 14. Serre–Frobenius groups of simple supersingular threefolds.

(a_1, a_2, a_3)	p	d	**Type**	$\tilde{h}(T)$	**SF**(X)	**Example**
$(\sqrt{q}, q, q\sqrt{q})$	$7 \nmid (p^3-1)$	even	Z-1	$\Phi_7(T)$	C_7	3.9.d_j_bb
$(-\sqrt{q}, q, -q\sqrt{q})$	$7 \nmid (p^3-1)$	even	Z-1	$\Phi_{14}(T)$	C_{14}	3.9.ad_j_abb
$(0, 0, q\sqrt{q})$	$\not\equiv 1 \bmod 3$	even	Z-1	$\Phi_9(T)$	C_9	3.4.a_a_i
$(0, 0, -q\sqrt{q})$	$\not\equiv 1 \bmod 3$	even	Z-1	$\Phi_{18}(T)$	C_{18}	3.4.a_a_ai
$(\sqrt{7q}, 3q, q\sqrt{7q})$	$= 7$	odd	Z-3	$h_{7,1}(T)$	C_{28}	3.7.h_v_bx
$(-\sqrt{7q}, 3q, -q\sqrt{7q})$	$= 7$	odd	Z-3	$h_{7,1}(-T)$	C_{28}	3.7.ah_v_abx
$(0, 0, q\sqrt{3q})$	$= 3$	odd	Z-3	$h_{3,3}(T)$	C_{36}	3.3.a_a_j
$(0, 0, -q\sqrt{3q})$	$= 3$	odd	Z-3	$h_{3,3}(-T)$	C_{36}	3.3.a_a_aj

Building on their work, Haloui [12, Proposition 1.5] completed the classification of simple supersingular threefolds. This classification is also discussed in [29]; and we adapt their notation for the polynomials of Z-3 type. Denoting by (a_1, a_2, a_3) the isogeny class of abelian threefolds over $\mathbf{F}_q$ with Frobenius polynomial $P_X(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + qa_2T^2 + q^2a_1T + q^3$, the following lemma gives the classification of Serre–Frobenius groups of simple supersingular threefolds, which is a corollary of Haloui's result.

Lemma 6.8.1. (Node X-I in Figure 7). Let X be a simple supersingular abelian threefold defined over $\mathbf{F}_q$. The Serre–Frobenius group of X is classified according to Table 14.

Proof. By Theorem 6.1.1 and the discussion following it, we know that the Frobenius polynomial of every supersingular threefold $P_X(T)$, coincides with the minimal polynomial $h_X(T)$ with $e = 1$ in some row of the table. The first four rows of Table 14 correspond to isogeny classes of type (Z-1). By the discussion in Section 3.4, the minimal polynomials are of the form $\Phi_m^{[\sqrt{q}]}(T)$ and the normalized polynomials are just the usual cyclotomic polynomials $\Phi_m(T)$. (Recall that $f^{[a]}(T) := a^{\deg f} f(T/a)$.)

The last four rows of Table 14 correspond to isogeny classes of type (Z-3). The normalized Frobenius polynomials are $h_{7,1}(\pm T) = T^6 \pm \sqrt{7}T^5 + 3T^4 \pm \sqrt{7}T^3 + 3T^2 \pm \sqrt{7}T + 1$, and $h_{3,3}(\pm T) = T^6 \pm \sqrt{3}T^3 + 1$. Noting that $h_{7,1}(T)h_{7,1}(-T) = \Phi_{28}(T)$ and $h_{3,3}(T)h_{3,3}(-T) = \Phi_{36}(T)$ we conclude that the unit groups U_X are generated by ζ_{28} and ζ_{36}, respectively. ∎

6.9 Non-simple supersingular threefolds

If X is a non-simple supersingular abelian threefold over $\mathbf{F}_q$, then there are two cases:

(6.9.0-a) $X \sim S \times E$, with S a simple supersingular surface over $\mathbf{F}_q$ and E a supersingular elliptic curve.
(6.9.0-b) $X \sim E_1 \times E_2 \times E_3$, where each E_i is a supersingular elliptic curve.

The classification of the Serre–Frobenius group in these cases can be summarized in the following lemma.

Lemma 6.9.1. (Node X-J in Figure 7). If X is a non-simple supersingular abelian threefold as in (6.9.0-a), then $\mathrm{SF}(X) \cong C_m$, for $m \in M(p, d)$, where

- if d is even, $M(p, d) = \{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30\}$, and
- if d is odd, $M(p, d) = \{4, 8, 12, 20, 24\}$.

Proof. In this case, $m = \mathbf{lcm}(m_S, m_E)$, since this is the degree of the smallest extension over which the Serre–Frobenius group becomes connected. The list of values for m_E and m_S come from Tables 2 and 6. ■

Lemma 6.9.2. (Node X-J in Figure 7). If X is a non-simple supersingular abelian threefold as in (6.9.0-b), then $\mathrm{SF}(X) \cong C_m$, for $m \in M(p, d)$, where

- if d is even, $M(p, d) = \{1, 2, 3, 4, 6, 12\}$; and
- if d is odd, $M(p, d) = \{4, 8, 12\}$.

Proof. We know that m is the degree of the extension over which all the elliptic curve factors E_i become isogenous. This is precisely the least common multiple of the m_{E_i}'s. From Table 2, we can calculate the various possibilities for the $\mathbf{lcm}$'s depending on the parity of d. ■

Acknowledgments

We would like to thank David Zureick-Brown, Kiran Kedlaya, Francesc Fité, Brandon Alberts, Edgar Costa, and Andrew Sutherland for useful conversations about this paper. We thank Yuri Zarhin for providing us with useful references, and Hendrik Lenstra for pointing out one of the missing cases in Section 4. We would also like to thank Everett Howe for helping us with a missing piece of the puzzle in Theorem 3.2.1. This project started as part of the Rethinking Number Theory workshop in 2021. We thank the organizers of the workshop for giving us the opportunity and space to collaborate, and the funding sources for the workshop: AIM, the Number Theory Foundation, and the University of Wisconsin-Eau Claire Department of Mathematics. We are also grateful to Rachel Pries for her guidance at the beginning of the workshop, which helped launch this project. Finally, we thank the anonymous referee for the elucidating and pertinent suggestions that improved the exposition and results in the paper.

References

1. Ahmadi, O. and I. E. Shparlinski. "On the distribution of the number of points on algebraic curves in extensions of finite fields." *Math. Res. Lett.* **17**, no. 4 (2010): 689–99. https://doi.org/10.4310/MRL.2010.v17.n4.a9.
2. Arango-Piñeros, S., D. Bhamidipati, and S. Sankar. "Code accompanying Frobenius distributions of abelian varieties over finite fields". https://github.com/sarangop1728/Frobenius-distributions-AVs-Fq.
3. Chai, C.-L., B. Conrad, and F. Oort. "Complex multiplication and lifting problems." *Volume 195 of Mathematical Surveys and Monographs*. Providence, RI: American Mathematical Society, 2014.
4. Chi, W. C. "ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields." *Amer. J. Math.* **114**, no. 2 (1992): 315–53. https://doi.org/10.2307/2374706.
5. Deuring, M. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper." *Abh. Math. Sem. Hansischen Univ.* **14** (1941): 197–272. https://doi.org/10.1007/BF02940746.
6. Diem, C. and N. Naumann. "On the structure of Weil restrictions of abelian varieties." *J. Ramanujan Math. Soc.* **18**, no. 2 (2003): 153–74.
7. Dupuy, T., K. Kedlaya, D. Roe, and C. Vincent. "Isogeny classes of abelian varieties over finite fields in the LMFDB." *Arithmetic Geometry, Number Theory, and Computation, Simons Symp.*, 375–448. Cham: Springer, 2021.
8. Dupuy, T., K. S. Kedlaya, and D. Zureick-Brown. "Angle ranks of abelian varieties." *Math. Ann.* **389** (2024): 169–85. https://doi.org/10.1007/s00208-023-02633-7.
9. Fité. F., K. S. Kedlaya, and A. V. Sutherland. *Sato-Tate Groups of Abelian Threefolds*, 2023.
10. Fité, F. "Equidistribution, L-functions, and Sato-Tate groups." *Trends in Number Theory, volume 649 of Contemp. Math.* 63–88. Providence, RI: Amer. Math. Soc., 2015.
11. Fité, F., K. S. Kedlaya, V. Rotger, and A. V. Sutherland. "Sato-Tate distributions and Galois endomorphism modules in genus 2." *Compos. Math.* **148**, no. 5 (2012): 1390–442. https://doi.org/10.1112/S0010437X12000279.
12. Haloui, S. "The characteristic polynomials of abelian varieties of dimensions 3 over finite fields." *J. Number Theory* **130**, no. 12 (2010): 2745–52. https://doi.org/10.1016/j.jnt.2010.06.008.

13. Honda, T. "Isogeny classes of abelian varieties over finite fields." *J. Math. Soc. Japan* **20** (1968): 83–95. https://doi.org/10.2969/jmsj/02010083.
14. Howe, E. W. and H. J. Zhu. "On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field." *J. Number Theory* **92**, no. 1 (2002): 139–63. https://doi.org/10.1006/jnth.2001.2697.
15. Krajíček, J. and T. Scanlon. "Combinatorics with definable sets: Euler characteristics and Grothendieck rings." *Bull. Symbolic Logic* **6**, no. 3 (2000): 311–30. https://doi.org/10.2307/421058.
16. Lenstra, H., W., Jr., and Y. G. Zarhin. "The Tate conjecture for almost ordinary abelian varieties over finite fields." *Advances in Number Theory (Kingston, ON, 1991)*, *Oxford Sci. Publ.*, 179–94. New York: Oxford University Press, 1993.
17. The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 15 March 2024].
18. Maisner, D. and E. Nart. "Abelian surfaces over finite fields as Jacobians." *Exp. Math.* **11**, no. 3 (2002. With an appendix by Everett W. Howe): 321–37. https://doi.org/10.1080/10586458.2002.10504478.
19. Milne, J. S. "Algebraic groups." *Volume 170 of Cambridge Studies in Advanced Mathematics*. Cambridge: Cambridge University Press, 2017. The theory of group schemes of finite type over a field.
20. Morris, S., A. "Pontryagin duality and the structure of locally compact abelian groups." *London Mathematical Society Lecture Note Series, No. 29*. Cambridge-New York-Melbourne: Cambridge University Press, 1977.
21. Nart, E. and C. Ritzenthaler. "Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2." *Finite Fields Appl.* **14**, no. 3 (2008): 676–702. https://doi.org/10.1016/j.ffa.2007.09.006.
22. Oort, F. "Abelian varieties over finite fields." *Higher-Dimensional Geometry Over Finite Fields. Volume 16 of NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, 123–88. Amsterdam: IOS, 2008.
23. Pontrjagin, L. "The theory of topological commutative groups." *Ann. of Math. (2)* **35**, no. 2 (1934): 361–88.
24. Ruőck, H.-G. "Abelian surfaces and Jacobian varieties over finite fields." *Compos. Math.* **76**, no. 3 (1990): 351–66.
25. The Sage Developers. *Sagemath, the Sage Mathematics Software System (Version 9.5)*, 2024. https://www.sagemath.org.
26. Serre, J.-P. "Abelian ℓ-adic representations and elliptic curves." *Volume 7 of Research Notes in Mathematics*. Wellesley, MA: A K Peters, Ltd, 1998. With the collaboration of Willem Kuyk and John Labute. Revised reprint of the 1968 original.
27. Serre, J.-P. Oeuvres/Collected papers. IV. 1985–1998. *Springer Collected Works in Mathematics*. Springer, Heidelberg, 2013. Repri nt of the 2000 edition [MR1730973].
28. Serre, J.-P. Rational points on curves over finite fields, *volume 18 of Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, [2020] [INSERT FX]2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler.
29. Singh, V., G. McGuire, and A. Zaytsev. "Classification of characteristic polynomials of simple supersingular abelian varieties over finite fields." *Funct. Approx. Comment. Math.* **51**, no. 2 (2014): 415–36.
30. Sutherland, A. V. "Sato-Tate distributions." *Analytic Methods in Arithmetic Geometry, volume 740 of Contemp. Math.*, 197–248. Providence, RI: Amer. Math. Soc, 2019 [INSERT FX]2019.
31. Tate, J. "Endomorphisms of abelian varieties over finite fields." *Invent. Math.* **2** (1966): 134–44. https://doi.org/10.1007/BF01404549.
32. Tate, J. "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)." *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, volume 175 of Lecture Notes in Math., pages Exp. No. 352*. 95–110. Berlin: Springer, 1971.
33. Waterhouse, W. C. "Abelian varieties over finite fields." *Ann. Sci. École Norm. Sup.* **2**, no. 2 (1969): 521–60. https://doi.org/10.24033/asens.1183.
34. Weil, A. "Numbers of solutions of equations in finite fields." *Bull. Amer. Math. Soc.* **55** (1949): 497–508. https://doi.org/10.1090/S0002-9904-1949-09219-4.
35. Xing, C. "The characteristic polynomials of abelian varieties of dimensions three and four over finite fields." *Sci. China Ser. A* **37**, no. 2 (1994): 147–50.
36. Xing, C. "On supersingular abelian varieties of dimension two over finite fields." *Finite Fields Appl.* **2**, no. 4 (1996): 407–21. https://doi.org/10.1006/ffta.1996.0024.
37. Zarhin, Y. G. "The Tate conjecture for nonsimple abelian varieties over finite fields." *Algebra and Number Theory (Essen, 1992)*, 267–96. Berlin: de Gruyter, 1994.
38. Zarhin, Y. G. "Abelian varieties of K3 type and ℓ-adic representations." *Algebraic Geometry and Analytic Geometry (Tokyo, 1990)*, *ICM-90 Satell. Conf. Proc.* 231–55. Tokyo: Springer, 1991.

39. Zarhin, Y. G. "Abelian varieties of K3 type. In Séminaire de Théorie des Nombres, Paris, 1990–91." *Volume 108 of Progr. Math.*, 263–79. Boston, MA: Birkhäuser Boston, 1993.
40. Zarhin, Y. G. "Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension." *J. Pure Appl. Algebra* **219**, no. 6 (2015): 2076–98. https://doi.org/10.1016/j.jpaa.2014.07.024.
41. Zhu, H. J. "Supersingular abelian varieties over finite fields." *J. Number Theory* **86**, no. 1 (2001): 61–77. https://doi.org/10.1006/jnth.2000.2562.
42. Zywina, D. "Determining monodromy groups of abelian varieties." *Res. Number Theory* **8**, no. 4 (2022). Paper No. 89, 53