

ON THE DISTRIBUTION OF ORDERS OF FROBENIUS ACTION ON ℓ -TORSION OF ABELIAN SURFACES¹

N. S. Kolesnikov, S. A. Novoselov

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

E-mail: nikolesnikov1@kantiana.ru, snovoselov@kantiana.ru

The computation of the order of Frobenius action on the ℓ -torsion is a part of Schoof — Elkies — Atkin algorithm for point counting on an elliptic curve E over a finite field \mathbb{F}_q . The idea of Schoof's algorithm is to compute the trace of Frobenius t modulo primes ℓ and restore it by the Chinese remainder theorem. Atkin's improvement consists of computing the order r of the Frobenius action on $E[\ell]$ and of restricting the number $t \pmod{\ell}$ to enumerate by using the formula $t^2 \equiv q(\zeta + \zeta^{-1})^2 \pmod{\ell}$. Here ζ is a primitive r -th root of unity. In this paper, we generalize Atkin's formula to the general case of abelian variety of dimension g . Classically, finding of the order r involves expensive computation of modular polynomials. We study the distribution of the Frobenius orders in case of abelian surfaces and $q \equiv 1 \pmod{\ell}$ in order to replace these expensive computations by probabilistic algorithms.

Keywords: *abelian varieties, finite fields, Frobenius action, ℓ -torsion.*

1. Introduction

The computation of the Frobenius order and its usage for counting points on elliptic curves is a part of Atkin's contribution to Schoof — Elkies — Atkin (SEA) algorithm [1; 2, § 17.2.2].

An elliptic curve E over a finite field \mathbb{F}_q of characteristic $p \neq 2, 3$ is a non-singular curve defined by equation

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{F}_q$. For background on arithmetic of elliptic curves, we refer the reader to [2, § 13; 3]. Here, we briefly summarize the most important facts and notations. We denote by $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ a set of points on the curve E having coordinates in an extension K of \mathbb{F}_q together with a point at infinity \mathcal{O} . It is a well-known fact that the set of all points on the elliptic curve has a group structure. Let $\ell \neq p$ be a prime number. A point P on the curve E is called an ℓ -torsion point if the order of P divides ℓ . The set of ℓ -torsion points on the curve E with coordinates in algebraic closure of the field \mathbb{F}_q forms a group denoted by $E[\ell] = \{P \in E(\overline{\mathbb{F}_q}) : \ell P = \mathcal{O}\}$. The Frobenius endomorphism φ is an endomorphism of E given by $(x, y) \mapsto (x^q, y^q)$. Since it is known [3, p. 86] that $E[\ell] \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$, the endomorphism φ acts on $E[\ell]$ as a linear operator on a two-dimensional vector space. Thus, the Frobenius endomorphism on $E[\ell]$ can be represented as an element of $\text{PGL}_2(\mathbb{F}_\ell)$, a projective general linear group of matrices. In this representation the order r of the Frobenius endomorphism φ is the order of the corresponding element in $\text{PGL}_2(\mathbb{F}_\ell)$. With this definition of the order r , the trace of the Frobenius endomorphism t of the elliptic curve satisfies Atkin's formula [1, Prop. 6.2]:

$$t^2 \equiv q(\zeta + \zeta^{-1})^2 \pmod{\ell}, \tag{1}$$

¹The reported study was funded by RFBR according to the research project 18-31-00244.

where ζ is a primitive r -th root of unity. So to determine $t \pmod{\ell}$ in the SEA-algorithm, we only need to enumerate primitive roots ζ instead of enumerating all ℓ possible variants. The computation of r itself in SEA-algorithm is done by using the factorization of modular polynomials.

Further in the paper we consider abelian varieties that are by definition projective varieties equipped with a group law. The elliptic curve E defined above is an abelian variety of dimension 1. Another example of abelian variety is the Jacobian of a hyperelliptic curve. This motivates us not to focus just on elliptic curves. The formula (1) can be generalized to abelian varieties of dimension g greater than 1. The order r in this case is defined as the order of Frobenius endomorphism as an element of $\mathrm{PGL}_{2g}(\mathbb{F}_\ell)$ (see Section 2). If A is an abelian surface ($g = 2$) over a finite field \mathbb{F}_q and a_1, a_2 are coefficients of the characteristic polynomial of Frobenius endomorphism on A , that is

$$\chi_{A,q}(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2,$$

then

$$(a_2 - 2q)^2 = \eta_1 \eta_2 q^2 \pmod{\ell} \quad (2)$$

and

$$a_1^2 = (\sqrt{\eta_1} \pm \sqrt{\eta_2})^2 q \pmod{\ell}, \quad (3)$$

where $\eta_1 = \zeta_1 + \zeta_1^{-1} + 2$, $\eta_2 = \zeta_2 + \zeta_2^{-1} + 2$, and ζ_1, ζ_2 are r -th roots of unity. This formula appears in [4] in a slightly different form and with additional restrictions implying that ζ_1, ζ_2 are primitive. In [5, Prop. 3.14] there is a more restrictive formula for vanilla abelian surfaces with real multiplication. In our work, we give explicit formulae for any abelian variety of dimension g with relaxed restrictions on r -th roots to make it suitable for general case. We also provide simplified versions of our formulae for dimensions 2, 3.

Therefore, if we know the order r , we can reduce the number of coefficients of characteristic polynomial $\pmod{\ell}$ to enumerate in the genus 2 generalization of Schoof's algorithm [6]. However, modular polynomials [7, 8] for the case of dimension $g \geq 2$ are too big to be precomputed and the effective tools for computing them modulo p in general case are currently missing. In this work, we develop a probabilistic approach to point counting and study the distribution of order r in the case of abelian surfaces and $q \equiv 1 \pmod{\ell}$.

Our contribution. We give a generalization of Atkin's formula to abelian varieties of any dimension. Our formulae are explicit and can be efficiently computed. These new formulae allows us to limit the number of possibilities for $\chi_{A,q}(T) \pmod{\ell}$ in case when the order of the Frobenius on $A[\ell]$ is known. Our second contribution concerns the distribution of orders of matrices in the symplectic group $\mathrm{Sp}_4(\mathbb{F}_\ell)$ as elements of $\mathrm{PSp}_4(\mathbb{F}_\ell)$, a projective symplectic group. We obtained closed form expressions for the expected value and variance. Furthermore, we calculated the distribution for first primes $\ell \leq 3571$. We applied these results to obtain a distribution of the Frobenius orders of abelian surfaces over finite field of size $q \equiv 1 \pmod{\ell}$.

The rest of the paper is organized as follows. In Section 2 we briefly give the definition and properties for the matrices of the Frobenius action on $A[\ell]$. Section 3 contains a generalization of Atkin's formulae to any dimension. In Section 4 we give explicit formulae for the orders (up to a scalar) of conjugate classes in $\mathrm{Sp}_4(\mathbb{F}_\ell)$. In Section 5, using the assumption that the Frobenius elements are equidistributed in $\mathrm{Sp}_4(\mathbb{F}_\ell)$, we obtain properties of the Frobenius action distribution: expected order, variance and most common values (modes). In cryptographic applications we need Jacobians of genus $g = 2$ curves with group size at least 256 bit. Point counting on such curves using generalization of the Schoof's

algorithm requires computations modulo all primes $\ell \leq (9g + 3) \log q$ [9]. So in this section, we computed the distribution for $\ell = 3, \dots, 3571$ as required for applications. Section 6 contains experimental results.

A preliminary version of this paper was presented by the authors at SibeCrypt'19 [10].

2. Frobenius action on $A[\ell]$

In this section and further in the paper we will use the following notations:

- A general linear group $\mathrm{GL}_n(\mathbb{F}_\ell)$ is a group of non-degenerate $n \times n$ matrices with elements in \mathbb{F}_ℓ .
- A symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell) = \{M \in \mathbb{F}_\ell^{2g \times 2g} : M\Omega M^T = \Omega\}$, where Ω is a fixed $2g \times 2g$ nonsingular skew-symmetric matrix.
- A general symplectic group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell) = \{M \in \mathbb{F}_\ell^{2g \times 2g} : M\Omega M^T = c \cdot \Omega\}$, for some $c \in \mathbb{F}_\ell$.
- A projective symplectic group $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$ is a group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ modulo scalar matrices.

Let A be an abelian variety of dimension g over a finite field \mathbb{F}_q of characteristic p and $\ell \neq p$ is a prime. From [11], we have

$$\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Z}_\ell \simeq \mathrm{End}_{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(T_\ell(A)),$$

where $T_\ell(A)$ is the Tate module of A and \mathbb{Z}_ℓ is a ring of ℓ -adic integers. Since $T_\ell(A) \simeq (\mathbb{Z}_\ell)^{2g}$, the Frobenius endomorphism on A can be represented by the matrix $F \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Using Weil pairing, it can be shown [12, p. 358] that F has the following properties:

- 1) $F^T M F = q \cdot M$;
- 2) the matrix M is skew-symmetric;
- 3) $\det(M)$ is a unit in \mathbb{Z}_ℓ .

In other words, F belongs to $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. The matrix of the action of Frobenius on $A[\ell]$ is defined as $F_\ell = F \pmod{\ell}$. In the case of $q \equiv 1 \pmod{\ell}$ this matrix belongs to symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. The orders of groups $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$ are known [13, § 1.6.4]:

$$\begin{aligned} \#\mathrm{Sp}_{2g}(\mathbb{F}_\ell) &= \ell^{g^2} \prod_{i=1}^g (\ell^{2i} - 1), \\ \#\mathrm{PSp}_{2g}(\mathbb{F}_\ell) &= \ell^{g^2} \frac{\prod_{i=1}^g (\ell^{2i} - 1)}{\gcd(2, \ell - 1)}. \end{aligned} \tag{4}$$

In this paper, we study the orders of matrices F_ℓ as elements of $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$. From the introduction we know that in dimension 2 case these orders satisfy Eqs. (2) and (3). In next section we give equations for any dimension. So this information can be used for generalization of SEA-algorithm to higher dimension.

3. Generalization of Atkin's formula

Now, we derive explicit formulae that relates the order r of the Frobenius action on $A[\ell]$ and the characteristic polynomial $\chi_{A,q}(T) \pmod{\ell}$ of the Frobenius endomorphism on abelian variety A of dimension g . These formulae are direct generalization of Atkin's formula for the dimension 1 case [1, Proposition 6.2] which is used in SEA-algorithm. Our formulae can be used for point counting in higher dimension case.

Let φ be the Frobenius endomorphism on A and let

$$\chi_{A,q}(T) = T^{2g} + a_1 T^{2g-1} + \dots + a_g T^g + a_{g-1} q T + \dots + a_1 q^{g-1} T + q^g$$

be the characteristic polynomial of φ . It is known that we can arrange the roots λ_i of this polynomial in such way that $\lambda_i \lambda_{i+g} = q$ for i from 1 to g . So we can write

$$\chi_{A,q}(T) = \prod_{i=1}^g (T - \lambda_i) \left(T - \frac{q}{\lambda_i} \right).$$

We can associate [14, § 4] the real Weil polynomial $h_{A,q}(T)$ to the characteristic polynomial $\chi_{A,q}(T)$. This polynomial $h_{A,q}(T)$ has the properties:

$$\chi_{A,q}(T) = T^g h_{A,q} \left(T + \frac{q}{T} \right)$$

and

$$h_{A,q}(T) = \prod_{i=1}^g \left(T - \left(\lambda_i + \frac{q}{\lambda_i} \right) \right).$$

Let $h_{A,q}(T) = T^g + b_1 T^{g-1} + \dots + b_{g-1} T + b_g$. We can write [14, p. 4, Th. 9]:

$$a_{2k} = b_{2k} + \sum_{i=1}^k \binom{g-2(k-i)}{i} q^i b_{2(k-i)} \quad (5)$$

and

$$a_{2k+1} = b_{2k+1} + \sum_{i=1}^k \binom{g-2(k-i)-1}{i} q^i b_{2(k-i)+1}. \quad (6)$$

So if we know $h_{A,q}(T)$ then we can easily find $\chi_{A,q}(T)$. There are also recurrent formulae [2, § 17.1.2] for the coefficients a_k in terms of powers of roots which can be obtained via Newton – Girard formulae:

$$k a_k = S_k + S_{k-1} a_1 + S_{k-2} a_2 + \dots + S_1 a_{k-1},$$

where $S_k = -\sum_{i=1}^{2g} \lambda_i^k$. Similarly, we have for coefficients b_k :

$$k b_k = S'_k + S'_{k-1} b_1 + S'_{k-2} b_2 + \dots + S'_1 b_{k-1}, \quad (7)$$

where $S'_k = -\sum_{i=1}^g \left(\lambda_i + \frac{q}{\lambda_i} \right)^k$.

Now let us consider the situation modulo prime ℓ and the restriction of the Frobenius endomorphism φ on $A[\ell]$.

Proposition 1. Let A be an abelian variety of dimension g over a finite field \mathbb{F}_q of characteristic p , let $h_{A,q}(T) = \sum_{k=0}^g b_k T^k$ be the real Weil polynomial of the characteristic polynomial of the Frobenius endomorphism φ on A . If $\ell \neq p$ is a prime, r is the order of φ on $A[\ell]$, and $\gcd(r, \ell) = 1$, then

$$k b_k = S'_k + S'_{k-1} b_1 + S'_{k-2} b_2 + \dots + S'_1 b_{k-1} \pmod{\ell},$$

where $S'_{2k} = -\sum_{i=1}^g (\eta_i q)^k$, $S'_{2k+1} = -\sum_{i=1}^g (\pm (\eta_i q)^{k+1/2})$. Here, $\eta_i = \zeta_i + \frac{1}{\zeta_i} + 2$ for $i = 1, \dots, g$ and ζ_1, \dots, ζ_g are some r -th roots of unity in $\overline{\mathbb{F}}_\ell$ such that $\text{lcm}(\text{ord}(\zeta_1), \dots, \text{ord}(\zeta_g)) = r$ if r is odd and $\text{lcm}(\text{ord}(\zeta_1), \dots, \text{ord}(\zeta_g)) = r$ or $r/2$ if r is even.

Proof. Let F_ℓ be a matrix representing action of φ on $A[\ell]$. So r is the order of F_ℓ , i.e. a minimal integer r such that $F_\ell^r = \alpha I$ for some α . Let $P_i \in A[\ell]$ be such that $\varphi(P_i) = [\lambda_i]P_i$ and \tilde{P}_i be the corresponding vector from $(\mathbb{Z}/\ell\mathbb{Z})^{2g} \simeq A[\ell]$. On the one hand, we have $F_\ell^r \tilde{P}_i = \alpha^r \tilde{P}_i$ since φ^r is represented by the matrix $F_\ell^r = \alpha I$ for a constant α . On the other hand we have $F_\ell^r \tilde{P}_i = \lambda_i^r \tilde{P}_i$. So $\lambda_1^r = \lambda_2^r = \dots = \lambda_{2g}^r$. Since $\lambda_i \lambda_{i+g} = q$, we obtain $\lambda_i^r \lambda_{i+g}^r = \lambda_i^{2r} = q^r$. This implies the relation $\lambda_i^2 = \zeta_i q$ for some r -th roots of unity ζ_i and, since r is minimal, we can derive additional restrictions on the r -th roots. Let $n = \text{lcm}(\text{ord}(\zeta_1), \dots, \text{ord}(\zeta_g))$ then $\lambda_1^{2n} = \dots = \lambda_g^{2n} = q^{2n}$. From this in case of $2n < r$ we have a contradiction to the minimality of r . Hence $2n \geq r$ and, since $n \leq r$ and n is a divisor of r , we have $n = r$ or $n = r/2$.

Let $\eta_i = \zeta_i + \frac{1}{\zeta_i} + 2$ as in the $g = 1$ case. Since $\lambda_i + \frac{q}{\lambda_i} = \frac{(\zeta_i + 1)q}{\lambda_i} = \pm\sqrt{\eta_i q}$, the coefficients b_k of $h_{A,q}(T)$ are elementary symmetric polynomials in variables $\pm\sqrt{\eta_i q}$. Using the relation $\lambda_i^2 = \zeta_i q$, we can write S'_{2k} and S'_{2k+1} from Eq. (7) as

$$S'_{2k} = -\sum_{i=1}^g (\eta_i q)^k \quad \text{and} \quad S'_{2k+1} = -\sum_{i=1}^g (\eta_i q)^k (\eta_i - 2) \lambda_i = -\sum_{i=1}^g (\pm(\eta_i q)^{k+1/2}).$$

The Proposition is proved. ■

In case of $\gcd(\ell, r) \neq 1$ the Eq. (4) implies that we can write r as $r = \ell^k r_0$ where $k|g^2$ and $\ell \nmid r_0$. In this case we can take $r = r_0$ in Proposition 1.

Finally, we apply Proposition 1 to obtain relations modulo ℓ :

$$\begin{aligned} b_1 &= -\sum_{i=1}^g (\pm\sqrt{\eta_i q}), \\ 2b_2 &= -\sum_{i=1}^g (\eta_i q) + b_1^2, \\ 3b_3 &= -\sum_{i=1}^g \pm(\eta_i q)^{3/2} + (2b_2 - b_1^2)b_1 + b_1 b_2, \\ &\dots \\ (2k)b_{2k} &= -\sum_{i=1}^g (\eta_i q)^k + f_{2k}(b_1, \dots, b_{2k-1}), \\ (2k+1)b_{2k+1} &= -\sum_{i=1}^g (\pm(\eta_i q)^{k+1/2}) + f_{2k+1}(b_1, \dots, b_{2k}), \end{aligned} \tag{8}$$

where f_{2k} and f_{2k+1} are polynomials obtained by substituting the previously computed values of S'_i to the Eq. (7).

Thus, the coefficients a_k can be written in terms of $\sqrt{\eta_i q}$ for $k = 1, \dots, g$ by Eqs. (5) and (6). In the following we also use squaring and the fact that b_i are elementary symmetric polynomials in $\pm\sqrt{\eta_i q}$ to get rid of signs and to make formulae (8) simpler. For example, we can write $b_g^2 = \eta_1 \dots \eta_g q^g$ for the coefficient b_g .

Note that for $g = 1$ these formulae give us the formulae from [1, Proposition 6.2]. For the cases $g = 2$ and $g = 3$, we obtain the following propositions.

Proposition 2. Let A be an abelian surface over a finite field \mathbb{F}_q and $\chi_{A,q}(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$ be the characteristic polynomial of the Frobenius endomorphism φ on A , let r be the order of φ on $A[\ell]$ for $\ell \neq p$, and let $\gcd(\ell, r) = 1$. Then

$$a_1^2 = (\sqrt{\eta_1} \pm \sqrt{\eta_2})^2 q \pmod{\ell} \quad \text{and} \quad (a_2 - 2q)^2 = \eta_1 \eta_2 q^2 \pmod{\ell},$$

where $\eta_1 = \zeta_1 + \zeta_1^{-1} + 2$, $\eta_2 = \zeta_2 + \zeta_2^{-1} + 2$ and ζ_1, ζ_2 are some r -th roots of unity such that $\text{lcm}(\text{ord}(\zeta_1), \text{ord}(\zeta_2)) = r$ in case r is odd and $\text{lcm}(\text{ord}(\zeta_1), \text{ord}(\zeta_2)) = r$ or $r/2$ in case r is even.

Proof. By Eq. (6), we have $a_1 = b_1 = (\pm\sqrt{\eta_1} \pm \sqrt{\eta_2})\sqrt{q}$. Therefore, $a_1^2 = (\sqrt{\eta_1} \pm \sqrt{\eta_2})^2 q$. Since $b_2 = \pm\sqrt{\eta_1}\sqrt{\eta_2}q$, we have $b_2^2 = \eta_1\eta_2q^2$. From Eq. (5), we can write $a_2 = b_2 + 2q$ and therefore $(a_2 - 2q)^2 = \eta_1\eta_2q^2$. ■

If $\gcd(\ell, r) \neq 1$, then, as in the general case, we can take the integer r_0 such that $r = \ell^{k_0}r_0$, $\ell \nmid r_0$ and apply the Proposition 2 for $r = r_0$.

The formulae in Proposition 2 appears in [4] with additional restrictions on abelian variety A . Our version is fully general with weakened conditions on roots of unity.

Proposition 3. Let A be an abelian variety of dimension 3 over a finite field \mathbb{F}_q and $\chi_{A,q}(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + a_2qT^2 + a_1q^2T + q^3$ be the characteristic polynomial of the Frobenius endomorphism φ on A , let r be the order of φ on $A[\ell]$ for $\ell \neq p$, and let $\gcd(\ell, r) = 1$. Then

$$\begin{aligned} a_1^2 &= (\pm\sqrt{\eta_1} \pm \sqrt{\eta_2} \pm \sqrt{\eta_3})^2 q, \\ 2a_2 &= a_1^2 + 6q - (\eta_1 + \eta_2 + \eta_3), \\ (a_3 - 2a_1q)^2 &= \eta_1\eta_2\eta_3q^3 \end{aligned}$$

modulo ℓ , where $\eta_1 = \zeta_1 + \frac{1}{\zeta_1} + 2$, $\eta_2 = \zeta_2 + \frac{1}{\zeta_2} + 2$, $\eta_3 = \zeta_3 + \frac{1}{\zeta_3} + 2$ for some r -th roots of unity $\zeta_1, \zeta_2, \zeta_3$ such that $\text{lcm}(\text{ord}(\zeta_1), \text{ord}(\zeta_2), \text{ord}(\zeta_3)) = r$ in case r is odd and in case r is even, $\text{lcm}(\text{ord}(\zeta_1), \text{ord}(\zeta_2), \text{ord}(\zeta_3)) = r$ or $\frac{r}{2}$.

Proof.

- 1) First relation follows from the fact that $a_1 = b_1 = (\pm\sqrt{\eta_1} \pm \sqrt{\eta_2} \pm \sqrt{\eta_3})\sqrt{q}$.
- 2) Since $a_2 = b_2 + 3q$ by Eq. (5), we have $2a_2 - 6q = 2b_2 = -(\eta_1 + \eta_2 + \eta_3) + a_1^2$.
- 3) We have $b_3^2 = \eta_1\eta_2\eta_3q^3$. Equations (6) and (5) imply $a_3 = b_3 + 2qb_1 = b_3 + 2qa_1$. Then $(a_3 - 2qa_1)^2 = \eta_1\eta_2\eta_3q^3$.

The Proposition is proved. ■

4. Conjugacy classes and the orders of elements in $\text{Sp}_4(\mathbb{F}_\ell)$

In general case the orders of matrices over a finite field were considered in [15–19]. In this Section we study the distribution of orders of matrices in $\text{Sp}_4(\mathbb{F}_\ell)$ as elements of projective symplectic group $\text{PSp}_4(\mathbb{F}_\ell)$. We define the order of a matrix $M \in \text{Sp}_4(\mathbb{F}_\ell)$ to be the minimal number r such that $M^r = \lambda I$ for some scalar $\lambda \in \mathbb{F}_\ell$. We need such specific definition to derive the properties of Frobenius orders in the next section. All similar matrices have the same order, so it is enough to find the orders of conjugacy classes. A description of conjugate classes in $\text{Sp}_4(\mathbb{F}_\ell)$ with explicit representatives is given in [20, p. 489–491]. Using the same notation we denote the conjugacy classes in $\text{Sp}_4(\mathbb{F}_\ell)$ by $\overline{A}_\bullet, \overline{B}_\bullet(\bullet), \overline{C}_\bullet(\bullet), \overline{D}_\bullet$ with representative elements $A_\bullet, B_\bullet(\bullet), C_\bullet(\bullet), D_\bullet$ respectively. For each class we calculate orders $r = \text{ord}(M)$ of matrices by using the explicit representatives. Since the number of matrices in a class is also known, we can calculate the probability of a random matrix $M \in \text{Sp}_4(\mathbb{F}_\ell)$ to fall in a given class. We give the orders for classes with their respective probabilities in Table 1.

Table 1

Orders of matrices in $\text{Sp}_4(\mathbb{F}_\ell)$ as elements of $\text{PSp}_4(\mathbb{F}_\ell)$ and their probabilities

Classes in $\text{Sp}_4(\mathbb{F}_\ell)$	Order of matrices (projective)	Probability [$M \in \text{Sp}_4(\mathbb{F}_\ell)$ & $M \in \text{class}$]
$\overline{A}_1, \overline{A}'_1$	1	$1/(\ell^4(\ell^2 - 1)(\ell^4 - 1))$
$\overline{A}_{21}, \overline{A}'_{21}, \overline{A}_{22}, \overline{A}'_{22}$	ℓ	$1/(2\ell^4(\ell^2 - 1))$
$\overline{A}_{31}, \overline{A}'_{31}$	ℓ	$1/(2\ell^3(\ell - 1))$
$\overline{A}_{32}, \overline{A}'_{32}$	ℓ	$1/(2\ell^3(\ell + 1))$
$\overline{A}_{41}, \overline{A}'_{41}, \overline{A}_{42}, \overline{A}'_{42}$	ℓ	$1/(2\ell^2)$
$\overline{B}_1(i)$	$(\ell^2 + 1)/(2s), s = \gcd(i, (\ell^2 + 1)/2)$	$1/(\ell^2 + 1)$
$\overline{B}_2(i)$	$(\ell^2 - 1)/(2s), s = \gcd(i, (\ell^2 - 1)/2)$	$1/(\ell^2 - 1)$
$\overline{B}_3(i, j)$	$(\ell - 1)/\gcd(\ell - 1, i + j, i - j)$	$1/(\ell - 1)^2$
$\overline{B}_4(i, j)$	$(\ell + 1)/\gcd(\ell + 1, i + j, i - j)$	$1/(\ell + 1)^2$
$\overline{B}_5(i, j)$	$(\ell^2 - 1)/\gcd(\ell^2 - 1, i(\ell - 1) + j(\ell + 1), 2i(\ell - 1))$	$1/(\ell^2 - 1)$
$\overline{B}_6(i)$	$(\ell + 1)/(2s), s = \gcd(i, (\ell + 1)/2)$	$1/(\ell(\ell + 1)(\ell^2 - 1))$
$\overline{B}_7(i)$	$\ell(\ell + 1)/(2s), s = \gcd(i, \ell(\ell + 1)/2)$	$1/(\ell(\ell + 1))$
$\overline{B}_8(i)$	$(\ell - 1)/(2s), s = \gcd(i, (\ell - 1)/2)$	$1/(\ell(\ell - 1)(\ell^2 - 1))$
$\overline{B}_9(i)$	$\ell(\ell - 1)/(2s), s = \gcd(i, \ell(\ell - 1)/2)$	$1/(\ell(\ell - 1))$
$\overline{C}_1(i)$	$(\ell + 1)/s, s = \gcd(i, \ell + 1)$	$1/(\ell(\ell + 1)(\ell^2 - 1))$
$\overline{C}'_1(i)$	$\begin{cases} 2s, & \text{if } 2 \nmid s, \\ s/2, & \text{if } 2 \mid s \text{ and } 4 \nmid s, \\ s, & \text{if } 4 \mid s, \end{cases}$ where $s = (\ell + 1)/\gcd(i, \ell + 1)$	$1/(\ell(\ell + 1)(\ell^2 - 1))$
$\overline{C}_{21}(i), \overline{C}_{22}(i)$	$\ell(\ell + 1)/s, s = \gcd(i, \ell(\ell + 1))$	$1/(2\ell(\ell + 1))$
$\overline{C}'_{21}(i), \overline{C}'_{22}(i)$	$\begin{cases} 2s, & \text{if } 2 \nmid s, \\ s/2, & \text{if } 2 \mid s \text{ and } 4 \nmid s, \\ s, & \text{if } 4 \mid s, \end{cases}$ where $s = \ell(\ell + 1)/\gcd(i, \ell(\ell + 1))$	$1/(2\ell(\ell + 1))$
$\overline{C}_3(i)$	$(\ell - 1)/\gcd(i, \ell - 1)$	$1/\ell(\ell - 1)(\ell^2 - 1)$
$\overline{C}'_3(i)$	$\begin{cases} 2s, & \text{if } 2 \nmid s, \\ s/2, & \text{if } 2 \mid s \text{ and } 4 \nmid s, \\ s, & \text{if } 4 \mid s, \end{cases}$ where $s = (\ell - 1)/\gcd(i, \ell - 1)$	$1/\ell(\ell - 1)(\ell^2 - 1)$
$\overline{C}_{41}(i), \overline{C}_{42}(i)$	$\ell(\ell - 1)/\gcd(i, \ell(\ell - 1))$	$1/(2\ell(\ell - 1))$
$\overline{C}'_{41}(i), \overline{C}'_{42}(i)$	$\begin{cases} 2s, & \text{if } 2 \nmid s, \\ s/2, & \text{if } 2 \mid s \text{ and } 4 \nmid s, \\ s, & \text{if } 4 \mid s, \end{cases}$ where $s = \ell(\ell - 1)/\gcd(i, \ell(\ell - 1))$	$1/(2\ell(\ell - 1))$
\overline{D}_1	2	$1/(\ell^2(\ell^2 - 1)^2)$
$\overline{D}_{21}, \overline{D}_{22}, \overline{D}_{23}, \overline{D}_{24}$	2ℓ	$1/(2\ell^2(\ell^2 - 1))$
$\overline{D}_{31}, \overline{D}_{32}, \overline{D}_{33}, \overline{D}_{34}$	2ℓ	$1/(4\ell^2)$

Having explicit information on orders of matrices in classes, we can now derive numerical characteristics of the distribution of orders. Let ξ be a random variable that takes values in $\{\text{ord}(M) : M \in \text{Sp}_4(\mathbb{F}_\ell)\}$. Our next goal is to find an expected value and variance of the random variable ξ . Define the expected order of a matrix in $\text{Sp}_4(\mathbb{F}_\ell)$ as $\mu_4 = \frac{1}{\#\text{Sp}_4(\mathbb{F}_\ell)} \sum_{M \in \text{Sp}_4(\mathbb{F}_\ell)} \text{ord}(M)$, where the order is defined for M as an element of $\text{PSp}_4(\mathbb{F}_\ell)$.

Since all matrices in a conjugacy class have the same order, we can split the sum μ_4 into parts which correspond to the conjugacy classes. For a conjugacy class \overline{M} the corresponding

term in the sum μ_4 is given by the formula

$$\mu(\overline{M}) = \text{ord}(M) \frac{\#\overline{M}}{\#\text{Sp}_4(\mathbb{F}_\ell)} = \text{ord}(M) \mathbb{P}[\xi = \text{ord}(M)].$$

For classes $\overline{A}, \overline{D}$ the order is fixed. For classes of types $\overline{B}_k(i, j), \overline{B}_k(i), \overline{C}_k(i), \overline{C}'_k(i)$ the order depends on parameters i, j and we assume that parameters i, j are distributed uniformly among their value sets as $\ell \rightarrow \infty$. So, we can use the following approximation [21] for $\gcd(i, x)$:

$$E(x) = \frac{6}{\pi^2} \log(x) + O(1).$$

The expected orders of symplectic matrices in $\bigcup_{i,j} \overline{B}_k(i, j), \bigcup_i \overline{B}_k(i), \bigcup_i \overline{C}_k(i), \bigcup_i \overline{C}'_k(i)$ are presented in Table 2.

Table 2

**Expected orders of symplectic matrices $\text{Sp}_4(\mathbb{F}_\ell)$
as elements of $\text{PSp}_4(\mathbb{F}_\ell)$**

Classes	Quantity of i, j	Expected order
$\overline{B}_1(i)$	$\frac{1}{4}(\ell^2 - 1)$	$\frac{1}{2}E^{-1}\left(\frac{\ell^2 + 1}{2}\right)$
$\overline{B}_2(i)$	$\frac{1}{4}(\ell - 1)^2$	$\frac{1}{2}E^{-1}\left(\frac{\ell^2 - 1}{2}\right)$
$\overline{B}_3(i, j)$	$\frac{1}{8}(\ell - 3)(\ell - 5)$	$\frac{1}{\ell - 1}E^{-1}(\ell - 1)$
$\overline{B}_4(i, j)$	$\frac{1}{8}(\ell - 1)(\ell - 3)$	$\frac{1}{\ell + 1}E^{-1}(\ell + 1)$
$\overline{B}_5(i, j)$	$\frac{1}{4}(\ell - 1)(\ell - 3)$	$E^{-1}(\ell^2 - 1)$
$\overline{B}_6(i)$	$\frac{1}{2}(\ell - 1)$	$\frac{1}{2\ell(\ell^2 - 1)}E^{-1}\left(\frac{\ell + 1}{2}\right)$
$\overline{B}_7(i)$	$\frac{1}{2}(\ell - 1)$	$\frac{1}{2}E^{-1}\left(\frac{\ell(\ell + 1)}{2}\right)$
$\overline{B}_8(i)$	$\frac{1}{2}(\ell - 3)$	$\frac{1}{2\ell(\ell^2 - 1)}E^{-1}\left(\frac{\ell - 1}{2}\right)$
$\overline{B}_9(i)$	$\frac{1}{2}(\ell - 3)$	$\frac{1}{2}E^{-1}\left(\frac{\ell(\ell - 1)}{2}\right)$
$\overline{C}_1(i), \overline{C}'_1(i)$	$(\ell - 1)$	$\frac{1}{\ell(\ell^2 - 1)}E^{-1}(\ell + 1)$
$\overline{C}_{21}(i), \overline{C}'_{21}(i),$ $\overline{C}_{22}(i), \overline{C}'_{22}(i)$	$2(\ell - 1)$	$\frac{1}{2}E^{-1}(\ell + 1)$
$\overline{C}_3(i), \overline{C}'_3(i)$	$(\ell - 3)$	$\frac{1}{\ell(\ell^2 - 1)}E^{-1}(\ell - 1)$
$\overline{C}_{41}(i), \overline{C}'_{41}(i),$ $\overline{C}_{42}(i), \overline{C}'_{42}(i)$	$2(\ell - 3)$	$\frac{1}{2}E^{-1}(\ell - 1)$

Now, we obtain the expected order and the variance of the symplectic matrix applying the well-known formulae to the data from this table.

Proposition 4. Let M be a matrix from $\text{Sp}_4(\mathbb{F}_\ell)$. Define the order of M to be the order of M in the group $\text{PSp}_4(\mathbb{F}_\ell)$. Then

1) The expected order of matrix M is equal to

$$\mu_4 = \frac{\pi^2}{48\ell(\ell^2 - 1)} (2\ell^5 + 15\ell^4 - 47\ell^3 + \ell^2 + 65\ell - 40) \log^{-1}(\ell).$$

2) The variance of the order's distribution is equal to

$$\delta_4 = \left(\frac{\pi}{24\ell(\ell^2 - 1)} \right)^2 \psi(\ell) \log^{-1}(\ell) - \mu_4^2,$$

where

$$\psi(\ell) = 6\ell^{10} - 27\ell^9 + 420\ell^8 - 1443\ell^7 + 828\ell^6 + 3375\ell^5 - 3804\ell^4 - 825\ell^3 + 2550\ell^2 - 1080\ell.$$

5. Distribution of orders of the Frobenius action on $A[\ell]$

Let A be an abelian surface defined over a finite field \mathbb{F}_q of odd characteristic p . From Section 2 we know that the action of the Frobenius endomorphism on ℓ -torsion subgroup in case $q \equiv 1 \pmod{\ell}$ is represented by a symplectic matrix from $\mathrm{Sp}_4(\mathbb{F}_\ell)$. To find the distribution of the Frobenius orders, we use a heuristic assumption that the elements of Frobenius are equidistributed in $\mathrm{Sp}_4(\mathbb{F}_\ell)$. The assumption was already used in [22] in the context of counting the number of isogeny classes of abelian varieties. Thus, from Proposition 4 we obtain our results for expected order and variance of the Frobenius order.

Theorem 1. Let A be an abelian surface defined over a finite field \mathbb{F}_q of characteristic p . If $\ell \neq p$ is a prime number and $q \gg \ell$, then the expected order of the Frobenius action on $A[\ell]$ is equal to μ_4 .

Theorem 2. Let A be an abelian surface defined over a finite field \mathbb{F}_q of characteristic p . If $\ell \neq p$ is a prime number, $q \gg \ell$, then the variance of order distribution of the Frobenius action on $A[\ell]$ is equal to δ_4 .

Theorem 3 (Heuristic). The modes of the random variable ξ are $(\ell^2 + 1)/2$ and $(\ell^2 - 1)/2$.

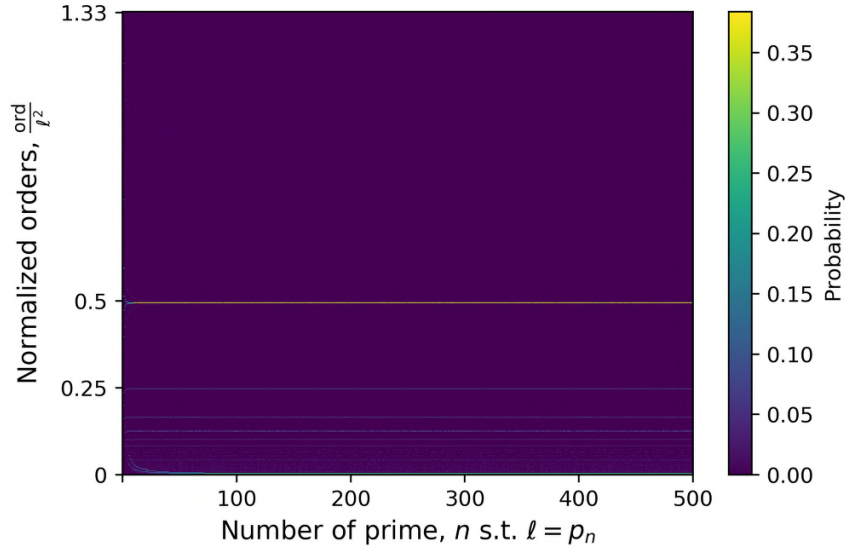
In point counting algorithms, we have to enumerate all primes $\ell \leq (9g + 3) \log q$. For cryptography on genus 2 curves we work with fields of size 160 bit. In this case the size of the group will be equal to $O(q^2)$ by the Hasse — Weil bound, i.e. 320 bit. So we have to find the characteristic polynomial $\chi_{A,q}(T) \pmod{\ell}$ for all primes $\ell \leq 3360$ to restore the coefficients of $\chi_{A,q}(T)$ by CRT.

Using the data from Table 1, we calculated the distribution of the Frobenius orders for the first 500 primes $\ell = 3, \dots, 3571$. Since the order of any matrix depends linearly on ℓ^2 , as follows from Theorem 1, we normalize the order by calculating the value $\mathrm{ord}(M)/\ell^2$ instead of $\mathrm{ord}(M)$ itself. An obtained family of distributions is shown on Fig. 1. Taking an average value of order on different ℓ 's, one can construct the averaged distribution of orders. We present this distribution in the Table 3.

Table 3

The distribution for orders of the Frobenius action on $A[\ell]$

Order	$(1, \ell]$				$(\ell, 2\ell]$		$(2\ell, (\ell^2 + 1)/2]$					$((\ell^2 + 1)/2, \ell(\ell + 1)]$
	$\frac{\ell - 1}{2}$	$\frac{\ell + 1}{2}$	$\ell - 1$	Other	$\ell + 1$	Other	$\frac{\ell^2 - 1}{4}$	$\frac{\ell^2 + 1}{4}$	$\frac{\ell^2 - 1}{2}$	$\frac{\ell^2 + 1}{2}$	Other	
%	4.0	4.0	5.0	6.3	5.0	1.5	6.6	5.0	13.4	15.7	29.7	3.8

Figure 1. A distribution of orders for the first 500 primes ℓ

6. Application to point counting

In Schoof—Pila [9] algorithm determining $\chi_{A,q}(T) \pmod{\ell}$ is done by direct enumeration of at most ℓ^g possible coefficients. Each test requires expensive operations like ideal membership test and operations with division polynomials of degree ℓ^{2g} . So reducing the number of elements to enumerate is crucial.

The obtained results can be used for point counting on abelian variety A in the following modification of Schoof—Pila method.

- 1) Choose primes ℓ such that $\prod_{\ell \leq H \log q} \ell > 2 \binom{2g}{g} q^g$, where $H = (9g + 3)$.
- 2) For each prime ℓ :
 - a) Build a list L of tuples (a_1, \dots, a_g, w) , where $a_1, \dots, a_g \pmod{\ell}$ are the candidates for coefficients of characteristic polynomial $\chi_{A,q}(T) \pmod{\ell}$ and w is a probability of (a_1, \dots, a_g) to be the coefficients of $\chi_{A,q}(T) \pmod{\ell}$. This probability is computed by using the distribution of the orders and formulae (5), (6), (8).
 - b) Sort the list L by w .
 - c) Determine $\chi_{A,q}(T)$ by testing tuples from the list starting with the ones having high values of w .
- 3) Determine $\chi_A(T)$ from the list of $\chi_{A,q}(T) \pmod{\ell}$ using CRT.

To test applicability of the distribution to point counting using the method described above, we run a series of experiments in SageMath [23] system. We choose a set of random primes p of size $p > 2^{16}$. For each prime p we compute a set of $\ell \geq 5$ such that $p \equiv 1 \pmod{\ell}$ and a set of 10000 random genus 2 hyperelliptic curves with imaginary model

$$y^2 = f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

This model is most common in cryptography. Such a curve is generated by a random monic square-free polynomial $f(x)$ in $\mathbb{F}_p[x]$ of degree 5. By Proposition 2, for each pair (p, ℓ) we build a list L of pairs $(a_1^2, (a_2 - 2q)^2)$ corresponding to small orders $r = (\ell \pm 1)/2$ from Table 3. We choose these orders because they appear in many conjugacy classes from Table 1 and the most common orders $(\ell^2 \pm 1)/2$ lead to big lists. For each curve we compute

the characteristic polynomial $\chi_p(T)$ of the Frobenius endomorphism by built-in methods of SageMath and so we know the exact value of $\chi_p(T) \pmod{\ell}$. After that we compared the number of attempts to find $\chi_p(T) \pmod{\ell}$ using classical enumeration (as in Schoof — Pila algorithm) against our proposed search in the list L .

Our experiments show that the number of attempts to find the $\chi_p(T) \pmod{\ell}$ is reduced by $\approx 1\text{--}12\%$ for $\ell \leq 100$, where the success rate is decreasing with the growing of ℓ . In the case of $\ell > 100$ we have the number of attempts reduced by $\approx 1\text{--}2\%$.

To improve this, we should generalize Atkin’s “Match and Sort” algorithm for elliptic curves and use the data on Frobenius distribution in this generalized algorithm. This can be done by combining steps 2 and 3 in the algorithm above and by using baby-step giant-step algorithm to determine $\chi_{A,q}(T)$ from the lists L each corresponding to different ℓ . However, a realization of this method is still an open problem even in the case when we use modular polynomials to determine the Frobenius order and so we know the exact order.

Conclusion

In this paper, we present a generalization of Atkin’s formulae to any dimension and showed that the distribution of Frobenius orders is not uniform for abelian surfaces over a finite field \mathbb{F}_q with $q \equiv 1 \pmod{\ell}$. Furthermore, we described possible applications of this distribution to point counting purposes. The formulae can be used to limit the number of possible characteristic polynomials $\chi_{A,q}(T) \pmod{\ell}$ in case when we know the Frobenius order. The distribution allows us to sort the lists of possible $\chi_{A,q}(T) \pmod{\ell}$ by probability.

The further work is to use this modular information about distribution efficiently in the generalization of Schoof’s algorithm for genus 2 curves [6]. For elliptic curves there exist Atkin’s “Match and Sort” algorithm and “Chinese and Match” algorithm [24] due to Joux and Lercier. But for higher dimension this is still an open problem.

REFERENCES

1. *Schoof R.* Counting points on elliptic curves over finite fields. J. de Théorie des Nombres de Bordeaux, 1995, vol. 7, no. 1, pp. 219–254.
2. *Cohen H., Frey G., Avanzi R., et al.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2005.
3. *Silverman J. H.* The Arithmetic of Elliptic Curves. N.Y., Springer Verlag, 2009, vol. 106.
4. *Martindale C.* Counting points on genus 2 curves over finite fields. Talk at GAGA Seminar in Utrecht, Netherlands, 2017.
5. *Ballentine S., Guillevic A., García E. L., et al.* Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. Algebraic Geometry for Coding Theory and Cryptography, Springer, 2017, pp. 63–94.
6. *Gaudry P. and Schost É.* Genus 2 point counting over prime fields. J. Symbolic Computation, 2012, vol. 47, no. 4, pp. 368–400.
7. *Bröker R. and Lauter K.* Modular polynomials for genus 2. LMS J. Computation and Math., 2009, vol. 12, pp. 326–339.
8. *Gaudry P. and Schost É.* Modular equations for hyperelliptic curves. Mathematics of Computation, 2005, vol. 74, no. 249, pp. 429–454.
9. *Pila J.* Frobenius maps of abelian varieties and finding roots of unity in finite fields. Mathematics of Computation, 1990, vol. 55, no. 192, pp. 745–763.
10. *Kolesnikov N. S. and Novoselov S. A.* On the order of the frobenius endomorphism action on ℓ -torsion subgroup of abelian surfaces. Prikl. Diskr. Mat. Suppl., 2019, no. 12, pp. 11–12.

11. *Tate J.* Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 1966, vol. 2, no. 2, pp. 134–144.
12. *Rück H.-G.* Abelian surfaces and jacobian varieties over finite fields. *Compositio Mathematica*, 1990, vol. 76, no. 3, pp. 351–366.
13. *Bray J. N., Holt D. F., and Roney-Dougal C. M.* The Maximal Subgroups of the Low-Dimensional Finite Classical Groups. LMS Lecture Note Series, Cambridge University Press, 2013.
14. *Hurt N. E.* Many Rational Points: Coding Theory and Algebraic Geometry. Springer Science & Business Media, 2013, vol. 564.
15. *Stong R.* The average order of a matrix. *J. Combinatorial Theory, Ser. A*, 1993, vol. 64, no. 2, pp. 337–343.
16. *Schmutz E.* The order of a typical matrix with entries in a finite field. *Israel J. Mathematics*, 1995, vol. 91, no. 1–3, pp. 349–371.
17. *Fulman J.* Random matrix theory over finite fields. *Bull. Amer. Math. Society*, 2002, vol. 39, no. 1, pp. 51–85.
18. *Schmutz E.* The expected order of a random unitary matrix. *J. Group Theory*, 2008, vol. 11, no. 4, pp. 495–510.
19. *Aivazidis S. and Sofos E.* On the distribution of the density of maximal order elements in general linear groups. *Ramanujan J.*, 2015, vol. 38, no. 1, pp. 35–59.
20. *Srinivasan B.* The characters of the finite symplectic group $\mathrm{Sp}(4, q)$. *Trans. AMS*, 1968, vol. 131, no. 2, pp. 488–525.
21. *Diaconis P. and Erdős P.* On the distribution of the greatest common divisor. *A Festschrift for Herman Rubin*, Institute of Mathematical Statistics, 2004, pp. 56–61.
22. *Achter J. and Williams C.* Local heuristics and an exact formula for abelian surfaces over finite fields. *Canadian Math. Bull.*, 2015, vol. 58, no. 4, pp. 673–691.
23. SageMath, the Sage Mathematics Software System (Version 8.9), 2019. <https://www.sagemath.org>.
24. *Joux A. and Lercier R.* “Chinese & Match”, an alternative to Atkin’s “Match and Sort” method used in the SEA algorithm. *Mathematics of Computation*, 2001, vol. 70, no. 234, pp. 827–836.