On the cyclicity of the rational points group of abelian varieties over finite fields

Alejandro J. Giangreco-Maidana

Version of Record: https://www.sciencedirect.com/science/article/pii/S1071579719300164
Manuscript_8f96c7a4a22f037547e51646d1da5a95

On the cyclicity of the rational points group of abelian varieties over finite fields

Alejandro J. Giangreco-Maidana

Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, 13453 Marseille, France

Abstract

We propose a simple criterion to know if an abelian variety A defined over a finite field $\mathbb{F}_q$ is *cyclic*, *i.e.*, it has a cyclic group of rational points; this criterion is based on the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$. We also provide a criterion to know if an isogeny class is *cyclic*, *i.e.*, all its varieties are cyclic; this criterion is based on the characteristic polynomial of the isogeny class. We find some asymptotic lower bounds on the fraction of cyclic $\mathbb{F}_q$-isogeny classes among certain families of them, when q tends to infinity. Some of these bounds require an additional hypothesis. In the case of surfaces, we prove that this hypothesis is achieved and, over all $\mathbb{F}_q$-isogeny classes with endomorphism algebra being a field and where q is an even power of a prime, we prove that the one with maximal number of rational points is cyclic and ordinary.

Keywords: group of rational points, cyclic, abelian variety, finite field
2000 MSC: Primary 11G10, 14G15, 14K15

1. Introduction

The group structure of elliptic curves (EC) defined over finite fields has a theoretical interest, but also an interest in applications to cryptography and error-correcting codes. More precisely, those elliptic curves with cyclic groups of rational points are of special interest for various problems (see for example [7], [9] and [6]). In many algorithms that use elliptic curves over finite fields one chooses it at random, thus, knowing such statistics can be useful.

The structure of all possible groups for EC over a finite field was discovered (independently) in [15], [12],[18] and [21]. However, this result does not provide immediately the statistics for cyclic EC over a given field or its extensions, which was explored in [19] and [20]. See also [1], where the realizability of possible groups for EC was studied from a statistical point of view.

There are many other closely related topics which were considered in the literature. In [16] and [11] the order of points on the groups of rational points was studied, in particular lower bounds for the *exponent* (the largest order), and some applications as well. Also, the exponent under base field extensions was examined in [8]. This question is closely related to the question about cyclicity, since cyclicity is equivalent to the fact that the exponent equals the cardinality of the group of rational points.

For both theoretical and practical interests, it is very natural to extend this investigation to abelian varieties of higher dimensions. Many facts are still unknown in this case. Nevertheless, in a recent paper [14], Rybakov gives a very explicit description of all possible groups of rational points of an abelian variety in a

Email address: ajgiangreco@gmail.com (Alejandro J. Giangreco-Maidana)

given isogeny class. His result is formulated in terms of the Newton polygon of the variety and the Hodge polygon of the group. In particular, from this description it follows that varieties with cyclic group of rational points always exist in an isogeny class. In [2] it is shown that for abelian surfaces, "very split" groups of rational points occur with density zero. This result agree with the general framework of the Cohen–Lenstra heuristics, which establish that groups with a higher number of automorphisms appear less frequently, since the very split groups have many more automorphisms than the cyclic group of the same size.

Another related and widely explored topic is maximal curves, *i.e.*, those with a maximal number of rational points, such curves are very important for applications. Goppa showed that the applications of EC to coding theory are interesting only if the curve has many rational points ([5]). Theoretical and practical bounds were explored and many algorithms to construct it were proposed. Relating "maximal" abelian varieties with its structures of rational points does not seem to be a simple task, but with many promising applications.

In cryptography, the Discrete Logarithm Problem is extensively used in such systems and, under some conditions, cyclic groups are suitable for these purposes ([4]). In many applications, security is based on working with big cyclic subgroups of the group of rational points.

Another interesting related topic is counting isomorphism classes of abelian varieties defined over a fixed finite field. In the 1-dimensional case, this corresponds to compute class numbers of some orders in quadratic number fields, and in the general case, this was treated for example (very recently) in [23]. Isomorphism classes can be grouped in isogeny classes. In [3], DiPippo and Howe developed some techniques and gave an asymptotic formula (with explicit error terms) for the number of isogeny classes of n-dimensional abelian varieties over the finite field with q elements, for fixed n and q tending to infinity.

In this paper we give some statistical results concerning cyclic isogeny classes, namely, in Theorem 2.2 we present a simple criterion to know if an isogeny class is *cyclic*, *i.e.*, all its varieties have a cyclic group of rational points, this criterion is based on the characteristic polynomial of the isogeny class. Further, in Theorems 2.3 and 2.6 we give asymptotic lower bounds on the fraction of cyclic isogeny classes when some coefficients on the characteristic polynomial corresponding to these isogeny classes are fixed. Theorem 2.6 needs an extra condition and, we show that for "good" coefficients, this condition holds true for abelian surfaces. Finally, we prove in Theorem 4.3 that under some restrictions, isogeny classes of abelian surfaces defined over finite fields with maximal number of rational points are cyclic and ordinary. Also, we give some examples of families of cyclic isogeny classes of abelian surfaces.

The rest of this paper is organized as follows: in Section 2 we briefly recall some general facts about abelian varieties over finite fields and we state our results more precisely; in Section 3 we prove Theorems 2.2, 2.3 and 2.6 and, Section 4 is devoted to abelian surfaces.

2. Preliminaries and Statement of the Results

For the general theory of abelian varieties see for example [10], and for precise results over finite fields, see [22].

Let $q = p^r$ be a power of a prime, and let $k = \mathbb{F}_q$ be a finite field with q elements. Let A be an abelian variety of dimension g over k. For an extension field K of k, we denote by $\mathrm{End}_K(A)$ the ring of K-endomorphism of A and by $\mathrm{End}_K^0(A) = (\mathrm{End}_K(A)) \otimes \mathbb{Q}$ its endomorphism algebra, the latter being an invariant of its isogeny class $\mathcal{A}$, we can denote it by $\mathrm{End}_K^0(\mathcal{A})$. For an integer n, denote by $\widehat{n}$ the ratio of n to the product of different prime divisors of n; and by $A[n]$ the group of n-torsion points of A over $\overline{\mathbb{F}}_q$, *i.e.*, the kernel of the multiplication endomorphism $[n]$. Then

$$\begin{aligned} A[n] &\cong (\mathbb{Z}/n\mathbb{Z})^{2g}, \qquad p \nmid n \\ A[p] &\cong (\mathbb{Z}/p\mathbb{Z})^{i}, \qquad 0 \leq i \leq g \end{aligned} \tag{1}$$

For a fixed prime ℓ ($\neq p$), the Tate module $T_\ell(A)$ is defined by $\varprojlim A[\ell^n]$. The Frobenius endomorphism F of A acts on $T_\ell(A)$ by a semisimple linear operator, and its characteristic polynomial $f_A(t)$ is called *Weil polynomial of* A. Tate proved in [17] that the isogeny class $\mathcal{A}$ of abelian variety is determined by its characteristic polynomial $f_{\mathcal{A}}(t)$ and, if $\mathcal{A}$ is simple, $f_{\mathcal{A}}(t) = h_{\mathcal{A}}(t)^e$ for some irreducible polynomial $h_{\mathcal{A}}$ and the center of $\mathrm{End}_k^0(\mathcal{A})$ is isomorphic to the number field $\mathbb{Q}(F) \cong \mathbb{Q}[t]/(h_{\mathcal{A}}(t))$. The cardinality of the group of rational points $A(k)$ of A equals $f_{\mathcal{A}}(1)$, and thus, it is an invariant of the isogeny class. For a prime number ℓ, v_ℓ denotes the usual ℓ-adic valuation. We denote by $\mathcal{P}$ the set of prime integers and by $\mathcal{P}(n)$ the set of prime divisors of n.

For an elliptic curve E, we have that $E(\mathbb{F}_q)$ is non-cyclic if and only if there exist a prime $\ell \neq p$ such that $E[\ell] \subseteq E(\mathbb{F}_q)$. This is not the case for higher dimensional varieties, however, a slightly different criterion holds:

Lemma 2.1. *If A is simple, then*

$$A(\mathbb{F}_q) \text{ is not cyclic } \iff \exists \varphi \in \mathrm{End}_{\overline{\mathbb{F}}_q}(A),\ [f_A(1)/\ell] = \varphi \circ (1 - F) \text{ for some prime divisor } \ell | f_A(1).$$

Note that in this case we do not require $\ell \neq p$. Note also that if such φ exists, it has to be defined over $\mathbb{F}_q$ and it belongs to the center of its endomorphism ring. This lemma is an easy consequence of the theory of abelian varieties over finite fields and we will prove it here within the proof of Theorem 2.2. Lemma 2.1 implies that abelian varieties with few endomorphism are more likely to be cyclic. The group structure of an abelian variety is not necessarily determined by its endomorphism ring, but from Lemma 2.1 it follows that the property of being cyclic or not depends on its endomorphism ring, and thus, it is an invariant of it.

We say that A is *cyclic* if the group $A(\mathbb{F}_q)$ is cyclic. Counting cyclic varieties in a given isogeny class is the same as counting some fractional ideals in the center of $\mathrm{End}^0_{\mathbb{F}_q}(A)$. In this paper we will focus on *cyclic* isogeny classes, *i.e.*, those that contain only cyclic varieties. We have the following criterion:

Theorem 2.2. *Let $\mathcal{A}$ be a g-dimensional $\mathbb{F}_q$-isogeny class of abelian varieties corresponding to the Weil polynomial $f_{\mathcal{A}}(t)$. Then $\mathcal{A}$ is cyclic if and only if $f'_{\mathcal{A}}(1)$ is coprime with $\widehat{f_{\mathcal{A}}(1)}$.*

This can be proved by using Rybakov's Theorem ([14]) when $\mathrm{End}^0_{\mathbb{F}_q}(A)$ is commutative, and we shall prove it using the Lemma 2.1 in the general case. Note that we do not require $\mathcal{A}$ to be simple.

Every Weil polynomial has the form

$$f_{\mathcal{A}}(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + a_{g-1} q t^{g-1} + \ldots a_1 q^{g-1} t + q^g \in \mathbb{Z}[t], \tag{2}$$

and for simplicity, we write it as $f_{q,(a_1,\ldots,a_g)}(t)$.

Denote by $\mathcal{S}^g(q)$ the set of g-dimensional isogeny classes $\mathcal{A}$ of abelian varieties defined over the finite field $\mathbb{F}_q$, and by $\mathcal{S}^g_{\mathfrak{c}}(q)$ the subset of cyclic isogeny classes. The size of $\mathcal{S}^g(q)$ is $c(g)(1 - 1/p)q^{g(g+1)/4}$, when q tends to infinity and $c(g)$ is a constant depending only on the dimension g (see [3] for details). We write $(a_1, \ldots, a_g) \in \mathcal{S}^g(q)$ if the polynomial $f_{q,(a_1,\ldots,a_g)}(t)$ defines such an isogeny class.

Our first approach is to fix a vector $\mathbf{a} = (a_1, \ldots, a_{g-1}) \in \mathbb{Z}^{g-1}$ of $g - 1$ integers, and define two sets *of possible values of* a_g:

$$I_{\mathbf{a}}(q) := \{z \in \mathbb{Z} | (a_1, \ldots, a_{g-1}, z) \in \mathcal{S}^g(q)\}, \tag{3}$$

$$I_{\mathbf{a},\mathfrak{c}}(q) := \{z \in \mathbb{Z} | (a_1, \ldots, a_{g-1}, z) \in \mathcal{S}^g_{\mathfrak{c}}(q)\}. \tag{4}$$

It is obvious that $I_{\mathbf{a}}(q)$ is finite and non empty from a certain value of $q = q(\mathbf{a})$. Fixing a prime p, we are interested on the proportion

$$r_{p,\mathbf{a}}(n) := \frac{\sum_{i=1}^n \# I_{\mathbf{a},\mathfrak{c}}(p^i)}{\sum_{i=1}^n \# I_{\mathbf{a}}(p^i)}, \tag{5}$$

when n tends to infinity.

Finally, we define the polynomial $h(X, \mathbf{a}) := gf_{X,(\mathbf{a},z)}(1) - f'_{X,(\mathbf{a},z)}(1)$ (in fact, it is independent of z), and we have

Theorem 2.3. *Given $\mathbf{a} \in \mathbb{Z}^{g-1}$ and a prime p, then*

$$\liminf r_{p,\mathbf{a}}(n) \geq 1 - \frac{p}{p-1}\left[\left(1 - \prod_{\ell \in \mathcal{P}(h(p,\mathbf{a}))}\left(1 - \frac{1}{\ell^2}\right)\right)\left(1 - \frac{1}{p^{g/2}}\right) + \frac{1}{p^{g/2}}\right]. \tag{6}$$

Remark 2.4. Note that the limit of $r_{p,\mathbf{a}}$ does not necessarily exist. Also, it is easy to see that if $p \gg 0$, this bound is approximately

$$\prod_{\ell \in \mathcal{P}(h(p,\mathbf{a}))}\left(1 - \frac{1}{\ell^2}\right),$$

which is greater than $1/\zeta(2) = 0.6\ldots$, where ζ is the Riemann zeta function.

Let us follow now a different approach by fixing a vector $\mathbf{b} = (b_1, \ldots, b_g) \in \mathbb{Z}^g$ of g integers, we want to study when $f_{q,\mathbf{b}}(t)$ defines a cyclic isogeny class over $\mathbb{F}_q$ when q varies over the power of primes. We consider this problem in two ways: (i)q varies over primes and (ii) we fix a prime p and q varies over the powers of p.

For our next result, we will need an extra hypothesis, which we make explicit as follows:

> **Hyp**($\mathbf{b}$): there exist integers $\eta(\mathbf{b}), t(\mathbf{b})$ and $s(\mathbf{b})$ with no common factor, such that the only possible divisors of $f_{q,\mathbf{b}}(1)$ and $f'_{q,\mathbf{b}}(1)$ are divisors of η and $tq + s$.

Remark 2.5. The key idea is that these values, in particular η, are independent of q. Such η can always be obtained by successive Euclidean division, since we can see f and f' as polynomials in $\mathbb{Q}[q]$; but it is not sure to have a linear polynomial in q, with the condition of no common factors. Observe that η can be chosen as a product of different prime numbers. For the 2-dimensional case, we will see in Section 4 that this hypothesis holds for a wide range of values of $\mathbf{b}$, and we will explicit them.

Then we are interested on the following proportions:

$$x_{\mathbf{b}}(n) = \frac{\#\{\ell \leq n \text{ prime} | \mathbf{b} \in \mathcal{S}^g_{\mathfrak{c}}(\ell)\}}{\#\{\ell \leq n \text{ prime} | \mathbf{b} \in \mathcal{S}^g(\ell)\}}, \tag{7}$$

$$y_{p,\mathbf{b}}(n) = \frac{\#\{i \leq n | \mathbf{b} \in \mathcal{S}^g_{\mathfrak{c}}(p^i)\}}{\#\{i \leq n | \mathbf{b} \in \mathcal{S}^g(p^i)\}}, \tag{8}$$

when n tends to infinity. Note that the above fractions are defined from a big enough n. Then our next result is

Theorem 2.6. *Given $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{Z}^g$ and a prime number $p > 2$ such that*

1. **Hyp**($\mathbf{b}_i$) *holds, with η, t and s given,*
2. *p doesn't divide the last coordinate of $\mathbf{b}_2$, and*
3. *the multiplicative group $(\mathbb{Z}/\eta(\mathbf{b}_2)\mathbb{Z})^*$ is generated by p.*

Then

$$1.\quad \liminf x_{\mathbf{b}_1}(n) \geq L_1 \qquad \textit{and,} \qquad 2.\quad \liminf y_{p,\mathbf{b}_2}(n) \geq L_2,$$

where

$$L_i = \prod_{\ell \in \mathcal{P}(\eta(\mathbf{b}_i)) \setminus \mathcal{P}(t(\mathbf{b}_i)s(\mathbf{b}_i))} \frac{\ell - 2}{\ell - 1}, \qquad i = 1, 2.$$

Remark 2.7. As we can see, this bound depends on the choice of (η, t, s). We can verify that if (η_1, t_1, s_1) and (η_2, t_2, s_2) verify $\mathbf{Hyp}(\mathbf{b})$ for some fixed $\mathbf{b}$, then $((\eta_1, \eta_2), t_1, s_1)$ also does. Also, if (η, t_1, s_1) and (η, t_2, s_2) verify $\mathbf{Hyp}(\mathbf{b})$, and if there exist a prime $\ell \in \mathcal{P}(t_2 s_2) \setminus \mathcal{P}(t_1 s_1)$ dividing η, then $(\eta/\ell, t_1\ell, s_1\ell)$ also verifies $\mathbf{Hyp}(\mathbf{b})$. This allows us to optimize the bound in that way. However, in Section 4 we will see with an example that Theorem 2.6 does not provide necessarily the best bound.

Example 2.8. As example, we discuss the case of elliptic curves. Here we have

$$f_{q,a}(1) = (1+a) + q \qquad \text{and} \qquad f'_{q,a}(1) = 2 + a,$$

thus, $\mathbf{Hyp}(a)$ holds for all values of a if we take

$$\begin{cases} \eta(a) = 2 + a, \\ t(a) = 1, \\ s(a) = 1 + a. \end{cases}$$

Also, since $\eta(a)$ and $s(a)$ are always coprimes, the bound for Theorem 2.6 takes the form

$$L = \prod_{\ell \in \mathcal{P}(2+a)} \frac{\ell - 2}{\ell - 1}.$$

Concerning Theorem 2.3, we have that $h(p, \mathbf{a}) = p - 1$, where $\mathbf{a}$ can be considered empty. This provides a complete answer to the fraction of cyclic isogeny classes defined over some finite extension of $\mathbb{F}_p$, and for $p \gg 0$, the bound takes the form

$$\prod_{\ell \in \mathcal{P}(p-1)} \left(1 - \frac{1}{\ell^2}\right).$$

To finish this example, let us say that the question

For which values of q, all isomorphism classes of EC defined over $\mathbb{F}_q$ are cyclic?

is answered in Theorem 4.1 in [19], and in view of Theorem 2.2, this is equivalent to

For which values of q, $(\widehat{f_{q,a}(1)}, f'_{q,a}(1)) = 1 \quad \forall a \in [-2\sqrt{q}, 2\sqrt{q}]$?

3. General case: proof of theorems

In this section we prove Theorems 2.2, 2.3 and 2.6.

Proof of Theorem 2.2:
First we consider the case when $\mathcal{A}$ is simple. For an abelian variety $A \in \mathcal{A}$, the center of its endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is isomorphic to the number field $K = \mathbb{Q}(\pi)$, where π is a root of $f_{\mathcal{A}}$ and represents the Frobenius endomorphism F. For every variety A in $\mathcal{A}$, $\mathrm{End}_{\mathbb{F}_q}(A) \cap K$ is an order in K (thus contained in $\mathcal{O}_K$), and $\mathcal{O}_K$ is the endomorphism ring for some $B \in \mathcal{A}$ by Theorem 3.13 in [22]. For any $x \in K$, we have that $x \in \mathcal{O}_K$ holds if and only if its (unitary) minimal polynomial has integer coefficients, that is, is an algebraic integer.

Denote by N the value $f_{\mathcal{A}}(1)$, then Lemma 2.1

$$A(\mathbb{F}_q) \text{ is not cyclic } \iff \exists \varphi \in \mathrm{End}_{\overline{\mathbb{F}}_q}(A),\ [N/\ell] = \varphi \circ (1-F) \text{ for some prime divisor } \ell | N$$

follows from the fact that $A(\mathbb{F}_q)$ is not cyclic if and only if $A(\mathbb{F}_q) = \ker(1-F) \subset \ker([N/\ell]) = A[N/\ell]$ for some $\ell | N$, since $1-F$ is separable. Since A is simple, if such φ exist, it must be in K: if $\psi \in \mathrm{End}_{\mathbb{F}_q}(A)$, multiplying the previous equation in both sides and subtracting them, we have $0 = (\varphi\psi - \psi\varphi) \circ (1-F)$, thus, φ commutes with ψ. Similarly, we can show that this endomorphism is defined over $\mathbb{F}_q$.

We consider the minimal polynomial $p_\ell(t)$ of $\frac{N}{\ell(1-\pi)}$. All non-leading coefficients of p_ℓ are of the form $\frac{N^{i-1}}{\ell^i}$ times an integer, except for the coefficient of t^{2g-1}, which equals $-\frac{f'(1)}{\ell}$, and that the constant term equals $\frac{N^{2g-1}}{\ell^{2g}}$.

If $\mathcal{A}$ is cyclic, then all elements of $\{\frac{N}{\ell(1-\pi)}, \ell | N\}$ are algebraic non integers: if not, for some ℓ, $\frac{N}{\ell(1-\pi)} \in \mathcal{O}_K$ and for some abelian variety B with $\mathrm{End}_{\mathbb{F}_q}(B) \cap K = \mathcal{O}_K$ we will have that $B(\mathbb{F}_q)$ is not cyclic. Therefore p_ℓ have some non integer coefficient, either $\ell \nmid f'(1)$, either $v_\ell(N) = 1$. In consequence, $gcd(\widehat{N}, f'(1)) = 1$.

If $gcd(\widehat{N}, f'(1)) = 1$, then for any $\ell | N$, either $(\ell, f'(1)) = 1$, or $v_\ell(N) = 1$. In both cases, p_ℓ have some non integer coefficient, and thus, $\frac{N}{\ell(1-\pi)} \notin \mathcal{O}_K$. This implies that, for all $A \in \mathcal{A}$, there is no $\varphi \in \mathrm{End}(A)$ with $\left[\frac{N}{\ell}\right] = \varphi \circ (1-F)$: if such φ exist, it has to be equal to $\frac{N}{\ell(1-\pi)}$, which is a contradiction.

Now we consider the general case. Then $\mathcal{A}$ is isogenous to a product $\prod \mathcal{A}_i$ of simple isogeny classes, and we have that $f_{\mathcal{A}}(t) = \prod f_i(t)$, where $f_i(t)$ is the characteristic polynomial of $\mathcal{A}_i$. Suppose $\mathcal{A}$ is not cyclic, we have two possibilities: (i) one of its components is not cyclic or (ii) $\exists \ell$ prime such that $\ell | (f_1(1), f_2(1))$ (WLOG). In (i), by the first part of the theorem, $(\widehat{f_1(1)}, f_1'(1)) > 1$ (WLOG), writing $f'_{\mathcal{A}}(t) = f_1'(t)\prod_{i>1} f_i(t) + f_1(t)(\prod_{i>1} f_i(t))'$ we have that $(\widehat{f_{\mathcal{A}}(1)}, f'_{\mathcal{A}}(1)) > 1$. In (ii), writing $f'_{\mathcal{A}}(t) = f_1'(t)f_2(t)\prod_{i>2} f_i(t) + f_1(t)f_2'(t)\prod_{i>2} f_i(t) + f_1(t)f_2(t)(\prod_{i>2} f_i(t))'$ we have that $(\widehat{f_{\mathcal{A}}(1)}, f'_{\mathcal{A}}(1)) > 1$. Suppose now that $\ell | (\widehat{f_{\mathcal{A}}(1)}, f'_{\mathcal{A}}(1))$, thus, $\ell^2 | f_{\mathcal{A}}(1)$ and $\ell | f'_{\mathcal{A}}(1)$. Again, we have two possibilities: (i) $\ell | f_1(1)$ and $\ell | \prod_{i>1} f_i(1)$ or, (ii) $\ell^2 | f_1(1)$ and $\ell \nmid \prod_{i>1} f_i(1)$. In (i), $\mathcal{A}$ is not cyclic. In (ii), writing $f'_{\mathcal{A}}(t) = f_1'(t)\prod_{i>1} f_i(t) + f_1(t)(\prod_{i>1} f_i(t))'$ we see that $\ell | f_1'(1)$, thus, $\mathcal{A}$ is not cyclic by the first part of the theorem. Theorem 2.2 is thus proved. □

Note that Lemma 3.3.1 in [3] implies that for fixed $\mathbf{a} \in \mathbb{Z}^{g-1}$, $f_{q,(\mathbf{a},z)}(t)$ always defines an ordinary isogeny class from a q big enough when $p \nmid z$, and they are almost all the isogeny classes. This will be important for the proofs of both theorems that follow, and it will be explained at beginning of the next proof.

Proof of Theorem 2.3:
From now on, $\mathbf{a}$ and p are fixed. For simplicity, we denote by N_i and S_i the integers $\#I_{\mathbf{a}}(p^i)$ and the sets of prime divisors of $h(p^i, \mathbf{a})$, with $S = S_1$, respectively. From a certain value of i, $I_{\mathbf{a}}(p^i)$ is a finite non-empty set of integers, thus we can take its maximum $\max(I_{\mathbf{a}}(p^i))$ and minimum $\min(I_{\mathbf{a}}(p^i))$ values, and we set $M_i = \max(I_{\mathbf{a}}(p^i)) - \min(I_{\mathbf{a}}(p^i))$. Also, we write $f_{i,z}(t)$ instead of $f_{p^i,(\mathbf{a},z)}(t)$.

From Weil's "Riemann Hypothesis", if $z \in I_{\mathbf{a}}(p^i)$, then $|z| \leq 2p^{ic}$, where we set $c = g/2$. For a big enough i, among the integers z between $-2p^{ic}$ and $2p^{ic}$, those such that $(z,p) = 1$ define an ordinary isogeny class (this follows from the inequality in Lemma 3.3.1 in [3]) and the proportion of such z defining non-ordinary isogeny classes is less than $1/p^{i/2}$ (this follows from Proposition 3.1.3 in [3]). Then we deduce that

$$N_i/M_i \to \frac{p-1}{p} \qquad \text{and} \qquad M_i/4p^{ic} \to 1 \qquad \text{when } i \to \infty.$$

In order to take advantage of Theorem 2.2, the following elementary lemma allows us to identify the primes that can simultaneously divide the arithmetic progressions $f_{i,z}(1)$ and $f'_{i,z}(1)$ (as sequences on z):

Lemma 3.1. *Let x_n and y_n be two arithmetic progressions of difference d_x and d_y respectively, and let ℓ be a prime such that $d_x \not\equiv 0 \pmod{\ell}$. Then $\ell | (x_i, y_i)$ for some i if and only if $d_x y_j \equiv d_y x_j \pmod{\ell}$ for some j.*

Proof. First, observe that if the congruence $d_x y_j \equiv d_y x_j \pmod{\ell}$ is verified for some j, then it verifies for all i:

$$\begin{aligned} d_x y_i &\equiv d_x(y_i - y_j + y_j) \pmod{\ell} \\ &\equiv d_x y_j + d_x d_y (i-j) \\ &\equiv d_y x_j + d_x d_y (i-j) \\ &\equiv d_y (x_j + d_x (i-j)) \\ &\equiv d_y x_i \end{aligned}$$

Suppose now that $d_x y_j \equiv d_y x_j \pmod{\ell}$, then we have to solve the system

$$\begin{cases} x_0 + d_x i \equiv 0 \pmod{\ell} \\ y_0 + d_y i \equiv 0 \pmod{\ell} \end{cases}$$

We get that $i \equiv -x_0 d_x^{-1}$, and thus, $y_0 + d_y(-x_0 d_x^{-1}) \equiv y_0 - (d_y x_0) d_x^{-1} \equiv y_0 - d_x y_0 d_x^{-1} \equiv 0 \pmod{\ell}$. □

We apply the lemma to the sequences $f_{i,z}(1)$ and $f'_{i,z}(1)$, hence the modular condition becomes $g(f_{i,z}(1) - z) \equiv f'_{i,z}(1) - gz \pmod{\ell}$ and thus, from the definition of $h(p^i, \mathbf{a})$ only the primes in S_i can simultaneously divide $f_{i,z}(1)$ and $f'_{i,z}(1)$.

For an integer n and a finite set of integers Z, let denote

$$\begin{aligned} \sigma(n, Z) &= \sum_{i \geq 1} (-1)^{i+1} \sum_{R \subset Z, |R| = i} \left\lceil \frac{n}{\prod_{x \in R} x^2} \right\rceil, \\ \xi(Z) &= \sum_{i \geq 1} (-1)^{i+1} \sum_{R \subset Z, |R| = i} \frac{1}{\prod_{x \in R} x^2} = 1 - \prod_{x \in Z} \left(1 - \frac{1}{x^2}\right). \end{aligned}$$

Observe that ξ can be defined for infinite subsets of $\mathcal{P}$ since $\xi(\mathcal{P})$ converges and, if $Z \subseteq Z'$, $\xi(Z) \leq \xi(Z')$.

We will study the sequence $1 - r_{p,\mathbf{a}}$, *i.e.*, we will count non cyclic isogeny classes using the lemma above. Note that if $\ell^2 | f_{i,z}(1)$, then $\ell^2 \nmid f_{i,z+\ell}(1)$, thus after applying the inclusion-exclusion principle, we can see that the number $\#(I_{\mathbf{a}}(p^i) \setminus I_{\mathbf{a},\mathfrak{c}}(p^i))$ of non cyclic isogeny classes for p^i is at most $\sigma(M_i, S_i)$.

For every finite set T of prime numbers that does not divide $h(p, \mathbf{a})$ ($T \subset \mathcal{P} \setminus S_1$ finite), we consider the polynomial

$$g(X) = m(g)X + 1, \quad m(g) = \left(\prod_{\ell \in T} \ell - 1 \right),$$

thus, $h(p^i, \mathbf{a}) \equiv h(p, \mathbf{a}) \not\equiv 0 \pmod{\ell}$ for all $\ell \in T$ and for all $i \in g(\mathbb{N})$, hence $S_i \subset \mathcal{P} \setminus T$ for all $i \in g(\mathbb{N})$.

We get

$$\begin{aligned}
1 - r_{p,\mathbf{a}}(n) &\leq \frac{\sum \sigma(M_i, S_i)}{\sum N_i} \leq \frac{\sum\limits_{i \notin g(\mathbb{N})} M_i + \sum\limits_{i \in g(\mathbb{N})} \sigma(M_i, S_i)}{\sum N_i} \\
&\approx \frac{p}{p-1} \frac{\sum\limits_{i \notin g(\mathbb{N})} M_i + \sum\limits_{i \in g(\mathbb{N})} \sigma(M_i, S_i)}{\sum M_i} \\
&\approx \frac{p}{p-1} \frac{\sum\limits_{i \notin g(\mathbb{N})} M_i + \sum\limits_{i \in g(\mathbb{N})} M_i \xi(S_i)}{\sum M_i} \\
&\leq \frac{p}{p-1} \frac{\sum\limits_{i \notin g(\mathbb{N})} M_i + \sum\limits_{i \in g(\mathbb{N})} M_i \xi(\mathcal{P} \setminus T)}{\sum M_i} \\
&\approx \frac{p}{p-1} \frac{\sum\limits_{i \notin g(\mathbb{N})} (p^c)^i + \xi(\mathcal{P} \setminus T) \sum\limits_{i \in g(\mathbb{N})} (p^c)^i}{\sum (p^c)^i}
\end{aligned}$$

where all the sums are taken over $1 \leq i \leq n$ and $\approx$ means that both sequences have the same superior limit. The last sequence converges to

$$\frac{p}{p-1}\left[1 + (\xi(\mathcal{P} \setminus T) - 1)\frac{p^{cm(g)}(p^c - 1)}{p^{c(m(g)+1)} - 1}\right].$$

As we have the previous reasoning for all finite set T disjoint to S, thus,

$$\limsup(1 - r_{p,\mathbf{a}}(n)) \leq \frac{p}{p-1}\left[1 + (\xi(S) - 1)(1 - \frac{1}{p^c})\right] = \frac{p}{p-1}\left[\xi(S)\left(1 - \frac{1}{p^c}\right) + \frac{1}{p^c}\right].$$

Finally

$$\liminf r_{p,\mathbf{a}} \geq 1 - \frac{p}{p-1}\left[\xi(S)\left(1 - \frac{1}{p^c}\right) + \frac{1}{p^c}\right].$$

That finish the proof of Theorem 2.3. □

Proof of Theorem 2.6:
We write q for ℓ varying (i) over the primes or (ii) over powers p^i when i varies over positive integers.

As a consequence of Dirichlet's Theorem or Theorem's hypothesis, the values of q are (asymptotically) evenly distributed among the invertible congruence classes modulo η, when q varies according to (i) or (ii), respectively.

Set $\mathrm{j}(q) = tq + s$, then, by **Hyp**, the condition $(\mathrm{j}, \eta) = 1$ would imply that $\mathbf{b}_i \in \mathcal{S}^g_{\mathfrak{c}}(q)$, from a certain value of q when $f_{q,\mathbf{b}_i}(t)$ defines an isogeny class.

Observe that $(\mathrm{j}, \eta) = 1$ if and only if j is invertible in $\mathbb{Z}/\eta\mathbb{Z}$; then we conclude by using the following lemma. □

Lemma 3.2. *Let t, s and n be integers with no common factor, then*

$$\frac{\#\{x \in (\mathbb{Z}/n\mathbb{Z})^* | tx + s \in (\mathbb{Z}/n\mathbb{Z})^*\}}{\#(\mathbb{Z}/n\mathbb{Z})^*} = \prod_{\ell \in \mathcal{P}(n) \setminus \mathcal{P}(ts)} \frac{\ell - 2}{\ell - 1}.$$

Proof. Take an $\ell \in \mathcal{P}(n)$ and set $m = \ell^{v_\ell(n)}$, we have that $\#(\mathbb{Z}/m\mathbb{Z})^* = m - m/\ell$. If $\ell \nmid ts$ we have that $\#\{x \in (\mathbb{Z}/m\mathbb{Z})^* | tx+s \in (\mathbb{Z}/m\mathbb{Z})^*\} = m-2m/\ell$. If $\ell | ts$, for all $x \in (\mathbb{Z}/m\mathbb{Z})^*$ we have that $tx+s \in (\mathbb{Z}/m\mathbb{Z})^*$. We conclude by using the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \prod_{\ell|n} \mathbb{Z}/\ell^{v_\ell(n)}\mathbb{Z}$. □

4. The case of Abelian Surfaces

In this section we consider the case of abelian surfaces, where the characteristic polynomial takes the form

$$f_{\mathcal{A}}(t) = t^4 + at^3 + bt^2 + aqt + q^2,$$

thus, we have $\mathbf{b} = (a, b)$.

4.1. Theorems applied to Surfaces.

In order to apply Theorem 2.6 to surfaces, we need to verify **Hyp**(**b**); and this is a consequence of the proposition below and the conditions on **b** that follow:

Proposition 4.1. *Let a, b and q be integers, then the common divisors of*

$$N = 1 + a(q+1) + b + q^2 \text{ and}$$
$$J = 4 + a(q+3) + 2b$$

are divisors of $\eta(a,b) := (2a+b+2)(a^2-4a+4b-16)$.

Proof. Let ℓ be a prime divisor of N and J, then it divides

$$(q+3)N - (q+1)J = (q-1)(q^2+4q-1+b) \text{ and}$$
$$2N - J = (q-1)(2q+2+a).$$

If ℓ divides $q-1$, then $N = q^2 - 1 + a(q-1) + 2a + b + 2 \equiv 2a + b + 2 (\mod \ell)$. We set

$$\gamma = q^2 + 4q - 1 + b \text{ and}$$
$$\theta = 2q + 2 + a.$$

So, if ℓ doesn't divide $q-1$, then it divides γ and θ, and we have

$$4\gamma = \theta(2q + 6 - a) + (a^2 - 4a + 4b - 16).$$

Finally, the possible common divisors are the divisors of $(2a+b+2)(a^2-4a+4b-16)$. □

We have $\eta(a,b)$ as defined in the proposition and clearly $f'(1) = aq + 4 + 3a + 2b$, thus, we can take

$$\begin{cases} \eta(a,b) = (2a+b+2)(a^2-4a+4b-16), \\ t(a,b) = a, \\ s(a,b) = 4 + 3a + 2b. \end{cases}$$

To finish, and in order to have the condition of no common divisor (with the values previously chosen), the integers in $\mathbf{b} = (a, b)$ must verify:

$$(a, b+2) = 1, \qquad \text{and} \qquad a \equiv 1 \pmod 2.$$

A priori these values are not optimal in the sense of Remark 2.7, and as mentioned previously, Theorem 2.6 does not necessarily provide the optimal bound. For example, observe that $\mathbf{Hyp}(0,0)$ holds with $\eta = 2, t = 1, s = 1$, in which case $L_1 = L_2 = 0$, which are clearly very bad bounds. But by applying directly Theorem 2.2 we can have better bounds, first we have:

$$f_{q,\mathbf{b}}(1) = 1 + q^2 = (q^2 - 1) + 2 \qquad \text{and} \qquad f'_{q,\mathbf{b}}(1) = 4,$$

thus, $f_{q,\mathbf{b}}(1)$ is equivalent to 1 or 2 modulo 4, depending if p equals 2 or not, respectively, thus $L_1 = L_2 = 1$. This is because Theorem 2.6 uses only a weak result:

$$(f(1), f'(1)) = 1 \qquad \Rightarrow \qquad \text{cyclicity},$$

and not the stronger equivalence from Theorem 2.2:

$$(\widehat{f(1)}, f'(1)) = 1 \qquad \Leftrightarrow \qquad \text{cyclicity}.$$

Concerning Theorem 2.3 applied to abelian surfaces, this provides the fraction of cyclic isogeny classes with a fixed trace of Frobenius a and a fixed base field characteristic p. We have that $h(p,a) = (p-1)[2(p+1)+a]$. Thus, for $a = -4$ and a Fermat prime p, the lower bound for Theorem 2.3 is 0.75 and we cannot improve it. Even for primes of form $2\ell + 1$ (with $\ell \gg 0$ a prime number) we have a good bound, around 0.75.

4.2. Maximal Surfaces

Now, let us discuss about the other topic mentioned in the Introduction, varieties with many rational points. Rück's theorem [13] describes polynomials that occurs as Weil polynomials for abelian surfaces with endomorphism algebra being a field:

Theorem 4.2 (Rück)**.** *The set of $f_A(t)$ for all abelian varieties A over $\mathbb{F}_q$ of dimension 2 whose algebra $\mathrm{End}(A) \otimes \mathbb{Q}$ is a field is equal to the set of polynomials $f(t) = t^4 + at^3 + bt^2 + aqt + q^2$ where the integers a and b satisfy the conditions*

1. $|a| < 4\sqrt{q}, \quad 2|a|\sqrt{q} - 2q < b < a^2/4 + 2q,$
2. $\Delta = a^2 - 4b + 8q$ *is not a square in* $\mathbb{Z}$*, and*
3. *either*
   (a) $v_p(a) = 0, \quad v_p(b) \geq r/2$ *and* $(b + 2q)^2 - 4qa^2$ *is not a square in* $\mathbb{Z}_p$*,*
   (b) $v_p(b) = 0$*, or*
   (c) $v_p(a) \geq r/2, v_p(b) \geq r$*, and* $f(t)$ *has no root in* $\mathbb{Z}_p$*.*

Concerning this type of isogeny classes, we have the following result

Theorem 4.3. *Let $q = p^r$ with r even. Consider the $\mathbb{F}_q$-isogeny classes $\mathcal{A}$ of abelian surfaces with $\mathrm{End}^0_{\mathbb{F}_q}(\mathcal{A})$ being a field. Then the isogeny class with maximal number of rational points among such classes is ordinary and cyclic, and corresponds to the Weil polynomial*

$$f(t) = t^4 + at^3 + bt^2 + aqt + q^2, \quad \text{where} \quad a = 4\sqrt{q} - 3 \quad \text{and} \quad b = 6q - 6\sqrt{q} + 1.$$

Proof. For a fixed q, the number of rational points increases with a and b. From the conditions of Rück's Theorem we have that the biggest possible values are $a = 4\sqrt{q} - 3$ and $b = 6q - 6\sqrt{q} + 1$ with $\Delta = 5$, and the ordinariness is clear.

Then we have

$$f(1) = -1 - 2\sqrt{q} + 3q + 4(\sqrt{q})^3 + q^2 \text{ and}$$
$$f'(1) = -3 + 9q + 4(\sqrt{q})^3$$

Writing $f(1)$ and $f'(1)$ as functions N and j of $x = \sqrt{q}$, respectively, we see that

$$N(x) = x^4 + 4x^3 + 3x^2 - 2x - 1, \qquad \mathrm{j}(x) = 4x^3 + 9x^2 - 3,$$

and thus,

$$(14x^3 + 49x^2 + 28x - 14)\mathrm{j}(x) - (56x^2 + 98x - 7)N(x) = 35 = 5 \cdot 7$$

Finally, we can see case by case, that for $\ell \in \{5, 7\}$ we cannot have that $\ell | \mathrm{j}(x)$ and $\ell^2 | N(x)$ simultaneously:

- for $\ell = 5$,

$x \pmod 5$	0	1	2	3	4
$\mathrm{j} \pmod 5$	2	0	0	1	2

$x \pmod{25}$	1	2	6	7	11	12	16	17	21	22
$N \pmod{25}$	5	5	5	5	5	5	5	5	5	5

- for $\ell = 7$,

$x \pmod 7$	0	1	2	3	4	5	6
$\mathrm{j} \pmod 7$	4	5	3	1	2	2	4

□

Surfaces having more number of rational points N than those considered in Theorem 4.3 are only (in decreasing order of N):

$$E_{max}^2, \quad E_{max} \times E_{max-1}, \quad E_{max} \times E_{max-2}, \quad E_{max-1}^2 \quad \text{and} \quad E_{max-1} \times E_{max-2},$$

where E_{max}, E_{max-1} and E_{max-2} are the elliptic curves defined by its Frobenius traces $2\sqrt{q}, 2\sqrt{q} - 1$ and $2\sqrt{q} - 2$, respectively. We can easily check, by using Theorem 2.2, that E_{max} is always not cyclic, E_{max-2} is always cyclic, and E_{max-1} is cyclic or not, depending on $q \equiv 0, 1 \pmod 3$ or $q \equiv 2 \pmod 3$, respectively (since 3 is the only possible prime divisor of $f(1)$ and $f'(1)$); thus, the cyclicity of $E_{max-1} \times E_{max-2}$ depends only on the cyclicity of E_{max-1}, since the cardinalities of E_{max-1} and E_{max-2} are relatively prime.

On the other hand, note that for $q = 23^3$ the ordinary class with maximal number of rational points, among the classes considered in Theorem 4.3, is given by

$$f(t) = t^4 + 438t^3 + 72293t^2 + 438(23^3)t + 23^6$$

and is not cyclic since $7 | f'(1)$ and $49 | f(1)$, so Theorem 4.3 holds only for even powers.

4.3. Families of cyclic isogeny classes

We finish this section by giving two sequences of cyclic isogeny classes of abelian surfaces in Proposition 4.4 and 4.5. Basically, we get the cyclicity of these families by choosing appropriate values of q and $\mathbf{b}$.

Proposition 4.4. *Given an integer b and a power of a prime $q = p^r > 4$, such that:*

1. $p \nmid b$
2. $8\sqrt{q} - 4q \leq b \leq 4$,
3. $N_0 = b - 3 - 2q + q^2$ *is coprime with* $N_0' = 2(b-4)$

Let be $s = \prod_{\ell \in \mathcal{P}(N_0')} (\ell - 1)$. *Then for* $i \in \mathbb{Z}_{\geq 0}$

$$f_i(t) = t^4 - 4t^3 + b_i t^2 - 4q_i t + q_i^2, \quad \text{where} \quad q_i = p^{r+is} \quad \text{and} \quad b_i = b + 2q_i,$$

defines a ordinary cyclic isogeny class $\mathcal{A}_i$ of abelian surfaces over $\mathbb{F}_{q^i}$.

Proof. Note that $f_i(t) = f_{q_i,(-4,b_i)}(t)$. Every f_i defines an ordinary isogeny class of abelian surfaces since $p \nmid b_i$, and f_i is a Weil polynomial since

$$8\sqrt{q}p^{is/2} - 4qp^{is} \leq 8\sqrt{q} - 4q \leq b \qquad \Rightarrow \qquad 8\sqrt{q_i} - 2q_i \leq b + 2q_i = b_i$$
$$b_i = b + 2q_i \leq 4 + 2q_i = \frac{(-4)^2}{4} + 2q_i.$$

Observe that $f'_{q_i,(-4,b_i)}(1) = 4 - 4(q_i + 3) + 2(b + 2q_i) = N_0' = f'_{q,(-4,b)}(1)$. Also, we have that

$$f_{i+1}(1) - f_i(1) = (p^s - 1)[p^{2(r+is)}(p^s + 1) + 2p^{r+is}].$$

Thus, $(f_i(1), N_0') = 1$ implies $(f_{i+1}(1), N_0') = 1$, then if $\mathcal{A}_i$ is cyclic, $\mathcal{A}_{i+1}$ is cyclic as well. We conclude by using the theorem's hypothesis. □

It is not hard to find values (q, b) verifying the last hypothesis. Moreover, for a fixed prime p, there are infinite many pairs (r, b) such that (p^r, b) verifies it.

Proposition 4.5. *Given an integer b and an odd prime $p > b + 2$ such that $b \not\equiv 2 \pmod 4$ and*

$$\exists r \geq 1, (p^{2r} - 1, b + 2) = 1,$$

then for every $i \geq 0$,

$$f_i(t) = t^4 + bt^2 + q_i^2$$

defines an ordinary cyclic isogeny class $\mathcal{A}_i$ of abelian surfaces over $\mathbb{F}_{q^i}$, where $q_i = p^{r+is}$ and

$$s = \prod_{\ell \in \mathcal{P}(b+2)} (\ell - 1).$$

Proof. It is easy to check that $f_i(t)$ is a Weil polynomial and it defines an ordinary isogeny class since $p > b$. Put

$$c = \prod_{\ell \in \mathcal{P}(b+2)} \ell,$$

We have

$$f_i(1) = p^{2(r+is)} - 1 + (b+2),\ i \in \mathbb{Z}_{\geq 0}.$$

Observe that $f_i(t) = f_{q_i,(0,b)}(t)$ and $f_i'(1) = 2(b+2)$. For $\mathcal{A}_i$ to be cyclic it is enough to have $(f_i(1), 2(b+2)) = 1$, and since $f_i(1) \equiv b+2 \not\equiv 0 \pmod 4$, it is enough to have $(f_i(1), b+2) = (f_i(1), c) = 1$. The last statement is true since by hypothesis $(f_0(1), c) = 1$ and since c divides the difference $f_{i+1}(1) - f_i(1) = p^{2(r+is)}(p^s+1)(p^s-1)$ (using Fermat's little theorem). □

For a fixed p, big enough, take a prime ℓ such that $2 < \ell < p$ and $\ell \nmid p^2 - 1$, then set $b = \ell - 2$. This gives b and p satisfying the proposition hypothesis.

Acknowledgement

I would like to thank my advisor Serge Vlăduţ for very fruitful discussions and for his very useful comments and suggestions. I would like to thank also the anonymous reviewers and the editor for their helpful remarks.

References

[1] W. D. Banks, F. Pappalardi, and I. E. Shparlinski, *On group structures realized by elliptic curves over arbitrary finite fields*, Experimental Mathematics, 21 (2012), pp. 11–25.

[2] C. David, D. Garton, Z. Scherr, A. Shankar, E. Smith, and L. Thompson, *Abelian surfaces over finite fields with prescribed groups*, Bulletin of the London Mathematical Society, 46 (2014), pp. 779–792.

[3] S. A. DiPippo and E. W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, Journal of Number Theory, 73 (1998), pp. 426 – 450.

[4] S. Galbraith and A. Menezes, *Algebraic curves and cryptography*, Finite Fields and Their Applications, 11 (2005), pp. 544 – 577. Ten Year Anniversary Edition!

[5] V. D. Goppa, *Algebraico-geometric codes*, Mathematics of the USSR-Izvestiya, 21 (1983), pp. 75–91.

[6] B. S. Kaliski, *One-way permutations on elliptic curves*, Journal of Cryptology, 3 (1991), pp. 187–199.

[7] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of computation, 48 (1987), pp. 203–209.

[8] F. Luca and I. E. Shparlinski, *On the exponent of the group of points on elliptic curves in extension fields*, International Mathematics Research Notices, 2005 (2005), pp. 1391–1409.

[9] F. Morain, *Building cyclic elliptic curves modulo large primes*, in Advances in Cryptology — EUROCRYPT '91, D. W. Davies, ed., Berlin, Heidelberg, 1991, Springer Berlin Heidelberg, pp. 328–336.

[10] D. Mumford, *Abelian varieties*, vol. 5 of Tata Institute of fundamental research studies in mathematics, Oxford University Press, 1970.

[11] R. Murty and I. Shparlinski, *Group Structure Of Elliptic Curves Over Finite Fields And Applications*, Springer Netherlands, Dordrecht, 2007, pp. 167–194.

[12] H.-G. Rück, *A note on elliptic curves over finite fields*, Mathematics of Computation, 49 (1987), pp. 301–304.

[13] ——, *Abelian surfaces and jacobian varieties over finite fields*, Compositio Mathematica, 76 (1990), pp. 351–366.

[14] S. Rybakov, *The groups of points on abelian varieties over finite fields*, Central European Journal of Mathematics, 8 (2010), pp. 282–288.

[15] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, Series A, 46 (1987), pp. 183 – 211.

[16] I. E. Shparlinski, *Orders of points on elliptic curves*, in Affine algebraic geometry, vol. 369 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2005, pp. 245–251.

[17] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2 (1966), pp. 134–144.

[18] M. A. Tsfasman, *Group of points of an elliptic curve over a finite field*, Theory of numbers and its applications, Tbilisi, (1985), pp. 286–287.

[19] S. G. Vlăduţ, *Cyclicity statistics for elliptic curves over finite fields*, Finite Fields and Their Applications, 5 (1999), pp. 13 – 25.

[20] ——, *On the cyclicity of elliptic curves over finite field extensions*, Finite Fields and Their Applications, 5 (1999), pp. 354 – 363.

[21] J. F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France, 116 (1988), pp. 455–458.

[22] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure, 2 (1969), pp. 521–560.

[23] J. Xue and C.-F. Yu, *Counting abelian varieties over finite fields*, arXiv preprint arXiv:1801.00229, (2017).