Some arithmetic properties of Weil polynomials of the form $t^{2g} + at^g + q^g$

Alejandro J. Giangreco Maidana

Abstract. An isogeny class $\mathcal{A}$ of abelian varieties defined over a finite field is said to be *cyclic* if every variety in $\mathcal{A}$ has a cyclic group of rational points. In this paper we study the local cyclicity of Weil-central isogeny classes of abelian varieties, i.e. those with Weil polynomials of the form $f_{\mathcal{A}}(t) = t^{2g} + at^g + q^g$, as well as the local growth of the groups of rational points of the varieties in $\mathcal{A}$ after finite field extensions. We exploit the criterion: an isogeny class $\mathcal{A}$ with Weil polynomial f is cyclic if and only if $f'(1)$ is prime with $f(1)$ divided by its radical.

Contents

1 Introduction

In this paper we study abelian varieties defined over finite fields with a cyclic group of rational points, and "cyclic base field extensions". This subject is motivated by both applications and theory.

- Finite subgroups of abelian varieties over finite fields are suitable for multiple applications. Cyclic subgroups of the group of rational points are used, for example, in cryptography, where the discrete logarithm problem is exploited. Abelian varieties can be very abstract objects. Jacobians of algebraic curves are abelian varieties and they are more tractable for application purposes.

- The statistics on cyclic varieties are related to Cohen-Lenstra heuristics (see [1]), which, roughly speaking, states that random abelian groups tend to be cyclic. Historically, the question of cyclicity arose in the context of the conjectures of Lang and Trotter (see [7]): given an elliptic curve defined over the rational numbers, we are interested in the set of primes such that the reduction is a cyclic elliptic curve. This question was studied also by Serre, Gupta, and Murty. Generalizations to higher dimensions were also done.

We restrict our study to abelian varieties with Weil polynomial that have the form $t^{2g} + at^g + q^g$. This includes elliptic curves, widely used in cryptography, such as isogeny-based cryptography. It also includes abelian surfaces with zero trace, "almost all" of them being isogenous to a principally polarizable abelian surface and to a Jacobian of a genus 2 curve.

This leads to give the following:

Definition 1.1. Given an abelian variety A defined over a finite field k, an isogeny class $\mathcal{A}$ of abelian varieties defined over k and a rational prime ℓ, we say that

1. A is **cyclic** if its group $A(k)$ of rational points is cyclic;

2. A is **ℓ-cyclic** if the ℓ-primary component $A(k)_\ell$ of its group $A(k)$ of rational points is cyclic;

3. $\mathcal{A}$ is **cyclic** if the abelian variety A is cyclic for all $A \in \mathcal{A}$;

4. $\mathcal{A}$ is **ℓ-cyclic** if the abelian variety A is ℓ-cyclic for all $A \in \mathcal{A}$.

This paper concerns the cyclicity of isogeny classes. The Honda–Tate theory simplifies the study of isogeny classes by studying their Weil polynomials. Moreover, it is easy to verify the cyclicity of an isogeny class $\mathcal{A}$ given its Weil polynomial $f_\mathcal{A}$. Let $\widehat{n}$ denote the ratio of an integer n to its radical, then, the cyclicity criterion is stated as follows.

Theorem 1.2 (A. Giangreco, 2019, [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 is in fact a local criterion (see Section 3.3) that can be easily deduced from the proof of Theorem 1.2. Asymptotic results about the cyclicity of abelian varieties were found in [3]. Studying abelian varieties in all their generality is very complicated, so we will focus on the following family.

Definition 1.3. An isogeny class $\mathcal{A}$ of g-dimensional abelian varieties defined over the finite field $\mathbb{F}_q$ is said to be **Weil-central** if its Weil polynomial has the form

$$f_{\mathcal{A}}(t) = t^{2g} + at^g + q^g.$$

In this paper we study the local cyclicity of Weil-central isogeny classes after base field extension as well as the local growth of their group of rational points. Given an abelian variety A defined over the finite field $\mathbb{F}_q$ with q elements, and belonging to an isogeny class $\mathcal{A}$, we denote by $\mathcal{A}_n$ the $\mathbb{F}_{q^n}$-isogeny class of A. For any prime number ℓ, let $v_\ell(\cdot)$ be the usual ℓ-adic valuation over the rational numbers. Thus, for an ℓ-cyclic isogeny class $\mathcal{A}$ we are interested in the following sets:

$$\mathfrak{g}_\ell(\mathcal{A}) := \{n \in \mathbb{N} : \ v_\ell(f_{\mathcal{A}_n}(1)) > v_\ell(f_{\mathcal{A}}(1))\} \cup \{1\}, \text{ and,}$$
$$\mathfrak{c}_\ell(\mathcal{A}) := \{n \in \mathbb{N} : \ \mathcal{A}_n \text{ is } \ell\text{-cyclic and } v_\ell(f_{\mathcal{A}_n}(1)) > v_\ell(f_{\mathcal{A}}(1))\} \cup \{1\}.$$

The first set gives the extensions for which the ℓ-primary component of the group of rational points is strictly bigger than the one over the base field. The second set gives the cyclic behavior of the ℓ-component after such finite field extensions. Observe that we have

$$\mathfrak{c}_\ell(\mathcal{A}) = \mathfrak{g}_\ell(\mathcal{A}) \setminus \{n \in \mathbb{N} : \ \mathcal{A}_n \text{ is not } \ell\text{-cyclic}\}.$$

For an integer z we denote by $\omega_\ell(z)$ the order of z in the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^\times$, i.e. the smallest integer m such that $z^m \equiv 1 \pmod{\ell}$. Then, our main result is stated as follows.

Theorem 1.4. *Let ℓ be a prime and $\mathcal{A}$ be an ℓ-cyclic Weil-central isogeny class of ordinary abelian varieties of dimension g defined over $\mathbb{F}_q$. Suppose that ℓ does not divide $g(q^g - 1)$. Let $S_{g,\ell}$ be the set of positive odd multiples of ℓ which are coprime with g. Then, provided that $v_\ell(f_{\mathcal{A}}(1)) \geq 1$, the set $\mathfrak{g}_\ell(\mathcal{A})$ contains $S_{g,\ell}$ and the set $\mathfrak{c}_\ell(\mathcal{A})$ contains the numbers in $S_{g,\ell}$ which are not divisible by $\omega_\ell(q^g)$.*

Remark 1.5. From Lemma 3.5 about the cyclicity, it follows that $v_\ell(f_{\mathcal{A}}(1)) \geq 2$ implies that ℓ does not divide $q^g - 1$, provided that the cyclicity hypothesis of Theorem 1.4 holds.

Organization of the paper

In Section 2 we recall some generalities about abelian varieties. Section 3 is devoted to the proof of Theorem 1.4. It will be proved in different lemmas that can be useful by themselves. We first study (Lemma 3.1) for which extensions a Weil-central isogeny class "remains" Weil-central. Then we study in Lemma 3.3 the growth behavior and we prove the assertion of Theorem 1.4 about the set $\mathfrak{g}_\ell(\mathcal{A})$. Finally, we study the cyclicity and prove, as a consequence of Corollary 3.6, the assertion of Theorem 1.4 about the set $\mathfrak{c}_\ell(\mathcal{A})$. We discuss some examples in Section 4.

2 Generalities on abelian varieties

We refer the reader to [9] for the general theory of abelian varieties, and to [13] for abelian varieties over finite fields.

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. The set $A(k)$ of rational points of A is a finite abelian group. It is the kernel of the endomorphism $1 - F$, where F is the well known Frobenius endomorphism of A. Multiplication by an integer n is a group homomorphism whose kernel A_n is a finite group scheme of rank n^{2g}. The group structure of the groups of points over $\overline{k}$ is known:

$$
\begin{aligned}
A_n(\overline{k}) &\cong (\mathbb{Z}/n\mathbb{Z})^{2g}, & p \nmid n \\
A_p(\overline{k}) &\cong (\mathbb{Z}/p\mathbb{Z})^i, & 0 \leq i \leq g.
\end{aligned}
\tag{1}
$$

For a fixed prime ℓ ($\neq p$), the A_{ℓ^n} form an inverse system under $A_{n+1} \xrightarrow{\ell} A_n$, and we can define *the Tate module* $T_\ell(A)$ by its inverse limit $\varprojlim A_{\ell^n}(\overline{k})$. This is a free $\mathbb{Z}_\ell$-module of rank $2g$ and the absolute Galois $\mathcal{G}$ group of $\overline{k}$ over k operates on it by $\mathbb{Z}_\ell$-linear maps.

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 (also called *characteristic polynomial of* A). The Weil polynomial is independent of the choice of the prime ℓ. Tate proved in [10] that a k-isogeny class $\mathcal{A}$ is determined by the Weil polynomial f_A of any $A \in \mathcal{A}$, i.e. two abelian varieties A and B defined over k are isogenous (over k) if and only if $f_A = f_B$. Thus the notation $f_{\mathcal{A}}$ is justified. If $\mathcal{A}$ is simple, $f_{\mathcal{A}}(t) = h_{\mathcal{A}}(t)^e$ for some irreducible polynomial $h_{\mathcal{A}}$.

Weil proved that all of the roots of a Weil polynomial have absolute value $\sqrt{q}$ (they are called q-*Weil numbers*). Thus, the Weil polynomial of an isogeny class $\mathcal{A}$ has the general form

$$
f_{\mathcal{A}}(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + a_{g-1} q t^{g-1} + \cdots + a_1 q^{g-1} t + q^g.
$$

The cardinality of the group $A(k)$ of rational points of A equals $f_{\mathcal{A}}(1)$, and thus it is an invariant of the isogeny class. An abelian variety A is said to be *ordinary* if it has a maximal p-rank. This is equivalent of having the central term a_g of its Weil polynomial coprime with p. Thus, ordinariness it is also an invariant of the isogeny class.

Let $\{\alpha_i\}_{i=1}^{2g}$ be the set of roots of the Weil polynomial of the abelian variety $A \in \mathcal{A}$ defined over $\mathbb{F}_q$. For a positive integer n, we denote by $\mathcal{A}_n$ the $\mathbb{F}_{q^n}$-isogeny class of the variety A as defined over $\mathbb{F}_{q^n}$. If the polynomial $\prod(t - \alpha_i^n)$ has no repeated roots, then it corresponds to the Weil polynomial of $\mathcal{A}_n$.

3 Weil-central isogeny classes

As we stated, we are interested in Weil-central isogeny classes of abelian varieties. They have a Weil polynomial as follows

$$
f_{\mathcal{A}}(t) = t^{2g} + a t^g + q^g.
\tag{2}
$$

Among these isogeny classes are those of elliptic curves and zero-trace abelian surfaces, with Weil polynomials $f_{\mathcal{E}}(t) = t^2 + at + q$ and $f_{\mathcal{S}}(t) = t^4 + at^2 + q^2$, respectively. Cyclicity of elliptic curves and their extensions were studied by Vlăduţ in [11] and [12].

The following facts motivate the study of such isogeny classes. We know from [4] that among Weil-central isogeny classes of abelian surfaces, only such with Weil polynomial $t^4 - qt^2 + q^2$, and $p \equiv 1 \pmod 3$ do not contain a principally polarizable variety. Also, from [5], very few do not contain the Jacobian of a 2-genus curve.

Note that in order that a polynomial of the form (2) to be a Weil polynomial, we need that $0 \leq\mid a \mid\leq 2\sqrt{q^g}$. Indeed, if not, the polynomial $x^2 + ax + q^g$ would have two different real roots, which would imply that (2) has complex roots of absolute value different than $\sqrt{q}$. This also implies that the real part of the roots of $x^2 + ax + q^g$ is exactly $-a/2$.

Notations. We denote simply by $(a, q)_g$ the Weil-central isogeny class $\mathcal{A}$ with Weil polynomial given by the expression (2) above. We denote by $N_{g,n}(a)$ the cardinalities of the groups of rational points of the varieties in $\mathcal{A}_n$, where $\mathcal{A}$ is defined by $(a, q)_g$. If $\mathcal{A}$ is clear from the context, we write $N_{g,n}$. We write N instead of $N_{g,1}$ and N_n instead of $N_{g,n}$ if the dimension g is clear from the context. We recall that $N_{g,n}(\mathcal{A}) = f_{\mathcal{A}_n}(1)$.

3.1 Weil polynomial after field extension

Our results on cyclicity and growth are for Weil-central isogeny classes. Thus, in this section we study which extensions $\mathcal{A}_n$ of a Weil-central isogeny class $\mathcal{A}$ are Weil-central as well. Lemma 3.1 below gives the answer and is from where the set $S_{g,\ell}$ of Theorem 1.4 contains only numbers which are coprime with g.

When dealing with cyclicity, it is natural to ask about the simplicity or not of the abelian variety. For example, in the case of a Weil-central isogeny class $\mathcal{A}$ of abelian surfaces, we know that $\mathcal{A}_n$ splits for n even (see [6, Theorem 6]). However, our results about Weil-central isogeny classes (as well as our results on cyclicity) are independent on the simplicity or not of the considered abelian variety.

Lemma 3.1. *Suppose the isogeny class $\mathcal{A}$ has Weil polynomial $f_{\mathcal{A}}(t) = t^{2g} + a_1 t^g + q^g$, with $\gcd(a_1, p) = 1$, i.e. it is an ordinary isogeny class. Then, its extensions $\mathcal{A}_n$ have Weil polynomials $f_{\mathcal{A}_n}(t) = t^{2g} + a_n t^g + q^{ng}$ for every n such that $\gcd(n, g) = 1$, where a_n is obtained recursively*

$$a_n = (-1)^n a_1^n - \sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n}{i} a_{n-2i} q^{gi}.$$

Proof. We first prove that if $\mathcal{R} = \{\alpha_1, \dots, \alpha_g, q/\alpha_1, \dots, q/\alpha_g\}$ is the set of roots of $f_{\mathcal{A}}$, then

$$\{\alpha_1^n, \dots, \alpha_g^n, (q/\alpha_1)^n, \dots, (q/\alpha_g)^n\}$$

is the set of roots of $f_n(t) := t^{2g} + a_n t^g + q^{ng}$. Then we will prove that f_n has no repeated roots if and only if $\gcd(n, g) = 1$. Thus, for $\beta \in \mathcal{R}$, we will show that β^n is a root of

$$t^{2g} + a_n t^g + q^{ng}.$$

It is clear that β^n is a root of

$$t^{2g} - (\beta^{ng} + (q/\beta)^{ng})t^g + q^{ng} \in \mathbb{C}[t].$$

Thus we have to show that

$$a_n = -(\beta^{ng} + (q/\beta)^{ng}) \in \mathbb{Z}.$$

In general, if we define $c_n = -x^n - (z/x)^n$ for $n > 0$ and $c_0 = -1$, we have that

$$(-1)^n c_1^n = (x + z/x)^n$$
$$= x^n + (z/x)^n + \binom{n}{1}\left[x^{n-1}(z/x) + x(z/x)^{n-1}\right] + \dots$$
$$\dots + \binom{n}{i}\left[x^{n-i}(z/x)^i + x^i(z/x)^{n-i}\right] + \dots$$
$$\dots + \binom{n}{\lfloor n/2 \rfloor}A,$$

where (observe that for n odd we have that $\lfloor n/2 \rfloor = (n-1)/2$)

$$A = x^{n/2}(z/x)^{n/2} \text{ or } A = x^{(n+1)/2}(z/x)^{(n-1)/2} + x^{(n-1)/2}(z/x)^{(n+1)/2}$$

for n even or odd, respectively. Equivalently,

$$A = z^{\lfloor n/2 \rfloor}(x + z/x)^{2(n/2 - \lfloor n/2 \rfloor)}.$$

Then

$$(-1)^n c_1^n = -c_n - \binom{n}{1}zc_{n-2} - \dots - \binom{n}{i}z^i c_{n-2i} - \dots - \binom{n}{\lfloor n/2 \rfloor}z^{\lfloor n/2 \rfloor}c_\epsilon,$$

where $\epsilon = 0, 1$ for n even or odd, respectively. Finally

$$c_n = (-1)^{n+1}c_1^n - \sum_{i=1}^{\lfloor n/2 \rfloor}\binom{n}{i}c_{n-2i}z^i.$$

By taking $x = \alpha^g$ and $z = q^g$, we finish the first part of the proof.

Now we prove that $f_n(t)$ has no repeated roots if and only if $\gcd(n, g) = 1$. For $k = 0, 1, \dots, g-1$, let

$$\theta/g + k2\pi/g, \quad \text{and} \quad -\theta/g - k2\pi/g,$$

be the arguments of the complex roots in $\mathcal{R}$ of $f_\mathcal{A}$, respectively, where θ and $-\theta$ are the arguments of the roots of $t^2 + a_1 t + q^g$, and $0 < \theta < \pi$. The polynomial f_n has repeated roots if and only if two of the roots in $\mathcal{R}$ to the n-th power are equal. We have

1. either $\alpha_i^n = \alpha_j^n$ for some $i \neq j \in \{0, \ldots, g-1\}$. Then

$$\frac{2\pi n}{g}(i - j) \equiv 0 \pmod{2\pi},$$

which holds if and only if $n(i - j)/g \in \mathbb{Z}$ if and only if $\gcd(n, g) > 1$;

2. either $\alpha_i^n = (q^g/\alpha_j)^n$ for some $i, j \in \{0, \ldots, g-1\}$. Then

$$\frac{n}{g}[2\theta + 2\pi(i + j)] \equiv 0 \pmod{2\pi}.$$

A necessary condition is that $\theta \in \pi\mathbb{Q}$. Note that $\cos(\theta) = -a_1/(2\sqrt{q^g})$. On one hand, it can be shown (from [8, Thm. 1], for example) that $2\cos(\theta)$ is an algebraic integer if $\theta \in \pi\mathbb{Q}$. On the other hand, $a_1/\sqrt{q^g}$ is an algebraic number of degree ≤ 2 which is not an algebraic integer since $\gcd(a_1, p) = 1$. Thus, this would be a contradiction.

The Honda-Tate theory for ordinary abelian varieties ensures that the polynomial $f_n(t) = t^{2g} + a_n t^g + q^g$ obtained is indeed the Weil polynomial $f_{\mathcal{A}_n}$ of the extension $\mathcal{A}_n$. $\square$

3.2 Local growth

Given an ℓ-cyclic isogeny class $\mathcal{A}$ (with $\ell \mid f_{\mathcal{A}}(1)$, i.e. with non trivial ℓ-primary component) it is clear that for all n, $\ell \mid f_{\mathcal{A}_n}(1)$ since $A(\mathbb{F}_q) \subset A(\mathbb{F}_{q^n})$. Thus, it is more interesting to know for which of these values of n the ℓ-part increases (relatively to the base field). Lemma 3.3 below gives an answer.

We first fix a polynomial that will be useful. For every positive integer n, we set

$$P_n(x) := \sum_{i=0}^{n-1} x^i.$$

Note that $(x - 1)P_n(x) = x^n - 1$. Notice that Lemma 3.3 below is only valid for n odd (so only odd integers are considered in Theorem 1.4). We write first the polynomial P_n in a convenient way:

Lemma 3.2. *For n odd, the polynomial $P_n(x)$ can be obtained recursively:*

$$P_n(x) = (x + 1)^{n-1} - \sum_{i=1}^{(n-1)/2} \left[\binom{n}{i} - 2\binom{n-1}{i-1} \right] x^i P_{n-2i}(x),$$

with $P_1(x) = 1$.

Proof. The proof is straightforward by using induction on n and showing directly that the equality $(x - 1)P_n(x) = (x - 1)$"right-hand-side" holds. $\square$

Lemma 3.3. *For every positive odd integer n and any prime integer ℓ, we have*

$$v_\ell(N_n) \geq \min\{2v_\ell(N_1), v_\ell(N_1) + v_\ell(nP_n(q^g))\},$$

provided that $\ell \mid N_1$.

Proof. We suppose n odd. Recall that for Weil-central isogeny classes

$$N_{g,1} = q^g + a_1 + 1, \text{ and,}$$
$$N_{g,n} = q^{gn} + a_n + 1,$$

where a_n can be computed by using Lemma 3.1. From the hypothesis $v_\ell(N_1) := m > 0$ we have

$$N_{g,1} \equiv q^g + a_1 + 1 \equiv z\ell^m \pmod{\ell^{2m}}, \quad 0 < z < \ell^m, \ell \nmid z.$$

From now, all congruences are modulo ℓ^{2m}. First, we show by induction on n that:

$$a_n \equiv -q^{gn} - 1 + z\ell^m nP_n(q^g).$$

For $n = 1$,

$$a_1 \equiv -q^g - 1 + z\ell^m P_1(q^g),$$

with $P_1 = 1$.

Using the induction hypothesis for $i = 1, \ldots, (n-1)/2$ (so that $n - 2i < n$), we have that

$$a_{n-2i}q^{gi} \equiv \left[-q^{g(n-2i)} - 1 + z\ell^m(n-2i)P_{n-2i}(q^g)\right]q^{gi}$$
$$\equiv -q^{gn-gi} - q^{gi} + z\ell^m q^{gi}(n-2i)P_{n-2i}(q^g),$$

then taking the sum over $i = 1, \ldots, (n-1)/2$

$$\sum \binom{n}{i} a_{n-2i}q^{gi} \equiv \sum_{i=1}^{(n-1)/2} \binom{n}{i}\left[-q^{gn-gi} - q^{gi} + z\ell^m q^{gi}(n-2i)P_{n-2i}(q^g)\right]$$
$$\equiv -(q^g+1)^n + q^{gn} + 1 + z\ell^m \sum_{i=1}^{(n-1)/2} \binom{n}{i}(n-2i)\left[q^{gi}P_{n-2i}(q^g)\right].$$

From Lemma 3.1, and using the fact that for $m > 0$,

$$(x + y\ell^m)^n \equiv x^n + nx^{n-1}y\ell^m \pmod{\ell^{2m}}$$

at the step marked with $(*)$, we have

$$a_n \equiv a_1^n - \sum \binom{n}{i} a_{n-2i} q^{gi}$$

$$\equiv [-(q^g + 1) + z\ell^m]^n - \left[-(q^g + 1)^n + q^{gn} + 1 + z\ell^m \sum_{i=1}^{(n-1)/2} \binom{n}{i}(n - 2i) \left[q^{gi} P_{n-2i}(q^g) \right] \right]$$

$$\stackrel{(*)}{\equiv} -(q^g + 1)^n + n(q^g + 1)^{n-1} z\ell^m$$

$$- \left[-(q^g + 1)^n + q^{gn} + 1 + z\ell^m \sum_{i=1}^{(n-1)/2} \binom{n}{i}(n - 2i) \left[q^{gi} P_{n-2i}(q^g) \right] \right]$$

$$\equiv -q^{gn} - 1 + z\ell^m \left[n(q^g + 1)^{n-1} - \sum_{i=1}^{(n-1)/2} \binom{n}{i}(n - 2i) \left[q^{gi} P_{n-2i}(q^g) \right] \right]$$

$$\equiv -q^{gn} - 1 + z\ell^m n \underbrace{\left[(q^g + 1)^{n-1} - \sum_{i=1}^{(n-1)/2} \left[\binom{n}{i} - 2\binom{n-1}{i-1} \right] \left[q^{gi} P_{n-2i}(q^g) \right] \right]}_{P_n(q^g)},$$

which completes the induction part. Then we compute N_n:

$$N_n \equiv q^{gn} + a_n + 1$$
$$\equiv q^{gn} + [-q^{gn} - 1 + z\ell^m n P_n(q^g)] + 1$$
$$\equiv z\ell^m n P_n(q^g).$$

Finally, we have $N_n = z\ell^m n P_n(q^g) + s\ell^{2m}$, for some integer s. The result follows. $\square$

Since $v_\ell(n P_n(q^g)) \geq 1$ if $\ell \mid n$, we have then proved the assertion about $\mathfrak{g}_\ell(\mathcal{A})$ of Theorem 1.4.

Remark 3.4. From Lemma 3.3 above, we also have that $\mathfrak{g}_\ell(\mathcal{A}) \supset \{n \in \mathbb{N} : \ell \mid P_n(q^g)\}$. However, from Lemma 3.5 (see Section 3.3 below), $\ell \mid P_n(q^g)$ implies $\ell \mid (q^g)^n - 1$, then $\mathcal{A}_n$ is not necessarily ℓ-cyclic.

3.3 Local cyclicity

In this section we will give the characterization of the local cyclicity of Weil-central isogeny classes and their extensions. Following the definition of cyclicity for isogeny classes, a local version of [2, Theorem 2.2] gives the *cyclicity criterion*: for any prime ℓ and for any isogeny class $\mathcal{A}$ we have that

$$\mathcal{A} \text{ is } \ell\text{-cyclic if and only if } \ell \text{ does not divide } \gcd(\widehat{f_{\mathcal{A}}(1)}, f'_{\mathcal{A}}(1)). \tag{3}$$

This has a meaning only if $A(k)_\ell$ is not trivial for some $A \in \mathcal{A}$ (and thus for all $A \in \mathcal{A}$), equivalently if ℓ divides $f_{\mathcal{A}}(1)$. Sometimes we use a weaker version of the cyclicity criterion, namely $\ell \nmid \gcd(f_{\mathcal{A}}(1), f'_{\mathcal{A}}(1))$ implies that the isogeny class is ℓ-cyclic. We give a complete description of the local cyclicity:

Lemma 3.5. *Given a Weil-central isogeny class $(a, q)_g$ and a rational prime ℓ:*

1. *if $\ell \nmid g$ and $\ell \nmid q^g - 1$, then $(a, q)_g$ is ℓ-cyclic;*

2. *if $\ell \nmid g, \ell \mid q^g - 1$ and $\ell \mid f(1)$, then $(a, q)_g$ is ℓ-cyclic if and only if $\ell^2 \nmid f(1)$;*

3. *if $\ell \mid g$, then $(a, q)_g$ is ℓ-cyclic if and only if $\ell^2 \nmid f(1)$.*

Proof. Recall that $(a, q)_g$ corresponds to the isogeny class with Weil polynomial of the form $f(t) = t^{2g} + at^g + q^g$. Then we have

$$f(1) = 1 + a + q^g = (q^g - 1) + (a + 2),$$
$$f'(1) = g(2 + a).$$

Then we prove the lemma point by point using the *cyclicity criterion* (3), which is equivalent to

$$\mathcal{A} \text{ is not } \ell\text{-cyclic if and only if } \ell^2 \mid f(1) \text{ and } \ell \mid f'(1). \tag{4}$$

1. If we suppose that $(a, q)_g$ is not ℓ-cyclic, then $\ell^2 \mid (q^g - 1) + (a + 2)$ and $\ell \mid a + 2$. This implies $\ell \mid q^g - 1$, a contradiction.

2. We prove the assertion by contraposition:

$$
\begin{aligned}
(a, q)_g \text{ is not } \ell\text{-cyclic} &\Leftrightarrow \ell^2 \mid f(1), \; \ell \mid f'(1) && \text{from criterion (4)} \\
&\Leftrightarrow \ell^2 \mid f(1), \; \ell \mid a + 2 && \text{since } \ell \nmid g \\
&\Leftrightarrow \ell^2 \mid f(1) && \text{since } \ell \mid q^g - 1.
\end{aligned}
$$

3. In the case $\ell \mid g$, we have that $\ell \mid f'(1)$. The result can be deduced from the contrapositive version (4) of the cyclicity criterion.

$\square$

As we consider here Weil-central isogeny classes such that the ℓ-part grows, this implies in particular that $\ell^2 \mid f_n(1)$. Thus, Lemma 3.5 says that the local cyclicity at a prime ℓ is possible only if $\ell \nmid g$ and $\ell \nmid (q^n)^g - 1$.

Corollary 3.6. *Suppose $\ell \nmid g$ and $\ell \nmid q^g - 1$ (in particular $\mathcal{A}_1$ is ℓ-cyclic), then*

$$\{n \in \mathbb{N} : \mathcal{A}_n \text{ is } \ell\text{-cyclic}\}$$

contains the set of positive integers with no common factor with g and which are not multiple of $\omega_\ell(q^g)$.

Proof. In order to have that $\mathcal{A}_n$ is Weil-central, we do not consider n with a common factor with g (see Lemma 3.1). For the ℓ-cyclicity of $(a_n, q^n)_g$ we use item (1) of Lemma 3.5. Observe that in this case, the cyclicity is independent of the value a_n. We set $\delta := \omega_\ell(q^g)$ and we consider the Euclidean division

$$n = c\delta + r,\ 0 \le r < \delta.$$

Then we have

$$q^{gn} \equiv q^{g(c\delta+r)} \equiv q^{gc\delta} q^{gr} \equiv q^{gr} \pmod{\ell},$$

which is congruent to 1 if and only if r is zero, if and only if n is a multiple of δ. $\qquad\square$

Observe that here we do not consider the growth of the ℓ-part, only the cyclicity. Moreover, the isogeny classes $\mathcal{A}_n$ can be "ℓ-trivial". We have then proved the assertion about $\mathfrak{c}_\ell(\mathcal{A})$. Finally, this completes the proof of Theorem 1.4.

4   Examples

Consider the ordinary elliptic curve $(g = 1)$ defined by the Weil polynomial

$$f_\mathcal{E}(t) = t^2 + t + 73.$$

We have $f_\mathcal{E}(1) = 75 = 3 \times 5^2$ and $q^g - 1 = 72$ is not divisible by 5. Then the isogeny class $\mathcal{E} = (1, 73)_1$ is 5-cyclic and so the conditions of Theorem 1.4 are verified. We also have $\omega_5(73) = 4$. Consequently

$$\mathfrak{g}_5(\mathcal{E}) \supset \{n \in \mathbb{N} : 5 \mid n, 2 \nmid n\},$$
$$\mathfrak{c}_5(\mathcal{E}) \supset \{n \in \mathbb{N} : 5 \mid n, 2 \nmid n, 4 \nmid n\} = \{n \in \mathbb{N} : 5 \mid n, 2 \nmid n\}.$$

Note that the elliptic curve $\mathcal{E}$ is 3-cyclic since $v_3(f_\mathcal{E}(1)) = 1$. However, we cannot apply Theorem 1.4 for $\ell = 3$ since $q^g - 1 = 72$ is divisible by 3. This and another few examples are listed in Table 1.

$(a,q)_g$	$f_\mathcal{A}(1)$	ℓ	$\omega_\ell(q^g)$	$\subset \mathfrak{g}_\ell(\mathcal{A})$	$\subset \mathfrak{c}_\ell(\mathcal{A})$
$(1,73)_1$	3×5^2	5	4	$\{n \in \mathbb{N} : 5 \mid n, 2 \nmid n\}$	$\{n \in \mathbb{N} : 5 \mid n, 2 \nmid n\}$
$(11,17)_3$	$5^2 \times 197$	5	4	$\{n \in \mathbb{N} : 5 \mid n, 2 \nmid n, 3 \nmid n\}$	$\{n \in \mathbb{N} : 5 \mid n, 2 \nmid n, 3 \nmid n\}$
$(17,19)_3$	13×23^2	23	22	$\{n \in \mathbb{N} : 23 \mid n, 2 \nmid n, 3 \nmid n\}$	$\{n \in \mathbb{N} : 23 \mid n, 2 \nmid n, 3 \nmid n, 22 \nmid n\}$
$(20,7)_6$	70×41^2	41	20	$\{n \in \mathbb{N} : 41 \mid n, 2 \nmid n, 3 \nmid n\}$	$\{n \in \mathbb{N} : 41 \mid n, 2 \nmid n, 3 \nmid n, 20 \nmid n\}$

Table 1: Examples related to Theorem 1.4

Note that in the last two rows of Table 1, the parts $22 \nmid n$ and $20 \nmid n$ are unnecessary. For all cases, the sets obtained and included in $\mathfrak{g}_\ell(\mathcal{A})$ and $\mathfrak{c}_\ell(\mathcal{A})$, respectively, are the same.

Table 2 shows the valuations $v_\ell(\mathcal{A}_5), v_\ell(\mathcal{A}_{15}), v_\ell(\mathcal{A}_{25}), \ldots$ for the elliptic curve case, as well as the valuations for the other examples of Table 1.

$(a,q)_g$	ℓ	$v_\ell(\mathcal{A})$							$v_\ell(\mathcal{A}_n)$											Last n
$(1,73)_1$	5	2	3	3	4	3	3	3	3	4	3	3	3	3	5	3	3	3	3	4	175
$(11,17)_3$	5	2	3	4	3	3	3	3	3	3	5	3	3	4	3	3	3	3	3	3	265
$(17,19)_3$	23	2	4	4	4	6	4	4	4	6	4	4	4	4	4	4	4	4	4	4	1219
$(20,7)_6$	41	2	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	2173

Table 2: Valuation $v_\ell(\mathcal{A}_n)$ for n in the sets of Table 1

Consider the example given previously $\mathcal{A}_1 = (11,17)_3$, that is, defined by the Weil polynomial

$$f_\mathcal{A}(t) = t^6 + 11t^3 + 17^3.$$

Table 3 shows information about extensions $\mathcal{A}_n$ for n up to 10. As expected from (the proof of) Lemma 3.1, when n and g have a common factor, the isogeny class $\mathcal{A}_n$ is not Weil-central. The Weil polynomial of $\mathcal{A}_n$ is of the form h^e, with h irreducible and ordinary. So $\mathcal{A}_n$ is the power of a lower dimensional class of abelian varieties, which are Weil central. We represent them as $(a,q)_{g'}^e$ in Table 3. For example, $\mathcal{A}_3$ is the product of three copies of the isogeny class of elliptic curves with Weil polynomial $t^2 + 11t + 17^3$. Theorem 1.4 says that the 5-part grows with respect to the base field for $n = 5$. Besides that, we see that for $n \in \{4, 8, 10\}$ the 5-part grows as well. Among these extensions, $\mathcal{A}_n$ is 5-cyclic for $n = 5$ (Theorem 1.4). It is not 5-cyclic for $n = 4$, and thus for $n = 8$ (since $\mathcal{A}_8$ is an extension of $\mathcal{A}_4$), but it is 5-cyclic for $n = 10$.

n	$\mathcal{A}_n$	Simple?	Weil-central?	$v_5(f_n(1))$	5-cyclic?
1	$(11, 17^1)_3$	Yes	Yes	2	Yes
2	$(9705, 17^2)_3$	Yes	Yes	2	Yes
3	$(11, 17^3)_1^3$	No	No	2	No
4	$(-45911887, 17^4)_3$	Yes	Yes	3	No
5	$(1295031331, 17^5)_3$	Yes	Yes	3	Yes
6	$(9705, 17^6)_1^3$	No	No	2	No
7	$(-8687006247293, 17^7)_3$	Yes	Yes	2	Yes
8	$(-942656893441247, 17^8)_3$	Yes	Yes	3	No
9	$(-160798, 17^9)_1^3$	No	No	2	No
10	$(4047739954748000025, 17^{10})_3$	Yes	Yes	3	Yes

Table 3: $\mathcal{A}_n$ for n up to 10, where $\mathcal{A}_1 = (11,17)_3$

Acknowledgments

References

[1] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[2] A. J. Giangreco-Maidana. On the cyclicity of the rational points group of abelian varieties over finite fields. *Finite Fields Appl.*, 57:139–155, 2019.

[3] A. J. Giangreco-Maidana. Local cyclicity of isogeny classes of abelian varieties defined over finite fields. *Finite Fields Appl.*, 62:101628, 9, 2020.

[4] E. W. Howe, D. Maisner, E. Nart, and C. Ritzenthaler. Principally polarizable isogeny classes of abelian surfaces over finite fields. *Math. Res. Lett.*, 15(1):121–127, 2008.

[5] E. W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1):239–289, 2009.

[6] E. W. Howe and H. J. Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory*, 92(1):139–163, 2002.

[7] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83(2):289–292, 1977.

[8] D. H. Lehmer. Questions, Discussions, and Notes: A Note on Trigonometric Algebraic Numbers. *Amer. Math. Monthly*, 40(3):165–166, 1933.

[9] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Tata Institute of Fundamental Research, Bombay; by Oxford University Press, London, 1970.

[10] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[11] S. G. Vlăduţ. Cyclicity statistics for elliptic curves over finite fields. *Finite Fields Appl.*, 5(1):13–25, 1999.

[12] S. G. Vlăduţ. On the cyclicity of elliptic curves over finite field extensions. *Finite Fields Appl.*, 5(4):354–363, 1999.

[13] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.