RIMS Kôkyûroku Bessatsu
B86 (2021), 047–062

The Characteristic Polynomials Of Abelian Varieties Over Finite Fields

By

Daiki Hayashida*

Abstract

The characteristic polynomials of abelian varieties over finite fields have a lot of arithmetic and geometric information. In this article, we consider the problem of exactly which Weil polynomials of degree $2g$ occur as the characteristic polynomials of abelian varieties of dimension g over finite fields and give a survey of the recent results on the problem.

§ 1. Introduction

An abelian variety over a field k is a complete group variety over k. It has various extremely good properties. In particular, abelian varieties over finite fields can be used to approach various practical issues, e.g. cryptography. Since the characteristic polynomial has a lot of information on abelian varieties, it is important to investigate the characteristic polynomials of abelian varieties in detail.

Let p be a prime, $\mathbb{F}_q$ a finite field with $q = p^n$ elements and X an abelian variety of dimension g over $\mathbb{F}_q$. Fix a prime $l \neq p$ and let $T_l(X)$ be the l-adic Tate module of X. The q-th power Frobenius endomorphism $\pi_X : X \to X$ induces a homomorphism as $\mathbb{Z}_l$-modules

$$T_l(\pi_X) : T_l(X) \longrightarrow T_l(X).$$

The characteristic polynomial $f_X(t)$ of π_X is defined by

$$f_X(t) = \det(t - T_l(\pi_X)),$$

Received March 30, 2019. Revised October 27, 2019.
2020 Mathematics Subject Classification(s):
Key Words: *characteristic polynomial, abelian variety, finite field*
*Department of Mathematics, Faculty of Science, Kyoto University Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8502, Japan
e-mail: hayashid@math.kyoto-u.ac.jp

which is known to have coefficients in $\mathbb{Z}$ independent of l. In this article, we call $f_X(t)$ the characteristic polynomial of X or the characteristic polynomial for short instead of the characteristic polynomial of the Frobenius endomorphism of X. The characteristic polynomial $f_X(t)$ is of the form

$$f_X(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{g-1}t^{g-1} + a_g t^g + a_{g-1}qt^{g-1} + \cdots + a_1 q^{g-1}t + q^g,$$

where $a_1, \cdots, a_g \in \mathbb{Z}$. The set of roots in $\mathbb{C}$ of $f_X(t)$ is in the form $\{w_1, \overline{w_1}, \cdots, w_g, \overline{w_g}\}$, where w_i is a Weil number for $i = 1, \cdots, g$. A (q-)*Weil number* w is an algebraic integer such that for any embedding $\sigma : \mathbb{Q}(w) \hookrightarrow \mathbb{C}$, $|\sigma(w)| = \sqrt{q}$. A monic polynomial with integer coefficients whose roots are (q-)Weil numbers is called a (q-)*Weil polynomial*. Thus the characteristic polynomial of the Frobenius endomorphism is a Weil polynomial, but the converse is not necessarily true. Our main question is the following:

Under what conditions does a given Weil polynomial of degree $2g$ *occur as the characteristic polynomial of an abelian variety of dimension* g *over a finite field?*

Let X, Y be abelian varieties defined over $\mathbb{F}_q$ and $f_X(t), f_Y(t)$ the characteristic polynomials of X and Y respectively. Then, by Tate's theorem, X is ($\mathbb{F}_q$-)isogenous to Y if and only if $f_X(t) = f_Y(t)$. It is known that any abelian variety X over $\mathbb{F}_q$ is isogenous to

$$X_1^{r_1} \times \cdots \times X_m^{r_m},$$

where X_i is a simple abelian variety over $\mathbb{F}_q$, X_i is not isogenous to X_j for $i \neq j$ and $r_i \geq 1$ is an integer. If $f_{X_i}(t)$ is the characteristic polynomial of X_i, then

$$f_X(t) = f_{X_1}(t)^{r_1} \cdots f_{X_m}(t)^{r_m}.$$

Therefore to determine characteristic polynomials of abelian varieties of dimension g over finite fields, it is sufficient to determine characteristic polynomials of *simple* abelian varieties of dimension less than or equal to g. Moreover, if X is ($\mathbb{F}_q$-)simple, then $f_X(t) = m_X(t)^e$, where $m_X(t)$ is an irreducible polynomial and $e \geq 1$ is an integer, which we call the multiplicity of X. From this equality, it is obvious that e divides $2\dim(X)$.

To solve the above problem, we divide the problem into several steps. First problem is the following:

Problem 1. Find a necessary and sufficient condition for a polynomial $f(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{g-1}t^{g+1} + a_g t^g + a_{g-1}qt^{g-1} + \cdots + a_1 q^{g-1}t + q^g$ with integer coefficients to be a Weil polynomial.

Problem 1 seems to be elementary, but the general solution or algorithm is not known at present. The higher the degree is, the more complicated rapidly the answer for this problem becomes. This problem has only been solved up to degree 10. Problem 1 on degree 4 is solved in [6, Lemma 3.1] and [5, Lemma 2.1], on degree 6 is solved in [10, Theorem 1.1], on degree 8 is solved in [4, Theorem 1.1] and on degree 10 is solved in [7].

Second problem is the following:

Problem 2. Determine all possible multiplicities e.

From the viewpoint of determining all characteristic polynomials, this problem is the step to deal with Problem 3 efficiently. Lemma 3.5 plays an important role in dealing with Problem 2. Theorem 3.8, which states that e divides n with a specific situation, is also important as another approach to Problem 2.

Finally, for each e examined in Problem 2, we consider the following problem.

Problem 3. Find a necessary and sufficient condition for a Weil polynomial $f(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{g-1} t^{g+1} + a_g t^g + a_{g-1} q t^{g-1} + \cdots + a_1 q^{g-1} t + q^g$ to be the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q$. Namely, for a Weil polynomial $f(t)$, find a condition on the coefficients of $f(t)$ under which there exists a simple abelian variety over $\mathbb{F}_q$ whose characteristic polynomial coincides with $f(t)$.

In section 2, we prepare for the study on the characteristic polynomials of abelian varieties and explain that the behavior in endomorphisms of abelian varieties reduces it in the characteristic polynomials. In section 3, we survey the recent results on Problem 1,3 for now.

Problem \ Dimension	$g = 1$	$g = 2$	$g = 3$	$g = 4$	$g = 5$	$g > 5$
Problem 1	clear	[6, 5]	[2]	[4]	[7]	Open
Problem 3	[8]	[6, 5]	[10, 2]	[10, 4]	[3]	[3] ($e = g$ case) Open (the others)

Table 1. Recent results

§ 2. Preliminaries

Now we briefly review the Honda-Tate theory (cf. [9]) which is a powerful classification theory of (simple) abelian varieties over finite fields.

We denote the set of q-Weil numbers by $W(q)$ and define the following equivalence relation on $W(q)$: We say that $\pi, \pi' \in W(q)$ are *conjugate* (and write $\pi \sim \pi'$) if π and π' have the same minimal polynomial over $\mathbb{Q}$.

Theorem 2.1 (cf. [9, Theorem 9])**.** *There is a bijection $X \longmapsto \pi_X$ from the set of $\mathbb{F}_q$-isogeny classes of simple abelian varieties over $\mathbb{F}_q$ to the set of conjugacy classes of $W(q)$.*

In other words, this theorem claims that there is a one-to-one correspondence between two seemingly unrelated objects — abelian varieties and algebraic integers.

Let X be a simple abelian variety over $\mathbb{F}_q$ and π_X the q-th power Frobenius endomorphism of X. Let $E := \mathrm{End}^0_{\mathbb{F}_q}(X) = \mathrm{End}_{\mathbb{F}_q}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $F := \mathbb{Q}[\pi_X] \subseteq E$. Then E is a division algebra whose center is F. The dimension of X in Theorem 2.1 satisfies the following property.

Proposition 2.2 (cf. [9, Theorem 8])**.** *With notation as above, the dimension of the abelian variety X satisfies*

$$2\dim(X) = \sqrt{[E : F]} \cdot [F : \mathbb{Q}].$$

Let v be a place of F, F_v the completion of F at v and $\mathrm{Br}(F_v)$ the Brauer group of F_v. Then we have the following formula for the invariant $\mathrm{inv}_v(E) := \mathrm{inv}_{F_v}(E \otimes_F F_v) \in \mathrm{Br}(F_v) \subset \mathbb{Q}/\mathbb{Z}$.

Proposition 2.3 (cf. [9, Theorem 8])**.** *We have*

(1) $\mathrm{inv}_v(E) = 1/2$ *if v is a real place,*

(2) $\mathrm{inv}_v(E) = 0$ *if v is a finite place not dividing p or v is a complex place,*

(3) $\mathrm{inv}_v(E) = \dfrac{v_p(\pi_X)}{v_p(q)} \cdot [F_v : \mathbb{Q}_p] \bmod \mathbb{Z}$ *if v is a place dividing p.*

The following lemma plays an important role in a specific situation.

Lemma 2.4. *[5, Proposition 2.5] Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements. Let X be a simple abelian variety over $\mathbb{F}_q$ with characteristic polynomial $f_X(t) = (t^2 + at + q)^{\dim(X)}$, where $a \in \mathbb{Z}$ such that $|a| < 2\sqrt{q}$. Let $m = v_p(a)$ and $d = a^2 - 4q$. Then*

$$\dim(X) = \begin{cases} \frac{n}{(m,n)} & \text{if } m < \frac{n}{2} \\ 2 & \text{if } m \geq \frac{n}{2} \text{ and } d \in \mathbb{Q}_p^{\times 2} \\ 1 & \text{if } m \geq \frac{n}{2} \text{ and } d \notin \mathbb{Q}_p^{\times 2}. \end{cases}$$

Next we state that the properties on endomorphisms of abelian varieties over finite fields reduce them in the characteristic polynomials.

Lemma 2.5. *The least common denominator of* $\mathrm{inv}_v(E)$ *for all places* v *of* F *is equal to* e*, where* e *is the multiplicity of* X*.*

We write $\mathrm{lcd}(a_1, \cdots, a_m)$ for the least common denominator of $a_1, \cdots, a_m \in \mathbb{Q}/\mathbb{Z}$ and $\mathrm{d}(a)$ for the denominator of $a \in \mathbb{Q}/\mathbb{Z}$.

This lemma follows from Proposition 2.2 and a theory of Brauer groups over global fields. (cf. [1, 3])

Note that if X is a simple abelian variety, then $f_X(t) = m_X(t)^e$, where $m_X(t)$ is an irreducible Weil polynomial. We have the following corollary on the irreducibility.

Corollary 2.6. *An irreducible Weil polynomial* $f(t)$ *of degree* $2g$ *is the characteristic polynomial of a simple abelian variety of dimension* g *over* $\mathbb{F}_q$ *(i.e.* $e = 1$*) if and only if* $f(t)$ *has no real root and the following condition holds:*

$$\begin{cases} \dfrac{v_p(f_i(0))}{n} \in \mathbb{Z}, \\ \text{where } f_i(t) \text{ runs through all monic irreducible factors of } f(t) \text{ in } \mathbb{Q}_p[t]. \end{cases}$$

This corollary is the basic tool to deal with Problem 3 by investigating the coefficients of a given Weil polynomial.

§ 3. Recent results

§ 3.1. Problem 1

We enumerate the relevant results up to $g = 5$. (We omit the result [7] on $g = 5$, since this article is too small to write down the result.)

Theorem 3.1. *A polynomial* $t^2 - at + q \in \mathbb{Z}[t]$ *is a Weil polynomial if and only if* $|a| \leq 2\sqrt{q}$*.*

Theorem 3.2. *[6, Lemma 3.1][5, Lemma 2.1] Let* $f(t) = t^4 + a_1t^3 + a_2t^2 + a_1qt + q^2 \in \mathbb{Z}[t]$*. This polynomial* $f(t)$ *is a Weil polynomial if and only if the following conditions hold:*

(1) $|a_1| \leq 4\sqrt{q}$*,*

(2) $2|a_1|\sqrt{q} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q$*.*

Theorem 3.3. *[2, Theorem 1.1] Let* $f(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + a_2qt^2 + a_1q^2t + q^3 \in \mathbb{Z}[t]$. *This polynomial* $f(t)$ *is a Weil polynomial if and only if either* $f(t) = (t^2 - q)(t^2 + at + q)$, *where* $a \in \mathbb{Z}$ *and* $|a| < 2\sqrt{q}$, *or the following conditions hold:*

(1) $|a_1| < 6\sqrt{q}$,

(2) $4|a_1|\sqrt{q} - 9q < a_2 \leq \frac{a_1^2}{3} + 3q$,

(3) $-\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leq a_3 \leq -\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}$,

(4) $-2qa_1 - 2a_2\sqrt{q} - 2q\sqrt{q} < a_3 < -2qa_1 + 2a_2\sqrt{q} + 2q\sqrt{q}$.

Theorem 3.4. *[4, Theorem 1.1] Let* $f(t) = t^8 + a_1t^7 + a_2t^6 + a_3t^5 + a_4t^4 + a_3qt^3 + a_2q^2t^2 + a_1q^3t + q^4 \in \mathbb{Z}[t]$. *This polynomial* $f(t)$ *is a Weil polynomial if and only if either* $f(t) = (t^2 \pm \sqrt{q})^2h(t)$, *where* $h(t)$ *is a Weil polynomial of degree* 4 *(See Theorem 3.2), or the following conditions hold:*

(1) $|a_1| < 8\sqrt{q}$,

(2) $6|a_1|\sqrt{q} - 20q < a_2 \leq \frac{3a_1^2}{8} + 4q$,

(3) $-9qa_1 - 4\sqrt{q}a_2 - 16q\sqrt{q} < a_3 < -9qa_1 + 4\sqrt{q}a_2 + 16q\sqrt{q}$,

(4) $-\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 - (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2} \leq a_3 \leq -\frac{a_1^3}{8} + \frac{a_1a_2}{2} + qa_1 + (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2}$,

(5) $2\sqrt{q}|qa_1 + a_3| - 2qa_2 - 2q^2 < a_4$,

(6) $\frac{9a_1^4}{256} - \frac{3a_1^2a_2}{16} + \frac{a_1a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + \omega + \overline{\omega} \leq a_4 \leq \frac{9a_1^4}{256} - \frac{3a_1^2a_2}{16} + \frac{a_1a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + j\omega + j^2\overline{\omega}$,

where $\omega^{1/3} = |\omega|^{1/3}e^{\frac{arg(\omega)i}{3}}$, $j = e^{\frac{2i\pi}{3}}$ *and* $\omega = \frac{1}{24}(8(-\frac{3a_1^2}{8} + a_2 - 4q)^6 + 540(-\frac{3a_1^2}{8} + a_2 - 4q)^3(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^2 - 729(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^4 + i9|\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3|(-(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^2 - \frac{8}{27}(-\frac{3a_1^2}{8} + a_2 - 4q)^3)^{3/2})^{1/3}$.

§ 3.2. Problem 3

In this section, we survey the recent results on our main problem, Problem 3. As we stated in Section 1, it is efficient to deal with Problem 2 and solve Problem 3 on the obtained e's before solving Problem 3.

Let X be a simple abelian variety. Since $f_X(t) = m_X(t)^e$, we compare with the degrees of the both sides and obtain that $2g = \deg(m_X) \cdot e$, hence e divides $2g$. Moreover, we can specialize the choices of e by using the following lemma. This useful lemma shows that an abelian variety corresponding to a real Weil number must be of dimension less than or equal to 2.

Lemma 3.5. *Let X be a simple abelian variety over $\mathbb{F}_q$ with $q = p^n$ elements and $f_X(t)$ the characteristic polynomial. Suppose that $f_X(t)$ has a real root. Then we have*

(1) if n is even, then $\dim(X) = 1$, *or*

(2) if n is odd, then $\dim(X) = 2$.

Remark 3.6. It is known that an abelian variety corresponding to a real Weil number is *supersingular*. See [1, 5.1] for details.

Example 3.7. We consider simple abelian varieties of odd prime dimension l over $\mathbb{F}_q$. Note that the prime number l is not necessarily different from p. In this case, the multiplicity e of their abelian varieties satisfies that e divides $2l$, so we have either $e = 1, 2, l$ or $2l$. However, $e = 2$ or $e = 2l$ contradicts that the dimension l is greater than or equal to 3 since the characteristic polynomial has a real root.

Many studies so far of characteristic polynomials of a simple abelian variety X over $\mathbb{F}_q$ are done with n fixed, where the possibility of e is examined only by using the divisibility condition $e \mid 2\dim(X)$ unrelated to the value of n. On the other hand, the following theorem gives rise to another direction of study depending on the value of n.

Theorem 3.8. *[3, Theorem 1.1] Let X be a simple abelian variety over $\mathbb{F}_q$ with $q = p^n$ elements, $f_X(t)$ the characteristic polynomial of X, and e the multiplicity of X. Then e divides n except for the case where $f_X(t)$ has a real root.*

Example 3.9. Assume $q = p$, then $n = 1$, hence $e = 1$ by Theorem 3.8. Thus we conclude that the characteristic polynomial of a simple abelian variety over $\mathbb{F}_p$ must be irreducible, unless it has a real root.

Remark 3.10. When $f_X(t)$ has a real root, the assertion of Theorem 3.8 does not hold in general. Indeed, assume that n is odd and let X be a simple abelian variety over $\mathbb{F}_q$ corresponding to the Weil number $\sqrt{q}$. As $t^2 - q$ is irreducible over $\mathbb{Q}$, we may write $f_X(t) = (t^2 - q)^e$. Now, by Lemma 3.5, we have $\dim(X) = 2$, hence $e = 2$. Thus, e does not divide n.

3.2.1. Elliptic curves First, we explain the characteristic polynomials of elliptic curves [8]. This is the most primitive case of abelian varieties.

Let X be an elliptic curve over the finite field $\mathbb{F}_q$ with $q = p^n$ elements. The characteristic polynomial of X is of the form

$$f_X(t) = t^2 - at + q$$

and the coefficient a satisfies $a = 1 + q - \#X(\mathbb{F}_q)$, where $\#X(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points of X.

As elliptic curves behave mathematically the simplest way among abelian varieties, we do not need a special discussion that is necessary in general dimensions, and in fact, there is no examination in [8, Theorem 4.1] corresponding to Problem 2. However, in order to describe in a unified way, although it is obvious, we evaluate e.

Since elliptic curves are simple as abelian varieties, the characteristic polynomials of elliptic curves are of the form $f_X(t) = m_X(t)^e$, where $m_X(t)$ is an irreducible polynomial and $e \geq 1$ is an integer. The degree of $f_X(t)$ is equal to 2, hence e is 1 or 2.

Theorem 3.11. *[8, Theorem 4.1] Let $f(t) = t^2 - at + q$ be a Weil polynomial. Then the polynomial $f(t)$ is the characteristic polynomial of an elliptic curve over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) $(a, p) = 1$,

(2) *n is even and* $a = \pm 2\sqrt{q}$,

(3) *n is even,* $p \not\equiv 1 \bmod 3$ *and* $a = \pm\sqrt{q}$,

(4) *n is even,* $p \not\equiv 1 \bmod 4$ *and* $a = 0$,

(5) *n is odd and* $a = 0$,

(6) *n is odd,* $p = 2, 3$ *and* $a = \pm p^{\frac{n+1}{2}}$.

This (2) corresponds to the case of $e = 2$ and the others correspond to the case of $e = 1$.

3.2.2. Abelian surfaces Let X be a simple abelian variety of dimension 2 over $\mathbb{F}_q$. Then the characteristic polynomial $f_X(t)$ is of the form

$$f_X(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 q t + q^2.$$

The multiplicity e of X is either $1, 2$ or 4 since e divides 4. Suppose $e = 4$. We have $f_X(t) = (t \pm \sqrt{q})^4$ and n is even. However, this contradicts $\dim(X) = 2$ by Lemma 3.5. The following proposition corresponds to the case of $e = 2$.

Proposition 3.12. *[5, Theorem 2.9] Let $f(t) = (t^2 + at + b)^2$ be a Weil polynomial, where $a, b \in \mathbb{Z}$. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension 2 over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) n is even, $p \equiv 1 \bmod 3$ and $(a,b) = (\pm\sqrt{q}, q)$,

(2) n is even, $p \equiv 1 \bmod 4$ and $(a,b) = (0,q)$,

(3) n is odd and $(a,b) = (0,-q)$.

The following proposition corresponds to the case of $e = 1$.

Proposition 3.13. *[6, Theorem 1.1][5, Theorem 2.9] Let $f(t) = t^4 + a_1t^3 + a_2t^2 + a_1qt + q^2$ be an irreducible Weil polynomial. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension 2 over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$ and $(a_2 + 2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_p$,

(2) $v_p(a_2) = 0$,

(3) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$ and $f(t)$ has no root in $\mathbb{Z}_p$.

3.2.3. Abelian varieties of dimension 3 Next, we describe the characteristic polynomials of simple abelian varieties of dimension 3 over $\mathbb{F}_q$. Let X be a simple abelian variety of dimension 3 over $\mathbb{F}_q$. Then the characteristic polynomial $f_X(t)$ is of the form

$$f_X(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + a_2qt^2 + a_1q^2t + q^3.$$

Now we compute e in Problem 2. From $f_X(t) = m_X(t)^e$, e divides 6, i.e. $e = 1, 2, 3$ or 6. Suppose $e = 6$. Then $f_X(t)$ has a real root, so the dimension of the abelian variety X must be 1 or 2 by Lemma 3.5, which contradicts the assumption that $\dim(X) = 3$. Suppose $e = 2$. Then since $\deg(m_X(t))$ is odd, $m_X(t)$ has at least one real root, so $\dim(X)$ must be 1 or 2 as well. Hence we obtain that e is 1 or 3. First, we consider $e = 3$.

Proposition 3.14. *[10, Proposition 2] Let $f(t) = (t^2 + at + q)^3 \in \mathbb{Z}[t]$, where $a \in \mathbb{Z}$ and $|a| < 2\sqrt{q}$. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension 3 over $\mathbb{F}_q$ if and only if 3 divides n and $a = kq^{1/3}$, where k is an integer and $(k,p) = 1$.*

This proposition ($e = g$ case) can be generalized to arbitrary dimension. See Theorem 3.19 (later).

The following proposition corresponds to the case of $e = 1$.

Proposition 3.15. *[2, Theorem 1.4] Let $f(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + a_2qt^2 + a_1q^2t + q^3$ be an irreducible Weil polynomial. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension 3 over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(2) $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(3) $v_p(a_3) = 0$,

(4) $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$ *and* $f(t)$ *has no root in* $\mathbb{Q}_p$,

(5) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) \geq 3n/2$ *and* $f(t)$ *has no root nor factor of degree* 3 *in* $\mathbb{Q}_p$.

3.2.4. Abelian varieties of dimension 4 Next, we describe the characteristic polynomials of simple abelian varieties of dimension 4 over $\mathbb{F}_q$. Let X be a simple abelian variety of dimension 4 over $\mathbb{F}_q$. Then the characteristic polynomial $f_X(t)$ is of the form

$$f_X(t) = t^8 + a_1t^7 + a_2t^6 + a_3t^5 + a_4t^4 + a_3qt^3 + a_2q^2t^2 + a_1q^3t + q^4.$$

Now we compute e in Problem 2. From $f_X(t) = m_X(t)^e$, e divides 8, i.e. $e = 1, 2, 4$ or 8. Suppose $e = 8$. Then $f_X(t)$ has a real root, so $\dim(X)$ must be 1 or 2 by Lemma 3.5, which contradicts the assumption that $\dim(X) = 4$. Hence we obtain that e is 1, 2, or 4.

The case of $e = 4$ is included in Theorem 3.19 (later). The following proposition corresponds to the case of $e = 2$.

Proposition 3.16. *[10, Proposition 4] Let* $m(t) = t^4 + b_1t^3 + b_2t^2 + b_1qt + q^2$ *be an irreducible Weil polynomial. Then the polynomial* $m(t)^2$ *is the characteristic polynomial of a simple abelian variety of dimension* 4 *over finite fields if and only if one of the following conditions holds:*

(1) $v_p(b_1) = 0$, $v_p(b_2) > 0$ *and* $(b_2 + 2q)^2 - 4qb_1^2$ *is a square in* $\mathbb{Z}_p$,

(2) $v_p(b_1) \geq n/4$, $v_p(b_2) = n/2$ *and* $m(t)$ *has no root in* $\mathbb{Z}_p$,

(3) $v_p(b_1) \geq n/2$, $v_p(b_2) \geq n$ *and* $m(t)$ *has at least one root in* $\mathbb{Z}_p$.

Finally we describe the case of $e = 1$.

Proposition 3.17. *[4, Theorem 1.2] Let* $f(t) = t^8 + a_1t^7 + a_2t^6 + a_3t^5 + a_4t^4 + a_3qt^3 + a_2q^2t^2 + a_1q^3t + q^4$ *be an irreducible Weil polynomial. Then the polynomial* $f(t)$ *is the characteristic polynomial of a simple abelian variety of dimension* 4 *over* $\mathbb{F}_q$ *if and only if one of the following conditions holds:*

(1) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 3n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *nor factor of degree* 3 *in* $\mathbb{Q}_p$,

(2) $v_p(a_1) = 0$, $v_p(a_2) \geq n/3$, $v_p(a_3) \geq 2n/3$, $v_p(a_4) = n$ *and* $f(t)$ *has no root of valuation* $n/3$ *and* $2n/3$ *in* $\mathbb{Q}_p$,

(3) $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq n$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(4) $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(5) $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$, $v_p(a_4) \geq 3n/2$ *and* $f(t)$ *has no root in* $\mathbb{Q}_p$,

(6) $v_p(a_4) = 0$,

(7) $v_p(a_1) \geq n/4$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq 3n/4$, $v_p(a_4) = n$ *and* $f(t)$ *has no root nor factor of degree* 2 *and* 3 *in* $\mathbb{Q}_p$,

(8) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) \geq 3n/2$, $v_p(a_4) \geq 2n$ *and* $f(t)$ *has no root nor factor of degree* 3 *in* $\mathbb{Q}_p$.

3.2.5. Abelian varieties of dimension 5 We describe the characteristic polynomials of simple abelian varieties of dimension 5 over $\mathbb{F}_q$. Let X be a simple abelian variety of dimension 5 over $\mathbb{F}_q$. Then the characteristic polynomial $f_X(t)$ is of the form

$$f_X(t) = t^{10} + a_1t^9 + a_2t^8 + a_3t^7 + a_4t^6 + a_5t^5 + a_4qt^4 + a_3q^2t^3 + a_2q^3t^2 + a_1q^4t + q^5.$$

Now we compute e in Problem 2. From $f_X(t) = m_X(t)^e$, e divides 10, i.e. $e = 1, 2, 5$ or 10. Suppose $e = 2$ or $e = 10$. Then $f_X(t)$ has a real root, so $\dim(X)$ must be 1 or 2 by Lemma 3.5, which contradicts the assumption that $\dim(X) = 5$. Hence we obtain that e is 1 or 5.

The case of $e = 5$ is included in Theorem 3.19 (later). The following proposition corresponds to the case of $e = 1$.

Theorem 3.18. *[3, Theorem 1.3] Let* $f(t) = t^{10} + a_1t^9 + a_2t^8 + a_3t^7 + a_4t^6 + a_5t^5 + a_4qt^4 + a_3q^2t^3 + a_2q^3t^2 + a_1q^4t + q^5$ *be an irreducible Weil polynomial. Then* $f(t)$ *is the characteristic polynomial of a simple abelian variety of dimension 5 over* $\mathbb{F}_q$ *if and only if one of the following conditions holds:*

(1) $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 3n/2$, $v_p(a_5) \geq 2n$ *and* $f(t)$ *has no root of valuation* $n/2$ *nor a factor of degree* 3 *in* $\mathbb{Q}_p$,

(2) $v_p(a_1) = 0$, $v_p(a_2) \geq n/3$, $v_p(a_3) \geq 2n/3$, $v_p(a_4) = n$, $v_p(a_5) \geq 3n/2$ *and* $f(t)$ *has no root of valuation* $n/3, n/2$ *or* $2n/3$ *in* $\mathbb{Q}_p$,

(3) $v_p(a_1) = 0$, $v_p(a_2) \geq n/4$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq 3n/4$, $v_p(a_5) = n$ *and* $f(t)$ *has no root of valuation* $n/4$ *or* $3n/4$ *nor an irreducible factor of degree* 2 *in* $\mathbb{Q}_p$,

(4) $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq n$, $v_p(a_5) \geq 3n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *nor an irreducible factor of degree* 3 *in* $\mathbb{Q}_p$,

(5) $v_p(a_2) = 0$, $v_p(a_3) \geq n/3$, $v_p(a_4) \geq 2n/3$, $v_p(a_5) = n$ *and* $f(t)$ *has no root of valuation* $n/3$ *or* $2n/3$ *in* $\mathbb{Q}_p$,

(6) $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$, $v_p(a_5) \geq n$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(7) $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) = n$, $v_p(a_4) \geq 3n/2$, $v_p(a_5) \geq 2n$ *and* $f(t)$ *has no root of valuation* $n/3$, $n/2$ *or* $2n/3$ *in* $\mathbb{Q}_p$,

(8) $v_p(a_4) = 0$, $v_p(a_5) \geq n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,

(9) $v_p(a_1) \geq n/4$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq 3n/4$, $v_p(a_4) = n$, $v_p(a_5) \geq 3n/2$ *and* $f(t)$ *has no root of valuation* $n/4, n/2$ *or* $3n/4$ *and has two irreducible factors of degree* 4 *in* $\mathbb{Q}_p$,

(10) $v_p(a_5) = 0$,

(11) $v_p(a_1) \geq n/5$, $v_p(a_2) \geq 2n/5$, $v_p(a_3) \geq 3n/5$, $v_p(a_4) \geq 4n/5$, $v_p(a_5) = n$ *and* $f(t)$ *has two irreducible factors of degree* 5 *in* $\mathbb{Q}_p$,

(12) $v_p(a_1) \geq 2n/5$, $v_p(a_2) \geq 4n/5$, $v_p(a_3) \geq 6n/5$, $v_p(a_4) \geq 8n/5$, $v_p(a_5) = 2n$ *and* $f(t)$ *has two irreducible factors of degree* 5 *in* $\mathbb{Q}_p$,

(13) $v_p(a_1) \geq n/2$, $v_p(a_2) \geq n$, $v_p(a_3) \geq 3n/2$, $v_p(a_4) \geq 2n$, $v_p(a_5) \geq 5n/2$ *and* $f(t)$ *has no root of valuation* $n/2$ *nor a factor of degree* 3 *or* 5 *in* $\mathbb{Q}_p$.

Proof Sketch. Since $f(t)$ is an irreducible Weil polynomial, we can apply Corollary 2.6 to $f(t)$. We need to analyze the irreducible factors of $f(t)$ over $\mathbb{Q}_p$, therefore we use the *Newton polygon* of $f(t)$.

Let $\mathcal{NP}(f)$ denote the Newton polygon of $f(t)$. Then $\mathcal{NP}(f)$ has 10 possible vertices $(0, 5n), (1, 4n + v_p(a_1)), (2, 3n + v_p(a_2)), (3, 2n + v_p(a_3)), (4, n + v_p(a_4)), (5, v_p(a_5))$, $(6, v_p(a_4)), (7, v_p(a_3)), (8, v_p(a_2)), (9, v_p(a_1))$ and $(10, 0)$. Note that if some of these points is a vertex, then the point must be a lattice point belonging to $\mathbb{Z} \times n\mathbb{Z}$. (cf. [4, p.64].) By symmetry of $\mathcal{NP}(f)$, it is sufficient to classify cases according to whether either $(1, 4n + v_p(a_1)), (2, 3n + v_p(a_2)), (3, 2n + v_p(a_3)), (4, n + v_p(a_4))$ or $(5, v_p(a_5))$ is a vertex or not.

Case 1. $(1, 4n + v_p(a_1))$ is a sole vertex:

In this case, $\mathcal{NP}(f)$ is as in Figure 1. This occurs if and only if $v_p(a_1) = 0, v_p(a_2) \geq n/2, v_p(a_3) \geq n, v_p(a_4) \geq 3n/2$ and $v_p(a_5) \geq 2n$. Then we can decompose $f(t)$ as

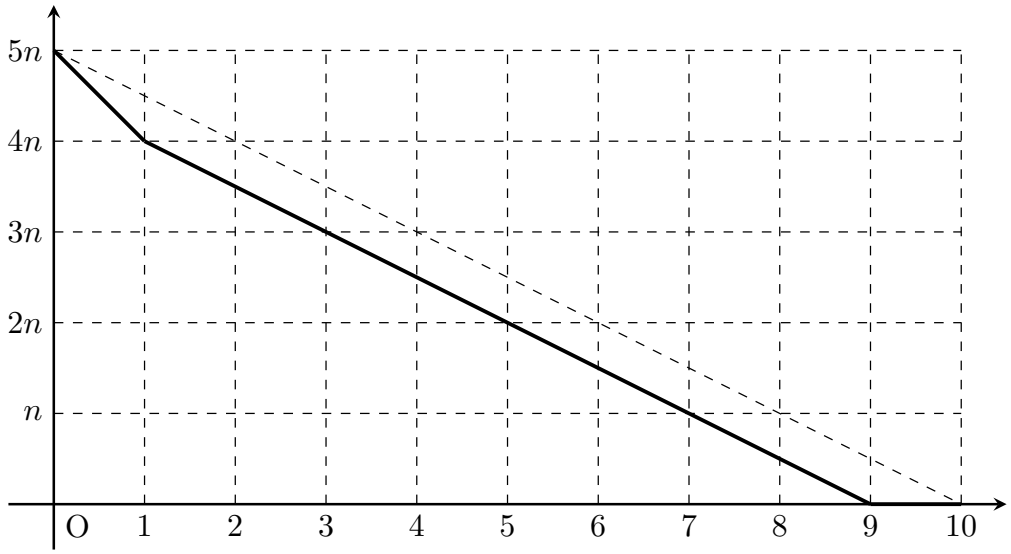

Figure 1. $(1, 4n + v_p(a_1))$ is a vertex.

$\prod_{i=1}^{10}(t - \alpha_i)$ in $\overline{\mathbb{Q}}_p[t]$ so that

$$t - \alpha_1,\ t - \alpha_{10},\ \prod_{i=2}^{9}(t - \alpha_i) \in \mathbb{Q}_p[t],$$
$$v_p(\alpha_1) = n, v_p(\alpha_{10}) = 0, v_p(\alpha_i) = n/2 \text{ for } i = 2, \cdots, 9.$$

Corollary 2.6 holds if and only if $f(t)$ has no root of valuation $n/2$ nor a factor of degree 3 in $\mathbb{Q}_p$. We omit the other cases.

□

3.2.6. Higher dimensional abelian varieties Little is known for the studies on the characteristic polynomials of abelian varieties of arbitrary dimension. In this section, we introduce the study on abelian varieties with a specific characteristic polynomial.

If X is a simple abelian variety of dimension g, then the multiplicity e of X divides $2g$. For example, as we saw Example 3.7, we consider simple abelian varieties of odd prime dimension l. We can specialize the multiplicity e to either 1 or l, however one can easily predict that both Problem 1 and Problem 3 will be very complicated in the case of $e = 1$. On the other hand, the case of $e = g$ is generally solved.

Theorem 3.19. *[3, Theorem 1.2] Let $a, b \in \mathbb{Z}$ and $2 < g \in \mathbb{Z}$. Set $f(t) = (t^2 + at + b)^g \in \mathbb{Z}[t]$. Then the polynomial $f(t)$ is the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q$ with $q = p^n$ elements if and only if g*

divides n, $b = q$, $|a| < 2\sqrt{q}$ *and* $a = kq^{s/g}$, *where* k, s *are integers satisfying* $(k, p) = 1$, $(s, g) = 1$ *and* $1 \leq s < g/2$.

Proof. Assume first that g divides n, $b = q$, $|a| < 2\sqrt{q}$ and $a = kq^{s/g}$, where k, s are integers satisfying $(k, p) = 1$, $(s, g) = 1$ and $1 \leq s < g/2$. Since $f(t)$ is a Weil polynomial, there exists a simple abelian variety X corresponding to a root of $f(t)$ in Theorem 2.1. Then we have $f_X(t) = (t^2 + at + q)^{\dim(X)}$. Since

$$\begin{aligned} m := v_p(a) &= v_p(kq^{s/g}) \\ &= v_p(p^{ns/g}) \qquad \text{since } (k, p) = 1, \\ &= ns/g < n/2, \end{aligned}$$

we obtain $\dim(X) = g$ from Lemma 2.4.

Conversely, we assume that the polynomial $f(t) = (t^2+at+b)^g$ is the characteristic polynomial of a simple abelian variety X of dimension g over $\mathbb{F}_q$. Since $f(t)$ is a Weil polynomial, we get $|a| \leq 2\sqrt{q}$ and $|b| = q$.

First, suppose $b = -q < 0$. This implies that $f(t)$ has a real root, which contradicts $g > 2$ from Lemma 3.5.

Second, suppose $b = q$ and $|a| = 2\sqrt{q}$. Then $f(t)$ has a real root again. Similarly, this contradicts $g > 2$. Hence we obtain $b = q$ and $|a| < 2\sqrt{q}$. Moreover, g divides n by Theorem 3.8. We note that the least common denominator of all invariants of $\mathrm{End}^0(X)$ is g. We consider the Newton polygon for $t^2 + at + q$. This has 3 possible vertices $(0, n), (1, v_p(a))$ and $(2, 0)$.

Suppose the Newton polygon is a line, i.e. $v_p(a) \geq n/2$ or $a = 0$ (See Figure 2). Then we can decompose t^2+at+q as $(t-\alpha_1)(t-\alpha_2)$ in $\overline{\mathbb{Q}}_p[t]$ so that $v_p(\alpha_1) = v_p(\alpha_2) = n/2$. We have

$$\begin{aligned} &\mathrm{lcd}\left(\frac{v_p(\alpha_1)}{n}[\mathbb{Q}_p(\alpha_1) : \mathbb{Q}_p], \frac{v_p(\alpha_2)}{n}[\mathbb{Q}_p(\alpha_2) : \mathbb{Q}_p]\right) \\ &= \mathrm{lcd}\left(\frac{1}{2}[\mathbb{Q}_p(\alpha_1) : \mathbb{Q}_p], \frac{1}{2}[\mathbb{Q}_p(\alpha_2) : \mathbb{Q}_p]\right), \end{aligned}$$

which is 1 or 2 since $[\mathbb{Q}_p(\alpha_i) : \mathbb{Q}_p] = 1$ or 2. This contradicts Lemma 2.5 since $g > 2$.

Hence the point $(1, v_p(a))$ must be a vertex of the Newton polygon. In other words, we have $v_p(a) < n/2$ and $a \neq 0$ (See Figure 2). Then we can decompose $t^2 + at + q$ as $(t - \alpha_1)(t - \alpha_2)$ so that $t - \alpha_1, t - \alpha_2 \in \mathbb{Q}_p[t]$, $v_p(\alpha_1) = n - v_p(a)$ and $v_p(\alpha_2) = v_p(a)$.

We have

$$\begin{aligned}&\operatorname{lcd}\left(\frac{v_p(\alpha_1)}{n}[\mathbb{Q}_p(\alpha_1):\mathbb{Q}_p], \frac{v_p(\alpha_2)}{n}[\mathbb{Q}_p(\alpha_2):\mathbb{Q}_p]\right)\\ &= \operatorname{lcd}\left(1-\frac{v_p(a)}{n}, \frac{v_p(a)}{n}\right)\\ &= \mathrm{d}\left(\frac{v_p(a)}{n}\right) = g\end{aligned}$$

if and only if $v_p(a) = ns/g$ with an integer s satisfying $(s,g) = 1$. Further, since $v_p(a) < n/2$, we have $s < g/2$. This implies that (g divides n and) $a = kq^{s/g}$, where k, s are integers satisfying $(k,p) = 1$, $(s,g) = 1$ and $1 \le s < g/2$. □

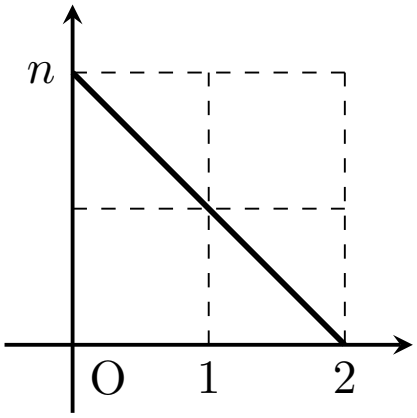

Figure 2. a line

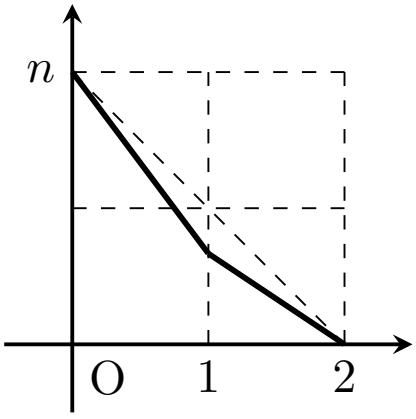

Figure 3. $(1, v_p(a))$ is a vertex

We can count the isogeny classes of a specific abelian variety from Tate's theorem by determining the characteristic polynomials explicitly.

Example 3.20. Consider the abelian varieties of dimension $g = 5$ over $\mathbb{F}_{2^{10}}$ with characteristic polynomial $(t^2 + at + b)^5$. By Theorem 3.19, we get that $b = 2^{10}$ and $s = 1, 2$. Thus $a = k\cdot(2^{10})^{s/5} = k\cdot 2^{2s} = 4k$ or $16k$, where $|a| < 2\cdot 2^5 = 64$ and k is an integer such that $(k,2) = 1$. By simple calculation, $a = \pm 4, \pm 12, \pm 16, \pm 20, \pm 28, \pm 36, \pm 44, \pm 48, \pm 52$ or ± 60. Hence, the number of the isogeny class of simple abelian varieties of dimension 5 over $\mathbb{F}_{2^{10}}$ with characteristic polynomial $(t^2 + at + 2^{10})^5$ is 20.

Acknowledgement

I am deeply grateful to Prof. Akio Tamagawa who recommended me to Algebraic Number Theory and Related Topics 2018. I also thank anonymous reviewers for their helpful comments on this article.

References

[1] K.Eisenträger, *"The theorem of Honda and Tate"*, http://personal.psu.edu/kxe8/honda tate.pdf

[2] S.Haloui, *"The characteristic polynomial of abelian varieties of dimension 3 over finite fields"*, *Journal of Number Theory*, Vol 130, no 12, 2010, p.2745-2752.

[3] D.Hayashida, *"The characteristic polynomials of abelian varieties of higher dimension over finite fields"*, *Journal of Number Theory*, Vol 196, 2019, p.205-222.

[4] S.Haloui and V.Singh, *"The characteristic polynomials of abelian varieties of dimension 4 over finite fields"*, *Contemporary Mathematics*, Vol 574, 2012, p.59-68.

[5] D.Maisner, E.Nart and E.W. Howe, *"Abelian surfaces over finite fields as Jacobians"*, *Experimental Mathematics*, 11:3, 2002, p.321-337.

[6] H.G. Rück, *"Abelian surfaces and Jacobian varieties over finite fields"*, *Compositio Mathematica*, Vol 76, no 3, 1990, p.351-366.

[7] G.Sohn, *"The bounds of the coefficients of the characteristic polynomials for abelian varieties of dimension 5 over finite fields"*, *Advanced Studies in Contemporary Mathematics*, Vol 23, no 3, 2013, p.415-421.

[8] W.C. Waterhouse, *"Abelian varieties over finite fields"*, *Ann. scient. E.N.S*, no 4, 1969, p.521-560.

[9] W.C. Waterhouse and J.S. Milne, *"Abelian varieties over finite fields"*, In 1969 *Number Theory Institute* (Proceedings of Symposia in Pure Mathematics, Vol.20), AMS, Providence, R.I., 1971, p.53-64.

[10] C.P. Xing, *"The characteristic polynomials of abelian varieties of dimension three and four over finite fields"*, *Science in China*, Vol 37, no 3, 1994, p.147-150.