CHARACTERISTIC POLYNOMIALS OF SIMPLE
ORDINARY ABELIAN VARIETIES OVER FINITE FIELDS

LENNY JONES

(Received 1 December 2020; accepted 15 January 2021; first published online 19 February 2021)

Abstract

We provide an easy method for the construction of characteristic polynomials of simple ordinary abelian varieties $A$ of dimension $g$ over a finite field $\mathbb{F}_q$, when $q \geq 4$ and $2g = \rho^{b-1}(\rho - 1)$, for some prime $\rho \geq 5$ with $b \geq 1$. Moreover, we show that $A$ is absolutely simple if $b = 1$ and $g$ is prime, but $A$ is not absolutely simple for any prime $\rho \geq 5$ with $b > 1$.

2020 Mathematics subject classification: primary 11G25; secondary 14G15, 14K05.

Keywords and phrases: simple ordinary abelian variety, absolutely simple abelian variety, finite field, characteristic polynomial.

1. Introduction

For positive integers $g$ and $q$, we say $f(t) \in \mathbb{Z}[t]$ is a $q$-polynomial if

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

$$= t^{2g} + a_g t^g + q^g + \sum_{j=1}^{g-1} a_j (t^{2g-j} + q^{g-j} t^j), \quad (1.1)$$

and all zeros of $f(t)$ have modulus $q^{1/2}$. Not all polynomials of the form (1.1) are $q$-polynomials since the condition on the moduli of the zeros of $f(t)$ imposes severe restrictions on its coefficients. For example,

$$f(t) = t^6 + t^5 + t^4 + 5t^3 + 2t^2 + 4t + 8$$

has the form (1.1) with $g = 3$ and $q = 2$, and although $f(t)$ has four zeros with modulus $2^{1/2}$, $f(t)$ has two real zeros, neither of which has modulus $2^{1/2}$.

Most likely, D. H. Lehmer [14] in 1932 was the first mathematician to investigate $q$-polynomials. He was mainly interested in $q$-polynomials with the property that all zeros have the form $q^{1/2} \zeta$, for some root of unity $\zeta$. Lehmer called such polynomials quasi-cyclotomic. Since then, certain $q$-polynomials, including Lehmer’s quasi-cyclotomics, have become central to the study of abelian varieties over finite fields.

© 2021 Australian Mathematical Publishing Association Inc.
Throughout this paper we let $k$ denote the finite field $\mathbb{F}_q$, where $q = p^n$ for some prime $p$ and positive integer $n$. It is well known from the Honda–Tate theorem [10, 18–20] that the isogeny class of an abelian variety $\mathcal{A}$ of dimension $g$ over $k$ is determined by the characteristic polynomial $f_{\mathcal{A}}(t) \in \mathbb{Z}[t]$ of its Frobenius endomorphism [18, 20]. With a slight abuse of terminology, we refer here to $f_{\mathcal{A}}(t)$ as the characteristic polynomial of $\mathcal{A}$. It follows from the Weil conjectures [9, 21] (conjectured in 1949 by Weil and subsequently proven by Dwork [4], Grothendieck [5], Deligne [2] and others) that $f_{\mathcal{A}}(t)$ has the form in (1.1) [17], and all zeros of $f_{\mathcal{A}}(t)$ have modulus $q^{1/2}$. In other words, $f_{\mathcal{A}}(t)$ is a $q$-polynomial. If a $q$-polynomial $f(t)$ is such that $f(t) = f_{\mathcal{A}}(t)$, for some abelian variety $\mathcal{A}$ over $k$, then $f(t)$ is called a Weil polynomial. Not every $q$-polynomial is a Weil polynomial, since additional restrictions on the coefficients of $f_{\mathcal{A}}(t)$ are imposed by the Honda–Tate theorem.

**Remark 1.1.** We caution the reader that while we have chosen to follow [12] in making no distinction between Weil polynomials and characteristic polynomials $f_{\mathcal{A}}(t)$, certain authors [7, 8, 15] have given a broader definition for Weil polynomials.

For small dimensions, explicit necessary and sufficient conditions on the coefficients of (1.1) have been given [7, 8, 15–17, 20] to determine which irreducible $q$-polynomials actually arise as characteristic polynomials of abelian varieties. Typically, Newton polygons are useful in the derivation of such conditions. For larger dimensions, however, this task becomes increasingly difficult and a complete characterisation in arbitrary dimension seems infeasible.

An abelian variety $\mathcal{A}$ over $k$ of dimension $g$ is called simple if $\mathcal{A}$ has no proper nontrivial subvarieties over $k$, and $\mathcal{A}$ is called absolutely simple if $\mathcal{A}$ is simple over the algebraic closure of $k$. Additionally, $\mathcal{A}$ is called ordinary if the rank of its group of $p$-torsion points over the algebraic closure of $k$ equals $g$.

It is the purpose of this paper to present an easy method for the construction of characteristic polynomials $f_{\mathcal{A}}(t)$, where $\mathcal{A}$ is a simple ordinary abelian variety of dimension $g$ over $k$ such that $q \geq 4$ and $2g = \rho^{b-1}(\rho - 1)$ for some prime $\rho \geq 5$ with $b \geq 1$. More precisely, we prove the following result.

**Theorem 1.2.** Let $\rho \geq 5$ be a prime, let $b \geq 1$ be an integer and let $2g = \rho^{b-1}(\rho - 1)$. Let $r$ be a prime such that $r$ is a primitive root modulo $\rho^2$. Let $p$ be a prime and let $n$ be a positive integer such that $q := p^n \geq 4$ and $q \equiv 1 \pmod{r}$. Let $m$ be an integer such that $m \neq -1/r \pmod{p}$ and

$$0 \leq m \leq \frac{2q^{b-1/2}(q^{b-1/2} - 1) - 1}{r}.$$
Define

\[ f(t) := t^{2g} + (mr + 1)t^g + q^g + \sum_{j=1}^{g-1} a_j(t^{2g-j} + q^{g-j}t^j), \tag{1.2} \]

where

\[ a_j = \begin{cases} 1 & \text{if } j \equiv 0 \pmod{\rho^{b-1}} \\ 0 & \text{otherwise} \end{cases} \quad \text{for } j \in \{1, 2, \ldots, g-1\}. \tag{1.3} \]

Then \( f(t) \) is the characteristic polynomial \( f_A(t) \) of a simple ordinary abelian variety \( A \) of dimension \( g \) over the field \( k = \mathbb{F}_q \). Furthermore,

1. if \( b = 1 \) and \( g \) is prime, then \( A \) is absolutely simple;
2. if \( b > 1 \) and \( \rho \) is arbitrary, then \( A \) is not absolutely simple.

2. Preliminaries

For any integer \( N \geq 1 \), let \( \Phi_N(x) \) denote the cyclotomic polynomial of index \( N \).

**Theorem 2.1** [6]. Let \( r \) be a prime such that \( r \nmid n \). Let \( \text{ord}_n(r) \) denote the order of \( r \) modulo \( n \). Then \( \Phi_n(x) \) factors modulo \( r \) into a product of \( \phi(n)/\text{ord}_n(r) \) distinct irreducible polynomials, each of degree \( \text{ord}_n(r) \).

**Corollary 2.2.** Let \( \rho \geq 3 \) and \( r \) be primes such that \( r \) is a primitive root modulo \( \rho^2 \). Let \( b \geq 1 \) be an integer. If \( f(x) \in \mathbb{Z}[x] \) is monic with \( f(x) \equiv \Phi_{\rho^b}(x) \pmod{r} \), then \( f(x) \) is irreducible over \( \mathbb{Q} \).

**Proof.** Since \( r \) is a primitive root modulo \( \rho^2 \), \( r \) is a primitive root modulo \( \rho^e \) for all \( e \geq 1 \) [1]. That is, \( \text{ord}_{\rho^e}(r) = \phi(\rho^e) \). Thus, it follows from Theorem 2.1 that \( f(x) \) is irreducible modulo \( r \) and hence irreducible over \( \mathbb{Q} \). \( \square \)

**Definition 2.3.** We say that \( f(x) \in \mathbb{R}[x] \) is reciprocal if \( f(x) = x^{\deg f} f(1/x) \).

**Theorem 2.4** [13]. Let \( N \geq 2 \) be an integer and let

\[ P_N(x) = \sum_{j=0}^{N} c_j x^j \in \mathbb{R}[x] \]

be reciprocal with \( c_N \neq 0 \). If there exists \( \delta \in \mathbb{R} \) with \( c_N \delta \geq 0 \) and \( |c_N| \geq |\delta| \), such that

\[ |c_N + \delta| \geq \sum_{j=1}^{N-1} |c_j + \delta - c_N|, \]

then all zeros of \( P_N(x) \) are on the unit circle.

**Theorem 2.5** [3]. Let \( n \) and \( g \) be positive integers. Let \( p \) be a prime and let \( q = p^n \). Suppose that \( f(t) \in \mathbb{Z}[t] \) is monic with \( \deg(f) = 2g \) and that \( a_g \) is the coefficient of \( t^g \).
If all zeros of $f(t)$ have modulus $q^{1/2}$ and $\gcd(a_g, p) = 1$, then $f(t)$ is the characteristic polynomial $f_{\mathcal{A}}(t)$ of an ordinary abelian variety $\mathcal{A}$ of dimension $g$ over $k$.

By the Honda–Tate theorem, we have the following result.

**Theorem 2.6** [11, 12]. Let $\mathcal{A}$ be an ordinary abelian variety of dimension $g$ over $k$, and let $f_{\mathcal{A}}(t)$ be the characteristic polynomial of $\mathcal{A}$. Then $\mathcal{A}$ is simple if and only if $f_{\mathcal{A}}(t)$ is irreducible.

The following theorem gives an easy test for determining whether a simple ordinary abelian variety $\mathcal{A}$ of dimension 2 over $k$ is absolutely simple.

**Theorem 2.7** [12, 15]. Let $\mathcal{A}$ be a simple ordinary abelian variety of dimension 2 over $k$ with characteristic polynomial $f_{\mathcal{A}}(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 q t + q^2$. Then $\mathcal{A}$ is absolutely simple if and only if $a_1^2 \notin \{0, q + a_2, 2a_2, 3a_2 - 3q\}$.

**Proposition 2.8** [12, Lemma 5]. Let $\theta$ be an algebraic number with minimal polynomial $f \in \mathbb{Q}[x]$, and suppose that $d$ is a positive integer such that the field $\mathbb{Q}(\theta^d)$ is a proper subfield of $\mathbb{Q}(\theta)$ and such that $\mathbb{Q}(\theta^z) = \mathbb{Q}(\theta)$ for all positive integers $z < d$. Then either $f \in \mathbb{Q}[x^d]$ or there is a primitive $d$th root of unity $\zeta_d$ such that $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^d, \zeta_d)$.

The following theorem addresses when a simple ordinary abelian variety $\mathcal{A}$ of arbitrary dimension over $k$ is absolutely simple.

**Theorem 2.9** [12]. Let $\mathcal{A}$ be a simple ordinary abelian variety over $k$ with characteristic polynomial $f_{\mathcal{A}}(t)$. Suppose that $f_{\mathcal{A}}(\theta) = 0$. Then $\mathcal{A}$ is absolutely simple if and only if $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^d)$ for all integers $d > 0$.

### 3. Proof of Theorem 1.2

We first prove that $f(t)$ is a $q$-polynomial. To accomplish this task, it is enough to show that all zeros of $f(t)$ have modulus $q^{1/2}$, since it is obvious that $f(t)$ has the form (1.1). Let $a_g := mr + 1$. Since

$$\left\lceil \frac{g - 1}{\rho^{b-1}} \right\rceil = \frac{g}{\rho^{b-1}} - 1 = \frac{\rho - 3}{2},$$

we have from (1.3) that

$$f(t) = t^{2g} + a_g t^g + q^g + \sum_{u=1}^{(\rho-3)/2} (t^{2g-qp^{b-1}} + q^{g-qp^{b-1}}).$$

Thus

$$F(t) := f(q^{1/2}t) = q^{g} t^{2g} + q^{g/2} a_g t^g + q^g + \sum_{u=1}^{(\rho-3)/2} q^{(2g-qp^{b-1})/2} (t^{2g-qp^{b-1}} + tp^{b-1})$$
is reciprocal. Let

\[ S = |c_N + \delta| - \sum_{j=1}^{N-1} |c_j + \delta - c_N|, \]

where \( N = 2g \), \( c_N = \delta = q^j \) and \( c_j \) is the coefficient of \( t^j \) in \( F(t) \), for \( j = 1, 2, \ldots, N - 1 \). Then, using the fact that

\[ a_g \leq 2q^{b-1/2}(q^{b-1/2} - 1), \]

we have

\[
S = 2q^g - 2(q^{[2g - \rho b - 1]/2} + q^{[2g - (\rho - 3)/2]q^{b-1}/2} + \cdots + q^{[2g - (\rho - 3)/2]q^{b-1}/2}) - a_g q^g/2 \\
= 2q^g - 2q^{[2g - (\rho - 3)/2]q^{b-1}/2}((q^{b-1/2})^{(\rho - 3)/2} + \cdots + q^{b-1/2}) - a_g q^g/2 \\
= 2q^g - 2q^{[2g - (\rho - 3)/2]q^{b-1}/2}((q^{b-1/2})^{(\rho - 3)/2} - 1)\frac{q^{b-1/2} - 1}{q^{b-1/2}} - a_g q^g/2 \\
\geq 2q^g - 2q^{[2g - (\rho - 3)/2]q^{b-1}/2}((q^{b-1/2})^{(\rho - 3)/2} - 1)\frac{q^{b-1/2} - 1}{q^{b-1/2} - 1} \\
= 2q^{(2g + 3\rho - 1)/2} - 4q^g - 2q^{(g + 3\rho - 1)/2} + 4q^{(g + 2\rho - 1)/2} \\
\geq 2q^{(2g + 3\rho - 1)/2} - 1 \\
\]

since \( g \geq 2\rho - 1 \) and \( q \geq 4 \). Hence, from Theorem 2.4, all zeros of \( F(t) \) are on the unit circle, and consequently, all zeros of \( f(t) \) have modulus \( q^{1/2} \).

We now show that \( f(t) \) is a Weil polynomial. In particular, we prove that \( f(t) = f_{\mathcal{A}}(t) \) for a simple ordinary abelian variety of dimension \( g \) over \( k \). Observe that \( \gcd(a_g, \rho) = 1 \) since \( m \not\equiv -1/r \) (mod \( p \)), and so we deduce from Theorem 2.5 that \( f(t) = f_{\mathcal{A}}(t) \), where \( \mathcal{A} \) is an ordinary abelian variety of dimension \( g \) over \( k \). Since \( r \) is a primitive root modulo \( p^2 \) and \( f_{\mathcal{A}}(t) \equiv \Phi_{\rho r}(t) \) (mod \( r \)), it follows from Corollary 2.2 that \( f_{\mathcal{A}}(t) \) is irreducible over \( Q \). Therefore, since \( \mathcal{A} \) is ordinary, we conclude that \( \mathcal{A} \) is simple by Theorem 2.6.

For part (1), suppose that \( b = 1 \) and \( g \) is prime. Since all zeros of \( f_{\mathcal{A}}(t) \) have modulus \( q^{1/2} \), the only possible real zeros of \( f_{\mathcal{A}}(t) \) are \( \pm q^{1/2} \). Clearly, \( q^{1/2} \) is not a zero since \( f_{\mathcal{A}}(q^{1/2}) > 0 \). If \( f_{\mathcal{A}}(-q^{1/2}) = 0 \), then the zero \( -q^{1/2} \) has even multiplicity since \( \deg(f_{\mathcal{A}}) \equiv 0 \) (mod 2), which contradicts the fact that \( f_{\mathcal{A}}(t) \) is separable. Thus, \( f_{\mathcal{A}}(t) \) has no real zeros. It follows that \( Q(\theta^d) \) is a CM-field for every integer \( d \geq 1 \). By way of contradiction, assume that \( d \) is the smallest positive integer such that \( Q(\theta^d) \) is a proper subfield of \( Q(\theta) \). Let \( K \) be the maximal real subfield of \( Q(\theta^d) \), so that \([Q(\theta^d) : K] = 2\). Thus, since \( g \) is prime, it follows that \( K = Q \) and

\[
[Q(\theta) : Q(\theta^d)] = g. \tag{3.1}
\]
Since $f_A \not\in \mathbb{Q}[x^d]$, we conclude from Proposition 2.8 that $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^d, \zeta_d)$ for some primitive $d$th root of unity $\zeta_d$. Hence,

$$[\mathbb{Q}(\theta) : \mathbb{Q}(\theta^d)] = \phi(d).$$

Combining (3.1) and (3.2), we see that $\phi(d) = g$. Consequently, $g = 2$. In this case we have from (1.2) that

$$f_A(t) = r^4 + r^3 + (mr + 1)t^2 + qt + q^2,$$

where $a_1 = 1$ and $a_2 = mr + 1$. Thus, it is easy to check from Theorem 2.7 that $\mathcal{A}$ is absolutely simple, and hence $\mathbb{Q}(\theta^d) = \mathbb{Q}(\theta)$ by Theorem 2.9. This contradiction proves (1).

Finally, to establish (2), suppose that $f_A(\beta) = 0$. Since $b > 1$, it follows from (1.2) and the irreducibility of $f_A(t)$ that the minimal polynomial of $\beta^{b^{-1}}$ has degree $\rho - 1$. Hence, $\mathbb{Q}(\beta^{b^{-1}}) \neq \mathbb{Q}(\beta)$, and $\mathcal{A}$ is not absolutely simple by Theorem 2.9.

4. Examples

We give two examples to illustrate Theorem 1.2. The first example, with $b = 1$, gives the characteristic polynomial of an absolutely simple ordinary abelian variety $\mathcal{A}$ of dimension 3 over $\mathbb{F}_{11^2}$. The second example, with $b = 3$, gives the characteristic polynomial of an ordinary abelian variety $\mathcal{A}$ of dimension 50 over $\mathbb{F}_7$, which is simple but not absolutely simple.

**EXAMPLE 4.1.** Let $b = 1$ and $\rho = 7$, so that $g = 3$ is prime. Since $\text{ord}_{49}(5) = 42 = \phi(49)$, we see that $r = 5$ is a prime primitive root modulo $\rho^2$. Let $n = 2$ and $p = 11$. Then $q = 11^2 \equiv 1 \pmod{5}$. Finally, we choose $m = 1$, noting that

$$m \not\equiv -1/r \equiv -1/5 \equiv 2 \pmod{11}.$$ 

Thus, $mr + 1 = 6$. Since $\rho^{b^{-1}} = 1$, we have $a_j = 1$ for $j \in \{1, 2\}$ in (1.3). Therefore,

$$f_A(t) = r^6 + 6r^3 + (11^2)^3 + \frac{2}{11^2} \left( (t^{b-j} + (11^2)^{3-j}t^j) \right)$$

$$= r^6 + r^5 + r^4 + 6t^3 + 112t^2 + (11^2)^2t + (11^2)^3$$

$$= r^6 + r^5 + r^4 + 6t^3 + 121t^2 + 14641t + 1771561.$$

**EXAMPLE 4.2.** Let $b = 3$ and $\rho = 5$, so that $g = \rho^2(\rho - 1)/2 = 50$. Since $\text{ord}_{25}(2) = 20 = \phi(25)$, we see that $r = 2$ is a prime primitive root modulo $\rho^2$. Let $n = 1$ and $p = 7$. Then $q = 7 \equiv 1 \pmod{2}$. Finally, we choose $m = 9$, noting that

$$m \equiv 2 \not\equiv 3 \equiv -1/2 \equiv -1/r \pmod{7}.$$ 

Thus, $mr + 1 = 19$. Since $\rho^{b^{-1}} = 25$, it follows that $a_j = 1$ for $j = 25$ and $a_j = 0$ for $j \in \{1, 2, \ldots, 49\} \setminus \{25\}$ in (1.3). Therefore,

$$f_A(t) = t^{100} + t^{75} + 19t^{50} + 7^{25}t^{25} + 7^{50}.$$
Acknowledgement

The author thanks the anonymous referee for helpful comments.

References

[1] D. Burton, *Elementary Number Theory*, 7th edition (McGraw-Hill, New York, 2011).
[2] P. Deligne, ‘La conjecture de Weil. I’, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.
[3] S. A. DiPippo and E. W. Howe, ‘Real polynomials with all roots on the unit circle and abelian varieties over finite fields’, *J. Number Theory* **73**(2) (1998), 426–450.
[4] B. Dwork, ‘On the rationality of the zeta function of an algebraic variety’, *Amer. J. Math.* **82** (1960), 631–648.
[5] A. Grothendieck, ‘Formule de Lefschetz et rationalité des fonctions *L*’, *Séminaire Bourbaki*, **9**, Exp. No. 279 (Société Mathématique de France, Paris, 1995), 41–55.
[6] W. J. Guerrier, ‘The factorization of the cyclotomic polynomials mod *p*’, *Amer. Math. Monthly* **75** (1968) 46.
[7] S. Haloui, ‘The characteristic polynomials of abelian varieties of dimensions 3 over finite fields’, *J. Number Theory* **130**(12) (2010), 2745–2752.
[8] S. Haloui and V. Singh, ‘The characteristic polynomials of abelian varieties of dimension 4 over finite fields’, *Arithmetic, Geometry, Cryptography and Coding Theory*, Contemporary Mathematics, 574 (American Mathematical Society, Providence, RI, 2012), 59–68.
[9] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, 52 (Springer-Verlag, New York, 1977).
[10] T. Honda, ‘Isogeny classes of abelian varieties over finite fields’, *J. Math. Soc. Japan* **20** (1968), 83–95.
[11] E. W. Howe, ‘Principally polarized ordinary abelian varieties over finite fields’, *Trans. Amer. Math. Soc.* **347** (1995), 2361–2401.
[12] 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) (2002), 139–163.
[13] P. Lakatos and L. Losonczi, ‘Circular interlacing with reciprocal polynomials’, *Math. Inequal. Appl.* **10**(4) (2007), 761–769.
[14] D. H. Lehmer, ‘Quasi-cyclotomic polynomials’, *Amer. Math. Monthly* **39**(7) (1932), 383–389.
[15] D. Maisner and E. Nart, ‘Abelian surfaces over finite fields as Jacobians’, with an appendix by Everett W. Howe, *Experiment. Math.* **11**(3) (2002), 321–337.
[16] H. Rück, ‘Abelian surfaces and Jacobian varieties over finite fields’, *Compositio Math.* **76**(3) (1990), 351–366.
[17] V. Singh, G. McGuire and A. Zaytsev, ‘Classification of characteristic polynomials of simple supersingular abelian varieties over finite fields’, *Funct. Approx. Comment. Math.* **51**(2) (2014), 415–436.
[18] J. Tate, ‘Endomorphisms of abelian varieties over finite fields’, *Invent. Math.* **2** (1966) 134–144.
[19] W. C. Waterhouse, ‘Abelian varieties over finite fields’, *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.
[20] W. C. Waterhouse and J. S. Milne, ‘Abelian varieties over finite fields’, *Proc. Sympos. Pure Math.* **20** (1971), 53–64.
[21] A. Weil, ‘Numbers of solutions of equations in finite fields’, *Bull. Amer. Math. Soc.* **55** (1949), 497–508

LENNY JONES, Professor Emeritus of Mathematics, Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, USA

e-mail: lkjone@ship.edu