On The Characteristic Polynomial of Frobenius of Supersingular Abelian Varieties Of Dimension up to 7 over Finite Fields

Vijaykumar Singh, Alexey Zatysev, Gary McGuire

May 12, 2010

Abstract

In this article, we derive a list of possible characteristic polynomials of the Frobenius of simple supersingular abelian varieties of dimension $1,\ 2,\ 3,\ 4,\ 5, 6, 7$ over $\mathbb{F}_q$ where $q = p^n,\ \ n$ odd.

1 Introduction

Supersingular abelian varieties have applications in cryptography and coding theory. Identity based ecryption and computation of weights of some Reed Muller codes are some of them. The important (isogeny) invariant which carries most of the information about supersingular curves is the characteristic polynomial of the Frobenius. Here we give a list of such polynomials up to dimension 7 over $\mathbb{F}_q$ where $q = p^n,\ \ n$ odd. We also give the procedure, which extends to all dimensions.

Let A be an abelian variety of dimension g over $\mathbb{F}_q$ where $q = p^n$. The characteristic polynomial $P(X) \in \mathbb{Z}[X]$ of the Frobenius endomorphism is given by

$$P_A(X) = X^{2g} + a_1X^{2g-1} + \cdots + a_gX^g + qa_{g-1}X^{g-1} \cdots + q^g.$$

An abelian variety A is simple if it is not isogenous to a product of abelian varieties of lower dimensions. In that case $P_A(X)$ is either irreducible over $\mathbb{Z}$ or $P(X) = h(X)^e$ where $h(x) \in \mathbb{Z}[X]$ is irreducible, see [8]. An elliptic curve E over $\mathbb{F}_q$ is supersingular if $E(\bar{\mathbb{F}_q})$ has no points of order p. An abelian variety A over $\mathbb{F}_q$ is called supersingular if A is isogenous over $\bar{\mathbb{F}_q}$ to a product of supersingular elliptic curves. Given $P_A(X)$ for an abelian variety of dimension g, we have the following test from Stichtenoth and Xing [5] for supersingularity.

Theorem 1.1. *Suppose $q = p^n$ and suppose that A is an abelian variety of dimension g over $\mathbb{F}_q$. Let $P_A(X) = X^{2g} + a_1X^{2g-1} + \cdots + a_gX^g + qa_{g-1}X^{g-1} \cdots + q^g$ be the characteristic polynomial of the Frobenius endomorphism on A. Then A is supersingular if and only if, for all $1 \leq j \leq g$,*

$$p^{\lceil \frac{jn}{2} \rceil} | a_j.$$

We can factor $P(X)$ over the complex numbers as $P(X) = \prod_{i=1}^{2g}(X - \alpha_i)$ where the α_i are algebraic integers. If A is supersingular then Manin [6] and Oort [4] proved that numbers $\frac{\alpha_i}{\sqrt{q}}$ are roots of unity.

In this article we are interested in the characterization of the Frobenius for simple supersingular abelian varieties of the dimension g over $\mathbb{F}_{q^n}$, where $1 \leq g \leq 7$ and n is odd. We write $P(x)$ instead of $P_A(x)$ when the underlying abelian variety is understood.

2 Frobenius Polynomial

In this section we give the results and procedure for computing the characteristic polynomial of Frobenius.

Theorem 2.1. *If $P(X)$ is irreducible with $a_{2i+1} \neq 0$ for some i, then the a_i's satisfy*

$$(t^{2g} + \frac{a_2 t^{2g-2}}{q} + \ldots + \frac{a_{2i} t^{2g-2i}}{q^i} + \ldots + 1)^2 - \frac{1}{q}(a_1 t^{2g-1} + \frac{a_3 t^{2g-3}}{q} + \ldots + a_1 t)^2 = 0.$$

Proof. By dividing the characteristic polynomial of Frobenius by q^g we get,

$$\frac{P(X)}{q^g} = \frac{X^{2g}}{q^g} + a_1 \frac{X^{2g-1}}{q^g} + \ldots + a_g \frac{X^g}{q^g} + q^{g-1} + \frac{X}{q^g} + 1 = 0.$$

Doing the transformation $\frac{X}{\sqrt{q}} \to t$ over $\mathbb{Q}(\sqrt{q})$ and rearranging we get

$$G(t) := (t^{2g} + \frac{a_2 t^{2g-2}}{q} + \ldots + \frac{a_{2i} t^{2g-2i}}{q^i} + \ldots + 1) + \frac{1}{\sqrt{q}}(a_1 t^{2g-1} + \frac{a_3 t^{2g-3}}{q} + \ldots + a_1 t) = 0.$$

Since $q = p^n$, n odd, $Gal(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) = \{1, \sigma\}$ where $\sigma(\sqrt{q}) = -\sqrt{q}$. Therefore

$$H(t) := G(t)G(t)^\sigma = (t^{2g} + \frac{a_2 t^{2g-2}}{q} + \ldots + \frac{a_{2i} t^{2g-2i}}{q^i} + \cdots + 1)^2 - \frac{1}{q}(a_1 t^{2g-1} + \frac{a_3 t^{2g-3}}{q} + \ldots + a_1 t)^2 = 0.$$

□

The polynomial $H(t)$ defined above has only even powers of t. We proved the following.

Proposition 2.2. *Let $G(t) \in \mathbb{Q}(\sqrt{q})[t]$ (as defined above) be reducible over $\mathbb{Q}(\sqrt{q})$. Then $G(t) = F_1(t)F_2(t)$ where F_1, F_2 are irreducible over $\mathbb{Q}(\sqrt{q})[t]$ with $\deg F_1, \deg F_2 = g$.*

Proposition 2.3. *Assume $a_{2i+1} \neq 0$.*

1. *If $G(t)$ is irreducible over $\mathbb{Q}(\sqrt{q})$ then $H(t)$ is an irreducible cyclotomic factor of $t^m - 1$ of degree $4g$ where $\phi(m) = 4g$ over $\mathbb{Q}$.*

2. *If $G(t)$ is reducible over $\mathbb{Q}(\sqrt{q})$ then $G(t) = F_1(t)F_2(t)$ where at least one of F_1, $F_2 \in \mathbb{Q}(\sqrt{q})[t] \setminus \mathbb{Q}[t]$. If $F_i \in \mathbb{Q}[t]$ then it is an irreducible cyclotomic factor of $t^m - 1$ of degree g where $\phi(m) = g$, else $F_i F_i^\sigma \in \mathbb{Q}[t]$ is an irreducible cyclotomic factor of $t^m - 1$ of degree $2g$ where $\phi(m) = 2g$.*

Proposition 2.4. *If $a_{2i+1} = 0$ for all i then*

1. *If $G(t)$ is irreducible over $\mathbb{Q}$, it is an irreducible cyclotomic factor of $t^m - 1$ of degree g where $\phi(m) = 2g$.*

2. *If $G(t)$ is reducible over $\mathbb{Q}$, then $G(t) = F_1F_2$ where F_i are irreducible cyclotomic factor of $t^m - 1$ of degree g with $\phi(m) = g$.*

Using the above propositions we have the following procedure to derive the characteristic polynomial.

2.1 Procedure

1. Suppose $P(x)$ is irreducible.
   (a) If $a_{2i+1} \neq 0$ for some i.
      i. If $G(t)$ is irreducible, then as in proposition 2.3 find appropriate $H(t)$ and solve for the a_i's.
      ii. If $G(t)$ is reducible then use proposition 2.3 to find appropriate $H(t) = G(t)G(t)^\sigma$ and solve for the a_i's .
   (b) If $a_{2i+1} = 0$ for all i.
      i. If $G(t)$ is irreducible over $\mathbb{Q}$ then use proposition 2.4 to find appropriate cyclotomic factors and compare with $G(t)$ to solve for a_i's.
      ii. If $G(t)$ is reducible over $\mathbb{Q}$ then use proposition 2.4 to compute $G(t) = F_1(t)F_2(t)$ and compare coefficients to solve for a_i's.
2. Suppose $P(x)$ is reducible ie; $P(x) = h(x)^e$ with $e|g$. Then for $\frac{h(x)}{q^{\frac{g}{e}}}$, doing the transformation $\frac{x}{\sqrt{q}} \to t$, we get a new polynomial $G(t)$ whose roots are roots of unity, and using above tools we can find $h(x)$.

Using the procedure above we have proved the following.

Theorem 2.5. *The characteristic polynomial of a simple supersingular abelian variety over $\mathbb{F}_q$, $q = p^n$, n odd is one of the following*

1. dimension 1
   (a) $p = 2 : x^2 \pm \sqrt{2q}x + q$
   (b) $p = 3 : x^2 \pm \sqrt{3q}x + q$
   (c) $x^2 + q$
2. dimension 2
   (a) $p \neq 3 : x^4 - qx^2 + q^2$
   (b) $x^4 + qx^2 + q^2$
   (c) $p = 2 : x^4 \pm \sqrt{pq}x^3 + qx^2 \pm \sqrt{pq}x + q^2$

(d) $p = 5 : x^4 \pm \sqrt{pq}x^3 + 3qx^2 \pm \sqrt{pq}x + q^2$

(e) $(x^2 - q)^2$

(f) $p \neq 2 : x^4 + q^2$

3. dimension 3

(a) $p = 3 : x^6 \pm q\sqrt{pq}x^3 + q^3$

(b) $p = 7 : x^6 \pm \sqrt{pq}x^5 + 3qx^4 \pm q\sqrt{pq}x^3 + 3q^2x^2 \pm q^2\sqrt{pq}x + q^3$

4. dimension 4

(a) $p = 2 : x^8 \pm \sqrt{2q}x^7 + qx^6 - q^2x^4 + q^3x^2 \pm q^3\sqrt{2q}x + q^4$

(b) $p = 3 : x^8 \pm \sqrt{3q}x^7 + 2qx^6 \pm q\sqrt{3q}x^5 + q^2x^4 \pm q^2\sqrt{3q}x^3 + 2q^3x^2 \pm q^3\sqrt{3q}x^+q^4$

(c) $x^8 + q^4$

(d) $x^8 - qx^6 + q^2x^4 - q^3x^2 + q^4$

(e) $p \neq 5 : x^8 + qx^6 + q^2x^4 + q^3x^2 + q^4$

(f) $p \neq 2 : x^8 - q^2x^4 + q^4$

(g) $p = 5 : x^8 \pm \sqrt{5q}x^7 + 2qx^6 \pm q\sqrt{5q}x^5 + 3q^2x^4 \pm q^2\sqrt{5q}x^3 + 2q^3x^2 + \pm q^3\sqrt{5q}x^+q^4$

5. dimension 5

(a) $p = 11 : X^{10} \pm \sqrt{11q}X^9 + 5qX^8 \pm q\sqrt{11q}X^7 - q^2X^6 \pm q^2\sqrt{11q}X^5 - q^3X^4 \pm q^3\sqrt{11q}X^3 + 5q^4X^2 \pm q^4\sqrt{11q}X + q^5.$

6. dimension 6

(a) $p = 2 : x^{12} \pm \sqrt{2q}x^{11} + qx^{10} - q^2x^8 - q^2(\pm\sqrt{2q})x^7 - q^3x^6 - q^3(\pm\sqrt{2q})x^5 - q^4x^4 + q^5x^2 \pm q^5\sqrt{2q}x + q^6$

(b) $p = 2 : x^{12} \pm q\sqrt{2q}x^9 + q^3x^6 \pm q^4\sqrt{2q}x^3 + q^6$

(c) $p = 3 : x^{12} \pm \sqrt{3q}x^{11} + 2qx^{10} \pm 3q\sqrt{3q}x^9 + q^2x^8 - q^3x^6 + q^4x^4 \pm 3q^4\sqrt{3q}x^3 + 2q^5x^2 \pm q^5\sqrt{3q}x + q^6$

(d) $p = 7 : x^{12} \pm \sqrt{7q}x^{11} + 4qx^{10} \pm q\sqrt{7q}x^9 - q^2x^8 - 2q^2(\pm\sqrt{7q})x^7 - 7q^3x^6 - 2q^3(\pm\sqrt{7q})x^5 - q^4x^4 \pm q^4\sqrt{7q}x^3 + 4q^5x^2 \pm q^5\sqrt{7q}x + q^6$

(e) $p = 7 : x^{12} \pm 2\sqrt{7q}x^{11} + 13qx^{10} \pm 8q\sqrt{7q}x^9 + 29q^2x^8 \pm 14q^2\sqrt{7q}x^7 + 41q^3x^6 \pm 14q^3\sqrt{7q}x^5 + 29q^4x^4 \pm 8q^4\sqrt{7q}x^3 + 13q^5x^2 \pm 2q^5\sqrt{7q}x + q^6$

(f) $p = 13 : x^{12} \pm \sqrt{13q}x^{11} + 7qx^{10} \pm 3q\sqrt{13q}x^9 + 15q^2x^8 \pm 5q^2\sqrt{13q}x^7 + 19q^3x^6 \pm 5q^3\sqrt{13q}x^5 + 15q^4x^4 \pm 3q^4\sqrt{13q}x^3 + 7q^5x^2 \pm q^5\sqrt{13q}x + q^6$

(g) $p = 3 : x^{12} \pm 2q\sqrt{3q}x^9 + 5q^3x^6 \pm 2q^4\sqrt{3q}x^3 + q^6$

(h) $x^{12} + qx^{10} + q^2x^8 + q^3x^6 + q^4x^4 + q^5x^2 + q^6$

(i) $p \neq 7 : x^{12} - qx^{10} + q^2x^8 - q^3x^6 + q^4x^4 - q^5x^2 + q^6$

(j) $p \neq 3 : x^{12} - q^3x^6 + q^6$

(k) $x^{12} + q^3x^6 + q^6$

7. dimension 7*: None*

Remarks:

The procedure above can be extended to any genus.

Work is in progress for n even.

An important question is whether the above actually occur as the characteristic polynomial of the Frobenius. Work is in progess on this question. For genus 1, 2 and 3 all of the polynomials listed occur, see [2], [7] and [9] respectively. For genus 4 the following occur as Jacobians of hyperelliptic curves of genus 4 over $\mathbb{F}_q$ where $q = 2^n, n$ odd. An example of each is given here for $q = 2^5$ where α is a primitive root. These are cases (a), (c), (e) of the theorem.

$P(x)$	Curve
$x^8 + \sqrt{2q}x^7 + qx^6 - q^2x^4 + q^3x^2 + q^3\sqrt{2q}x + q^4$	$y^2 + y = x^9 + \alpha^2x^5 + \alpha^9x^3$
$x^8 - \sqrt{2q}x^7 + qx^6 - q^2x^4 + q^3x^2 - q^3\sqrt{2q}x + q^4$	$y^2 + y = x^9 + \alpha^2x^5 + \alpha^{25}x^3$
$x^8 + q^4$	$y^2 + y = x^9 + x^5 + \alpha^3x^3$
$x^8 + qx^6 + q^2x^4 + q^3x^2 + q^4$	$y^2 + y = x^9 + x^5 + \alpha x^3$

References

[1] H-G Ruck,Abelian Surfaces and Jacobian varieties over finite fields, Compositio Math. 76(1990),351-366.

[2] Waterhouse Abelian Varieties over finite fields, ANn.Sci.Ecole Norm.Sup (4) 2 (1969),521-560.

[3] C.P.Xing, On supersingular abelian varieties of dimension two over finite fields, Finite fields and their app. 2, 407-421 (1996).

[4] Frans Oort, Subvarieties of Moduli Spaces, Invent.Math., 24:95-119, 1974.

[5] H. Stichtenoth and C. Xing, On the structure of the divisor class group of a class of curves over finite fields, Arch. Math., Vol. 65 (1995) 141-150.

[6] Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, Russ. Math. Surv., 18, No. 6 (1963) 1983.

[7] D. Maisner, E. Nart, appendix of E. W. Howe. Abelian surfaces over finite fields as jacobians.Experiment. Math.. Vol 11, p. 321-337, 2002.

[8] Waterhouse W. C., Milne J. S. Abelian varieties over finite fields. Proceedings of Symposia in Pure Mathematics (1971) 20:5364

[9] E. Nart, C. Ritzenthaler. Jacobians in isogeny classes of supersingular threefolds in characteristic 2. Finite Fields and Their Applications. no 14, p. 676-702, 2008.