



# The characteristic polynomials of abelian varieties of dimensions 4 over finite fields

Safia Haloui, Vijaykumar Singh

## ► To cite this version:

Safia Haloui, Vijaykumar Singh. The characteristic polynomials of abelian varieties of dimensions 4 over finite fields. 2011. hal-00559807

**HAL Id: hal-00559807**

**<https://hal.science/hal-00559807>**

Preprint submitted on 26 Jan 2011

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# THE CHARACTERISTIC POLYNOMIALS OF ABELIAN VARIETIES OF DIMENSIONS 4 OVER FINITE FIELDS

SAFIA HALOUI, VIJAYKUMAR SINGH

ABSTRACT. We describe the set of characteristic polynomials of abelian varieties of dimension 4 over finite fields.

## 1. INTRODUCTION AND RESULTS

The aim of this paper is to give a description of the set of characteristic polynomials of abelian varieties of dimension 4 as it was done in [1] for dimension 3.

It is well known that the characteristic polynomial of an abelian variety of dimension  $g$  over  $\mathbb{F}_q$  (with  $q = p^n$ ) is monic, with integer coefficients, of degree  $2g$  and that the sets of its roots consist of couples of complex conjugated numbers of modulus  $\sqrt{q}$ . Any polynomial having those properties is called a *Weil polynomial*. Obviously, every Weil polynomial of degree 8 has the form

$$p(t) = t^8 + a_1 t^7 + a_2 t^6 + a_3 t^5 + a_4 t^4 + q a_3 t^3 + q^2 a_2 t^2 + q^3 a_1 t + q^4$$

for certain integers  $a_1, a_2, a_3$  and  $a_4$ . In Section 2 we prove the following proposition which gives a characterization of the quadruples  $(a_1, a_2, a_3, a_4)$  corresponding to Weil polynomials of degree 8 (see [8, 4, 1] for a characterization of Weil polynomials of lower degrees):

**Theorem 1.1.** *Let  $p(t) = t^8 + a_1 t^7 + a_2 t^6 + a_3 t^5 + a_4 t^4 + q a_3 t^3 + q^2 a_2 t^2 + q^3 a_1 t + q^4$  be a polynomial with integer coefficients. Then  $p(t)$  is a Weil polynomial if and only if either*

$$p(t) = (t^2 \pm \sqrt{q})^2 h(t)$$

where  $h(t)$  is a Weil polynomial, or the following conditions hold:

- (1)  $|a_1| < 8\sqrt{q}$ ,
- (2)  $6\sqrt{q}|a_1| - 20q < a_2 \leq \frac{3a_1^2}{8} + 4q$ ,
- (3)  $-9qa_1 - 4\sqrt{q}a_2 - 16q\sqrt{q} < a_3 < -9qa_1 + 4\sqrt{q}a_2 + 16q\sqrt{q}$ ,
- (4)  $-\frac{a_1^3}{8} + \frac{a_1 a_2}{2} + qa_1 - (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2} \leq a_3 \leq -\frac{a_1^3}{8} + \frac{a_1 a_2}{2} + qa_1 + (\frac{2}{3}(\frac{3a_1^2}{8} - a_2 + 4q))^{3/2}$ ,
- (5)  $2\sqrt{q}|qa_1 + a_3| - 2qa_2 - 2q^2 < a_4$ ,
- (6)  $\frac{9a_1^4}{256} - \frac{3a_1^2 a_2}{16} + \frac{a_1 a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + \omega + \bar{\omega} \leq a_4 \leq \frac{9a_1^4}{256} - \frac{3a_1^2 a_2}{16} + \frac{a_1 a_3}{4} + \frac{a_2^2}{6} + \frac{2qa_2}{3} + \frac{2q^2}{3} + j\omega + j^2\bar{\omega}$

where

$$\omega = \frac{1}{24} \left( 8 \left( -\frac{3a_1^2}{8} + a_2 - 4q \right)^6 + 540 \left( -\frac{3a_1^2}{8} + a_2 - 4q \right)^3 \left( \frac{a_1^3}{8} - qa_1 - \frac{a_1 a_2}{2} + a_3 \right)^2 - 729 \left( \frac{a_1^3}{8} - qa_1 - \frac{a_1 a_2}{2} + a_3 \right)^4 \right)$$

---

*Date:* January 26, 2011.

*2000 Mathematics Subject Classification.* 14G15, 11C08, 11G10, 11G25.

*Key words and phrases.* Abelian varieties over finite fields, Weil polynomials.

$$+i9|\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3|(-(\frac{a_1^3}{8} - qa_1 - \frac{a_1a_2}{2} + a_3)^2 - \frac{8}{27}(-\frac{3a_1^2}{8} + a_2 - 4q)^3)^{1/3},$$

$$\omega^{1/3} = |\omega|^{1/3}e^{\frac{arg(\omega)i}{3}} \text{ and } j = e^{\frac{2i\pi}{3}}.$$

Now it remains to give criterions to determine when a Weil polynomial is the characteristic polynomial of an abelian variety of dimension 4. Since the characteristic polynomial of a non-simple abelian variety is a product of characteristic polynomials of abelian varieties of smaller dimensions and our problem is already solved for smaller dimensions [8, 4, 1], it is sufficient to consider the simple case.

By results of Honda and Tate, the characteristic polynomial of a simple abelian variety of dimension 4 over  $\mathbb{F}_q$  has the form  $p(t) = h(t)^e$  where  $h(t)$  is an irreducible Weil polynomial and  $e$  is an integer. Xing [10] and Maisner and Nart [2] gave independently a description of characteristic polynomials of abelian varieties of dimension 4 with  $e > 1$ . Therefore, we can restrict our attention to the case  $e = 1$ , that is,  $p(t)$  is irreducible.

If  $p(t)$  is irreducible, the determination of the possible Newton polygons for  $p(t)$  (Section 3) gives us the following proposition:

**Theorem 1.2.** *Let  $p(t) = t^8 + a_1t^7 + a_2t^6 + a_3t^5 + a_4t^4 + qa_3t^3 + q^2a_2t^2 + q^3a_1t + q^4$  be an irreducible Weil polynomial. Then  $p(t)$  is the characteristic polynomial of an abelian variety of dimension 4 if and only if one of the following conditions holds:*

- (1)  $v_p(a_4) = 0$ ,
- (2)  $v_p(a_3) = 0$ ,  $v_p(a_4) \geq n/2$  and  $p(t)$  has no root of valuation  $n/2$  in  $\mathbb{Q}_p$ ,
- (3)  $v_p(a_2) = 0$ ,  $v_p(a_3) \geq n/2$ ,  $v_p(a_4) \geq n$  and  $p(t)$  has no root of valuation  $n/2$  in  $\mathbb{Q}_p$ ,
- (4)  $v_p(a_1) = 0$ ,  $v_p(a_2) \geq n/2$ ,  $v_p(a_3) \geq n$ ,  $v_p(a_4) \geq 2n$  and  $p(t)$  has no root of valuation  $n/2$  nor factor of degree 3 in  $\mathbb{Q}_p$ ,
- (5)  $v_p(a_1) = 0$ ,  $v_p(a_2) \geq n/3$ ,  $v_p(a_3) \geq 2n/3$ ,  $v_p(a_4) = n$  and  $p(t)$  has no root of valuation  $n/3$  and  $2n/3$  in  $\mathbb{Q}_p$ ,
- (6)  $v_p(a_1) \geq n/3$ ,  $v_p(a_2) \geq 2n/3$ ,  $v_p(a_3) = n$ ,  $v_p(a_4) \geq 3n/2$  and  $p(t)$  has no root in  $\mathbb{Q}_p$ ,
- (7)  $v_p(a_1) \geq n/4$ ,  $v_p(a_2) \geq n/2$ ,  $v_p(a_3) = 3n/4$ ,  $v_p(a_4) = n$  and  $p(t)$  has no root nor factor of degree 2 and 3 in  $\mathbb{Q}_p$ ,
- (8)  $v_p(a_1) \geq n/2$ ,  $v_p(a_2) \geq n$ ,  $v_p(a_3) = 3n/2$ ,  $v_p(a_4) \geq 2n$  and  $p(t)$  has no root nor factor of degree 3 in  $\mathbb{Q}_p$ .

The  $p$ -ranks of abelian varieties in cases (1), (2), (3), (4), (5), (6), (7) and (8) are respectively 4, 3, 2, 1, 1, 0, 0 and 0. The abelian varieties in case (8) are supersingular.

It is possible to make condition (8) of Theorem 1.2 more explicit. Indeed, in [6], Singh, McGuire and Zaytsev gave the list of irreducible characteristic polynomials of supersingular abelian varieties of dimension 4, where  $q$  is not a square. We complete the classification by finding the list in the case  $q$  is a square in the following proposition (see Section 4).

**Theorem 1.3.** *The polynomial  $p(t)$  is the irreducible characteristic polynomial of a supersingular abelian variety of dimension 4 if and only if one of the following conditions holds*

- $q$  is a square and  $(a_1, a_2, a_3, a_4)$  belongs to the following list:
  - (1)  $(-q^{1/2}, 0, q^{3/2}, -q^2)$ ,  $p \not\equiv 1 \pmod{15}$ ,
  - (2)  $(q^{1/2}, 0, -q^{3/2}, -q^2)$ ,  $p \not\equiv 1 \pmod{30}$ ,
  - (3)  $(0, 0, 0, 0)$ ,  $p \not\equiv 1 \pmod{16}$ ,
  - (4)  $(0, -q, 0, q^2)$ ,  $p \not\equiv 1 \pmod{20}$ ,

- (5)  $(0, 0, 0, -q^2)$ ,  $p \not\equiv 1 \pmod{24}$ ,
- $q$  is not a square and  $(a_1, a_2, a_3, a_4)$  belongs to the following list:
  - (1)  $(\pm\sqrt{pq}, q, 0, -q^2)$ ,  $p = 2$ ,
  - (2)  $(\pm\sqrt{pq}, 2q, \pm q\sqrt{pq}, q^2)$ ,  $p = 3$ ,
  - (3)  $(0, 0, 0, 0)$ ,
  - (4)  $(0, -q, 0, q^2)$ ,
  - (5)  $(0, q, 0, q^2)$ ,  $p \neq 5$ ,
  - (6)  $(0, 0, 0, -q^2)$ ,  $p \neq 2$ ,
  - (7)  $(\pm\sqrt{pq}, 2q, \pm q\sqrt{pq}, 3q^2)$ ,  $p = 5$ .

## 2. THE COEFFICIENTS OF WEIL POLYNOMIALS OF DEGREE 8

In this section, we prove Theorem 1.1. It is clear that a Weil polynomial with a real root must have the form

$$p(t) = (t^2 \pm \sqrt{q})^2 h(t)$$

where  $h(t)$  is a Weil polynomial. Conversely, these polynomials are Weil polynomials.

Let  $p(t) = t^8 + a_1 t^7 + a_2 t^6 + a_3 t^5 + a_4 t^4 + q a_3 t^3 + q^2 a_2 t^2 + q^3 a_1 t + q^4 \in \mathbb{Z}[t]$  be a polynomial with no real root. Then the set of the roots of  $p(t)$  consists of pairs of complex conjugated numbers, say  $\omega_1, \bar{\omega}_1, \dots, \omega_4, \bar{\omega}_4$ . Letting  $x_i = -(\omega_i + \bar{\omega}_i)$  we have  $p(t) = \prod_{i=1}^4 (t^2 + x_i t + q)$ . Arguing as in [1],  $p(t)$  is a Weil polynomial if and only if the polynomials  $f^+(t) = \prod_{i=1}^4 (t - (2\sqrt{q} + x_i))$  and  $f^-(t) = \prod_{i=1}^4 (t - (2\sqrt{q} - x_i))$  have only real and positive roots.

First, we determine a necessary and sufficient condition of some polynomial of degree 4 having all real roots.

Let  $f(t) = t^4 + r_1 t^3 + r_2 t^2 + r_3 t + r_4$  be a monic polynomial of degree 4 with real coefficients. Looking at the table of variation of  $f(t)$ , we see that there exists some  $r_4$  for which  $f(t)$  has all real roots if and only if  $f'(t)$  has all real roots. This condition is equivalent to

$$(1) \quad \Delta_{f'} \geq 0$$

where  $\Delta_{f'}$  is the discriminant of  $f'(t)$ .

The discriminant of  $f(t)$  is a polynomial of degree 3 in  $r_4$  which we will denote  $\Delta_f(t)$  (that is,  $\Delta_f(r_4)$  is the discriminant of  $f(t)$ ). It is well known that if  $f(t)$  has all real roots then  $\Delta_f(r_4) \geq 0$ . Moreover, the function which associate to  $r_4$  the number of roots of  $f(t)$  is constant on the intervals delimited by the roots of  $\Delta_f(t)$  (because  $\Delta_f(r_4) = 0$  when  $f(t)$  has a multiple root).

When  $r_4$  is very big, the graph of  $f(t)$  doesn't touch the  $x$ -axis and therefore  $f(t)$  has no real roots. Thus if  $\gamma_3$  is the biggest root of  $\Delta_f(t)$ , by the previous discussion,  $f(t)$  has no real root for  $r_4 \in ]\gamma_3; +\infty[$ .

We deduce that if (1) is satisfied then  $\Delta_f(t)$  must have 3 real roots  $\gamma_1 \leq \gamma_2 \leq \gamma_3$  and  $f(t)$  has all real roots if and only if

$$(2) \quad \gamma_1 \leq r_4 \leq \gamma_2.$$

The roots of  $\Delta_f(t)$  can be found using Cardan's method. Let us recall quickly what it is.

Given a polynomial  $h(t) = t^3 + u_2 t + u_3$ , we set  $\delta = -u_3^2 - \frac{4}{27}u_2^3$ . Then  $h(t)$  has all real roots if and only if  $\delta \geq 0$ . If this is the case, the roots of  $h(t)$  are  $\gamma_1 = \omega + \bar{\omega}$ ,  $\gamma_2 = j\omega + j^2\bar{\omega}$  and  $\gamma_3 = j^2\omega + j\bar{\omega}$  where  $j = e^{\frac{2i\pi}{3}}$  and  $\omega = (\frac{-u_3 + i\sqrt{\delta}}{2})^{1/3}$ . Moreover, with the convention  $\omega^{1/3} = |\omega|^{1/3} e^{\frac{\arg(\omega)i}{3}}$ , we have  $\gamma_1 \leq \gamma_2 \leq \gamma_3$ .

In the general case, we have  $h(t) = v_0 t^3 + v_1 t^2 + v_2 t + v_3$  and we conclude using the fact that  $\frac{1}{v_0} h(t - \frac{v_1}{3v_0}) = t^3 + u_2 t + u_3$  with  $u_2 = -\frac{v_1^2}{3v_0^2} + \frac{v_2}{v_0}$  and  $u_3 = \frac{2v_1^3}{27v_0^3} - \frac{v_1 v_2}{3v_0^2} + \frac{v_3}{v_0}$ .

For  $i = 1, 2, 3, 4$ , let  $s_i$  denote the  $i$ th symmetric function of the  $x_i$ 's (that is,  $\prod_{i=1}^4 (t + x_i) = t^4 + \sum_{i=1}^4 s_i t^{4-i}$ ). Expanding the expression  $p(t) = \prod_{i=1}^4 (t^2 + x_i t + q)$ , we find:

$$\begin{aligned} s_1 &= a_1 \\ s_2 &= a_2 - 4q \\ s_3 &= a_3 - 3qa_1 \\ s_4 &= a_4 - 2qa_2 + 2q^2. \end{aligned}$$

Now, in order to simplify the calculation, we remark that  $f^+(t)$  and  $f^-(t)$  have all real roots if and only if the polynomial  $f(t) = \prod_{i=1}^4 (t + x_i - \frac{a_1}{4})$  has. Therefore, it is equivalent to apply our results to  $f(t)$ .

Expanding the expression of  $f(t)$ , we find that  $f(t) = t^4 + r_2 t^2 + r_3 t + r_4$ , where

$$\begin{aligned} r_2 &= -\frac{3s_1^2}{8} + s_2 \\ r_3 &= \frac{s_1^3}{8} - \frac{s_1 s_2}{2} + s_3 \\ r_4 &= -\frac{3s_1^4}{256} + \frac{s_1^2 s_2}{16} - \frac{s_1 s_3}{4} + s_4. \end{aligned}$$

Substituting  $s_1, s_2, s_3$  and  $s_4$  with their expressions in  $a_1, a_2, a_3$  and  $a_4$  we obtain

$$\begin{aligned} r_2 &= -\frac{3a_1^2}{8} + a_2 - 4q \\ r_3 &= \frac{a_1^3}{8} - qa_1 - \frac{a_1 a_2}{2} + a_3 \\ r_4 &= -\frac{3a_1^4}{256} + \frac{qa_1^2}{2} + \frac{a_1^2 a_2}{16} - \frac{a_1 a_3}{4} - 2qa_2 + 2q^2 + a_4. \end{aligned}$$

We have

$$\Delta_f(t) = 256t^3 - 128r_2^2 t^2 + 16r_2(r_2^3 + 9r_3^2)t - r_3^2(4r_2^3 + 27r_3^2).$$

Now, we use Cardan's method. Set

$$\begin{aligned} u_2 &= -\frac{r_2^4}{48} + \frac{9r_2 r_3^2}{16} \\ u_3 &= \frac{r_2^6}{864} + \frac{5r_2^3 r_3^2}{64} - \frac{27r_3^4}{256} \\ \delta &= -u_3^2 - \frac{4}{27}u_2^3 = \frac{r_3^2(-8r_2^3 - 27r_3^2)^3}{1769472}. \end{aligned}$$

Suppose that (1) is satisfied. Then  $\delta \geq 0$  and the roots of  $\Delta_f(t)$  are

$$\begin{aligned} \gamma_1 &= \omega + \bar{\omega} + \frac{r_2^2}{6} \\ \gamma_2 &= j\omega + j^2\bar{\omega} + \frac{r_2^2}{6} \\ \gamma_3 &= j^2\omega + j\bar{\omega} + \frac{r_2^2}{6}. \end{aligned}$$

where

$$\omega = \frac{1}{24} \left( 8r_2^6 + 540r_2^3r_3^2 - 729r_3^4 + i9|r_3|(-r_3^2 - \frac{8}{27}r_2^3)^{3/2} \right)^{1/3}.$$

Substituting  $r_2$ ,  $r_3$  and  $r_4$  with their expressions in  $a_1$ ,  $a_2$ ,  $a_3$  and  $a_4$  we obtain condition (6) of Theorem 1.1.

Next we have to determine when (1) is satisfied. We have:

$$\Delta_{f'} = -16(8r_2^3 + 27r_3^2).$$

Therefore, (1) is equivalent to

$$r_2 \leq 0 \quad \text{and} \quad -\left(\frac{-2r_2}{3}\right)^{3/2} \leq r_3 \leq \left(\frac{-2r_2}{3}\right)^{3/2}.$$

This gives us the second inequality of condition (2) and condition (4) of Theorem 1.1.

Finally, we determine when the polynomials  $f^+(t)$  and  $f^-(t)$  have only positive roots.

For  $i = 1, 2, 3$ , let  $r_i^+$  and  $r_i^-$  denote the respective  $i$ th coefficients of  $f^+(t)$  and  $f^-(t)$ . Expanding the expressions  $f^+(t) = \prod_{i=1}^4(t - (2\sqrt{q} + x_i))$  and  $f^-(t) = \prod_{i=1}^4(t - (2\sqrt{q} - x_i))$ , we find:

$$\begin{aligned} r_1^+ &= -8\sqrt{q} - s_1 \\ r_2^+ &= 24q + 6\sqrt{q}s_1 + s_2 \\ r_3^+ &= -32q\sqrt{q} - 12qs_1 - 4\sqrt{q}s_2 - s_3 \\ r_4^+ &= 16q^2 + 8q\sqrt{q}s_1 + 4qs_2 + 2\sqrt{q}s_3 + s_4 \end{aligned}$$

and

$$\begin{aligned} r_1^- &= -8\sqrt{q} + s_1 \\ r_2^- &= 24q - 6\sqrt{q}s_1 + s_2 \\ r_3^- &= -32q\sqrt{q} + 12qs_1 - 4\sqrt{q}s_2 + s_3 \\ r_4^- &= 16q^2 - 8q\sqrt{q}s_1 + 4qs_2 - 2\sqrt{q}s_3 + s_4. \end{aligned}$$

Substituting  $s_1$ ,  $s_2$ ,  $s_3$  and  $s_4$  with their expressions in  $a_1$ ,  $a_2$ ,  $a_3$  and  $a_4$  we obtain

$$\begin{aligned} r_1^+ &= -8\sqrt{q} - a_1 \\ r_2^+ &= 20q + 6\sqrt{q}a_1 + a_2 \\ r_3^+ &= -16q\sqrt{q} - 9qa_1 - 4\sqrt{q}a_2 - a_3 \\ r_4^+ &= 2q^2 + 2q\sqrt{q}a_1 + 2qa_2 + 2\sqrt{q}a_3 + a_4 \end{aligned}$$

and

$$\begin{aligned} r_1^- &= -8\sqrt{q} + a_1 \\ r_2^- &= 20q - 6\sqrt{q}a_1 + a_2 \\ r_3^- &= -16q\sqrt{q} + 9qa_1 - 4\sqrt{q}a_2 + a_3 \\ r_4^- &= 2q^2 - 2q\sqrt{q}a_1 + 2qa_2 - 2\sqrt{q}a_3 + a_4. \end{aligned}$$

Suppose that  $f^+(t)$  and  $f^-(t)$  have all real roots. Then by [7, §2, Lemma],  $f^+(t)$  and  $f^-(t)$  have only positive roots if and only if  $(-1)^i r_i^+ > 0$  and  $(-1)^i r_i^- > 0$  for  $i = 1, 2, 3, 4$ . This gives us the remaining conditions of Theorem 1.1 and concludes the proof.

**Remark.** We could have used [7, §2, Lemma] to determine when a polynomial of degree 4 has only real roots but the computation and the results would have been longer.

## 3. NEWTON POLYGONS

Let  $p(t)$  be an irreducible Weil polynomial. By [3],  $p(t)^e$  is the characteristic polynomial of a simple abelian variety, where  $e$  the least common denominator of  $v_p(f(0))/n$  where  $f(t)$  runs through the irreducible factors of  $p(t)$  over  $\mathbb{Q}_p$ . Thus  $p(t)$  is the characteristic polynomial of an abelian variety of dimension 4 if and only if  $e$  is equal to 1 that is,  $v_p(f(0))/n$  are integers.

In order to determine when this condition is satisfied, we consider the Newton polygon of  $p(t)$  (see [9]). Each of its edges define a factor of  $p(t)$  over  $\mathbb{Q}_p$ . The degree of this factor is the length of the projection onto the  $x$ -axis of the edge and all the roots of this factor have a valuation equal to the slope of the edge. Therefore  $e = 1$  implies that the length of the projection onto the  $x$ -axis of any edge times its slope is a multiple of  $n$ .

We graph the Newton polygons satisfying this condition and in each case, we give a necessary and sufficient condition to have  $e = 1$ . The obtained results are summarized in Theorem 1.2.

**Ordinary case:  $v_p(a_4) = 0$** 

The Newton polygon of  $p(t)$  is represented in Figure 1 and we always have  $e = 1$ .

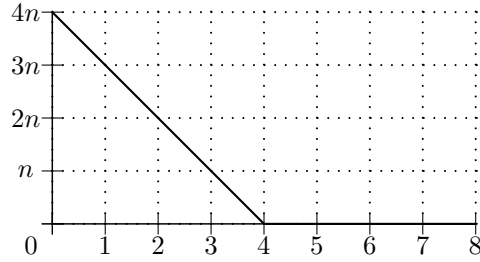
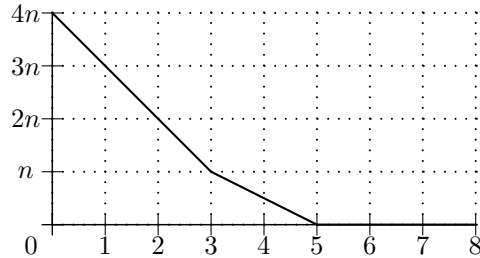


FIGURE 1. Ordinary case

 **$p$ -rank 3 case:  $v_p(a_4) > 0$  and  $v_p(a_3) = 0$** 

The only Newton polygon for which  $e = 1$  is represented in Figure 2.

FIGURE 2.  $p$ -rank 3 case

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_4) \geq n/2$ . If this condition holds,  $p(t)$  has a factor in  $\mathbb{Q}_p$  of degree 2 with roots of valuation  $n/2$  and  $e = 1$  if and only if this factor is irreducible, that is, if and only if  $p(t)$  has no root of valuation  $n/2$  in  $\mathbb{Q}_p$ .

**p-rank 2 case:**  $v_p(a_4) > 0$ ,  $v_p(a_3) > 0$  and  $v_p(a_2) = 0$

The only Newton polygon for which  $e = 1$  is represented in Figure 3.

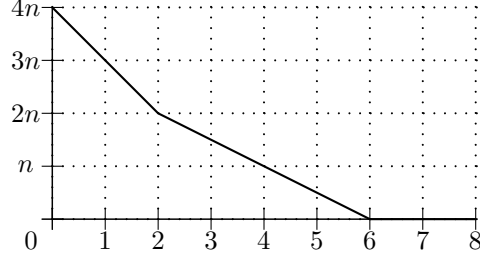


FIGURE 3.  $p$ -rank 2 case

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_3) \geq n/2$  and  $v_p(a_4) \geq n$ . If these conditions hold,  $p(t)$  has a factor in  $\mathbb{Q}_p$  of degree 4 with roots of valuation  $n/2$  and  $e = 1$  if and only if this factor has no root in  $\mathbb{Q}_p$ , that is, if and only if  $p(t)$  has no root of valuation  $n/2$  in  $\mathbb{Q}_p$ .

**p-rank 1 case:**  $v_p(a_4) > 0$ ,  $v_p(a_3) > 0$ ,  $v_p(a_2) > 0$  and  $v_p(a_1) = 0$

There are two Newton polygons for which  $e = 1$ . One is represented in Figure 4.

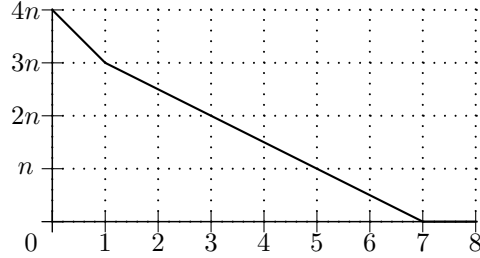


FIGURE 4.  $p$ -rank 1 first case

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_2) \geq n/2$ ,  $v_p(a_3) \geq n$  and  $v_p(a_4) \geq 2n$ . If these conditions hold,  $e = 1$  if and only if  $p(t)$  has no root of valuation  $n/2$  nor factor of degree 3 in  $\mathbb{Q}_p$ .

The other Newton polygon is represented in Figure 5.

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_2) \geq n/3$ ,  $v_p(a_3) \geq 2n/3$  and  $v_p(a_4) = n$ . If these conditions hold  $e = 1$  if and only if  $p(t)$  has no root of valuation  $n/3$  and  $2n/3$  in  $\mathbb{Q}_p$ .

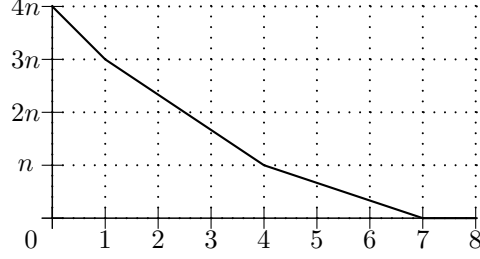
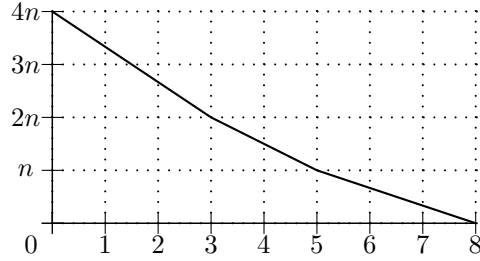
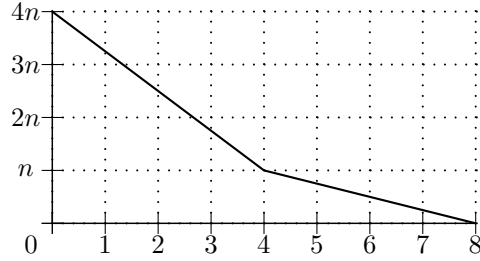
**p-rank 0 case:**  $v_p(a_4) > 0$ ,  $v_p(a_3) > 0$ ,  $v_p(a_2) > 0$  and  $v_p(a_1) > 0$

There are three Newton polygons for which  $e = 1$ . One is represented in Figure 6.

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_1) \geq n/3$ ,  $v_p(a_2) \geq 2n/3$ ,  $v_p(a_3) = n$  and  $v_p(a_4) \geq 3n/2$ . If these conditions hold,  $e = 1$  if and only if  $p(t)$  has no root in  $\mathbb{Q}_p$ .

The second Newton polygon is represented in Figure 7.



FIGURE 5.  $p$ -rank 1 second caseFIGURE 6.  $p$ -rank 0 first caseFIGURE 7.  $p$ -rank 0 second case

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_1) \geq n/4$ ,  $v_p(a_2) \geq n/2$ ,  $v_p(a_3) \geq 3n/4$  and  $v_p(a_4) = n$ . If these conditions hold,  $e = 1$  if and only if  $p(t)$  has no factor of degrees 1, 2 and 3 in  $\mathbb{Q}_p$ .

The last Newton polygon is represented in Figure 8; the corresponding abelian varieties are supersingular.

This is the Newton polygon of  $p(t)$  if and only if  $v_p(a_1) \geq n/2$ ,  $v_p(a_2) \geq n$ ,  $v_p(a_3) \geq 3n/2$  and  $v_p(a_4) \geq 2n$ . If these conditions hold,  $e = 1$  if and only if  $p(t)$  has no root nor factor of degree 3 in  $\mathbb{Q}_p$ .

#### 4. SUPERSINGULAR CASE

In [6], Singh, McGuire and Zaytsev gave the list of irreducible characteristic polynomials of supersingular abelian varieties of dimension 4, where  $q$  is not a square. Here we derive the list when  $q$  is a square.

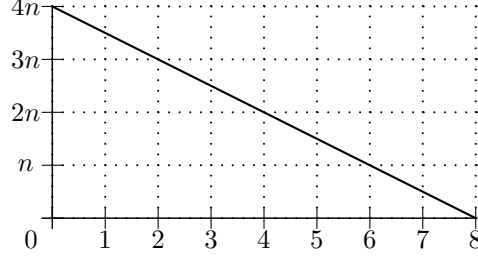


FIGURE 8. Supersingular case

Let  $p(t)$  be an irreducible supersingular Weil polynomial of degree 8, where  $q$  is a square. By Honda-Tate Theorem,  $\frac{1}{q^4}p(\sqrt{q}t)$  is a cyclotomic polynomial of degree 8 i.e;  $\frac{1}{q^4}p(\sqrt{q}t) = \Phi_m(t)$  such that  $\phi(m) = 8$  or  $m \in \{15, 16, 20, 24, 30\}$ . Therefore for each  $m$  above,  $p(t) = q^g \Phi_m(\frac{t}{\sqrt{q}})$  gives a supersingular Weil polynomial of degree 8. Let  $p(t) = \prod_i p_i(t)$  be the decomposition in irreducible factors of  $p(t)$  over  $\mathbb{Q}_p$  with  $\pi = \sqrt{q}\zeta_n$  as a root, where  $\zeta_n$  is primitive  $n$ th root of unity. To determine the dimension of the corresponding abelian variety, recall from [3],  $p(t)^e$  is a characteristic polynomial of an abelian variety of dimension  $4e$ , where  $e$  is the least common denominator of  $\frac{v_p(\pi)}{v_p(q)} \deg p_i(t) = \frac{\deg p_i}{2}$ . Since  $p(t) = q^g \Phi_m(\frac{t}{\sqrt{q}})$ ,  $\deg p_i = \deg r_i$  where  $\Phi_m(t) = \prod_i r_i(t)$ . But from chapter IV.4 in [5], we have  $\deg r_i = r$  where  $r$  is the multiplicative order of  $p$  in  $(\frac{\mathbb{Z}}{m\mathbb{Z}})^*$ . Hence,  $e = 1$  if  $r$  is even. In each case of  $m$  above, since  $\phi(m) = 2^3$ ,  $r$  is either even or  $r = 1$ . The later case only happens when  $p \equiv 1 \pmod{m}$ . Hence,  $p(t) = q^g \Phi_m(\frac{t}{\sqrt{q}})$ , where  $p \not\equiv 1 \pmod{m}$  is an irreducible characteristic polynomial of a supersingular abelian variety of dimension 4, for each  $m \in \{15, 16, 20, 24, 30\}$ .

## REFERENCES

- [1] S. Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *J. Number Theory*. no 130, p. 2745-2752, 2010.
- [2] D. Maisner, E. Nart, appendix of E. W. Howe. Abelian surfaces over finite fields as jacobians. *Experiment. Math.*. Vol 11, p. 321-337, 2002.
- [3] J. Milne, W. Waterhouse. Abelian varieties over finite fields. *1969 Number Theory Institute*, Proceedings of Symposia in Pure Math., Vol XX, p.53-64, A.M.S., Providence, RI, 1971. Vol 76, p. 351-366, 1990.
- [4] H.G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*. Vol 76, p. 351-366, 1990.
- [5] J.P.Serre, *Local Fields*, Springer-Verlag, 1979.
- [6] Vijaykumar Singh, Alexey Zaytsev and Gary McGuire. On the characteristic polynomial of frobenius of supersingular abelian varieties of dimension up to 7 over finite fields. <http://arxiv.org/abs/1005.3635>.
- [7] C. Smyth. Totally positive algebraic integers of small trace. *Ann. Inst. Fourier*. Vol 33, p. 285-302, 1973.
- [8] W. Waterhouse. Abelian varieties over finite fields. *Ann. sci. Ecole Norm. Sup.* (4), t. 2, p. 521-560, 1969.
- [9] E. Weiss. *Algebraic number theory*. McGraw, New-York, 1963.
- [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, p. 147-150, 1994.

INSTITUT DE MATHÉMATIQUES DE LUMINY, MARSEILLE, FRANCE, AND, CLAUDE SHANNON INSTITUTE, DUBLIN, IRLAND

*E-mail address:* `haloui@iml.univ-mrs.fr, vijaykumar.singh@ucdconnect.ie`