Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 124–131

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

# On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields

Omran Ahmadi [a], Gerardo Vega [b,*]

[a] *Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*
[b] *Dirección General de Servicios de Cómputo Académico, Universidad Nacional Autónoma de México, 04510 México D.F., Mexico*

Received 24 March 2006; revised 7 September 2006

Available online 24 October 2006

Communicated by Gary L. Mullen

**Abstract**

Using the Stickelberger–Swan theorem, the parity of the number of irreducible factors of a self-reciprocal even-degree polynomial over a finite field will be hereby characterized. It will be shown that in the case of binary fields such a characterization can be presented in terms of the exponents of the monomials of the self-reciprocal polynomial.

*Keywords:* Finite fields; Irreducible polynomials; Self-reciprocal polynomials

## 1. Introduction

Let $\mathbb{F}_q$ denote the finite field of order $q$, where $q$ is a prime power, and let $\mathbb{F}_q[x]$ denote the ring of all polynomials over $\mathbb{F}_q$ in the variable $x$. For $f(x)$, a polynomial of degree $m$ over $\mathbb{F}_q$ whose constant term is nonzero, its reciprocal is the polynomial $f^*(x) = x^m f(1/x)$ of degree $m$ over $\mathbb{F}_q$. A polynomial $f(x)$ is called self-reciprocal if $f^*(x) = f(x)$. The reciprocal of an irreducible polynomial is also irreducible. The roots of the reciprocal polynomial are the reciprocals of the roots of the original polynomial, and hence, any self-reciprocal irreducible monic polynomial (*srim*) of degree $> 1$ must have even degree, say $2n$.

[*] Corresponding author.
*E-mail addresses:* oahmadid@uwaterloo.ca (O. Ahmadi), gerardov@servidor.unam.mx (G. Vega).

1071-5797/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2006.09.004

Self-reciprocal irreducible polynomials over finite fields have been studied by many authors. In [3], Carlitz obtained the number of srim polynomials of degree $2n$ over a finite field for every $n$ using $L$-functions. In [4], Cohen obtained the same result by a simpler method. In [10], Varshamov and Garakov studied the construction of srim polynomials over binary fields. In [7], Meyn generalized Varshamov and Garakov's work and also gave a simpler proof of Carlitz's result. In [11], Yucas and Mullen classified srim polynomials based on their orders. In [11] and [1], the weight of srim polynomials was studied. There are many other related papers in the literature. In this paper we study the parity of the number of irreducible factors of self-reciprocal monic (*srm*) polynomials of even degree and we show that this number can be easily determined. Since every srm polynomial whose number of irreducible factors is even is certainly reducible, our result enables one to show easily that some families of srm polynomials are reducible.

## 2. Preliminary results

We will begin this section by recalling the discriminant and the resultant of polynomials over a field. For a more detailed treatment see, for example, [2,6].

Let $K$ be a field, and let $F(x) \in K[x]$ be a polynomial of degree $s \geqslant 2$ with leading coefficient $a$. Then the *discriminant*, $\mathrm{Disc}(F)$, of $F(x)$ is defined by

$$\mathrm{Disc}(F) = a^{2s-2} \prod_{i<j} (x_i - x_j)^2,$$

where $x_0, x_1, \ldots, x_{s-1}$ are the roots of $F(x)$ in some extension of $K$. Although $\mathrm{Disc}(F)$ is defined in terms of the elements of an extension of $K$, it is actually an element of $K$ itself. There is an alternative formulation of $\mathrm{Disc}(F)$, given below, which is very helpful for the computation of the discriminant of a polynomial.

Let $G(x) \in K[x]$ and suppose $F(x) = a\prod_{i=0}^{s-1}(x - x_i)$ and $G(x) = b\prod_{j=0}^{t-1}(x - y_j)$, where $a, b \in K$ and $x_0, x_1, \ldots, x_{s-1}, y_0, y_1, \ldots, y_{t-1}$ are in some extension of $K$. Then the *resultant*, $\mathrm{Res}(F, G)$, of $F(x)$ and $G(x)$ is

$$\mathrm{Res}(F, G) = (-1)^{st} b^s \prod_{j=0}^{t-1} F(y_j) = a^t \prod_{i=0}^{s-1} G(x_i). \tag{1}$$

The following statements are immediate from the definition of the resultant of two polynomials.

**Corollary 1.** *If $F$ is as above, and $G_1, G_2, G_3, R \in K[x]$, then*:

(i) $\mathrm{Res}(F, -x) = F(0)$.
(ii) $\mathrm{Res}(F, G_1G_2) = \mathrm{Res}(F, G_1)\,\mathrm{Res}(F, G_2)$.
(iii) $\mathrm{Res}(F, G_3F + R) = a^l\,\mathrm{Res}(F, R)$, *where* $l = \deg(G_3F + R) - \deg(R)$ *and* $\deg(\cdot)$ *denotes the degree of a polynomial.*

**Corollary 2.** *If $F$ is as above, and $F' \in K[x]$ is the derivative of $F$, then*

$$\mathrm{Disc}(F) = (-1)^{\frac{s(s-1)}{2}} a^{-1}\,\mathrm{Res}(F, F'). \tag{2}$$

The next lemma directly follows from the two previous corollaries.

**Lemma 3.** [5] *Let $F$ be as above and suppose, furthermore that $a = 1$, $F(0) \neq 0$ and $c \in K$. Then*

$$\mathrm{Disc}(F) = (-1)^{\frac{s(s-1)}{2}} F(0)^{-1} \mathrm{Res}(F, xF' - cF).$$

The following results, called the Stickelberger and Stickelberger–Swan theorems, respectively, are our main tools for determining the parity of the number of irreducible factors of a polynomial over a finite field.

**Theorem 4.** [8] *Suppose that the $s$-degree polynomial $f(x) \in \mathbb{F}_q[x]$, where $q$ is an odd prime power, is the product of $r$ pairwise distinct irreducible polynomials over $\mathbb{F}_q$. Then $r \equiv s \pmod 2$ if and only if, $\mathrm{Disc}(f)$ is a square in $\mathbb{F}_q$.*

**Theorem 5.** [8,9] *Suppose that the $s$-degree polynomial $f(x) \in \mathbb{F}_2[x]$ is the product of $r$ pairwise distinct irreducible polynomials over $\mathbb{F}_2$ and, let $F(x) \in \mathbb{Z}[x]$ be any monic lift of $f(x)$ to the integers. Then $\mathrm{Disc}(F) \equiv 1$ or $5 \pmod 8$, and more importantly, $r \equiv s \pmod 2$ if and only if, $\mathrm{Disc}(F) \equiv 1 \pmod 8$.*

If $s$ is even and $\mathrm{Disc}(F) \equiv 1 \pmod 8$, then Theorem 5 asserts that $f(x)$ has an even number of irreducible factors and therefore is reducible over $\mathbb{F}_2$. Thus one can find necessary conditions for the irreducibility of $f(x)$ by computing $\mathrm{Disc}(F)$ modulo 8.

## 3. The main results

We start with the following lemma which is probably well known but we include its proof for the sake of completeness.

**Lemma 6.** *Let $K$ be a field and let $F(x) \in K[x]$ be a self-reciprocal polynomial of degree $2n$. Then, for some $G(x) \in K[x]$ of degree $n$, we have*

$$F(x) = x^n G\left(x + x^{-1}\right). \tag{3}$$

**Proof.** Let $F(x) = \sum_{i=0}^{2n} a_i x^i \in K[x]$ be a self-reciprocal polynomial of degree $2n$. Since $F(x)$ is self-reciprocal, we have $a_{2n-i} = a_i$ for $i = 0, 1, \ldots, 2n$. From this we have

$$F(x) = a_n x^n + \sum_{i=0}^{n-1} a_i \left(x^{2n-i} + x^i\right),$$

and hence

$$F(x) = x^n \left(a_n + \sum_{j=1}^{n} a_{n-j}\left(x^j + x^{-j}\right)\right).$$

Now let $F_0(x) = 1$ and $F_j(x) = x^j + x^{-j}$ for $j \geqslant 1$. We claim that, for $j \geqslant 0$, there exists $G_j(x) \in K[x]$ such that $F_j(x) = G_j(x + x^{-1})$. The claim is trivial for $j = 0, 1$. On the other hand, we have

$$\left(x^1 + x^{-1}\right)^j = x^j + x^{-j} + \sum_{l=0}^{j-1} b_l F_l(x), \tag{4}$$

for some $b_0, b_1, \ldots, b_{j-1} \in K$. Thus the claim follows from Eq. (4) by induction. Finally if we let

$$G(x) = a_n + \sum_{j=1}^{n} a_{n-j} G_j(x),$$

we obtain Eq. (3). □

**Remark.** When $F(x)$ is a self-reciprocal polynomial of degree $2n + 1$, similar arguments can be used to show that there exists a degree $n$ polynomial $G(x) \in K[x]$ so that

$$F(x) = (x + 1)x^n G\left(x + x^{-1}\right).$$

Now let $F(x)$ and $G(x)$ be as in Lemma 6 and let $x_0, \ldots, x_{n-1}, x_0^{-1}, \ldots, x_{n-1}^{-1}$ be the roots of $F(x)$ in some extension of $K$. For simplicity, assume that $a_{2n} = a_0 = 1$. Using Lemma 3 with $c = n$ and using the fact that the roots of $F(x)$ are nonzero, we have

$$\operatorname{Disc}(F) = (-1)^n \operatorname{Res}\left(F, \left(x^2 - 1\right)x^{n-1} G'\left(x + x^{-1}\right)\right),$$

where $G'$ is the derivative of $G$. Thus using Corollary 1

$$\operatorname{Disc}(F) = (-1)^n \operatorname{Res}\left(F, x^2 - 1\right) \operatorname{Res}\left(F, x^{n-1} G'\left(x + x^{-1}\right)\right).$$

Applying Eq. (1), $\operatorname{Res}(F, x^2 - 1) = F(1)F(-1)$ and if we let $H = x^{n-1}G'(x + x^{-1})$, then

$$\begin{aligned} \operatorname{Res}(F, H) &= \prod_{i=0}^{n-1} x_i^{n-1} G'\left(x_i + x_i^{-1}\right) \prod_{i=0}^{n-1} x_i^{1-n} G'\left(x_i^{-1} + x_i\right) \\ &= \left(\prod_{i=0}^{n-1} G'\left(x_i + x_i^{-1}\right)\right)^2. \end{aligned}$$

Comparing the right-hand side of the above equation with Eqs. (1) and (2), and using the fact that the roots of $G(x)$ are precisely $x_0 + x_0^{-1}, x_1 + x_1^{-1}, \ldots, x_{n-1} + x_{n-1}^{-1}$ we see that $\operatorname{Res}(F, H) = \operatorname{Disc}(G)^2$. Thus

$$\operatorname{Disc}(F) = (-1)^n F(1)F(-1) \operatorname{Disc}(G)^2. \tag{5}$$

We are now able to present our main results. Applying Theorem 4 and using the above identity we have the following:

**Theorem 7.** *Let $f(x)$ be a srm polynomial of degree $2n$ over $\mathbb{F}_q$ having $r$ pairwise distinct irreducible factors over $\mathbb{F}_q$. Then $r$ is an even number if and only if, $(-1)^n f(1)f(-1)$ is a square in $\mathbb{F}_q$.*

For binary polynomials, since the coefficients are 0 or 1, we can relate the parity of the number of irreducible factors of a polynomial to its monomials, as follows:

A self-reciprocal binary polynomial $f(x)$ of degree $2n$ can be written as

$$f(x) = ax^n + \sum_{i=1}^{u} \left(x^{e_i} + x^{2n-e_i}\right),$$

where each $e_i$ is an integer such that $0 < e_i < n$ for $i = 2, 3, \dots, u$, $e_1 = 0$ and $a \in \mathbb{F}_2$. If $a = 0$, then $f(1) = 0$ and $f(x)$ is reducible and hence it is not interesting to study the parity of the number of irreducible factors of such polynomials. Thus we assume that $a = 1$ and

$$f(x) = x^n + \sum_{i=1}^{u} \left(x^{e_i} + x^{2n-e_i}\right). \tag{6}$$

Now let $v$ be the number of $i$, $i = 1, 2, \dots, u$, for which the exponent $e_i$ is an odd number. We have the following theorem.

**Theorem 8.** *Let $f(x)$, $u$ and $v$ be as above and assume that $f(x)$ has $r$ pairwise distinct irreducible factors over $\mathbb{F}_2$. Then $r \equiv v + nu \pmod 2$.*

**Proof.** Let $F(x)$ be a self-reciprocal lift of $f(x)$ to the integers where the coefficients of $F(x)$ are 0 or 1. Now, applying Theorem 5 and using Eq. (5), we conclude that $\mathrm{Disc}(G)$ is an odd number, and therefore, $4r + 1 \equiv (-1)^n F(1)F(-1) \pmod 8$. Clearly, $F(1) = 2u + 1$ and $F(-1) = 2u + (-1)^n - 4v$. Thus the claim follows from the fact that if $n$ is even, then $(-1)^n F(1)F(-1) \equiv -4v + 1 \equiv 4(v + nu) + 1 \pmod 8$ and, on the other hand, if $n$ is odd then $(-1)^n F(1)F(-1) \equiv 4(v - u^2) + 1 \equiv 4(v + nu) + 1 \pmod 8$. □

Now it is natural to ask whether the above two theorems are valid if $f(x)$ has repeated irreducible factors. In fact this is the case and the rest of this section is devoted to its proof. First we give the proof for binary srm polynomials and then we sketch the proof for srm polynomials over finite fields of odd characteristic. We need the following lemma:

**Lemma 9.** *Let $f(x) \in \mathbb{F}_2[x]$ be as in Eq.* (6). *Then $f(x) = f_1(x) \cdots f_p(x)$ where*

(i) *$f_j(x) = x^{n_j} + \sum_{i=1}^{u_j} x^{e_{ij}} + x^{2n_j - e_{ij}} \in \mathbb{F}_2[x]$, $e_{ij}$ is an integer, $0 < e_{ij} < n_j$ for $j = 1, 2, \dots, p$ and $i = 2, \dots, u_j$, $e_{1j} = 0$ for $j = 1, \dots, p$, and*

(ii) *$f_j(x)$ has pairwise distinct irreducible factors.*

*Equivalently, $f(x)$ has a factorization into srm polynomials of even degree, where each srm factor has pairwise distinct irreducible factors over $\mathbb{F}_2$, and does not have 1 as a root.*

**Proof.** Using Lemma 6, there exists an $n$-degree polynomial $g(x) \in \mathbb{F}_2[x]$ such that $f(x) = x^n g(x + x^{-1})$. Now let $g(x) = g_1(x) \cdots g_p(x)$, where each $g_j(x)$ is an irreducible polynomial of degree $n_j$ over $\mathbb{F}_2$. If we let $f_j(x) = x^{n_j} g_j(x + x^{-1})$, then $f(x) = f_1(x) \cdots f_p(x)$ where each $f_j(x)$ is an srm polynomial of degree $2n_j$ which is either irreducible or is the product of two distinct polynomials which are reciprocal of one another. We have $f_j(1) \neq 0$ since otherwise we would have $f(1) = 0$. Therefore, each $f_j(x)$ is of the required form and this finishes the proof. □

Now we are ready to state the generalization of Theorem 8.

**Theorem 10.** *Let $f(x)$ be in the form given in Eq.* (6), *$v$ be the number of $i$, $i = 1, 2, \ldots, u$, for which the exponent $e_i$ is an odd number, and let $r$ be the number of irreducible factors* (*counted with multiplicity*) *of $f(x)$. Then $r \equiv v + nu$* (mod 2).

**Proof.** Using Theorem 8 and Lemma 9 we just need to prove the following claim:

**Claim.** *Let $a(x) = x^s + \sum_{i=1}^{u_a} x^{a_i} + x^{2s-a_i}$ and $b(x) = x^t + \sum_{i=1}^{u_b} x^{b_i} + x^{2t-b_i}$ having $r_a$ and $r_b$ irreducible factors, respectively, and let $c(x) = a(x)b(x) = x^{s+t} + \sum_{i=1}^{u_c} x^{c_i} + x^{2(s+t)-c_i}$. Suppose that $v_a$, $v_b$ and $v_c$ are the numbers related to the odd exponents of $a(x)$, $b(x)$ and $c(x)$ as $v$ was related to odd exponents of $f(x)$ after Eq.* (6). *Also assume that the theorem is true for $a(x)$ and $b(x)$ or equivalently $r_a \equiv v_a + su_a$* (mod 2) *and $r_b \equiv v_b + tu_b$* (mod 2). *Then, $r_a + r_b \equiv v_c + (s + t)u_c$* (mod 2).

One might try to prove the above claim by computing $c(x)$ and keeping track of its exponents, but this seems rather cumbersome. We can instead lift the polynomials to the integers and prove the claim.

Let $A(x)$, $B(x)$ and $C(x)$ be the self-reciprocal lifts of the polynomials $a(x)$, $b(x)$ and $c(x)$ to the integers where the coefficients of $A(x)$, $B(x)$ and $C(x)$ are 0 or 1. It follows from the proof of Theorem 8 that $4(v_a + su_a) + 1 \equiv (-1)^s A(1)A(-1) \pmod 8$ and $4(v_b + tu_b) + 1 \equiv (-1)^t B(1)B(-1) \pmod 8$. Thus, since the theorem is true for polynomials $a(x)$ and $b(x)$, then $4r_a + 1 \equiv (-1)^s A(1)A(-1) \pmod 8$ and $4r_b + 1 \equiv (-1)^t B(1)B(-1) \pmod 8$. Using similar arguments we see that in order to prove that the theorem is true for $c(x)$, we need to prove that $4(r_a + r_b) + 1 \equiv (-1)^{s+t} C(1)C(-1) \pmod 8$. Now we have

$$\begin{aligned} 4(r_a + r_b) + 1 &\equiv (4r_a + 1)(4r_b + 1) \\ &\equiv (-1)^{s+t} A(1)A(-1)B(1)B(-1) \pmod 8. \end{aligned}$$

Hence, using the above equation we just need to show that

$$C(1)C(-1) \equiv A(1)A(-1)B(1)B(-1) \pmod 8. \tag{7}$$

Now let $D(x) = A(x)B(x) - C(x)$. Then since $A(x)B(x)$ and $C(x)$ reduced modulo 2 result in the same polynomial over $\mathbb{F}_2$, we have $D(x) = 2E(x)$, where $E(x)$ is a polynomial over the integers. On the other hand, since $A(x)$, $B(x)$ and $C(x)$ are self-reciprocal, it follows that

$$E(x) = wx^{s+t} + \sum_{i=1}^{u_e} w_i \left(x^{f_i} + x^{2(s+t)-f_i}\right), \tag{8}$$

where $w$, $w_i$'s and $f_i$'s are integer numbers, and $0 < f_i < s + t$ for $i = 1, 2, \ldots, u_e$. We have $A(1)B(1) = C(1) + 2E(1)$ and $A(-1)B(-1) = C(-1) + 2E(-1)$, thus

$$A(1)B(1)A(-1)B(-1) = C(1)C(-1) + 2(X),$$

where $X = 2E(1)E(-1) + E(1)C(-1) + E(-1)C(1)$. Hence, in order to prove Eq. (7), we need to show that $X$ is divisible by 4. Now, observe that $E(1) = w + 2\sum_{i=1}^{u_e} w_i$, $E(-1) = w(-1)^{s+t} + 2\sum_{i=1}^{u_e} w_i(-1)^{f_i}$, $C(1) = 2u_c + 1$ and $C(-1) = 2u_c + (-1)^{s+t} - 4v_c$. Thus

$$2E(1)E(-1) \equiv 2\,\mathrm{odd}(w) \pmod 4 \quad \text{and}$$
$$C(-1) \equiv C(1) + 2\,\mathrm{odd}(s+t) \pmod 4,$$

where "odd" is the integer functions from $\mathbb{Z}$ into $\{0, 1\}$, such that $\mathrm{odd}(x) = 1$ if and only if, $x$ is an odd number. Considering the two previous congruences, we have

$$X \equiv 2\,\mathrm{odd}(w) + C(1)\big(E(1) + E(-1)\big) + 2E(1)\,\mathrm{odd}(s+t) \pmod 4.$$

The integer $X$ is now clearly divisible by 4, since $C(1)$ is an odd number, $E(1) + E(-1) \equiv 2w\,\mathrm{odd}(s+t+1) \pmod 4$ and $2E(1) \equiv 2\,\mathrm{odd}(w) \pmod 4$. □

Using the above theorem we can show that some families of reciprocal polynomials are always reducible. The following result is of this flavor.

**Corollary 11.** *Let $m > 1$ be an integer. If $m$ is odd or if $m$ is even with $m \equiv 0$ or $6 \pmod 8$, then $f(x) = 1 + x + x^2 + x^3 + \cdots + x^{m-1} + x^m$ is reducible over $\mathbb{F}_2$.*

When $\mathbb{F}_q$ is of odd characteristic we have the following generalization of Theorem 7.

**Theorem 12.** *Let $f(x)$ be an srm polynomial of degree $2n$ over $\mathbb{F}_q$, having $r$ irreducible factors (counted with multiplicity) over $\mathbb{F}_q$, and suppose that $f(1)f(-1) \neq 0$. Then $r$ is an even number if and only if, $(-1)^n f(1)f(-1)$ is a square in $\mathbb{F}_q$.*

**Proof.** Similar to Lemma 9, we can prove that if $f(1)f(-1) \neq 0$, then $f(x)$ can be factored into srm polynomials, where each srm factor has pairwise distinct irreducible factors. Then using the same arguments as in the proof of the previous theorem, we just need to show that if Theorem 12 is true for $a(x)$ and $b(x)$, being of degrees $2s$ and $2t$ and having $r_a$ and $r_b$ irreducible factors, respectively, then it is also true for $a(x)b(x)$ having $r_a + r_b$ irreducible factors. But this claim is pretty straightforward, unlike the case for the binary field. We can prove the claim in four different cases depending on the parities of $r_a$ and $r_b$. First suppose that $r_a$ and $r_b$ are odd numbers. Then $(-1)^s a(1)a(-1)$ and $(-1)^t b(1)b(-1)$ are not squares in $\mathbb{F}_q$, and thus $(-1)^{s+t}a(1)b(1)a(-1)b(-1)$ is a square in $\mathbb{F}_q$. Now the claim follows in this case since $r_a + r_b$ is an even number. Other cases follow similarly. □

## Acknowledgments

The authors thank Luis Cota for helpful numerical computations and Alfred Menezes for reviewing an earlier draft of this paper.

## References

[1] O. Ahmadi, Self-reciprocal irreducible pentanomials over $\mathbb{F}_2$, Des. Codes Cryptogr. 38 (2006) 395–397.

[2] A. Bluher, A Swan-like theorem, Finite Fields Appl. 12 (2006) 128–138.

[3] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967) 212–220.

[4] S.D. Cohen, On irreducible polynomials of certain types in finite fields, Proc. Cambridge Philos. Soc. 66 (1969) 335–344.

[5] A. Hales, D. Newhart, Irreducibles of tetranomial type, in: Mathematical Properties of Sequences and Other Combinatorial Structures, Kluwer, 2003.

[6] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, revised ed., Cambridge Univ. Press, Cambridge, 1994.

[7] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990) 43–53.

[8] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, in: Verh. 1 Internat. Math. Kongresses, Zurich, 1897, pp. 182–193.

[9] R. Swan, Factorization of polynomials over finite fields, Pacific J. Math. 12 (1962) 1099–1106.

[10] R.R. Varshamov, G.A. Garakov, On the theory of selfdual polynomials over a Galois field, Bull. Math. Soc. Sci. Math. Roumaine (N.S.) 13 (1969) 403–415.

[11] J.L. Yucas, G.L. Mullen, Self-reciprocal irreducible polynomials over finite fields, Des. Codes Cryptogr. 33 (2004) 275–281.