Finite Fields and Their Applications 49 (2018) 166–179

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Factoring polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$

F.E. Brochero Martínez [*], Lucas Reis

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil

ARTICLE INFO

Article history:
Received 12 September 2016
Received in revised form 27 May 2017
Accepted 16 October 2017
Available online 26 October 2017
Communicated by D. Panario

MSC:
primary 12E20
secondary 11T30

Keywords:
Irreducible polynomial in a finite field
Irreducible factors
Cyclotomic polynomials

ABSTRACT

Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and exponent e. For each positive integer n, such that $\nu_p(q-1) \geq \nu_p(e) + \nu_p(n)$ for all prime divisors p of n, we show a fast algorithm to determine the irreducible factors of $f(x^n)$. Using this algorithm, we give the complete factorization of $x^n - 1$ into irreducible factors in the case where $n = dp^t$, p is an odd prime, q is a generator of the group $\mathbb{Z}_{p^2}^*$ and either $d = 2^m$ with $m \leq \nu_2(q-1)$ or $d = r^a$, where r is a prime dividing $q-1$ but not $p-1$.

1. Introduction

An important problem in finite field theory is to determine if a polynomial is irreducible and, in the case where the polynomial is reducible, how to find its irreducible factors. These problems have important practical and theoretical consequences in a wide

[*] Corresponding author.
E-mail addresses: fbrocher@mat.ufmg.br (F.E. Brochero Martínez), lucasreismat@gmail.com (L. Reis).

https://doi.org/10.1016/j.ffa.2017.10.003
1071-5797/© 2017 Elsevier Inc. All rights reserved.

variety of technological situations including error-correcting codes (see [4]), cryptography (see [12]) and efficient and secure communications.

For each polynomial $f(x) \in \mathbb{F}_q[x]$ with $f(0) \neq 0$, the exponent e of $f(x)$ is the least positive integer such that $f(x)$ divides $x^e - 1$. If $f(x)$ is irreducible of degree m, then it divides $x^{q^m-1} - 1$ and therefore e divides $q^m - 1$. The following classical result shows necessary and sufficient conditions to verify the irreducibility of polynomials of the form $f(x^n)$.

Theorem 1.1 *([13] Theorem 3.35). Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and exponent e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:*

(1) Every prime divisor of n divides e,
(2) $\gcd(n, (q^m - 1)/e) = 1$ and
(3) if $4|n$ then $4|q^m - 1$.

In addition, in the case where the polynomial $f(x^n)$ is irreducible, it has degree mn and exponent en.

Observe that, in particular, this theorem gives necessary and sufficient conditions to determine when the polynomial $x^n - a \in \mathbb{F}_q[x]$ is irreducible (see Theorem 3.75 in [13]). In addition, if $a = 1$ and $n > 1$, the polynomial $x^n - 1$ is always reducible and the problem of finding the irreducible factors of $x^n - 1 \in \mathbb{F}_q[x]$ is strongly related to the problem of finding the irreducible factors of the cyclotomic polynomials $\Phi_n(x)$. In fact, $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial (see [13] Theorem 2.45). In general, an "efficient algorithm" to split $\Phi_n(x)$ in $\mathbb{F}_q[x]$ for arbitrary n and q remains an open problem. We note that the problem of determining the irreducible factors of $x^n - 1$ and $\Phi_n(x)$ in $\mathbb{F}_q[x]$ has been considered by many authors: Mey [14] and Blake, Gao, Mullin [5] considered the case where $n = 2^m$; Fitzgerald and Yucas [9] found explicit factors of the cyclotomic polynomials $\Phi_{2^m 3}(x)$ and studied the polynomials $\Phi_{2^n r}(x)$ in the case where r divides $(q - 1)$; the same problem was studied by Wang and Wang for the cyclotomic polynomials $\Phi_{2^m 5}(x)$ and Tuxanidy and Wang [16] for the case when the factorization of $\Phi_r(x)$ is known; Chen, Li and Tuerhong [8] considered the polynomials $x^{2^m p^t} - 1$ in the case where p is a prime factor of $q - 1$ and in [6] the authors found the explicit factorization of $x^n - 1$, in the case where $\operatorname{rad}(n)|(q - 1)$, where $\operatorname{rad}(n)$ denotes the product of all distinct prime factors of n.

In the present paper we consider $f(x)$ an irreducible polynomial of degree m and exponent e and we impose restrictions on e and n to violate some condition in Theorem 1.1. If we do this, the polynomial $f(x^n)$ will be reducible and then we present a computationally fast algorithm that finds every irreducible factor of $f(x^n)$.

Finally, as an application, we use our method to split $x^{dp^t} - 1$ into irreducible factors in the case where p is prime, q is a primitive element of the multiplicative group $\mathbb{Z}_{p^l}^*$,