**EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS**
Vol. 14, No. 1, 2021, 265-267
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

# Note on irreducible polynomials over finite field

Amara Chandoul[1,*], Alanod M. Sibih[2]

[1] *Department of Mathematics Institut Supérieure d'Informatique et de Multimedia de Sfax, Sfax, Tunisia*
[2] *Department of Mathematics, Jamoum University College, Umm Al-qura University, Saudi Arabia*

**Abstract.** In this note we extend an irreducibility criterion of polynomial over finite fields. We prove the irreducibility of the polynomial $P(Y) = Y^n + \lambda_{n-1}Y^{n-1} + \lambda_{n-2}Y^{n-2} + \cdots + \lambda_1 Y + \lambda_0$, such that $\lambda_0 \neq 0$, $\deg \lambda_{n-2} = 2\deg \lambda_{n-1} + l > \deg \lambda_i$, for all $i \neq n-2$ and odd integer $l$.

**2020 Mathematics Subject Classifications**: 11R09, 11C08.

**Key Words and Phrases**: Finite fields, Irreducible polynomials, Viéte theorem.

## 1. Introduction

Irreducibility of polynomial functions seems like one of the major topics in introductory abstract algebra. It is not hard to see, using the fundamental theorem of algebra, that the only irreducible polynomials in $\mathbb{C}[x]$ are polynomials of degree 1. Then, it will be clear that the only irreducible polynomials in $\mathbb{R}[x]$ are polynomials of degree 1 and polynomials of the form $ax^2 + bx + c$ with $b^2 - 4ac < 0$ [4].

The situation over $\mathbb{Q}$ is much different from the situation over $\mathbb{R}$ or $\mathbb{C}$. Over $\mathbb{Q}$, there are many irreducible polynomials of every degree, and determining which polynomials are irreducible is difficult, compared to the real or complex case.

Eisenstein's criterion gives a sufficient condition for a polynomial with integer coefficients to be irreducible over $\mathbb{Q}$.

This criterion is very nice when it works, but there are many irreducible polynomials to which it does not apply. Then, to decide irreducibility, one can try another approaches, like the so called "brute force" [4].

In this paper, we will consider the setting over a finite field. Let, $p$ be a prime and $q$ a power of $p$. Let $\mathbb{F}_q$ be a finite field with $q$ elements of characteristic $p$. It is known that there are no explicitly formula discribing irreduciblility of polynomials over $\mathbb{F}_q$.

Wherefore, we still need to provides methods to decide if a polynomial over $\mathbb{F}_q$ is irreducible.

[*] Corresponding author.

DOI: https://doi.org/10.29020/nybg.ejpam.v14i1.3898

*Email addresses:* amarachandoul@yahoo.fr (A. Chandoul), amsibih@uqu.edu.sa (A. M. Sibih)

Irreducible polynomials over $\mathbb{F}_q$, are used for many applications in mathematics. They are used to carry out the arithmetic in field extension of $\mathbb{F}_q$ [6]. Computations in such extensions occur in coding theory [1], complexity theory [7] and cryptography [5]. Random polynomial time algorithms exist for finding irreducible polynomials of any degree over $\mathbb{F}_q$, [2, 7], and so as a practical matter the problem is solved. However, the deterministic complexity of the problem has yet to be established.

In [2, 3], It was proved the following theorem, which gives an irreducibility criterion over $\mathbb{F}_q[X]$.

**Theorem 1.** *Let* $P(Y) = Y^n + A_{n-1}Y^{n-1} + A_{n-2}Y^{n-2} + \cdots + A_0$ *with* $A_i \in \mathbb{F}_q[X]$, $A_0 \neq 0$ *and* $\deg A_{n-1} > \deg A_i$, *for each* $i \neq n-1$. *Then* $P(Y)$ *is irreducible over* $\mathbb{F}_q[X]$.

In the following, we want to extend this result, in order to define a new family of irreducible polynomials over $\mathbb{F}_q[X]$.

## 2. Main result

We present the following result:

**Theorem 2.** *Let* $P(Y) = Y^n + \lambda_{n-1}Y^{n-1} + \lambda_{n-2}Y^{n-2} + \cdots + \lambda_1 Y + \lambda_0$ *be a polynomial over* $\mathbb{F}_q[X]$, *such that* $\lambda_0 \neq 0$, $\deg \lambda_{n-2} > \deg \lambda_i$, *for each* $i \neq n-2$. *If* $\deg \lambda_{n-2} = 2\deg \lambda_{n-1} + l$, *with* $l$ *is odd, then* $P$ *is irreducible.*

*Proof.*

Using Viéte theorem, which establishes relations between the roots and the coefficients of a polynomial, one can easily see that if $w = w_1, w_2, \cdots, w_n$ be the roots of $P$, then we have exactly 2 of its, with modulus strictly greater than 1.

Suppose now, that $P(Y) = Q_1(Y)Q_2(Y)$, where $Q_1$ and $Q_2$ are in $\mathbb{F}_q[X][Y]$. We can not suppose that the roots $w_1, w_2$ of $P$, with modulus strictly greater than 1 are roots of $Q_1$, cause of the absolute value of the leading coefficient of the polynomial $Q_2$ is superior or equal 1, which will be absurd because $Q_2$ has only roots with modulus strictly less than 1. So, suppose that $w_1$ is a root of $Q_1$ and $w_2$ is a root of $Q_2$.

Let $P(Y) = Q_1(Y)Q_2(Y)$, with

$$Q_1(X) = Y^s + A_{s-1}Y^{s-1} + A_{s-2}Y^{s-2} + \cdots\cdots + A_1 Y + A_0$$

and

$$Q_2(X) = Y^m + B_{m-1}Y^{m-1} + B_{m-2}Y^{m-2} + \cdots + B_1 Y + B_0.$$

It is clear that $\deg A_{s-1} > \deg A_j$, for all $1 \leq j \leq s$, and $\deg B_{m-1} > \deg B_k$, for all

$1 \leq k \leq m.$

A simple calculation gives

$$\lambda_{n-1} = A_{s-1} + B_{m-1} \text{ and } \lambda_{n-2} = A_{s-1}B_{m-1} + A_{s-2} + B_{m-2},$$

which implies

$$\deg \lambda_{n-1} = \sup(\deg A_{s-1}, \deg B_{m-1}) \text{ and } \deg \lambda_{n-2} = \deg A_{s-1} + \deg B_{m-1}.$$

One can easily see, that we have two cases:
First case: If $\deg A_{s-1} > \deg B_{m-1}$, then, we have $\deg \lambda_{n-1} = \deg A_{s-1}$ and $\deg \lambda_{n-2} < 2 \deg \lambda_{n-1}$, which is absurd because $\deg \lambda_{n-2} = 2 \deg \lambda_{n-1} + l$.
Second case: If $\deg A_{s-1} = \deg B_{m-1}$, then, we get $\deg \lambda_{n-2} = 2 \deg A_{s-1}$, So $\deg \lambda_{n-2}$ is even. But $\deg \lambda_{n-2} = 2 \deg \lambda_{n-1} + l$, then it is odd, which is the desired contradiction. Completing the proof.

**Remark**

The converse is not always true.

Consider the Polynomial $P(Y) = Y^3 + (X^2 + X)Y^2 + X^3Y + 1$ in $\mathbb{F}_2[X][Y]$. $P$ is an irreducible polynomial over $\mathbb{F}_2[X]$ but $\deg(X^3) \neq 2\deg(X^2 + X) + l$, for all $l \in \mathbb{N}^*$.

## Acknowledgements

All our thanks to the referees for careful reading of this manuscript and for theirs corrections and many important remarks.

## References

[1] ER Berlekamp. Algebraic coding theory mcgraw-hill. *New York*, 8, 1968.

[2] A Chandoul, M Jellali, and M Mkaouar. Irreducibility criterion over finite fields. *Communications in Algebra*, 39(9):3133–3137, 2011.

[3] Amara Chandoul. *Fractions continues multidimensionnelles: fractions continues multidimensionelles, polynômes irréductibles et nombres de Pisot.* Éditions universitaires européennes, 2012.

[4] Lindsay N Childs. *A concrete introduction to higher algebra.* Springer, 2009.

[5] Benny Chor and Ronald L Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 34(5):901–909, 1988.

[6] Dirk Hachenberger and Dieter Jungnickel. Irreducible polynomials over finite fields. In *Topics in Galois Fields*, pages 197–239. Springer, 2020.

[7] Michael O Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on computing*, 9(2):273–280, 1980.