wjert, 2020, Vol. 6, Issue 4, 165-176. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

PRIMITIVITY AND IRREDUCIBILITY OF $X^N + X + 1$ OVER A BINARY FIELD $\mathbb{F}_2$

Ahmed Asimi*

Department of Mathematics, Faculty of Sciences, Ibn Zohr University Information Systems and Vision Laboratory B.P. 8106 Agadir, Maroc.

Article Received on 25/05/2020 **Article Revised on 15/06/2020** **Article Accepted on 05/07/2020**

***Corresponding Author**
Ahmed Asimi
Department of Mathematics, Faculty of Sciences, Ibn Zohr University Information Systems and Vision Laboratory B.P. 8106 Agadir, Maroc.

ABSTRACT

In cryptography, more particularly for the linear Feedback Shift Register (LFSR) of length n, the irreducibility of the polynomial $P(x) = x^n + x + 1$ over $\mathbb{F}_2$ is very important to generate a binary pseudorandom sequence corresponding to the nonzero initial state vector derived from the secret key, because it is well known[9] that any LFSR of length n whose characteristic polynomial is a primitive polynomial over $\mathbb{F}_2$ will generate a periodic sequence of period 2^n-1 for any nonzero initial state vector. In this paper, we start with the study of the reducibility and the parity of the number of irreducible factors of the polynomial $P(x) = x^n + x + 1$ in $\mathbb{F}_2[x]$. We show that 1) If n = 2 or n = 3, the polynomial P(x) is irreducible over $\mathbb{F}_2$; 2) If n ≡ 2 mod 3 and n > 3, the polynomial P(x) is reducible over $\mathbb{F}_2$; 3) If n ≡ 0 or 2 or 3 or 5 mod 8 and n > 3, the polynomial P(x) has an even number of irreducible factors over $\mathbb{F}_2$, then P(x) is reducible over $\mathbb{F}_2$; 4) If n ≡ 1 or 4 or 6 or 7 or 9 or 15 or 22 mod 24 and n > 3 then P(x) has an odd number of irreducible factors over $\mathbb{F}_2$; 5) If $P(x) = x^n + x + 1$ is irreducible over $\mathbb{F}_2$, then n ≡ 1 or 4 or 6 or 7 or 9 or 15 or 22 mod 24 and n > 3. The converse is not true. We close this paper by proposing two programs, in Python language, to build irreducible and primitive polynomials, $P(x) = x^n + x + 1$, over $\mathbb{F}_2$. For example, we build all irreducible polynomials, $P(x) = x^n + x + 1$, over $\mathbb{F}_2$ of degree at less greater than 1000 and primitive polynomials of

KEYWORDS: Cryptography, Feedback shift register, Pseudorandom sequence, Irreducible and Primitive polynomials.

1 INTRODUCTION AND NOTATIONS

Cryptography, broadly defined, is the science that studies a wide range of issues in the transmission and safeguarding of information. The increasing importance of cryptography in the ”information age” and the concomitant flourishing of cryptographic research have had a profound impact on number theory to acquire a practical urgency. A stream cipher is an important class of symmetric-key encryption scheme. Their essential property is that the encryption transformation changes for each symbol of the plaintext and they are advantageous because they avoid error propagation. In a narrow sense, it generates cryp- tographically secure pseudorandom numbers from a shored key, and takes exclusive-OR with the plain message to obtain ciphered message. One way to generate such pseudoran- dom numbers is to use a non-secure generator like Feedback Shift Register, in particular a linear Feedback Shift Register (LFSR), the basic building blocks in most stream ciphers, that one can initialize by using the key, and then apply some complicated functions to its outputs to obtain a secure sequence, called the keystream generator.

Recall that LFSR of length n which produces a sequence with minimal period of maximal possible value $2^n - 1$ starting from an arbitrary nonzero initial state is called maximum-length and the produced sequence is called m-sequence. It is well-known that an n stage LFSR is a maximal-length register if and only if a polynomial associated to it is primitive of degree n of $\mathbb{F}_2 n$ (i.e an irreducible polynomial $f(x) \in \mathbb{F}_2[x]$. of degree n such that $x^{\frac{2^n-1}{r}} \not\equiv 1 \mod (f(x))$ for all prime factor r of $2^n - 1$).[9] If the Mersenne number $2^n - 1$ is prime then for any non trivial $x \in \mathbb{F}_2 n$ is a generator of $\mathbb{F}_2 n$, we then deduce : if $2^n - 1$ is a prime number then every monic irreducible of degree n over $\mathbb{F}_2$ is a primitive polynomial.

Therefore, it is necessary to require for an irreducible polynomial over $\mathbb{F}_2$ to have its degree equal to length of LFSR. Irreducibility of polynomials in $\mathbb{F}_2[x]$ can be tested in a variety of ways.[8] For instance, $f(x) \in \mathbb{F}_2[x]$ of degree n is irreducible if only if $gcd(f(x), x^{2^i} + x) = 1$ for all $i = 1, 2, \ldots, E\left(\frac{n}{2}\right)$. This follows from the facts that $x^{2^i} - x \in \mathbb{F}_2[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree dividing i, and that if f is irreducible it has a factor of degree at most $E\left(\frac{n}{2}\right)$. This irreducibility condition can be tested efficiently using generalizations of Euclidean algorithm. The number of terms must be odd, as otherwise $x + 1$ would be a factor. The number $N_2(n)$ of monic irreducible of degree n over $\mathbb{F}_2$ is given by the following formula

$$N(n) = \frac{1}{n}\sum_{d/n}\mu(d)2^{\frac{n}{d}} \simeq \frac{2^n}{n}[7]$$

For purpose of the fastest software realization of LFSR of length n, it is desirable to have an irreducible polynomial $f \in \mathbb{F}_2[x]$ of degree n with as a few terms as possible because only few bits of feedback shift register must be combined with or exclusive. The specialists of cryptography like to use the trinomial x^n+x+1 for implanting LFSR because only two bits of feedback shift register must be OXRed.

In this paper, we start with the study of the reducibility and the parity of the number of irreducible factors for the polynomial $P(x) = x^n + x + 1$ in $\mathbb{F}_2[x]$. We show that:

1) If $n = 2$ or $n = 3$, the polynomial $P(x)$ does not have a root in $\mathbb{F}_2$, then $P(x)$ is irreducible over $\mathbb{F}_2$ (Proposition 3.1);
2) If $n \equiv 2 \bmod 3$ and $n > 3$, the polynomial x^2+x+1 divides $P(x)$ in $\mathbb{F}_2[x]$, then $P(x)$ is reducible over $\mathbb{F}_2$ (Proposition 3.3);
3) If $n \equiv 2$ or 5 or 8 or 11 or 14 or 17 or 20 or 23 mod 24, the polynomial $P(x)$ is reducible over $\mathbb{F}_2$ (Corollary 2);
4) If $n \equiv 0$ or 2 or 3 or 5 mod 8 and $n > 3$, the polynomial $P(x)$ has an even number of irreducible factors over $\mathbb{F}_2$ (Proposition 3.2), then $P(x)$ is reducible over $\mathbb{F}_2$;
5) If $n \equiv 1$ or 4 or 6 or 7 mod 8 and $n > 3$, the polynomial $P(x)$ has an odd number of irreducible factors over $\mathbb{F}_2$ (Proposition 3.2);
6) If $n \equiv 1$ or 4 or 6 or 7 or 9 or 15 or 22 mod 24 and $n > 3$, the polynomial $P(x)$ has an odd number of irreducible factors over $\mathbb{F}_2$ (Proposition 3.2);
7) If $P(x) = x^n + x + 1$ is irreducible over $\mathbb{F}_2$, then $n \equiv 1$ or 4 or 6 or 7 or 9 or 15 or 22 mod 24 and $n > 3$. The converse is not true. Indeed, we show that the polynomials $x^{25}+x+1$, $x^{31}+x+1$, $x^{33}+x+1$, $x^{39}+x+1$, $x^{52}+x+1$, $x^{54}+x+1$ and $x^{70}+x+1$ are reducible over $\mathbb{F}_2$. Because $x^8+x^4+x^3+x^2+1$ divides $x^{25}+x+1$, x^3+x+1 divides $x^{31}+x+1$ and $x^{52}+x+1$, x^3+x^2+1 divides $x^{33}+x+1$ and $x^{54}+x+1$, $x^7+x^6+x^3+x+1$ divides $x^{39}+x+1$ and $x^8+x^7+x^5+x^4+x^3+x^2+1$ divides $x^{70}+x+1$ in $\mathbb{F}_2[x]$.

We close this paper by proposing two programs, in Python language, to build irreducible and primitive polynomials, $P(x) = x^n+x+1$, over $\mathbb{F}_2$. For example, we build all irreducible polynomials, $x^n + x + 1$, over $\mathbb{F}_2$ of degree at least greater than 1000 and all primitive polynomials of degree at least greater than 100.

In this section we introduce the notation that will be used throughout this paper.

$\mathbb{F}_2 n$: the finite field of order 2^n. If $n = 1$, $\mathbb{F}_2 = \{0,1\}$ is called the binary finite field of characteristic 2.

$\mathbb{F}_{2^n}^*$: the cyclic multiplicative group of all non zero elements in $\mathbb{F}_2 n$ of order $2^n - 1$.

$\mathbb{F}_2[x]$: the ring of polynomials in the indeterminate x and with coefficients from $\mathbb{F}_2$.

$gcd(k, m)$: the greatest common divisor of positive integers k and m.

ϕ : the Euler function; if m is a positive integer, $\phi(m)$ is the number of integers k with $1 \leq k \leq m$ and $\gcd(k, m) = 1$.

$E(x)$: The integer part of a real number x.

2 Preliminaries

We recall some results from R. Lidl, H. Niederreiter.[9,11] and Selmer.[15]

Theorem 2.1. *Euler's theorem (also known as the Fermat-Euler theorem or Euler's to- tient theorem) states that if n and a are coprime positive integers, then* $a^{\phi(n)} \equiv 1 \bmod n$.

Definition 2.1. *Let* $f(x) \in \mathbb{F}_2[x]$ *be a polynomial of degree at least* 1. *Then* $f(x)$ *is said to be irreducible over* $\mathbb{F}_2$ *if it cannot be written as the product of two polynomials in* $\mathbb{F}_2[x]$, *each of positive degree.*

Proposition 2.1. *Let* $f(x) \in \mathbb{F}_2[x]$ *be an irreducible polynomial of degree n. Then* $\mathbb{F}_2[x]/(f(x))$, *the set of polynomials in* $\mathbb{F}_2[x]$ *of degree less than* n, *is a field of order* 2^n. *Addition and multiplication are performed modulo* $f(x)$, *Therefore* $\mathbb{F}_2 n = \mathbb{F}_2[x]/(f(x))$. *In this case,* $\mathbb{F}_2 n$ *is called the splitting field of* $f(x)$.

Proposition 2.2. *For each* $n \geq 1$, *there exists a monic irreducible polynomial of degree n over* $\mathbb{F}_2$.

Definition 2.2. *Let* $f(x) \in \mathbb{F}_2[x]$ *an irreducible polynomial over* $\mathbb{F}_2$ *of degree n and* α *a root of* $f(x)$. $f(x)$ *is called a primitive polynomial over* $\mathbb{F}_2$ *if* α *is a generator of a cyclic group* $\mathbb{F}_2^* n$.

Proposition 2.3. *The irreducible polynomial* $f(x) \in \mathbb{F}_2[x]$ *of degree n is a primitive polynomial if and only if* $f(x)$ *divides* $x^k - 1$ *for* $k = 2^n - 1$ *and for not small positive integer k.*

Proposition 2.4. *For each* $n \geq 1$, *there exists a monic primitive polynomial of degree n over* $\mathbb{F}_2$. *There are precisely* $\phi(2^n - 1)/n$ *such polynomials.*

Lemma 2.1. *Let n be a positive integer. Then we have :*

$$n^n \equiv \begin{cases} 1 \mod 8 & \text{If } n \equiv 1 \mod 8 \\ 3 \mod 8 & \text{If } n \equiv 3 \mod 8 \\ 5 \mod 8 & \text{If } n \equiv 5 \mod 8 \\ 7 \mod 8 & \text{If } n \equiv 7 \mod 8 \\ 0 \mod 2^{2n} & \text{If } n \equiv 0 \mod 4 \\ 2^n \mod 2^{n+2} & \text{If } n \equiv 2 \mod 4 \text{ and } n > 3 \\ 0 \mod 2^n & \text{If } n \equiv 0 \mod 2 \end{cases}$$

Proof. This proof relies on

i) $n^n \equiv r^n \equiv r \bmod 8$ if n is an old number and $n \equiv r \bmod 8$.

ii) If $n = 4k$ ($n \equiv 0 \bmod 4$), then $n^n = 4^n k^n = 2^{2n} k^n$.

iii) If $n = 2 + 4k$ ($n \equiv 2 \bmod 4$), then $n^n = 2^n(1 + 2k)^n = 2^n(1 + 2k)^{2+4k} = 2^n(1 + 2k)^2(1 + 4k)^{4k} = 2^n(1 + 4k + 16k^2)(1 + 4k)^{4k}$

From Arjen K. Lenstra,[5] we deduce the following results

Lemma 2.2. *$f \in \mathrm{F}_2[x]$ of degree n is irreducible if and only if $\gcd(f(x), x^{2^k} + x) = 1$ for $k = 1, \ldots, E\left(\frac{n}{2}\right)$.*

Theorem 2.2. *[12] Let $f(x) \in \mathbb{F}_2[x]$, and suppose $\mathrm{disc}(f)\, f = 0$. Let t denotes the number of irreducible factors of $f(x)$ over $\mathbb{F}_2[x]$, and let $F \in \mathbb{Z}[x]$ be any monic polynomial such that $F(x) \equiv f(x) \bmod \mathbb{F}_2[x]$. Then $t = \deg(f)$ modulo 2 if only if $\mathrm{disc}(F) = 1$ modulo 8.*

Proposition 2.5. *Let d be an integer, and assume that there exist a positive integer n such that $d = (-1)^{\frac{n(n-1)}{2}} (n^n - (n-1)^{n-1})$ we then get*

1) *If n is an odd number then*

$$d \equiv \begin{cases} 5 \mod 8 & \text{if } n \equiv 3 \text{ or } 5 \mod 8 \text{ and } n > 3. \\ 1 \mod 8 & \text{if } n \equiv 1 \text{ or } 7 \mod 8 \text{ or } n = 3. \end{cases}$$

2) *If $n \neq 2$ is an even number then*

$$d \equiv \begin{cases} 1 \mod 8 & \text{if } n \equiv 0 \mod 8 \text{ or } n \equiv 2 \mod 8 \\ 5 \mod 8 & \text{if } n \equiv 4 \mod 8 \text{ or mod } 8 \text{ if } n \equiv 6 \mod 8 \end{cases}$$

Proof. 1) Assume that n is an odd number.

1.1) If $n = 3$, then $d = 4 - 27 = -23 \equiv 1 \bmod 8$.

1.2) If $n \geq 4$, we then have $n \equiv 1 \bmod 2$, then $n-1 \equiv 0 \bmod 2$ and $(n-1)^{n-1} \equiv 0 \bmod 8$, hence $d \equiv (-1)^{\frac{n(n-1)}{2}} n^n \bmod 8$.

1.2.1) If $n \equiv 1 \bmod 8$ then $n^n \equiv 1 \bmod 8$ and $(-1)^{\frac{n(n-1)}{2}} = 1$, therefore $d \equiv 1 \bmod 8$.

1.2.2) If $n \equiv 3 \bmod 8$ then $n^n \equiv 3 \bmod 8$ and $(-1)^{\frac{n(n-1)}{2}} = -1, \bmod 8$, therefore $d \equiv 5 \bmod 8$.

1.2.3) If $n \equiv 5 \bmod 8$ then $n^n \equiv 5 \bmod 8$ and $(-1)^{\frac{n(n-1)}{2}} = 1, \bmod 8$, therefore $d \equiv 5 \bmod 8$.

1.2.4) If $n \equiv 7 \bmod 8$ then $n^n \equiv 7 \bmod 8$ and $(-1)^{\frac{n(n-1)}{2}} = -1, \bmod 8$, Therefore $d \equiv 1 \bmod 8$.

2) Assume that $n \neq 2$ is an even number, then $n^n \equiv 0 \bmod 8$ (Lemma 3.1), therefore

$d \equiv (-1)^{\frac{n(n-1)}{2}} (1-n)^{n-1} \bmod 8$

2.1) If $n \equiv 2 \bmod 4$, then $n-1 \equiv 1 \bmod 4$ and $(-1)^{\frac{n(n-1)}{2}} = -1$, therefore $d \equiv (n-1)^{n-1} \bmod 8$.

2.1.1) If $n \equiv 2 \bmod 8$, then $n-1 \equiv 1 \bmod 8$, therefore $d \equiv 1 \bmod 8$.

2.1.2) If $n \equiv 6 \bmod 8$ then $n-1 \equiv 5 \bmod 8$, therefore $d \equiv 5 \bmod 8$.

2.2) If $n \equiv 0 \bmod 4$, then $n-1 \equiv 3 \bmod 4$ and $(-1)^{\frac{n(n-1)}{}} = 1$, therefore $d \equiv (1-n)^{n-1} \bmod 8$.

2.2.1) If $n \equiv 0 \bmod 8$, then $n-1 \equiv 7 \bmod 8$ and $1-n \equiv 1 \bmod 8$, therefore $d \equiv 1 \bmod 8$.

2.2.2) If $n \equiv 4 \bmod 8$ then $n-1 \equiv 3 \bmod 8$ and $1-n \equiv 5 \bmod 8$, therefore $d \equiv 5 \bmod 8$.

3) Irreducibility and primitivity of $P(x) = x^n + x + 1$ over $\mathbb{F}_2$

All over this section we describe the conditions for which $P(x) = x^n + x + 1$ is irreducible over $\mathbb{F}_2$.

Lemma 3.1. *The polynomial* $P(x) = x^n + x + 1 \in \mathbb{F}_2[x]$ *has all roots* $\alpha_1, \ldots, \alpha_n$ *distinct.*

Proof. Since d is the discriminant of the polynomial $P(x) = x^n + x + 1$, n and $n-1$ are relatively prime, we then get $d = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} (n^n - (n-1)^{n-1}) \equiv 1 \bmod 2$ modulo 2, therefore $\alpha i \neq \alpha j$ for all $i \neq j$.

Theorem 3.1. *Let* $P(x) = x^n + x + 1$ *be a polynomial in* $\mathbb{F}_2[x]$ *and* α *its root in its splitting field over* $\mathbb{F}_2$. *Then for all positive integer* k, α^{2^k} *are roots of* $P(x) = x^n + x + 1$.

Proof. The proof of this theorem is done by recursion on k. If $k = 0$, then α is a root of $P(x) = x^n + x + 1$.

Assume that the hypothesis of recursion is true until k and show that for $k + 1$. We have $(\alpha^{2^k})^n = \alpha^{2^k} + 1$.

$$\begin{aligned}(\alpha^{2^{k+1}})^n &= (\alpha^{2^k \times 2})^n \\ &= (\alpha^{2^k})^{2n} \\ &= ((\alpha^{2^k})^n)^2 \\ &= (\alpha^{2^k} + 1)^2 \\ &= (\alpha^{2^k})^2 + 1 \\ &= \alpha^{2^{k+1}} + 1\end{aligned}$$

Then for all positive integer k, α^{2^k} are roots of $P(x) = x^n + x + 1$.

Corollary 1: *Let $P(x) = x^n + x + 1$ be a primitive polynomial in $\mathbb{F}_2[x]$ and α its root in its splitting field over* F. *Then the set of all roots of $P(x) = x^n + x + 1$ is $\{\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}\}$. In this case $\mathbb{F}_2[\alpha]$ is the splitting field of $P(x) = x^n + x + 1$ over $\mathbb{F}_2$.*

The proof of this corollary relies on theorem 3.1 and $\theta(\alpha) = 2^n - 1$.

Proposition 3.1. *The polynomial $P(x) = x^n + x + 1$ is irreducible in $\mathbb{F}_2[x]$ for $n \in \{2, 3\}$.*

Proof. The polynomial $P(x) = x^n + x + 1$ is irreducible in $\mathbb{F}_2[x]$ for $n \in \{2, 3\}$ if and only if $P(x)$ does not have a root in $\mathbb{F}_2$.

Proposition 3.2. *Let $n > 3$ be a positive integer, $P(x) = x^n + x + 1$ a polynomial in $\mathbb{F}_2[x]$ and d its discriminant.*

1) *If $n \equiv 1$ or 4 or 6 or 7 mod 8 then $P(x)$ has an odd number of irreducible factors.*

2) *If $n \equiv 0$ or 2 or 3 or 5 mod 8 then $P(x)$ has an even number of irreducible factors.*

Proof. Let N be the number of factors of $P(x) = x^n + x + 1$.

By proposition 2.5, we deduce $d \equiv 1 \bmod 2$ for all positive integer n, therefore $d \neq 0$ in $\mathbb{F}_2$.

1) *i*) If $n \equiv \pm 1 \bmod 8$ or $n = 3$ then $d \equiv 1 \bmod 8$ proposition 2.5, therefore $N \equiv n \equiv 1 \bmod 2$ theorem 2.2. Hence P has an odd number of irreducible factors.

ii) If $n \equiv 4$ or $6 \bmod 8$ then $d \equiv 5 \bmod 8$ proposition 2.5, therefore $N \not\equiv n \bmod 2$ theorem 2.2. Since $n \equiv 0 \bmod 2$, then P has an odd number of irreducible factors.

2) *i*) If $n \equiv \pm 3 \bmod 8$, then $d \equiv 5 \bmod 8$ proposition 2.5, therefore $N \not\equiv n \bmod 2$ theorem 2.2. Since $n \equiv 1 \bmod 2$, then P has an even number of irreducible factors.

ii) If $n \equiv 0$ or $2 \bmod 8$, then $d \equiv 1 \bmod 8$ proposition 2.5, therefore $N \equiv n \equiv 0 \bmod 2$ theorem 2.2. Hence P has an even number of irreducible factors.

Proposition 3.3. *Let* $P(x) = x^n + x + 1$ *be a polynomial in* $\mathbb{F}_2[x]$ *and* $n > 3$.
If $n \equiv 2$ *mod* 3 *then* $P(x)$ *is reducible over* $\mathbb{F}_2$.

Proof: Let $\boldsymbol{j}$ be a third root of unity (ie $\boldsymbol{j}^3 = 1$).
If $n \equiv 2 \bmod 3$, then $\boldsymbol{j}^n = \boldsymbol{j}^{2+3k} = \boldsymbol{j}^2 = -\boldsymbol{j} - 1$, hence $\boldsymbol{j}$ and $\boldsymbol{j}^2$ are roots of $P(x)$, therefore $x^2 + x + 1$ divides $P(x)$ in $\mathbb{F}_2[x]$. Since $n > 3$, then $P(x) \neq x^2 + x + 1$. We get then $P(x)$ is reducible over $\mathbb{F}_2$.

Corollary 2. *Let* $P(x) = x^n + x + 1$ *be a polynomial in* $\mathbb{F}_2[x]$ *and* $n > 3$.
If $n \equiv 2$ *or* 5 *or* 8 *or* 11 *or* 14 *or* 17 *or* 20 *or* 23 *mod* 24 *then* $P(x)$ *is reducible over* $\mathbb{F}_2$.

Proof : Since $n \equiv 2$ or 5 or 8 or 11 or 14 or 17 or 20 or 23 mod 24 then $n \equiv 2 \bmod 3$ and $n > 3$. The proof of this corollary relies then on proposition 3.3.

The following results characterize the irreducible polynomials over a binary field of a fixed degree. The proof is well−known, see for example.[1,2,3,4,14]

Theorem 3.2. *For every* $n \in \mathrm{N}$, *the product of all monic irreducible polynomials over* F *whose degree divide n is equal to* $x^{2^n} + x$.

Lemma 3.2. *Let* $\boldsymbol{f}(x) \in \mathbb{F}_2[x]$ *be an irreducible polynomial of degree n. The following conditions are equivalent :*

1) $\boldsymbol{f}(x)$ *is irreducible over* $\mathbb{F}_2$.

2) $gcd(f(x); x^{2^k} + x) = 1$ *for* $i = 1, 2, \ldots, E\left(\frac{n}{2}\right)$ *and* $\boldsymbol{f}(x)$ *divides* $x^{2^n} + x$ *in* F $[x]$.

If $deg(f(x)) > 1$, *then* $\boldsymbol{f}(x)$ *is irreducible over* F *if and only if* $gcd(f(x); x^{2^{k-1}} + 1) = 1$ *for* $i = 1, 2, \ldots, E\left(\frac{n}{2}\right)$ *and* $\boldsymbol{f}(x)$ *divides* $x^{2^n} + x$ *in* F $[x]$.

Lemma 3.3. *Let* $\boldsymbol{f}(x) \in \mathbb{F}_2[x]$ *be an irreducible polynomial of degree m. The following conditions are equivalent :*

1) $\boldsymbol{f}(x)$ *divides* $x^{2^n} + x$ *in* F $[x]$.

2) M divides n.

Corollary 3. *If* $P(x) = x^n + x + 1 \in \mathbb{F}_2[x]$ *is an irreducible polynomial over* $\mathbb{F}_2$*, then* $P(x)$ *divides* $x^{2^n} + x$ *in* F $[x]$.

Theorem 3.3. *(Chinese Remainder Theorem) Given pairwise coprime positive integers* n_1, n_2, n_k *andarbitraryintegers* $a_1, a_2, \ldots, a_k$*,thesystemofsimultaneouscongruences*

$$\begin{cases} x & \equiv & a_1 & mod\ n_1 \\ x & \equiv & a_1 & mod\ n_2 \\ : & : & : & : \\ x & \equiv & a_k & mod\ n_k \end{cases}$$

Has a solution, and the solution is unique modulo $N = n_1 n_2 \cdots n_k$ *given by formulae :*
$x = a_1.N_1.y_1 + \cdots + a_k.N_k.y_k$

Where $Ni = \frac{N}{n_i}$ *and* $yi \equiv N^{-1}$ *mod ni for all* $i \in \{1, \cdots, k\}$.

Corollary 4. *The system of simultaneous congruences*

$$(S)\begin{cases} n & \equiv & a_1 & mod\ 8 \\ n & \equiv & a_2 & mod\ 3 \end{cases}$$

Has a solution, and the solution is unique modulo 24 *given by formulae:*
$n = 9a_1 + 16a_2$.

The proof of this corollary relies on Chinese Remainder Theorem 3.3.

Theorem 3.4. *If* $P(x) = x^n + x + 1 \in \mathbb{F}_2[x]$ *is an irreducible polynomial over* $\mathbb{F}_2$ *and* $n > 3$*, then* $n \equiv 1$ *or* 4 *or* 6 *or* 7 *or* 9 *or* 12 *or* 15 *or* 22 *mod* 24*. The converse is not true*

Proof : We refer to propositions 3.2 and 3.3 and we get :

If $P(x) = x^n + x + 1 \in \mathbb{F}_2[x]$ is an irreducible polynomial over $\mathbb{F}_2$, then n is a solution of the system of simultaneous congruences

$$(S)\begin{cases} n & \equiv & a_1 & \mod 8 \\ n & \equiv & a_2 & \mod 3 \end{cases}$$

Where $a_1 \in \{1, 4, 6, 7\}$ and $a_2 \in \{0, 1\}$, hence $n = 9a_1 + 16a_2 \mod 24$ corollary 4. Therefore

We get $n \in \{1, 4, 6, 7, 9, 12, 15, 22\}$ mod 24.

Reciprocally, we have the polynomials $x^{31}+x+1$, $x^{33}+x+1$, $x^{39}+x+1$, $x^{52}+x+1$, $x^{54}+x+1$ and $x^{70}+x+1$ are reducible over $\mathbb{F}_2$. Because x^3+x+1 divides $x^{31}+x+1$ and $x^{52}+x+1$, x^3+x^2+1 divides $x^{33}+x+1$ and $x^{54}+x+1$, $x^7+x^6+x^3+x+1$ divides $x^{39}+x+1$ and $x^8+x^7+x^5+x^4+x^3+x^2+1$ divides $x^{70}+x+1$ in $\mathbb{F}_2[x]$.

Algorithm 1 Determining all irreducible polynomials $x^n + x + 1$ over $\mathbb{F}_2$

```
import numpy, sympy, math
from math import *
from sympy import *
x = sympy.Symbol("x")
def irre(n):
Ir = [2, 3]
for d in range(4,n) : do
  if (d == 1 mod 24 or d == 4 mod 24 or d == 6 mod 24 or d == 7 mod 24 or
  d == 9 mod 24 or d == 15 mod 24 or d == 2) mod 24): then
    Ir.append(d)
  end if
  return Ir
end for
def sett(n):
T=[]
for d in irre(n): do
  L = factorlist(x**d + x + 1, modulus = 2)
  K = L[1]
  if  len(K) == 1 then
    T.append(d)
  end if
  print (T)
end for
```

While being based on these results, we deduce two programs for determining all ir- reducible and primitive polynomials $x^n + x + 1$ over a binary field $\mathbb{F}_2$, and we construct all irreducible polynomials $x^n + x + 1$ over $\mathbb{F}_2$ of degree at less greater than 1000 and all primitive polynomials of degree at less greater than 100.

The irreducible polynomials x^n+x+1 over $\mathbb{F}_2$ of degree at less greater than 1000 are those of degree $n \in \{2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900\}$.

Algorithm 2 Determining all primitive polynomials $x^n + x + 1$ over $\mathbb{F}_2$

```
import numpy, sympy, math
from math import *
from sympy import *
x = sympy.Symbol("x")
L=range(floor(n/2),2^n - 1)
K=factorint(24, multiple = True)
if isprime(2^n - 1)=True: then
  print(x^n + x + 1 is primitive)
else
  for d in irre(n) and n in L and n in K : do
    if ((x^d - 1)%(x^n + x + 1))%2 = 0 : then
      print(x^n + x + 1 not primitive)
    end if
  end for
  print(x^n + x + 1 is primitive)
end if
```

The primitive polynomials $x^n + x + 1$ over $\mathbb{F}_2$ of degree at less greater than 100 are those of degree $n \in \{2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63\}$.

REFERENCES

1. Ahmed Asimi, Determination of irreducible and primitive polynomials over a bi- nary finite field, International J. of Pure and Engg. Mathematics (IJPEM) ISSN 2348 − 3881, April, 2016; 4(*I):* 45 − 59.
2. Lidl R., Niederreiter H., Finite fields, Encyclopedia of math, and its Appl, 20, Addison-Wesley Publ. Co, Reading, Mass, Reprint, Cambridge Univ, Press, Cambridge, 1967.
3. Lidl R., Niederreiter H., Introduction to Finite Fields and Their Applications, Cambridge Univ, Press, Cambridge, Second Edition, 1994.
4. Swan R. G., Factorization of polynomials over finite fields, Paci c J. Math., 1962; 1099−1106.
5. Arjen K. Lenstra, Citibank, N.A., Computional methods in public key cryptology, 1 North gate road, Mendham, NJ 07945 −3104, U.S.A. *arjen.lenstra@citigroup.com.*
6. S.W. Golomb, Shift register sequences, Holden-Day, San Francisco, 1967.
7. H. Kenneth, Rosen, Applied cryptography, The CRC Press Series on discrete mathematics and its applications, 1996.
8. D.E. Knuth, The art of computer programming, volume 2, seminurecal algorithms, third edition, Addison-Wesley, 1998.

9. R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of math, and its Appl, vol 20, Addison-Wesley Publ. Co, Reading, Mass, 1983, reprint, Combridge Uni, Press, Combridge, 1967.
10. P. Ribenboim, L'Arithm´etique des corps, Hermann, Paris, 1972.
11. E.S. Selmer, Linear recurrence relations over finite fields, Departement of mathe- matics, Univ. of Bergen, 1966.
12. R. G. Swan, Factorization of polynomials over finite fields, Pacific J. Math 12, 1962; 1099−1106.
13. H. Wielandt, Finite permutation groups, Academic Press, 1964.
14. Dingyi, Pei and Arto, Salomaa and Cunsheng, Ding, Chinese remainder theorem: applications in computing, coding, cryptography, publisher: World Scientific, 1996.
15. Adler, Andrew and Coury, J, The theory of numbers, publisher: Jones and Bartlett Boston, MA., 1995.