International J. of Pure & Engg. Mathematics (IJPEM)
ISSN 2348-3881, Vol. 4 No. I (April, 2016), pp. 45-59

DETERMINATION OF IRREDUCIBLE AND PRIMITIVE POLYNOMIALS OVER A BINARY FINITE FIELD

AHMED ASIMI
Departement of Mathematics, Faculty of Sciences
University Ibnou Zohr, B. P. 8106 Agadir, Morroco
E-mail: asimiahmed2008@gmail.com, asimiahmed@yahoo.fr

Abstract

The theory of polynomials over a finite field $\mathbb{F}_2$ is important for many cryptographic applications. In cryptography [1], the irreducibility of polynomials 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 [8] and [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 give two fast programs for computing the number of irreducible polynomials of a fixed degree n and primitive polynomials of a fixed degree n over $\mathbb{F}_2$ for all positive integers n and we compute $N(n, 2)$ and $N(n, 2^n - 1, 2)$ for n at least than 100; and we give two fast programs for building the irreducible and primitive polynomials over $\mathbb{F}_2$, for example, we construct all irreducible and primitive polynomials over $\mathbb{F}_2$ of degree at least than 10.

1. Introduction and Notations

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

Key Words : *Cryptography, Feedback shift register, Program, Pseudorandom, Sequence, Irreducible and Primitive polynomial.*

$gcd(n,m)$: denotes the greatest common divisor of n and m. $\langle a\rangle = \{a^k; k \in \mathbb{Z}\}$: the multiplicative group generated by a. If $\{a^k; k \in \mathbb{Z}\}$ is a finite set then $\langle a\rangle$ is a cyclic group of order m, where m denotes the number of elements of $\langle a\rangle$. In this case $\langle a\rangle = \{1, \cdots, a^{m-1}\}$ with $a^m = 1$. Then its order is called the order of a. Otherwise, a is called an element of infinite order.

$\varphi()$: denotes the Euler's function and $\varphi(n)$ indicates the number of integers d with $1 \leq d \leq n$ that are relatively prime to n.

$\mathbb{F}_q$: denotes the finite field of q elements, with q a power of a prime number that is its characteristic. In our case, q is a power of two.

$\mathbb{F}_2$: the binary field of characteristic two.

$\phi_n()$: denotes the cyclotomic polynomial over $\mathbb{F}_2$; $\phi_n(x) = \prod_{\substack{s=1 \\ gcd(s,n)=1}}^{n} (x - \xi^s)$ where ξ is a primitive n^{th} root of unity and n an odd positive integer. The degree of the polynomial ϕ_n is $\varphi(n)$. The polynomial ϕ_n is clearly independent of the choice of ξ.

$N(n,2)$: the number of monic irreducible polynomials over $\mathbb{F}_2$ of degree n.

$N(n,e,2)$: the number of monic irreducible polynomials over $\mathbb{F}_2$ of degree n and order e.

$N(n,2^{n-1},2)$: the number of primitive polynomials over $\mathbb{F}_2$ of degree n.

$\theta(q)$ modulo n : denotes the least number m such that $q^m = 1$ modulo n.

$[a]$: denotes the whole part of a real number a.

$disc(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2$: the discriminant of the polynomial $P(x)$, where α_i is the root of $P(x) = 0$ [2].

μ : the Mbius function.

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

$deg(f)$: denotes the degree of the polynomial f.

We say that n is a Mersenne exponent if $2^n - 1$ is (Mersenne) prime. The theory of polynomials over finite fields is important for investigating the algebraic structure of finite fields which are used in cryptography, for example, they are used in the S-box of the Rijndael encryption algorithm [4] and [6], which have been adopted as the Advanced Encryption Standard (AES), and are used in a variety of coding and cryptographic applications [1], including cryptology using elliptic curves [3], and are also used in error correction, such as the Reed-Solomon codes [14] used for error corrections on Compact

Discs. Above all, irreducible and primitive polynomials are indispensable to construct finite fields. To represent the elements of $\mathbb{F}_{2^n}$, we regard $\mathbb{F}_{2^n}$ as a simple algebraic extension of $\mathbb{F}_2$ of degree n, which is obtained by adjunction of a root α of an irreducible polynomial over $\mathbb{F}_2$ [8] and [9] where each element can be represented as a power of α. In cryptography, on the one hand the Rijndael Encryption algorithm uses a primitive polynomial $x^8 + x^4 + x^3 + x + 1$ of degree eight over a binary field, and on the other hand, for the linear Feedback Shift Register (LFSR) of length n [11], the irreducibility of polynomials 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 [8] and [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.

2. Construction of Irreducible Polynomials Over a Binary Field

The following results characterize the irreducible polynomials over a binary field of a fixed degree. The proof is well-known, see for example [18], [9] and [10].

Definition 2.1 : A polynomial $f(x) \in \mathbb{F}_2[x]$ is said to be irreducible over $\mathbb{F}_2$ if $f(x)$ has a positive degree and every factorization of $f(x)$ in $\mathbb{F}_2[x]$ must involve a constant polynomial.

Theorem 2.1 : For every $n \in \mathbb{N}$, the product of all monic irreducible polynomials over $\mathbb{F}_2$ whose degree divide n is equal to $x^{2^n} - x$.

Corllary 1 : The number of monic irreducible polynomials over $\mathbb{F}_2$ satisfies :

$\sum_{d/n} N(d,2) = 2^n$ for all $n \in \mathbb{N}^*$.

Definition 2.2 : The Moebius function μ is the function on $\mathbb{N}$ defined by :

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct prime;} \\ 0, & \text{if } n \text{ is divisible by square of a prime.} \end{cases}$$

Lemma 2.1 : For $n \in \mathbb{N}$, the Moebius function μ satisfies :

$$\sum_{d/n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \geq 2. \end{cases}$$

Theorem 2.2 : The number $N(n,2)$ of monic irreducible polynomials over $\mathbb{F}_2$ of degree

m is given by :

$$\begin{aligned} N(n,2) &= \frac{1}{n}\sum_{d/n}\mu(d)2^{\frac{n}{d}} \\ &= \frac{1}{n}\sum_{d/n}\mu(\frac{n}{d})2^{d}. \end{aligned}$$

Lemma 2.2 : Let $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial over $\mathbb{F}_2$ of degree n. The following conditions are equivalent :

1.) $f(x)$ divides $x^{2^n} - x$.

2.) m divides n.

Corollary 2 : Let $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial over $\mathbb{F}_2$ of degree n . Then the splitting field of $f(x)$ over $\mathbb{F}_2$ is given by $\mathbb{F}_{2^n}$.

Corollary 3 : Any two irreducible polynomials in $\mathbb{F}_2[x]$ of the same degree have isomorphic splitting fields.

Lemma 2.3 : Let $f(x) \in \mathbb{F}_2[x]$ be a polynomial of degree n. The following conditions are equivalent :

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

2.) $gcd(f(x), x^{2^k} + x) = 1$ for $k = 1 \cdots [\frac{n}{2}]$.

If $deg(f(x)) > 1$, then $f(x)$ is irreducible over $\mathbb{F}_2$ if and only if $gcd(f(x), x^{2^k-1} + x) = 1$ for $k = 1 \cdots [\frac{n}{2}]$.

Theorem 2.3 : Let $f(x) \in \mathbb{F}_2[x]$, and suppose $f(x) \neq 0$. Let t denotes the number of irreducible factors of $f(x)$ over $\mathbb{F}_2$, and let $F(x) \in \mathbb{Z}[x]$ be any monic polynomial such that $F(x) = f(x)$ modulo $\mathbb{F}_2[x]$. Then $t = deg(f)$ modulo 2 if only if $disc(f) = 1$ modulo 8.

While being based on these results, we deduce two fast programs. The first for computing the number of irreducible polynomials, $N(n, 2)$, of a fixed degree n over a binary field. As example, we compute $N(n, 2)$ for n least 100 ; the second for determining all irreducible polynomials over a binary field, and we construct all irreducible polynomials over $\mathbb{F}_2$ of degree at least 10 .

Remakr 1 : The two programs for determining all irreducible and primitive polynomials over a binary field depend solely on the space memory to store the number $2^n - 1$.

Programme for computing the number of irreducible polynomials over a binary field
$Num := proc(m)$ local k, n, d, g, N; $with(numtheory)$: $g := (n, d) \rightarrow$ if n mod $d = 0$ then $mobius(d)$ else 0 fi : $N := n \rightarrow (add(g(n, d) * 2^{n/d}, d = 1..n))/n$: for k to m do $print(k, N(k))$; od ; end;

n	$N(n,2)$	n	$N(n,2)$
1	2	51	44152937520670
2	1	52	86607683851185
3	2	53	169947155749830
4	3	54	333599969907456
5	6	55	655069036708398
6	9	56	1286742745883790
7	18	57	2528336632900554
8	30	58	4969489234738635
9	56	59	9770521225481754
10	99	60	19215358392200893
11	186	61	37800705069076950
12	335	62	74382032520643617
13	630	63	146402730743693304
14	1161	64	288230376084602880
15	2182	65	567592125344909154
16	4080	66	1117984489185516357
17	7710	67	2202596307308603178
18	14532	68	4340410370031955245
19	27594	69	8555011744328945842
20	52377	70	16865594581186450683
21	99858	71	33256101992039755026
22	190557	72	65588423372234846720
23	364722	73	129379903640264252430
24	698870	74	255263053126231647315
25	1342176	75	503719091506095041632
26	2580795	76	994182417442624283055
27	4971008	77	1962541914958813595274
28	9586395	78	3874762242347531676435
29	18512790	79	7651429238067273257634

30	35790267	80	15111572745169120787664
31	69273666	81	29850020237398249570304
32	134215680	82	58971991200686800921575
33	260300986	83	116522970565265462622282
34	505286415	84	230271584688448434290055
35	981706806	85	455125014443154512829018
36	1908866960	86	899665726224738035908989
37	3714566310	87	177864948173186820489 1030
38	7233615333	88	351687511160599405 1576550
39	14096302710	89	695471932182797907 2466990
40	27487764474	90	137548893253927232 16145164
41	53634713550	91	272074733908874785 69211430
42	104715342801	92	538234799689288122 91873035
43	204560302842	93	106489465744978948355328066
44	399822314775	94	210713198176233443201038641
45	781874934568	95	416990329022443882071278430
46	1529755125849	96	825293359523583917857003520
47	2994414645858	97	163357036111885232151637 0110
48	5864061663920	98	323380255160262027983900 3712
49	11488774559616	99	640227575872843132060365 3208
50	22517997465744	100	126765060022822827559679 53152

Programme for determining all irreducible polynomials over a binary field
$Pr := proc(n)$ local P, d, S, T, Div; $with(numtheory)$: $Div := divisors(2^n - 1)\ minus\ \{2^n - 1\}$: $S := convert(Factor(x^{2n} + x) \bmod 2, set)$: for $d \in Div$ do $convert(Factor(x^{2^d} + x) \bmod 2, set)$; od : $print(Div),\ print(S)$; end;

n	Irreducible polynomials of degree n over a binary field
1	$x, x + 1$
2	$x^2 + x + 1$
3	$x^3 + x^2 + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$

6	$x^6+x+1, x^6+x^3+1, x^6+x^5+1,$ $x^6+x^5+x^4+x^2+1, x^6+x^5+x^2+x+1, x^6+x^4+x^3+x+1,$ $x^6+x^5+x^3+x^2+1, x^6+x^5+x^4+x+1, x^6+x^4+x^2+x+1.$
7	$x^7+x^4+1, x^7+x+1, x^7+x^6+1, x^7+x^5+x^4+x^3+x^2+x+1,$ $x^7+x^6+x^5+x^4+x^3+x^2+1, x^7+x^6+x^3+x+1,$ $x^7+x^6+x^5+x^3+x^2+x+1, x^7+x^6+x^5+x^2+1, x^7+x^3+x^2+x+1,$ $x^7+x^4+x^3+x^2+1, x^7+x^6+x^5+x^4+1, x^7+x^5+x^3+x+1,$ $x^7+x^3+1, x^7+x^6+x^4+x^2+1, x^7+x^6+x^4+x+1, x^7+x^5+x^4+x^3+1,$ $x^7+x^6+x^5+x^4+x^2+x+1, x^7+x^5+x^2+x+1.$
8	$x^8+x^6+x^5+x^3+1, x^8+x^7+x^5+x+1, x^8+x^7+x^6+x^5+x^4+x^2+1,$ $x^8+x^6+x^4+x^3+x^2+x+1, x^8+x^7+x^6+x^5+x^4+x^3+1,$ $x^8+x^7+x^6+x^4+x^2+x+1, x^8+x^6+x^5+x+1,$ $x^8+x^7+x^6+x^4+x^3+x^2+1, x^8+x^4+x^3+x+1,$ $x^8+x^6+x^5+x^2+1, x^8+x^5+x^4+x^3+x^2+x+1, x^8+x^6+x^5+x^4+1,$ $x^8+x^6+x^5+x^4+x^3+x+1, x^8+x^7+x^3+x^2+1,$ $x^8+x^6+x^5+x^4+x^2+x+1, x^8+x^7+x^5+x^4+x^3+x^2+1,$ $x^8+x^5+x^3+x^2+1, x^8+x^7+x^5+x^3+1, x^8+x^7+x^6+x^3+x^2+x+1,$ $x^8+x^7+x^4+x^3+x^2+x+1, x^8+x^4+x^3+x^2+1,$ $x^8+x^5+x^3+x+1, x^8+x^7+x^6+x^5+x^2+x+1,$ $x^8+x^5+x^4+x^3+1, x^8+x^6+x^3+x^2+1,$ $x^8+x^7+x^2+x+1, x^8+x^7+x^6+x+1,$ $x^8+x^7+x^6+x^5+x^4+x+1, x^8+x^7+x^3+x+1, x^8+x^7+x^5+x^4+1$
9	$x^9+x^5+1, x^9+x+1, x^9+x^8+x^6+x^5+x^3+x+1,$ $x^9+x^8+1, x^9+x^8+x^7+x^6+x^4+x^2+1, x^9+x^7+x^5+x^4+x^3+x^2+1,$ $x^9+x^4+x^3+x+1, x^9+x^8+x^6+x^4+x^3+x+1,$ $x^9+x^7+x^6+x^5+x^4+x^3+1, x^9+x^8+x^6+x^3+1,$ $x^9+x^7+x^6+x^4+x^3+x+1, x^9+x^6+x^4+x^3+x^2+x+1,$ $x^9+x^8+x^4+x^2+1, x^9+x^7+x^6+x^3+x^2+x+1,$ $x^9+x^8+x^6+x^5+x^4+x^3+x^2+x+1, x^9+x^8+x^7+x^3+x^2+x+1,$ $x^9+x^8+x^7+x^6+x^4+x^3+1, x^9+x^4+1,$ $x^9+x^8+x^7+x^6+x^3+x+1, x^9+x^6+x^5+x^3+x^2+x+1,$ $x^9+x^6+x^4+x^3+1, x^9+x^7+x^5+x^4+x^2+x+1,$ $x^9+x^8+x^7+x^6+x^5+x^3+1,$ $x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+1, x^9+x^5+x^4+x+1,$ $x^9+x^7+x^5+x^2+1, x^9+x^7+x^5+x+1,$ $x^9+x^8+x^7+x^2+1, x^9+x^5+x^3+x^2+1, x^9+x^4+x^2+x+1,$ $x^9+x^6+x^5+x^2+1, x^9+x^8+x^7+x^5+1, x^9+x^8+x^7+x^6+x^2+x+1,$ $x^9+x^8+x^5+x+1, x^9+x^7+x^2+x+1, x^9+x^7+x^4+x^2+1,$ $x^9+x^7+x^6+x^4+1, x^9+x^8+x^6+x^5+x^3+x^2+1,$ $x^9+x^8+x^5+x^4+1, x^9+x^8+x^6+x^5+1, x^9+x^8+x^7+x^5+x^4+x^3+1,$ $x^9+x^7+x^4+x^3+1, x^9+x^8+x^4+x+1, x^9+x^6+x^3+x+1,$ $x^9+x^6+x^5+x^3+1, x^9+x^6+x^5+x^4+x^3+x^2+1,$ $x^9+x^8+x^6+x^5+x^4+x+1, x^9+x^7+x^5+x^3+x^2+x+1,$

	$x^9+x^8+x^6+x^3+x^2+x+1, x^9+x^8+x^4+x^3+x^2+x+1,$ $x^9+x^8+x^7+x^5+x^4+x^2+1, x^9+x^8+x^5+x^4+x^3+x+1,$ $x^9+x^8+x^7+x^6+x^3+x^2+1, x^9+x^7+x^6+x^5+x^4+x^2+1,$ $x^9x^6+x^5+x^4+x^2+x+1, x^9+x^8+x^7+x^6+x^5+x+1$
10	$x^{10}+x^7+1, x^{10}+x^6+x^5+x^2+1, x^{10}+x^7+x^6+x^3+1,$ $x^{10}+x^9+x^8+x^3+x^2+x+1, x^{10}+x^8+x^5+x^4+1,$ $x^{10}+x^3+1, x^{10}+x^7+x^6+x^5+x^4+x^3+x^2+x+1,$ $x^{10}+x^9+x^7+x^6+x^5+x^4+x^2+x+1,$ $x^{10}+x^8+x^3+x+1, x^{10}+x^9+x^7+x^6+x^4+x+1,$ $x^{10}+x^9+x^6+x+1, x^{10}+x^8+x^7+x^5+x^3+x+1,$ $x^{10}+x^9+x^8+x^5+x^4+x^3+1, x^{10}+x^9+x^8+x^6+x^3+x^2+1,$ $x^{10}+x^8+x^7+x^2+1, x^{10}+x^9+x^5+x^2+1,$ $x^{10}+x^9+x^8+x^5+x^3+x+1, x^{10}+x^7+x^5+x^3+x^2+x+1,$ $x^{10}+x^6+x^5+x+1, x^{10}+x^4+x^3+x+1,$ $x^{10}+x^9+x^8+x^7+x^3+x^2+1, x^{10}+x^8+x^7+x^5+x^4+x^3+1,$ $x^{10}+x^9+x^7+x^3+1, x^{10}+x^7+x^6+x^4+x^2+x+1,$ $x^{10}+x^9+x^6+x^4+1, x^{10}+x^5+x^3+x^2+1,$ $x^{10}+x^9+x^7+x^5+x^3+x^2+1, x^{10}+x^7+x^5+x^3+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x+1,$ $x^{10}+x^9+x^7+x^5+x^2+x+1, x^{10}+x^9+x^8+x^4+x^2+x+1,$ $x^{10}+x^8+x^7+x^6+1, x^{10}+x^8+x^3+x^2+1,$ $x^{10}+x^9+x^8+x^5+x^4+x^2+1, x^{10}+x^9+x^7+x^6+1,$ $x^{10}+x^7+x^6+x^5+x^4+x+1, x^{10}+x^6+x^4+x+1,$ $x^{10}+x^6+x^5+x^3+x^2+x+1,$ $x^{10}+x^8+x^4+x^3+1, x^{10}+x^9+x^8+x^7+x^4+x+1,$ $x^{10}+x^9+x^8+x^4+1, x^{10}+x^7+x^6+x^5+x^3+x^2+1,$ $x^{10}+x^9+x^8+x^6+x^4+x^3+1, x^{10}+x^8+x^5+x^4+x^3+x^2+1,$ $x^{10}+x^9+x^5+x^4+1, x^{10}+x^8+x^7+x^6+x^5+x^2+1,$ $x^{10}+x^7+x^4+x^3+1, x^{10}+x^9+x^7+x^5+x^4+x^2+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1,$ $x^{10}+x^8+x^6+x^5+x^3+x+1, x^{10}+x^8+x^5+x+1,$ $x^{10}+x^8+x^7+x^3+x^2+x+1, x^{10}+x^4+x^3+x^2+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x+1, x^{10}+x^7+x^6+x^2+1,$ $x^{10}+x^5+x^2+x+1, x^{10}+x^8+x^4+x^3+x^2+x+1,$ $x^{10}+x^9+x^8+x^4+x^3+x^2+1, x^{10}+x^9+x^8+x^7+x^2+x+1,$ $x^{10}+x^9+x^8+x^5+1, x^{10}+x^9+x^8+x^6+x^5+x+1,$ $x^{10}+x^9+x^6+x^3+x^2+x+1, x^{10}+x^9+x^8+x^6+x^2+x+1,$ $x^{10}+x^6+x^2+x+1, x^{10}+x^9+x^8+x^7+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^2+1, x^{10}+x^3+x^2+x+1,$ $x^{10}+x^9+x^4+x^2+1, x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x^2+1,$ $x^{10}+x^5+x^4+x^2+1, x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1,$

	$x^{10}+x^8+x^7+x^6+x^2+x+1, x^{10}+x^9+x^7+x^6+x^4+x^3+x^2+x+1,$
	$x^{10}+x^8+x^7+x^4+x^3+x+1, x^{10}+x^8+x^6+x^5+x^2+x+1,$
	$x^{10}+x^7+x^6+x^5+x^2+x+1, x^{10}+x^9+x^5+x+1,$
	$x^{10}+x^8+x^7+x^6+x^5+x^4+x^2+x+1,$
	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^3+x+1,$
	$x^{10}+x^8+x^7+x^4+x^2+x+1, x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x+1,$
	$x^{10}+x^8+x^7+x^6+x^5+x^4+x^3+x+1,$
	$x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2+1, x^{10}+x^9+x^8+x^6+x^4+x^2+1,$
	$x^{10}+x^8+x^6+x^5+1, x^{10}+x^9+x^6+x^5+x^4+x^3+1,$
	$x^{10}+x^9+x^7+x^5+x^4+x^3+x^2+x+1,$
	$x^{10}+x^8+x^6+x+1, x^{10}+x^7+x^3+x+1,$
	$x^{10}+x^9+x^6+x^5+x^4+x^3+x^2+x+1,$
	$x^{10}+x^9+x^6+x^4+x^3+x+1, x^{10}+x^9+x^8+x^7+x^5+x^4+1,$
	$x^{10}+x^9+x^7+x^2+1, x^{10}+x^9+x^8+x^7+x^5+x^3+1,$
	$x^{10}+x^9+x^5+x^4+x^2+x+1, x^{10}+x^9+x^7+x^6+x^3+x^2+1,$
	$x^{10}+x^8+x^7+x^5+1, x^{10}+x^8+x^6+x^4+x^2+x+1, x^{10}+x^9+x^4+x+1.$

3. Construction of Primitive Polynomials Over a Binary Field

The following results characterize the primitive polynomials over a binary field of a fixed degree, and the proof of these results is well known, see for example [5], [7], [8], [9] and [12]. If n is a Mersenne exponent then the factorization of 2^n-1 is trivial and an irreducible polynomial over a binary field of degree n is necessarily primitive.

Lemma 3.1 : Let $f(x)\in\mathbb{F}_2[x]$ be a polynomial of degree $n\geq 1$ with $f(0)\neq 0$. Then there exists a positive integer $e\leq 2^n-1$ such that $f(x)$ divides x^e-1.

Definition 3.1 : Let $f(x)\in\mathbb{F}_2[x]$ be a nonzero polynomial. If $f(0)\neq 0$, then the least positive integer e for which $f(x)$ divides x^e-1 is called the order of f and denoted by $ord(f)=ord(f(x))$.

Theorem 3.2 : Let $f(x)\in\mathbb{F}_2[x]$ be an irreducible polynomial over $\mathbb{F}_2$ of degree n and with $f(0)\neq 0$. Then $ord(f)$ is equal to order of any root of f in the multiplicative group $\mathbb{F}_{2^n}^*$.

Corllary 4 : If $f(x)\in\mathbb{F}_2[x]$ is an irreducible polynomial over $\mathbb{F}_2$ of degree n, then $ord(f)$ divides 2^n-1.

Theorem 3.3 :

$$N(n,e,2)=\begin{cases}\frac{\varphi(e)}{n}, & \text{if } e\geq 2 \text{ and } n=O(2) \bmod e;\\ 2, & \text{if } n=e=2;\\ 0, & \text{otherwise.}\end{cases}$$

In particular, the degree of an irreducible polynomial in $\mathbb{F}_2[x]$ of order e must be equal to the multiplicative order of 2 modulo e. Therefore $N(n, e, 2) = \frac{\varphi(e)}{n}$ for all $n \geq 2$ the degree of an irreducible polynomial in $\mathbb{F}_2[x]$ of order e.

Lemma 3.2 : Let m be a positive integer. Then the polynomial $f(x) \in \mathbb{F}_2[x]$ with $f(0) \neq 0$ divides $x^m - 1$ if and only if $ord(f)$ divides m.

Definition 3.2 : A polynomial $f(x) \in \mathbb{F}_2[x]$ of degree m is a primitive polynomial over $\mathbb{F}_2$ if it is a minimal polynomial over $\mathbb{F}_2$ of a primitive element of $\mathbb{F}_{2^m}$.

Theorem 3.4 : A polynomial $f(x) \in \mathbb{F}_2[x]$ of degree m is a primitive polynomial over $\mathbb{F}_2$ if and only if f is monic, $f(0) \neq 0$ and $ord(f) = 2^m - 1$.

Theorem 3.3 : The monic polynomial $f(x) \in \mathbb{F}_2[x]$ of degree m is a primitive polynomial over $\mathbb{F}_2$ if and only if $(-1)^m f(0)$ is a primitive element of $\mathbb{F}_{2^m}$ and the least positive integer r for which x^r is congruent modulo $f(x)$ to some element of $\mathbb{F}_{2^m}$ is $r = 2^m - 1$.

Proposition 3.1 : 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 $k = 2^m - 1$ and for non small positive integers k.

While being based on these results, we deduce two fast programs. The first for computing the number of primitive polynomials, $N(n, 2^n - 1, 2)$, of a fixed degree n over a binary field. As example, we compute $N(n, 2^n - 1, 2)$ for n at least 100; the second for determining all primitive polynomials over a binary field, and we construct all primitive polynomials of degree at least than 10.

$Programme for computing the number of primitive polynomials over a binary field$
$Num := proc(n)$ local d; for d from 2 to n do $print(d, \frac{\varphi(2^d-1)}{d})$; od; end;

n	$N(n, 2^n - 1, 2)$	n	$N(n, 2^n - 1, 2)$
1	1	51	37456800827040
2	1	52	44980696051200
3	2	53	169917983040000
4	2	54	178118842613760
5	6	55	598690870272000
6	6	56	598975092817920
7	18	57	2167072830474048
8	16	58	3238370502193152
9	48	59	9770466930024800
10	60	60	6774451200000000
11	176	61	37800705069076950
12	144	62	49588021611155412
13	630	63	122428597145960448
14	756	64	143890337947975680
15	1800	65	549215642649655800
16	2048	66	594287364124624896
17	7710	67	2202596295934991760
18	7776	68	2295419955465369600
19	27594	69	7176808547444088960
20	24000	70	9416895732518400000
21	84672	71	33255955596453429120
22	120032	72	23312749520045998080
23	356960	73	129085132425950929920
24	276480	74	169316907563870779392
25	1296000	75	414139557888000000000
26	1719900	76	526755007970989572096
27	4202496	77	1841506581813189850944
28	4741632	78	2185037258519160864000
29	18407808	79	7648581626983221210888
30	17820000	80	6485183461903564800000
31	69273666	81	25225059102561477328896
32	67108864	82	38838084210665112870144
33	211016256	83	115825228226551298175440
34	336849900	84	89757882837568623476736
35	929275200	85	440440202020999664971800
36	725594112	86	598323702929870048962320
37	3697909056	87	151554834814870332621619 2
38	4822382628	88	165746730642030740688076 8
39	11928047040	89	695471932182797907246699 0
40	11842560000	90	638862301937059200000000 0

41	53630700752	91	269603188769955871853568 00
42	57802864896	92	279480648896077763454566 40
43	204064589160	93	912766848817636512772878 96
44	200778006528	94	139888531269039658954752000
45	634404960000	95	401425491677151869644500000
46	998132265920	96	319640106112747034042695680
47	2992477516800	97	163342765382776130620043425 6
48	2283043553280	98	208915132797086183239326105 6
49	11398311767808	99	509323008776497134976961740 8
50	13122000000000	100	570767634000000000000000000 0

Programme for building all primitive polynomials of a binary field
$Pr := proc(n)$ local d, S, R, Q, Div; $with(numtheory)$: $Div := divisors(2^n - 1)$ minus $\{1, 2^n - 1\}$; $S := convert(Factor()$ mod $2, set)$; $Q := \{\}$; for $d \in Div$ do $Q := \{op(Q), op(convert(Factor(x^d + 1)$ mod $2, set))$; od; $R :=$ S minus Q; if $isprime(2^n - 1)$ then $print(S$ minus $\{x + 1\}, (phi(2^n - 1))/n)$; else $print(R, (phi(2^n - 1))/n); fi$; end;

n	Primitive polynomials of degree n
3	$x^3 + x^2 + 1, x^3 + x + 1$
4	$x^4 + x^3 + 1, x^4 + x + 1$
5	$x^5 + x^2 + 1, x^5 + x^3 + 1, x^5 + x^4 + x^3 + x + 1,$ $x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x^2 + 1$
6	$x^6 + x^5 + 1, x^6 + x + 1, x^6 + x^5 + x^2 + x + 1, x^6 + x^5 + x^4 + x + 1,$ $x^6 + x^4 + x^3 + x + 1, x^6 + x^5 + x^3 + x^2 + 1$
7	$x^7 + x^6 + x^4 + x^2 + 1, x^7 + x^6 + 1, x^7 + x + 1,$ $x^7 + x^3 + 1, x^7 + x^4 + 1, x^7 + x^3 + x^2 + x + 1,$ $x^7 + x^6 + x^5 + x^4 + x^2 + x + 1, x^7 + x^5 + x^2 + x + 1,$ $x^7 + x^6 + x^5 + x^4 + 1, x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1,$ $x^7 + x^4 + x^3 + x^2 + 1, x^7 + x^5 + x^4 + x^3 + x^2 + x + 1,$ $x^7 + x^6 + x^5 + x^2 + 1, x^7 + x^5 + x^4 + x^3 + 1, x^7 + x^5 + x^3 + x + 1,$ $x^7 + x^6 + x^5 + x^3 + x^2 + x + 1, x^7 + x^6 + x^3 + x + 1, x^7 + x^6 + x^4 + x + 1$

8	$x^8+x^5+x^3+x+1, x^8+x^6+x^5+x^2+1,$ $x^8+x^7+x^6+x^5+x^4+x^2+1, x^8+x^6+x^5+x+1,$ $x^8+x^5+x^3+x^2+1, x^8+x^7+x^6+x+1,$ $x^8+x^6+x^4+x^3+x^2+x+1, x^8+x^6+x^3+x^2+1,$ $x^8+x^4+x^3+x^2+1, x^8+x^6+x^5+x^3+1,$ $x^8+x^7+x^6+x^5+x^2+x+1, x^8+x^6+x^5+x^4+1,$ $x^8+x^7+x^5+x^3+1, x^8+x^7+x^3+x^2+1,$ $x^8+x^7+x^2+x+1, x^8+x^7+x^6+x^3+x^2+x+1$
9	$x^9+x^5+1, x^9+x^4+1, x^9+x^8+x^6+x^5+1,$ $x^9+x^8+x^6+x^5+x^3+x+1, x^9+x^4+x^3+x+1,$ $x^9+x^8+x^4+x^3+x^2+x+1, x^9+x^7+x^2+x+1,$ $x^9+x^7+x^5+x^3+x^2+x+1, x^9+x^6+x^5+x^3+1,$ $x^9+x^8+x^5+x^4+1, x^9+x^8+x^7+x^3+x^2+x+1,$ $x^9+x^8+x^7+x^6+x^3+x+1, x^9+x^8+x^6+x^5+x^4+x+1,$ $x^9+x^7+x^6+x^3+x^2+x+1, x^9+x^8+x^6+x^5+x^3+x^2+1,$ $x^9+x^6+x^5+x^4+x^2+x+1, x^9+x^6+x^4+x^3+x^2+x+1,$ $x^9+x^8+x^6+x^5+x^4+x^3+x^2+x+1,$ $x^9+x^8+x^7+x^6+x^4+x^2+1, x^9+x^7+x^6+x^4+1,$ $x^9+x^7+x^5+x^2+1, x^9+x^7+x^4+x^2+1,$ $x^9+x^8+x^7+x^6+x^3+x^2+1, x^9+x^6+x^5+x^3+x^2+x+1,$ $x^9+x^8+x^7+x^5+x^4+x^2+1, x^9+x^5+x^4+x+1,$ $x^9+x^8+x^5+x+1, x^9+x^8+x^7+x^6+x^4+x^3+1,$ $x^9+x^8+x^4+x^2+1, x^9+x^8+x^4+x+1, x^9+x^8+x^7+x^6+x^2+x+1,$ $x^9+x^6+x^4+x^3+1, x^9+x^5+x^3+x^2+1,$ $x^9+x^6+x^5+x^4+x^3+x^2+1, x^9+x^8+x^7+x^6+x^5+x+1,$ $x^9+x^7+x^5+x+1, x^9+x^8+x^7+x^6+x^5+x^3+1, x^9+x^8+x^7+x^2+1,$ $x^9+x^7+x^5+x^4+x^3+x^2+1, x^9+x^8+x^6+x^4+x^3+x+1,$ $x^9+x^7+x^6+x^5+x^4+x^3+1, x^9+x^8+x^7+x^5+x^4+x^3+1,$ $x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+1,$ $x^9+x^7+x^5+x^4+x^2+x+1, x^9+x^7+x^6+x^5+x^4+x^2+1,$ $x^9+x^7+x^6+x^4+x^3+x+1, x^9+x^8+x^5+x^4+x^3+x+1,$ $x^9+x^8+x^6+x^3+x^2+x+1$
10	$x^{10}+x^9+x^8+x^6+x^2+x+1, x^{10}+x^9+x^8+x^7+x^3+x^2+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x+1,$ $x^{10}+x^8+x^5+x^4+x^3+x^2+1, x^{10}+x^6+x^5+x^3+x^2+x+1,$ $x^{10}+x^8+x^7+x^6+x^5+x^4+x^3+x+1,$ $x^{10}+x^9+x^8+x^5+x^4+x^3+1, x^{10}+x^3+1,$ $x^{10}+x^9+x^6+x^5+x^4+x^3+1, x^{10}+x^7+1,$ $x^{10}+x^9+x^8+x^7+x^5+x^4+1, x^{10}+x^7+x^6+x^5+x^4+x+1,$ $x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x^2+1,$ $x^{10}+x^8+x^7+x^6+x^5+x^4+x^2+x+1,$ $x^{10}+x^9+x^8+x^6+x^3+x^2+1, x^{10}+x^9+x^8+x^4+x^2+x+1,$ $x^{10}+x^9+x^5+x^4+x^2+x+1, x^{10}+x^8+x^7+x^3+x^2+x+1,$

$x^{10}+x^9+x^6+x^3+x^2+x+1, x^{10}+x^8+x^7+x^6+x^2+x+1,$
$x^{10}+x^9+x^7+x^5+x^4+x^2+1, x^{10}+x^7+x^6+x^4+x^2+x+1,$
$x^{10}+x^9+x^7+x^6+x^4+x^3+x^2+x+1,$
$x^{10}+x^8+x^6+x^4+x^2+x+1, x^{10}+x^9+x^6+x^5+x^4+x^3+x^2+x+1,$
$x^{10}+x^7+x^6+x^5+x^4+x^3+x^2+x+1,$
$x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2+1,$
$x^{10}+x^8+x^6+x^5+x^3+x+1, x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x+1,$
$x^{10}+x^9+x^7+x^6+1, x^{10}+x^8+x^5+x+1,$
$x^{10}+x^9+x^8+x^7+x^4+x+1, x^{10}+x^8+x^6+x+1,$
$x^{10}+x^8+x^7+x^2+1, x^{10}+x^7+x^6+x^2+1, x^{10}+x^9+x^6+x+1,$
$x^{10}+x^9+x^6+x^4+x^3+x+1, x^{10}+x^9+x^8+x^6+x^5+x+1,$
$x^{10}+x^7+x^6+x^5+x^2+x+1, x^{10}+x^9+x^7+x^3+1, x^{10}+x^9+x^5+x^2+1,$
$x^{10}+x^8+x^7+x^6+x^5+x^2+1, x^{10}+x^7+x^3+x+1,$
$x^{10}+x^8+x^3+x^2+1, x^{10}+x^4+x^3+x+1,$
$x^{10}+x^9+x^4+x^2+1, x^{10}+x^9+x^8+x^5+1,$
$x^{10}+x^9+x^4+x+1, x^{10}+x^8+x^4+x^3+1,$
$x^{10}+x^5+x^2+x+1, x^{10}+x^5+x^3+x^2+1,$
$x^{10}+x^8+x^7+x^5+1, x^{10}+x^8+x^7+x^4+x^2+x+1,$
$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1, x^{10}+x^8+x^5+x^4+1,$
$x^{10}+x^6+x^5+x^2+1, x^{10}+x^9+x^7+x^6+x^4+x+1,$
$x^{10}+x^9+x^8+x^6+x^4+x^2+1, x^{10}+x^9+x^8+x^4+x^3+x^2+1,$
$x^{10}+x^9+x^8+x^6+x^4+x^3+1$

References

[1] Kenneth H., Rosen, Applied cryptography, The CRC Press Series on discrete mathematics and its applications, (1996).

[2] Wielandt H., Finite Permutation Groups, Academic Press, (1964).

[3] Ivan Leung, A microcoded elliptic cuve cryptographic processor. Phd thesis, Departement of Computer Science and Enginneering, Chinese Universty of Hong Kong, (2001).

[4] Joan Daemen and Vincent Rijmen, AES proposal : Rijndael. http : //csrc.gov/encryption/aes/Rijndaelammended.pdf.

[5] Hernga J. W., Blte H. W. J. and Compagner A., New primitive trinomials of Mersenne exponent degrees for random-number generation, International J. of Modern Physics, C3 (1992), 561-564.

[6] Arjen Lenstra K., Citibank N. A., Computional methods in public key cryptology, 1 North gate road, Mendham, NJ 0794-3104, U.S.A. arjen.lenstra@citigroup .com.

[7] Zieler N., Primitive trinomials whose degree is a Mersenne exponent, Inform. and Control, 15 (1969), 67-69.

[8] Lidl R., Niederreiter H., Finite fields, Encyclopedia of math, and its Appl, 20, Addison- Wesley Publ. Co, Reading, Mass, (1983), Reprint, Cambridge Univ, Press, Cambridge, (1967).

[9] Lidl R., Niederreiter H., Introduction to Finite Fields and Their Applications, Cambridge Univ, Press, Cambridge, Second Edition, (1994).

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

[11] Golomb S. W., Shift Register Ssequences, Holden-Day, San Francisco, (1967).

[12] Kumada T., Leeb H., Kurita Y. and Matsumoto M., New primitive t-nomials $(t = 3, 5)$ over $GF(2)$ whose degree is a Mersenne exponent, Math. Comp., 69 (2000), 811-814.

[13] Kurita Y. and Matsumoto M., New primitive t-nomials $(t = 3, 5)$ over $GF(2)$ whose degree is a Mersenne exponent 44497, Math. Comp. 56 (1991), 817-821.

[14] Peterson W. W. and Weldon E. J. Jr, Error Correcting Codes. MIT Press, Second Edition, (1972).