World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

PRIMITIVE ELEMENTS OF FINITE FIELDS $\mathbb{F}_p$ WHERE $p = 1 + 2^n$ IS A PRIME NUMBER

Ahmed Asimi*

Departement of Mathematics, Faculty of Sciences, University Ibnou Zohr, B.P. 8106 Agadir, Morroco.

Article Received on 26/06/2020 **Article Revised on 16/07/2020** **Article Accepted on 06/08/2020**

***Corresponding Author**
Ahmed Asimi
Departement of Mathematics, Faculty of Sciences University Ibnou Zohr, B.P. 8106 Agadir, Morroco.

ABSTRACT

In this digital age, modern cryptographic techniques have many uses, such as to digitally sign documents, access control, implement electronic money, elliptic curves, IT security and network security for example design and validation of authentication and trust architectures. Because of these important uses it is necessary that users be able to estimate the efficiency and security of cryptographic techniques. It is ot sufficient for them to know only how the techniques work. One of the most useful of these structures is that of finite fields which are perfectly connected to these primitive elements. Indeed, every finite field is commutative and admits a primitive element. In this paper, we effectively determinate the primitive elements of finite fields $\mathbb{F}_p$ where $p = 1 + 2^n$ is a prime number. We show that 1) if p is a prime number then p is a Fermat prime number; 2) g is a primitive element of $\mathbb{F}_p$ if and only if g is not a quadratic residue modulo p; 3) the elements 3^{2n+1} modulo p for all $n \in \mathbb{N}$ are the primitive elements of $\mathbb{F}_p$ with $p > 3$; and 4) 2 is a primitive element of $\mathbb{F}_p$ if and only if $n = 1$ (ie $p = 3$).

KEYWORDS: Modern cryptographic techniques, elliptic curves, finite fields, primitive elements.

I. INTRODUCTION, NOTATIONS AND BACKGROUNDS

We start this section by introduce the notations and terminologies that will be used throughout this paper.

$\mathbb{F}_p$: The finite field of order a prime number p.

$\mathbb{F}_p^*$: The cyclic multiplicative group of all nonzero elements in $\mathbb{F}_p$ of order p-1.

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

G_p : The set of all primitive elements of $\mathbb{F}_p$.

S_p : The set of all quadratic residues mod p.

$\varphi()$: The Euler's function and $\varphi(m)$ indicates the number of integers k with $1 < k < m$ and gcd(k; m) = 1.

$\left(\frac{a}{p}\right)$: Legendre symbol where p is an odd prime number and $a \in \mathbb{Z}$.

$|A|$: The number of elements of a finite set A.

$A \setminus B$: $\{x \in A; x \notin B\}$.

$\langle a \rangle$: $\{a^k; k \in \mathbb{Z}\}$ The multiplicative group generated by a.

$\theta(a)$: The order of a.

mod : modulo.

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 $\langle a \rangle = \{1, \dots, a^{m-1}\}$ with $a^m = 1$. Then its order is called the order of a. Otherwise, a is called an element of infinite order.

The theory of finite fields is a branch of modern algebra and the finite fields are one of the most beautiful algebraic structures. They are the basis of many algorithmic applications, notably in cryptography, IT security, combinatorics, coding theory and correcting codes.[17] Today cryptology (cryptography and cryptanalysis), computer science and IT security are linked. We can say that the development of computers is at the origin of a new face of cryptology. This has led researchers in a natural way to consider methods based on some specified function fields in order to construct cryptographic schemes, such as schemes for unconditionally secure authentication, traitor tracing, secret sharing, broadcast encryption and secure multicast.[18]

Currently, most of the designers in modern cryptography are based on number theory to develop and approve computer security management protocols, in particular, the key exchange protocols of Diffie Hellman, the encryption protocols of ElGamal and the DSA signature protocol[19] and[20]; and cryptographic hash functions. However, the links between these two areas are deeper. The development of modern cryptography has taken place in parallel with developments and central questions in number theory. Indeed, these protocols are based on the knowledge of the primitive elements of $\mathbb{F}_p$ and their security levels relate to the study of the problem of the discrete logarithm in the multiplicative group of invertible elements of a finite fields and the problem of Cryptosystems using the discrete logarithm[3] and.[4] Hence the interest of a deep study of their structures, namely, the effective determination of their primitive elements, which is our objective in this paper in the case where $p = 1 + 2^n$ is a prime number.

In this paper we determinate the primitive elements of finite fields $\mathbb{F}_p$ where $p = 1 + 2^n$ is a prime number. We show that:

1) If p is a prime number, then p is a Fermat prime number.
2) g is a primitive element of $\mathbb{F}_p$ if and only if g is not a quadratic residue modulo p;
3) The elements 3^{2n+1} mod p for all $n \in \mathbb{N}$ are the primitive elements of $\mathbb{F}_p$ with $p > 3$;
4) 2 is a primitive element of $\mathbb{F}_p$ if and only if $n = 1$ (ie $p = 3$).

We refer to [1], [2], [9], [12], [13], [14], [16], and we deduce the following results.

Theorem 1.1. Every finite field is commutative and admits a primitive element.

Definition 1.1. For a nonnegative integer k, the k^{th} Fermat number F_k is defined by $F_k = 2^{2^k} + 1$.

Theorem 1.2. Let $(G; .)$ be a finite group and $g \in G$. Then for all $k \in \mathbb{N}^*$,

$$\theta(g^k) = \frac{\theta(g)}{gcd(\theta(g), k)}$$

Theorem 1.3. Let K be a finite field with q elements. Then for any divisor d of $q - 1$ there are exactly $\varphi(d)$ elements of order d in the unit group K^* .

Corollary 1. If K is a finite field with q elements, then its unit group K^* is cyclic of order $q - 1$. It has exactly $\varphi(q - 1)$ generators.

Lemma 1.1.

$$\varphi(n) = \begin{cases} (p-1)p^{m-1} & \text{If } n = p^m \text{ where } p \text{ is a prime number} \\ \phi(s)\phi(t) & \text{If } n = st \text{ where } \gcd(s, t) = 1. \end{cases}$$

Corollary 2. Let $g \in \mathbb{F}_\mathrm{p}$ and $n \in \mathbb{N}$. n is the order of g if and only if $g^n = 1 \bmod p$ and $g^{\frac{n}{p}} \neq 1 \bmod p$ for each prime divisor p of n.

Definition 1.2. Let $g \in \mathbb{F}_\mathrm{p}$. g is a primitive element of $\mathbb{F}_p$ if the order of g in the units' group $\mathbb{F}_p$ is $p-1$.

Lemma 1.2. The number of all primitive elements of $\mathbb{F}_p$ is $\varphi(q-1)$: $|G_p| = \varphi(p-1)$.

Proposition 1.1. The number of squares in $\mathbb{F}_p$ is $\frac{p-1}{2}$ for all odd prime number p: $|S_p| = \frac{p-1}{2}$.

Theorem 1.4. If a and n are relatively prime, then $a^{\varphi(n)} = 1 \bmod n$.

Definition 1.3. In modular arithmetic, we say that a natural integer q is a quadratic residue modulo p if there exists an integer x such that: $x^2 = q \bmod p$. In the opposite case, we say that q is a quadratic nonresidue modulo p.

In other words, a quadratic residue modulo p is a number which has a square root in modular arithmetic of modulo p.

Definition 1.4. Let p be a prime number and $a \in \mathbb{Z}$. The Legendre symbol $\left(\frac{a}{p}\right)$ defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{If } a \text{ is a quadratic residue modulo } p \\ -1 & \text{If } a \text{ is not a quadratic residue mod } p \\ 0 & \text{If } p \text{ divides } a \end{cases}$$

Theorem 1.5. Let p be a prime number and $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \text{ in } \mathbb{F}_p.$$

Theorem 1.6. Let p and q be two odd prime numbers.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Theorem 1.7. Let n be an odd integer.

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{If n } = 3 \bmod 4 \\ -1 & \text{If n } = 1 \bmod 4 \end{cases}$$

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{If n } = \pm 1 \bmod 8 \\ -1 & \text{If n } = \pm 3 \bmod 8 \end{cases}$$

Corollary 3. Let p and q be two odd different prime numbers.

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{If } p = p = 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{Otherwise} \end{cases}$$

Corollary 4. Let p and a be two numbers relatively primes.

$$\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right).$$

II. Primitive elements of finite fields $\mathbb{F}_p$ where $p = 1 + 2^n$ is a prime number

Lemma 2.1. The order of all elements of $\mathbb{F}_p^*$ is of the form 2^k where $k \in \{1, \dots, n\}$.

Corollary 5. For all $x \in \mathbb{F}_p$ we have $\theta(x) = \theta(-x) = \theta(p - x)$.

Proof. We have $p - x = x$ in $\mathbb{F}_p$ and from lemma 2.1, we deduce that there exists $k \in \{1, \dots, n\}$ such that $\theta(x) = 2^k$. So, we get $(-x)^{2^k} = x^{2^k} = 1$

Theorem 2.1. Let $p = 1 + 2^n$ be a prime number. We then get $G_p = \mathbb{F}_p^* \backslash S_p$.

Proof. We have $G_p \subseteq \mathbb{F}_p \backslash S_p$ and $|G_p| = 2^{n-1}$. Hence to prove this theorem it suffices to see that$|\mathbb{F}_p^* \backslash S_p| = 2^{n-1}$. Indeed $|\mathbb{F}_p^* \backslash S_p| = |\mathbb{F}_p^*| - |S_p| = 2^n - 2^{n-1} = 2^{n-1}$, so we deduce this theorem.

Corollary 6. Let $p = 1 + 2^n$ be a prime number and $g \in \mathbb{F}_p$. Then g is a primitive element of $\mathbb{F}_p$ if and only if $\left(\frac{g}{p}\right) = g^{2^{n-1}} = -1 \bmod p$.

Proof. $\Longrightarrow$) Since g is a prime element of $\mathbb{F}_p$, then $\theta(g) = 2^n$. Therefore, in $\mathbb{F}_p$, $g^{2^n} = 1$ and $g^{2^s} \neq 1$ for all $s \in \{1, \dots, n-1\}$. And since $1 = g^{2^n} = \left(g^{2^{n-1}}\right)^2$ mod p, implies $\left(\frac{g}{p}\right) = g^{2^{n-1}} = -1 \bmod p$.

$\Longleftarrow$) We assume that $\theta(g) = 2^s$ together with $s \in \{1, \dots, n-1\}$, then $g^{2^n} = 1$ mod p. So, we get $g^{2^{n-1}} = \left(g^{2^s}\right)^{2^{n-1-s}} = 1 \neq -1$ mod p. Which is absurd.

Corollary 7. Let $x \in \mathbb{F}_p^*$. The elements x^2 and $p - x^2$ will never be primitive elements of $\mathbb{F}_p^*$.

Proof. Let $x \in \mathbb{F}_p^*$. Since $(x^2)^{2^{n-1}} = x^{2^n} = 1 \neq -1$, then x^2 is not a primitive element of $\mathbb{F}_p^*$ (Theorem 1.5). And by (Corollary 6), we deduce $p - x^2$ is also not a primitive element of $\mathbb{F}_p^*$.

Lemma 2.2. Let $k \in \mathbb{F}_p^*$ such that k is not a perfect square in $\mathbb{F}_p$. Then k is a primitive element of $\mathbb{F}_p$ if and only if m^2k is a primitive element of $\mathbb{F}_p$ for all $\mathbb{F}_p^*$.

Proof. Let $k \in \mathbb{F}_p^*$. k is a primitive element of $\mathbb{F}_p^*$ is equivalent to $k^{2^{n-1}} = -1 \mod p$ (Lemma 2.1). Hence to prove this lemma it suffices to see that:
$(m^2k)^{2^{n-1}} = m^{2^n}\ k^{2^{n-1}} = \ k^{2^{n-1}} = -1 \bmod p$.

Lemma 2.3. If $p = 1 + 2^n$ is a prime number with $n \geq 3$, then $n \ = \ 0$ mod 4.

Proof. Since $n \geq 3$, then p is prime with 3 and 5.

Suppose that n is an odd number, then $n = 2m + 1$ and
$p = 1 + 2^n = 1 + 2^{2m+1} = 1 + \ 2.4^m = \ 0$ mod 3. Therefore 3 divides $p = 1 + 2^n$, which contradicts p and 3 are coprime.

Assume that $n \ = \ 2$ mod 4, then $n = 4m + 2$ and
$p = 1 + 2^n = 1 + 2^{4m+2} = 1 + \ 2.16^m = \ 0$ mod 5. Therefore 5 divides $p = 1 + 2^n$, which contradicts p and 5 are coprime.

Theorem 2.2. If $p = 1 + 2^n$ is a prime number, then there exists $s \in \mathbb{N}$ such that $n = 2^s$.

Proof. Assume that $n = \ 2^s(2m + 1)$ with $m \in \mathbb{N}$, and let $F_s = 1 \ + 2^{2^s}$ the Fermat number. Then $2^{2^s} \equiv -1$ modulo Fs and $2^{2^{s+1}} \equiv 1$ modulo Fs. Therefore
$p = 1 + 2^{2^s(2m+1)} = 1 + 2^{2^{s+1}m+2^s} = 1 + 2^{2^{s+1}m}2^{2^s} = 0$ modulo Fs. Which proves that Fs divides p. So, we deduce $m = 0$.

Theorem 2.3. Let $p = 1 + 2^n$ be a prime number. Then $2 \notin Gp$ if and only if $n \geq 3$.

Proof. $n \geq 3$ if and only if $p = 1 + 2^n = 1$ mod 8 if and only if $\left(\frac{2}{p}\right) = 1$ if and only if $2^{\frac{p-1}{2}} = 1$ mod p if and only if $2 \notin Gp$.

Theorem 2.4. We have $3 \in G_p$ for all prime number $p = 1 + 2^{2^n}$ with $n \geq 1$.

Proof. Since $p = 1 + 2^{2^n}$ with $n \geq 1$, then $p = 2$ mod 3.

Suppose that $n = 1$, then $p = 5$. Since $3^2 = -1$ mod 5. We refer to Corollary 6 and we deduce that $3 \in G_p$.

Suppose that $n \geq 2$, then $p = 1$ mod 8 and $\left(\frac{3}{p}\right) = \left(\frac{p \ mod \ 3}{3}\right) = \left(\frac{2}{3}\right) = -1$. We refer to Theorem 1.5 and we deduce that $3 \in G_p$.

Corollary 8. We have $G_p = \left\{3^{2k+1} \, mod \, p, \;\; k \in \{1, \ldots, 2^{n-1} - 1\}\right\}$ for all prime number $p = 1 + 2^{2^n}$ with $n \geq 1$.

Proof. We refer to theorems 2.5 and 1.2 and we deduce that $\left\{3^{2k+1} \, mod \, p, \;\; k \in \{1, \ldots, 2^{n-1} - 1\}\right\} \subseteq G_p$. Since $\left|\left\{3^{2k+1} \, mod \, p; \;\; k \in \{1, \ldots, 2^{n-1} - 1\}\right\}\right| = 2^{n-1}$, we refer to theorem 2.4 and lemma 2.1 and we deduce this corollary.

REFERENCES

1. Lenstra, Arjen K and Lenstra, Hendrik W and Manasse, Mark S and Pollard, John M. The factorization of the ninth Fermat number, in Mathematics of Computation, Vol. 61, number 203, pages 319 349, year 1993.
2. J.W.S. Cassels and A. Frohlich, Algebraic number theory, Academic Press, 1967.
3. Barbulescu, Razvan. Algorithmes de logarithmes discrets dans les corps finis,These, school=Université de Lorraine, year 2013.
4. Thome, Emmanuel. Algorithmes de calcul de logarithmes discrets dans les corps finis. These, year 2003.
5. T. Honda, On real quadratic fields whose class numbers are multiples of 3, J, Reine Angew. Math. 233: (1968), 101-102.
6. P. Kaplan, Sur le 2-groupe des classes d'idéaux des corps quadratiques, J, Reine Angew. Math. 283/284: (1976), 313-363.

7. B. Oriat, Table des groupes des classes des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ et imaginaires $\mathbb{Q}(\sqrt{-d})$, $d < 10000$, Faculte des Sciences de Be sancon 1974-1975.
8. P. Ribenboim, L'Arithmétique des corps, Hermann, Paris, 1972.
9. P. Samuel, Théorie algébrique des nombres, Hermann, Paris 1971.
10. C.L. Siegel, Uber einige anvendungen diophantisher aproximationen, esammelte abhandlungen band I, 209-266.
11. Uchida, Unramified extensions of quadratic number fields, I, Tôhoku Math. J. (1970); 22.
12. L. C. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics, Vol 83, Springer-Verlag, New York, 1982.
13. Vasilenko, O. N. Number theoretic algorithms in cryptography (Vol. 232). American Mathematical Soc, 2007.
14. Buchmann, J. Introduction to cryptography. Springer Science & Business Media, 2013.
15. Baldoni, M. W., Ciliberto, C., & Cattaneo, G. M. P. Elementary number theory, cryptography and codes (Vol. 2). Berlin: Springer, 2009.
16. Stein, W. Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach. Springer Science & Business Media, 2008.
17. Lidl, Rudolf and Niederreiter, Harald. Introduction to finite fields and their applications, publisher=Cambridge university press, 1994.
18. Niederreiter, Harald and Wang, Huaxiong and Xing, Chaoping. Function fields over finite fields and their applications to cryptography, booktitle=Topics in Geometry, Coding Theory and Cryptography, pages=59-104, publisher=Springer, year=2006.
19. Di e, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inform. Theory IT22 (6), 644-654 (1976).
20. Diffie, W.: Subject: Authenticity of non-secret encryption documents. Available at http://cryptome.org/ukpk-diffie.htm. October 6, 1999.